



D2.2

Inventories (2)

Document Identification	
Date	28.02.2017
Status	Final
Version	2.5

Related WP	WP 2, WP3	Related Deliverable(s)	D2.1
Lead Authors	Rachelle Sellung	Dissemination Level	PU
Lead Participants	USTUTT	Contributors	See list in Document.
Reviewers	Benno Overeinder (NLNET), Jon Shamah (EEMA)		

This document is issued within the frame and for the purpose of the LIGHTest project. LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No 700321.

This document and its content are the property of the *LIGHTest* Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the *LIGHTest* Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the *LIGHTest* Partners.

Each *LIGHTest* Partner may use this document in conformity with the *LIGHTest* Consortium Grant Agreement provisions.

Document name:	Inventories (2)	Page:	1 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



1. Executive Summary

In order to get a greater understanding of the basis that LIGHT^{est} is building upon, it is essential to conduct a state-of-the-art analysis of the key topics that will be built upon. That is the main goal of this deliverable, Inventories 2.2. After reviewing the key components and building blocks of the project, a set of eight different topics were taken into consideration. In particular, the key points of interest include the following: (i) existing trust schemes and trust (status) lists, (ii) existing device attestation schemes, (iii) relevant trust list formats, (iv) relevant delegation schemes, (v) relevant trust policies and policy languages, (vi) existing trust translation schemes, (vii) best practice derivation schemes for mobile identities, and (viii) best practices of interaction design. This deliverable will dedicate a chapter to each topic. With that, each topic will be seen from two different sides. First, there will be a broad academic perspective that will be explored. This will include gaining insight on current related research, relevant methods and strategies, definitions, relevant EU projects, etc. that are involved for the topic. Second, there will be a broad industry perspective that will be explored. Depending on the topic at hand and the existing material, the industry perspective includes relevant work in the industry that is being done and/or insight on the legal side involved in the topic, which may be useful later on in the project. Overall, by having both of these sides of insights it helps to gain a full rounded perspective that observes both the current and relevant research rigor and how these topics have been integrated or applied in practice.

Document name:	Inventories (2)	Page:	2 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



2. Document Information

2.1 Contributors

Name	Partner
Rachelle Sellung	USTUTT
Fabina Dietrich	USTUTT
Heiko Roßnagel	FHG
Bud Bruegger	FHG
Sue Dawes	OIX
Charo Encinas Bayán	CORREOS
Stefan More	TUG
Georg Wagner	TUG
Peter Lipp	TUG
Alberto Crespo Garcia	ATOS
Lorenzo Rosa	ATOS
Miryam Villegas Jimenez	ATOS
Niels Pagh-Rasmussen	IBM
Jan Camienisch	IBM
Charles Sederholm	GS
Sebastian Alexander Mödersheim	DTU
Rasmus Birkedal	DTU
Frank-Michael Kamm	G&D
Elif Ustundag Soykan	TUBITAK
Muhammet Yıldiz	TUBITAK
Melis Ozgur Cetinkaya Demir	TUBITAK
Burcin Bozkurt Gunay	TUBITAK
Edona Fasllija	TUBITAK
Berkay Topcu	TUBITAK
Cagatay Karabat	TUBITAK
Jesse Krutto	GS

2.2 History

Version	Date	Author	Changes
0.1	15.09.2016	USTUTT	Created Outline
0.2	03.10.2016	USTUTT	Inserted Partner Contribution
0.4	14.10.2016	USTUTT	Adjusted Structure and technical parts
0.5	04.11.2016	USTUTT	Merged and Inserted Contributing Partner Contribution
0.6	07.11.2016	USTUTT	Formatting, Merging and Inserting Remaining Partner Contributions
0.7	10.11.2016	USTUTT	Minor Changes
1.0	15.11.2016	USTUTT	Final Input Inserted and Touch ups for Review
1.1	28.11.2016	USTUTT	Integrated Review suggestions and formatting changes

Document name:	Inventories (2)	Page:	3 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



1.2	18.01.17	G&D	Integrated review suggestions
1.3	27.01.2017	TUG	Integrated review suggestions
1.5	31.01.2017	USTUTT, OIX,ATOS, TUBITAK, DTU	Integrated review suggestions
1.6	02.02.2017	ATOS	Integrated further review suggestions
1.7	03.02.2017	USTUTT	Formating and Touch ups
1.8	06.02.2017	DTU	Integrated new Trust Policy Language part
1.9	07.02.2017	ATOS	Integrated updated Trust Translation and Delegation Scheme parts
2.0	07.07.2017	USTUTT	Formating, and minor adjustments
2.1	24.02.2017	USTUTT	Integrated Reviewers Comments and suggestions
2.2	24.02.2017	USTUTT, OIX	Integrated OIX updated contribution
2.3	27.02.2017	FHG	Minor formattings
2.4	27.02.2017	USTUTT, GS	USTUTT added in GS Contribution: 6.2 and 10.2
2.5	27.02.2017	USTUTT	Final Integrations and Adjustments

Document name:	Inventories (2)	Page:	4 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



3. Table of Contents

1.	Executive Summary	2
2.	Document Information.....	3
2.1	Contributors	3
2.2	History	3
3.	Table of Contents	5
3.1	Table of Figures.....	6
3.2	Table of Tables.....	6
3.3	Table of Acronyms.....	7
4.	Existing Trust Schemes, Lists, and Formats	11
4.1	Academic Aspects	11
4.2	Industry Aspects	14
5.	Existing Device Attestation Schemes.....	31
5.1	Academic Perspective	31
5.2	Industry Perspective	37
6.	Relevant delegation Schemes	40
6.1	Academic Perspective	40
6.2	Industry Perspective	51
7.	Relevant Trust Policies and Policy Languages.....	64
7.1	Academic Perspective	64
7.2	Industry Perspective	69
8.	Existing Trust Translation Schemes.....	71
8.1	Academic Perspective	71
8.2	Industry Perspective	74
9.	Best Practice Derivation Schemes for Mobile Identities	128
9.1	Academic Perspective	128
9.2	Industry Perspective	129
10.	Best Practices of Interaction Design	136
10.1	Academic Perspective	136
10.2	Industry Perspective	137
11.	References	140
12.	Project Description.....	169

Document name:	Inventories (2)	Page:	5 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



3.1 Table of Figures

Figure 1 Imperial Valley (Anon., 2016).....	16
Figure 2 Minors Trust Framework (Privo, 2016).....	21
Figure 3 Personal channel (Respect, 2016).....	24
Figure 4 SecureKey Concierge service (SecureKey, 2015).....	26
Figure 5 Trust Framework Model Pillars (Brennan, 2016).....	29
Figure 6 ID.me (ID.me, 2016).....	30
Figure 7: Basic layout of electronic mandates (XML schema) in Austria	52
Figure 8: Legal Person Representation at Austrian Online infrastructure for delegation.....	54
Figure 9 Katso Management.....	58
Figure 10 Helen Self-Service Interface	62
Figure 11 Different levels of assurance for several trust schemes	76
Figure 12 Specs for AES and the associated seal container.....	97
Figure 13 Level of Assurance for eSeals	100
Figure 14 Trusted Timestamping.....	102
Figure 15 eDelivery Building Block Scope	109
Figure 16 Classification of existing types of commercial WACs	120
Figure 17 Available registries in OIXnet.....	124
Figure 18: Principle of PIV derived credentials flow and lifecycle management (right). The figure also illustrates the relation to the card-based PIV credentials (left) and their lifecycle. From (H. Ferraiolo, 2014).	131
Figure 19: Principle of the GSMA Mobile Connect authentication and attribute sharing flow. Source: (Eleven Paths, 2015).	132
Figure 20 User experience of the two FIDO protocol versions UAF (left) for password-less authentication and transaction signing and U2F (right) for two-factor authentication. Source: (FIDO Alliance, 2016).....	134
Figure 21 Model of Interaction Design Research by Daniel Fallman	137

3.2 Table of Tables

Table 1 Collection of Trust Definitions.....	12
Table 2 CAB Certification Authorities	19
Table 3 Trust Frameworks.....	20

Document name:	Inventories (2)	Page:	6 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



3.3 Table of Acronyms

AVANTSSAR	(EU project) Automated Validation of Trust and Security of Service oriented Architectures
A2A	Administration to Administration
A2B	Administration to Business
A2C	Administration to Citizen
AdESeal	Advanced Electronic Seal
AdESig	Advanced Electronic Signature
AdES	Advanced Electronic Signature covers AdESig, AdESeal, and AdESamp
AdESQC	Advanced Electronic Signature supported by a Qualified Certificate
AdESamp	Advanced Electronic Stamp
AES	Advanced Encryption Standard
ANSSI	<i>Agence nationale de la sécurité des systèmes d'information</i> (in English: National Cybersecurity Agency of France)
AQAA	Attribute Quality Authentication Assurance
BMBF	Bundesministerium für Bildung und Forschung (German Federal Ministry for Education and Research)
BAN-logic	Burrows Abadi Needham
B2A	Business to Administration
CA	Certification Authority
CEHRT	Certified Electronic Health Record Technology
COPPA	Children's Online Private Protection Act
C2A	Citizen to Administration
C2C	Citizen to Citizen
CADES	CMS Advanced Electronic Signature
CID	Commission Implementing Decision
CEF	Connecting Europe Facility
CFA	Consumer Facing Applications
CP	Credential Provider
CSP	Credential Service Provider
CROBIES	Cross-Border Interoperability of eSignatures project
CMS	Cryptographic Message Syntax
CRM	Customer Relationship Management
DPC	Derived PIV Credential
DL	Description Logic
DIACC	Digital Identification & Authentication Council of Canada
DAA	Direct Anonymous Attestation
DV	Domain Validated
ESSI	Electronic Exchange of Social Security Information
EHR	Electronic Health Record
eIDAS	Electronic IDentification And Signature
eID	Electronic IDentity

Document name:	Inventories (2)	Page:	7 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



eTS	Electronic Trust Services
EC	European Commission
CEN	European Committee for Standardisation
EN	European Norm
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
EVCP	Extended Validation Certificate Policy
XACML	eXtensible Access Control Markup Language
FIDO	Fast Identity Online
FBCA	Federal Bridge Certification Authority
FICAM	Federal Identity, Credential and Access
FIPS	Federal Information Processing Standard
FP	Fixedpoint
GSMA	Global System for Mobile Communications Association
HWAT	Hardware Based Device Attestation
HIE	Health Information Exchange
HISP	Health Information Systems Program
ID	Identity
laaS	Identity as a Service
IDEF	Identity Ecosystem Framework Registry
IMSC	Identity Management Sub-Committee
IdP	Identity Provider
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union (United Nations)
IETF	Internet Engineering Task Force
KTR	Kantara Trust Registry
LoA	Level of Assurance
MTF	Minors Trust Framework
MNO	Mobile Network Operator
MOA	Modules for Online Applications
MS	Member State
NBB4C	Nate Blue Button for Consumers Trust Bundle
NIST	National Institute of Standards and Technology
NSTIC	National Strategy for Trusted Identities in Cyberspace
NFC	Near Field Communication
nPA	Neuer Personalausweis (German eID card)
NPE	Non-Person Entity
NSL	Norton Secure Login
OIX	Open Identity Exchange
OASIS	Organization for the Advancement of Structured Information Standards
OV	Organization Validated
PCTF	Pan-Canadian Trust Framework
PADES	PDF Advanced Electronic Signature

Document name:	Inventories (2)	Page:	8 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



PHR	Personal Health Records
PIV	Personal Identity Verification
PUF	Physically Unclonable Function
PCR	Platform Configuration Register
PEP	Politically Exposed Person
PDF	Portable Document Format
PRIVO	Privacy Vaults Online
PP	Protection Profile
PKI	Public Key Infrastructure
PSCIOC	Public Sector Chief Information Officer Council
PSSDC	Public Sector Service Delivery Council
QESQC	QES based on Qualified Certificate
QC	Qualified Certificate
QESeal	Qualified Electronic Seal
QESig	Qualified Electronic Signature
QES	Qualified Electronic Signature/Seal
QTS	Qualified Timestamp
QTSP	Qualified Trust Service Provider
QWAC	Qualified Website Authentication Certificate
QAA	Quality Authentication Assurance
QR Code	Quick Response Code
RUP	Rational Unified Process
REM	Registered Electronic Mail
RP	Relying Party
RFC	Request for Comments
SEDA	Scalable Embedded Device Attestation
SCUBA	Secure Code Update By Attestation in Sensor Networks
SMART	Secure and Minimal Architecture for (Establishing a Dynamic) Root of Trust
SAML	Secure Assertion Markup Language
SE	Secure Element
STORK	Secure idenTity acrOss boRders linKed
SSL	Secure Socket Layer
SAML	Security Assertion Markup Language
SPM	Self Protecting Modules
SML	Service Metadata Locator
SMP	Service Metadata Publisher
SaaS	Software as a Service
SWAT	SoftWare Based Device ATtestation
SP	Special Publication (NIST)
SIM	Subscriber Identity Module
TS	Technical Specifications
TSA	Time Stamping Authority
TL	Trust List
TLS	Transport Layer Security

Document name:	Inventories (2)	Page:	9 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



TFI	Trust Framework Initiative
TFP	Trust Framework Provider
TSP	Trust Service Provider
TTS	Trust Translation Schemes
TCG	Trusted Computing Group
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
TTP	Trusted Third Party
US	United States
U2F	Universal 2nd factor
UAF	Universal Authentication Factor
UICC	Universal Integrated Circuit Card
UPU	Universal Postal Union
USB	Universal Serial Bus
VIPER	Verifying the Integrity of PERipherals
XAdES	XML Advanced Electronic Signature Time-Stamp Protocol

Document name:	Inventories (2)	Page:	10 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



4. Existing Trust Schemes, Lists, and Formats

This section provides insight on the existing Trust Schemes, Lists, and Formats from both an academic and industry side. The Academic aspect goes into greater detail on the definitions that will be used in the project, along with an introduction to trust lists with formats and examples. The industry side provides further examples on different existing trust frameworks from around the globe.

4.1 Academic Aspects

This section provides general information about trust schemes, trust lists and trust lists formats, as well as definitions and an introduction into trust lists.

4.1.1 Definitions

To support the discussion of trust schemes and trust lists, a common understanding of terms and concepts seems useful. For this reason, this section provides initial definitions of relevant terms. These originate from an early version of the LIGHTest Glossary that will eventually be part of Deliverable 2.14. Only the definitions relevant for trust schemes and trust lists are listed below:

Entity	An entity is a person, organization, or thing enrolled in a trust scheme.
Trust Domain	A trust domain defines a set of entities that are eligible to enroll in a scheme and describes the trust relevant aspects of the enrolled entities. A typical way to define such a set for a trust domain is the use of constraints.
Trust Scheme Authority	A trust scheme authority manages multiple trust schemes. The trust scheme authority may delegate the management to sub authorities.
Trust List	Provides relevant attributes of enrolled entities. A trust list provides relevant attributes of enrolled entities. A trust lists is usually signed by an issuing authority with an electronic signature to prove their trustworthiness. Different types of trust lists do exist. For example, a boolean trust list provides a boolean value for each entity. An entity can either be trusted or not trusted. As another example, an ordinal trust list provides an ordinal value for each entity. Typically, typical value for an ordinal value is a Level of Assurance (LoA).
Trust Scheme	A trust scheme comprises the organizational, regulatory, legal and technical measures to assert trust relevant attributes about enrolled entities in a given domain of trust. A trust scheme operates in a given trust domain and typically has a declared or implied purpose. The two major types of trust schemes are authority based and reputation based trust schemes. <ul style="list-style-type: none"> • Authority based trust schemes: An authority issues regulations and conditions that are necessary to certify attributes. A trust scheme may use supervision to ascertain that an entity complies with all conditions and regulations. If the entity complies with the conditions and regulations, it is part of the trust scheme data. Otherwise, the authority can remove it from the trust scheme data. • Reputation based trust schemes: A trusted party collects and publishes reputation data on entities and assembles the data into the trust scheme data.
Trust Scheme Data	Trust scheme data represents the current content of a trust scheme. It is a data set managed by the trust scheme authority and contains information on the status of an entity.

Document name:	Inventories (2)	Page:	11 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Trust Scheme Publication	<p>A trust scheme publication makes the trust scheme data available to verifiers either as complete or a subset of the trust scheme data.</p> <p>A trust scheme publication may contain different aspects of the trust scheme data including (from least to most accurate trust scheme publication mechanism)</p> <ul style="list-style-type: none"> • Historical publications: Include the full set of change events and make it possible to determine the status of the trust scheme data at different positions in time. • Snapshot publications: Report the status of the trust scheme data at a given point in time. • Sampled publications: Report the state of the trust scheme data at the point of time when it was last queried. • Real time publications: Report the state of the trust scheme data at the point of time of a query. <p>The LIGHTest infrastructure supports two trust scheme publications: Sampled and real time publications.</p>
Boolean Trust Scheme Publications	<p>Boolean trust scheme publications are defined as:</p> <ul style="list-style-type: none"> • entityID -> Boolean <p>Instead of explicitly stating the boolean value, every entity listed in a publication can have the same boolean value. Trusted (true) in the case of white lists and untrusted (false) in case of black lists.</p>
Ordinal Trust Scheme Publications	<p>Ordinal trust scheme publication are defined as</p> <ul style="list-style-type: none"> • entityID -> Ordinal value <p>An ordinal value describes a certain Level of Assurance. It is seen as a reputation rating for the entity. Examples for ordinal values are [low, medium, high], [level1, level2, level3, level4], or [0-stars, 1-star, 2-stars, 3-stars, 4-stars, 5-stars].</p> <p>Every entity listed in a publication is assigned to an ordinal value. Entities listed in a publication may have different ordinal values.</p> <p>Note that boolean trust scheme publications are a special case of ordinal trust scheme publications.</p>
Generic Trust Scheme Publications	<p>Generic trust scheme publication is defined as</p> <ul style="list-style-type: none"> • entityID -> tuple of attributes <p>A generic trust scheme contains a tuple of attributes for an entity. An attribute can be an LoA, date of foundation, legal form, social capital, etc.</p> <p>Note that boolean and ordinal trust scheme publications are a special case of generic trust scheme publications.</p>

Table 1 Collection of Trust Definitions

4.1.2 Trust List Introduction

A trust list is a list that contains all information for verification if a claim can be trusted. To build trust in a system, a trust path from a trusted root to the destination system is required. This usually happens by listing all trusted systems on a single list. It requires a digital signature to trust the list. The signature comes from a key certificate that all other parties trust.

For example, the eIDAS Regulation requires EU MS to publish a trust list of certain service providers established in their territory. Such service providers offer qualified services, such as issuing (and verifying) qualified signatures, eSeals, time stamping and electronic registered delivery or other services that the member state chooses to include on a voluntary basis.

Document name:	Inventories (2)	Page:	12 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



A signature needs to meet certain requirements in order to enroll in a trust scheme. A trust scheme may provide several requirements for different levels. ENISA (Barreira, 2013)(section 2.3) defines such a set for a binary trust scheme. In order for a signature to be legally valid in the same ways as a handwritten signature, it needs to fulfill these requirements. In this particular case, the signature is a qualified signature if it meets all requirements.

For the verification of a signature, a trust anchor may be used. A trust anchor acts as authoritative entry via public key and associated data and uses a public key to verify the signature.

A trust anchor must fulfill certain requirements. It must be transport independent, provide basic management operations, and security measures. RFC6024 (IETF, 2010) defines the requirements that a trust anchor must fulfill. RFC5914 (IETF, 2010) and RFC5934 (IETF, 2010) are the technical specification of the requirements.

The following sections list real-life trust lists already in use. Furthermore, it describes the formats and schemes used by those lists.

4.1.2.1 Trust List Formats

This section lists some of the trust list formats relevant for LIGHTest.

ETSI TS 102 231: Requirements for Trust Service Provider status information

ETSI's Technical Specification 102 231 (ETSI, 2009) specifies a standard for a Trust-service Status List (TSL) which makes available trust service status information such that interested parties may determine whether a trust service is or was operating under the approval of any recognized scheme at either the time the service was provided, or the time at which a transaction reliant on that service took place.

ETSI TS 119 612: Requirements for Trusted Lists

When the EC was in need of a Trust List format, ETSI Technical Specification 102 231 (ETSI, 2009) was adapted to Europe's needs.

Technical Specification 119 612 (ETSI, 2013) specifies a format and mechanisms for establishing, locating, accessing and authenticating a trusted list which makes available trust service status information so that interested parties may determine the status of a listed trust service at a given time. It defines the syntax and semantics of a TL as well as the mechanisms for accessing TLs. It also provides guidance for locating and authenticating TLs.

It applies to EU MS trusted lists as a means to express trust service status information with regards to their compliance with the relevant provisions laid down in Directive 1999/93/EC and in related national laws.

Document name:	Inventories (2)	Page:	13 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



In the context of non-EU countries or international organizations, scheme operators may issue trusted lists in accordance with the present document to facilitate mutual recognition of electronic signatures.

In addition, Technical Specification 119 612 (ETSI, 2013) defines requirements for relying parties to use TLs and the status information held within them.

Other Trust List Formats

Furthermore, there exists a series of proprietary systems which can be considered as trust anchors used by industry. Example for such systems are Microsoft's Certificate Trust List (Microsoft, 2016), Adobe's Approved Trust List (AATL) (Adobe, 2016) and eduRoam/eduGAIN (Geant, 2016). Since those lists are mainly a (unsigned) collection of certificates, they are not covered in detail.

4.1.2.2 Examples of Trust Lists

EU Trusted Lists & EU Member States Trust Lists

Regulation (EU) No 910/2014/EU Article 22 (eIDAS Regulation) (Regulation, 2014) provides the obligation for EU MS to provide trust lists. This includes the processes of establishing, maintaining and publishing trusted lists. The EU MS has to provide information about the qualified TSP as well as information about the trust services provided by the TSP. Article 22 also provides the obligation that the publication of trust lists happens in a secure manner, which means electronically signed or sealed, and that the trust lists are suitable for automated processing.

This regulation has a constitutive effect. A trust service provider and the services it provides is only qualified if it appears in the trusted list. Consequently, citizens, businesses or public administrations, in general the users, will benefit from the legal effect associated with a given qualified trust service only if it is listed as qualified service in the trusted lists.

EU MS may add additional trust services other than the qualified ones. This happens on a voluntary basis and on a national level. This entry must clearly indicate that the provider is not qualified according to Regulation (EU) No 910/2014 (Regulation, 2014).

To allow access to the trusted lists of all EU MS, the EC makes trusted lists available for the public as a list of trusted lists. This happens via a secure channel to an authenticated web server. This list of trusted list is also signed or sealed and suitable for further automated processing.

4.2 Industry Aspects

A trust framework legally binds participating entities in its identity system with role-specific sets of duties and liabilities. These will apply to the services offered by a participating entity within the context of the trust framework. The articulation typically takes a contractual form when the scope

Document name:	Inventories (2)	Page:	14 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



of the trust framework is in the private domain. In other domains such as government, the trust framework could also be in regulatory or statutory form (Esther Makaay, March, 2017).

There are a number of trust lists that are used by the industry and are interesting for LIGHTest to examine. Below is a description of the trust lists, their purpose and functionality as well as descriptions of the trust schemes that are registered on the trust lists (where available) for the purpose of showing how these trust lists are being used in practice and applied in organisations.

OIXnet (OIX, 2016) An official online and publicly accessible repository of documents and information relating to identity systems and identity system participants. OIXnet lists worldwide available trust frameworks and registered whitelists and functions as an official and centralized source of documents and information, much like a government-operated recorder of deeds. The purpose of OIXnet is to provide a neutral, authoritative registry of trust information to enable interoperability of identity systems and participants. OIXnet is a registry of registries which differs from other trust lists and aims to provide in one central location, all information related to multiple registrations. Other registries that are in operation generally have limited types of registration with respect to a particular identity.

OIXnet is relevant for trust translation across jurisdiction as a neutral, global platform accessible by anyone at any time with no cost associated; it helps provide the necessary transparency required for trust. It also helps the discovery, authentication and assessment of the trustworthiness of foreign certificates and other artifacts that verifiers need to know when determining which foreign trust schemes to accept and how these map to the trust schemes of a given local jurisdiction.

LIGHTest will be complimentary and not competitive to the Trust Frameworks that are registered at OIXnet. LIGHTest is intended to be cross industry and global, like many of the Trust Frameworks registered, but others are industry and jurisdictionally specific. Communities of interest determine the applicability of a given trust framework and so indicate in its terms of reference.

IDEF Identity Ecosystem Framework Registry (IDESG, 2016) has been created by the Identity Ecosystem Steering Group (IDESG) for organisations who are interested in independently assisting their own identity management standards against a common set of criteria found in the IDEF. The criteria used are: reliable security, privacy, ease of use, costs savings and user choice. These are taken from the NSTIC Guiding Principles (IDEF, 2016).

According to an article in Imperial Valley News (Anon., 2016) the introduction of the IDESG's registry has impacted more than 6.7 million individuals across 12 sectors up until September 30 2016.

Document name:	Inventories (2)	Page:	15 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



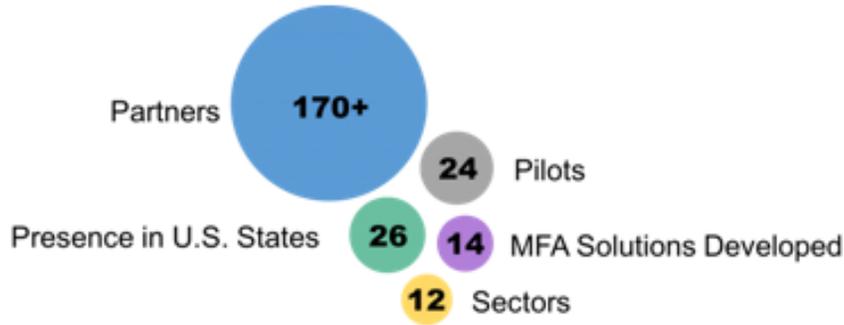


Figure 1 Imperial Valley (Anon., 2016)

Kantara Trust Registry - (Initiative, 2016) The Kantara Initiative covers: Connected Life (Internet of Things), and Trust Services. Kantara’s initiatives include: Identity Relationship Management, User Managed Access, Identities of Things, and Minimum Viable Consent Receipt. This Trust Framework Provider is aligned with the US NSTIC program and looks to approve Credential Service Providers (CSPs) and Accredits Assessors. All those who are approved will be listed on the KTR Trust Status List.

CAB (CA/Browser) Forum (CAB, 2016) The CAB forum is a voluntary group of Certification Authorities (CAs), vendors of Internet Browser software and suppliers of other applications that use digital certificates for SSL/TLS and code signing. Internet users wanted greater assurance about the websites they were visiting, so the group was formed to leverage the capabilities of SSL/TLS certificates.

As stated on the CAB Forum website, the CAB Forum has adopted version 1.0 of the Extended Validation (EV) Guidelines. EV certificates are issued after extended steps to verify the identity of the entity behind the domain receiving the certificate. Following the publication of the EV Guidelines they have adopted these guidelines for issuing code signing certificates and Baseline Requirements for the Issuance and Management of Publicly-Trusted SSL/TLS Certificates to improve accreditation and approval schemes for all applicants who request that their self-signed root certificates be embedded as trust anchors in software and to extend common standards for issuing SSL/TLS certificates beyond EV to include all Domain-validated (DV) and Organization-Validated (OV) certificates.

Document name:	Inventories (2)	Page:	16 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



CAB Certification Authorities:

Certification Authority	Link
Actalis	https://www.actalis.it/
Amazon	https://www.amazon.com/
ANF Autoridad de Certification	https://anf.es/
Buypass	https://www.buypass.no/
Certinomis	https://www.certinomis.fr/
certSign	http://www.certsign.ro/certsign/
Certum	http://www.certum.eu/certum/cert,eindex_en.xml
China Financial Certification Authority	http://www.cfca.com.cn/
Chunghwa Telecom Co., Ltd.	http://epki.com.tw/
China Internet Network Information Center	http://www1.cnnic.cn/IS/fwqzs/
Cisco	https://www.cisco.com/
Comodo CA Ltd	http://www.comodo.com/
D-TRUST GmbH	http://www.d-trust.net/
DigiCert, Inc.	https://www.digicert.com/
Digidentity	http://www.digidentity.eu/
Disig, a.s.	http://www.disig.sk/
DocuSign (formerly OpenTrust/KEYNECTIS)	https://www.opentrustdtm.com/
E-TUGRA Inc.	http://www.e-tugra.com.tr/
Entrust	http://www.entrust.com/
ESG de Electronische Signatuur B.V.	https://www.de-electronische-signatuur.nl/
Firmaprofesional	http://www.firmaprofesional.com/
Global Digital Cybersecurity Authority Co., Ltd	https://www.gdca.com.cn/

Document name:	Inventories (2)	Page:	17 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



GlobalSign	http://www.globalsign.com/
GoDaddy Inc	http://www.godaddy.com/
Hellenic Academic and Research Institutions Certification Authority (HARICA)	http://www.harica.gr/
Izenpe S.A.	http://www.izenpe.com/
Kamu Sertifikasyon Merkezi	http://www.kamusm.gov.tr/
KPN Corporate Market BV	http://www.kpn.com/
Let's Encrypt	https://letsencrypt.org/
Logius PKloverheid	http://www.logius.nl/english/
National Center for Digital Certification	http://www.ncdc.gov.sa/
Network Solutions, LLC	http://www.networksolutions.com/SSL-certificates/index.jsp
Open Access Technology International	http://www.oati.com/
Prvni certifikacni autorita, a.s.	http://www.ica.cz/
QuoVadis Ltd.	http://www.quovadisglobal.com/
Secom Trust Systems	http://www.secomtrust.net/
Shanghai Electronic Certification Authority Center Co. Ltd	http://www.sheca.com/
Skaitmeninio sertifikavimo centras (SSC)	http://www.ssc.lt/
StartCom Certification Authority	http://www.startssl.com/
Swisscom (Switzerland) Ltd	http://www.swisscom.ch/
SwissSign AG	http://www.swissign.com/
Symantec Corporation	http://www.symantec.com/
TAIWAN-CA Inc.	https://www.twca.com.tw/Portal/Portal.aspx
TrustCor Systems, S. de R.L.	https://www.trustcorsystems.com/
Trustis Limited	http://www.trustis.com/

Document name:	Inventories (2)	Page:	18 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Trustwave	http://www.trustwave.com/
TURKTRUST	http://www.turktrust.com.tr/
WoSign	http://www.wosign.com/english

Table 2 CAB Certification Authorities

Trust Framework	Trust List Member	Website
Minors Trust Framework	OIXnet	https://privo.com/minors-trust-framework/
Mydex Trust Framework	OIXnet	https://mydex.org/prnews/mydex-trust-framework-recognised-by-open-identity-exchange/
Nate Blue Button for Consumers Trust Bundle (NBB4C)	OIXnet	http://nate-trust.org/nbb4c-trust-bundle/
The Respect Trust Framework	OIXnet	https://respectnetwork.wordpress.com/respect-trust-framework/
SAFE-BioPharma FICAM Trust Framework Provider Program	OIXnet	https://www.safe-biopharma.org/SAFE_Trust_Framework.html
SecureKey Concierge™ Canada Trust Framework	OIXnet	http://securekey.com/wp-content/uploads/2015/09/SK-UN117-Trust-Framework-SecureKey-Concierge-Canada.pdf
tScheme	OIXnet	http://www.tscheme.org/
Pan Canadian Trust Framework		https://diacc.ca/2016/08/11/pctf-overview/
Personal Data and Trust Framework		https://pdtm.org/
DigiCert	IDEF	https://www.digicert.com/direct-project/
ID.me	IDEF	https://www.id.me/
MorphoTrust USA	IDEF	http://www.morphotrust.com/eID.aspx
Symantec Corporation	IDEF	https://www.idefregistry.org/registry/listing/norton-secure-login/
PRIVO	IDEF	https://www.idefregistry.org/registry/listing/privo-lock-and-the-privo-id-platform/

Document name:	Inventories (2)	Page:	19 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



MedAllies	Kantara	http://www.medallies.com/productsservices.html
-----------	---------	---

Table 3 Trust Frameworks

Some of the following trust frameworks and trust schemes do cover some industries that are not directly relevant to LIGHTest, however it is felt that they provide good examples that may further inform work projects and therefore are included.

4.2.1 Minors Trust Framework

General Description

Working in conjunction with the National Strategy for Trusted Identities in Cyberspace (NSTIC), the MTF (Privo, 2016) is a White House initiative aimed at helping individuals and organisations utilise secure, efficient, easy-to-use and interoperable identity credentials to access online services in a manner that promotes confidence, privacy, choice and innovation.

How the framework is being used practically

Under COPPA, every time a child wants to access an online service that they want to interact with, their parent must separately fill in each consent request. This is obviously time consuming and a burden for parents and also the online service provider. Research has shown that less than 1 in 10 consent requests are acted upon, which has obvious knock on effects to the service providers. A big problem is when children lie about their age in order to access online services as this puts children at risk and the service providers could run afoul of COPPA. The aim of the MTF is to allow credential service providers (CSPs) to create an online credential for parents and children that can be used by other online service providers. All CSPs agree to standards of privacy and security under the Federation. It is free and simple to use and the parents only need to have their identity verified once by an Identity Provider. Once accepted, parents can then pre-consent to their child’s access to other Federation approved online services. The children benefit from being able to interact online in a safe and privacy secure manner.

Document name:	Inventories (2)	Page:	20 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



How it Works Use Case

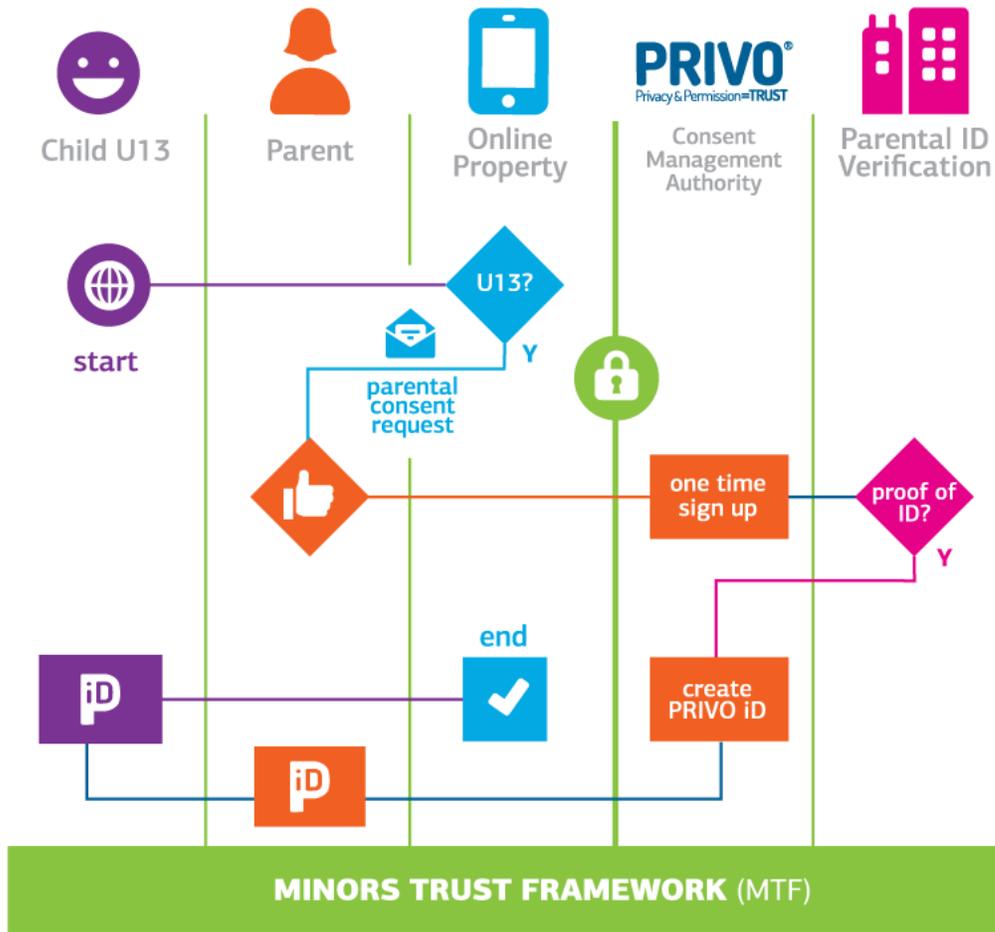


Figure 2 Minors Trust Framework (Privo, 2016)

Technical description

The MTF enables Credential Service Providers that issue a Child-unique pseudonymous identifier to interoperate and interact with RPs and other Members.

When someone attempts to access a protected service provider site, an Identity Provider is asked to provide 'identity attributes' to the service provider. Attributes could be a user ID, organisational affiliation status, email address etc. The Federation encourages the support of identity attributes by its participants to improve the COPPA consent process and to help protect

Document name:	Inventories (2)	Page:	21 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



personal privacy. The Federation provides the parent with a unique identifier/relationship link and tools to manage multiple consents, notifications, and associations.

Parents can view their child's data and permissions across all the multiple sites and manage this. However, Federation members are prohibited from assisting each other in tracking either Children or Parents by both MTF policy and technical enforcement due to the use of unique globally unique identifier (GUID). Credential holders are encouraged to have unique display names available at the online service level. CSPs and CMAs are permitted to maintain information about a user on multiple venues in order to support the use of federated credentials and consent.

Once the minor reaches an age where they are no longer under COPPA protection, the parent can transfer control of the parent-authorized credential to the minor. Minor's rights to control their credential will be determined by relevant law and the issuing CSP/RP Terms of Service or EULA, and may be viewable from the CMA's parent portal.

4.2.2 Mydex Trust Framework

General Description

The Mydex Trust Framework delivers a trusted digital identity via a secure personal data store and platform where individuals are able to connect to each other and organisations, allowing for and exchange of information in a secure and verified manner.

How the framework is being used practically

The Mydex Trust Framework gives individuals a trusted identity and digital letterbox that they can use online. For organisations, they can operate with large savings in distribution and identity verification costs. Individuals have more control over their data and can share and transact easily online without having to remember multiple usernames and passwords which creates higher levels of risk.

There is a standard data sharing agreement which takes into account the specific types of data that will be shared and how it will be used, with the individual being in control of the permission process. This allows individuals to engage with organisations in a more secure, flexible and convenient manner.

Technical Description

The Mydex Trust Framework works with an open API allowing all service providers and application developers signed up to the framework, to offer value. This way of working creates an environment of innovation and allows for new forms of engagement to develop between organisations and individuals.

Document name:	Inventories (2)	Page:	22 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



4.2.3 Nate Blue Button for Consumers Trust Bundle (NBB4C)

General Description

Although LIGHTest won't be handling healthcare data, the NBB4C provides an interesting example and guidance of how a trust framework in this sector can work.

The NBB4C works by using trust anchors of consumer-facing applications (CFAs) that securely move data from one application to another. Patients benefit from having access to their health information whilst relying parties can identify CFAs that meet or exceed the criteria of a trustworthy steward of consumer health information.

How the framework is being used practically

The NBB4C website (NATE, 2016) states that those who participate in NBB4C have a secure exchange of health information from provider-controlled applications to consumer-controlled applications. This could include personal health records and will use direct secure messaging protocols. If a provider organisation wishes to send messages to consumers using one of the recognized applications, they can load this bundle into their trust stores. In most cases, CFAs that are on boarded to the NBB4C have loaded publicly recognized trust bundles of provider facing applications and Direct Secure messaging should be enabled.

Technical Description

NATE uses trust bundles as a way to establish trust among the participating organisations and enables sharing of health information securely. On the NATE website (NATE, 2016) it states "Each Trust Bundle includes the trust anchors of organizations that have elected to adopt a common set of policies and practices corresponding to a specific health information exchange or purpose".

According to the NBB4C website consumer facing organisations that have completed the NBB4C onboarding include: Carebox Healthcare Solutions, GetRealHealth, Humetrix, iShare Medical, Medical Informatics Engineering, MedYear, Microsoft and Omedix.

4.2.4 The Respect Trust Framework

General Description

This was the first digital trust framework that was designed to create a mutual trust network for sharing private data safely between businesses and individuals online.

The Respect Trust Framework is designed to be self-reinforcing through use of a peer-to-peer reputation system called the Respect Reputation System™. The Respect Reputation System is based on peer-to-peer connections between Respect Network members and includes both positive reputation, called Vouching, and negative reputation, called Complaints.

How the framework is being used in practice

Document name:	Inventories (2)	Page:	23 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



The Respect Trust Framework has a set of five universal principles that govern the protection of identity and personal data: a promise of permission, protection, portability, and proof.

The framework has a network-wide reputation system with four levels of trust as the enforcement mechanism for compliance with the trust framework. This form of self-regulation is intended to ensure that members 'do the right thing' with regards personal data and communications.

Any sub community that requires more specific trust rules can use all the benefits of the Respect Trust Framework and the Respect Reputation System and add their own rules and regulations which apply to their own subnetwork. These communities could include a financial services network, a health information exchange or a social network.

Technical Description

The Respect Network uses the same four-party business model as the credit card networks. Instead of money, it is an exchange of information controlled by the customer. The exchange is directly between the customer's own personal cloud and the business's cloud over a customer controlled communications connection called a personal channel.

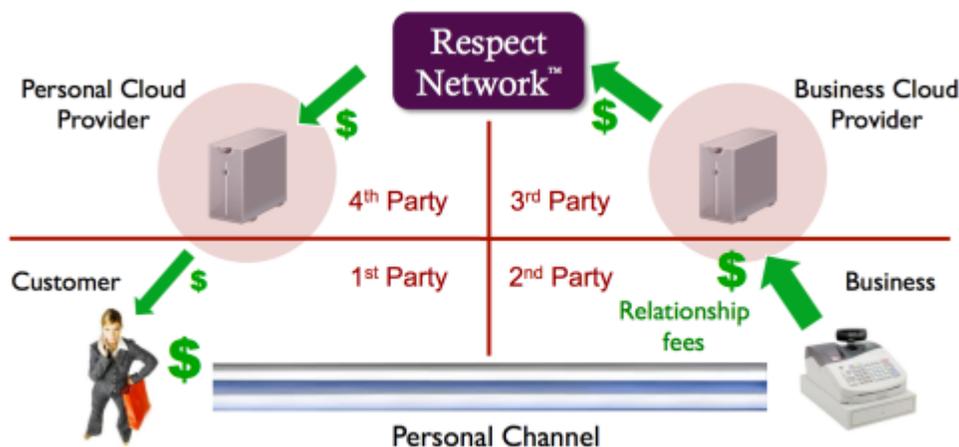


Figure 3 Personal channel (Respect, 2016)

Businesses on the Respect Network pay relationship fees which are based on the value of a customer relationship facilitated by the network. According to the Respect Network site, value components include:

- The value of the intimate customer profile, preference, and intention data that a customer is willing to share over a trusted, customer-controlled channel.
- The value of the bi-directional trusted messaging that can flow over the personal channel.
- The value of the automated event processing handled by the channel
- The customer acquisition and retention value of the channel.

Document name:	Inventories (2)	Page:	24 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



This model is called “Relationship-as-a-Service” because a business is outsourcing an extension of its own CRM system directly to the customer. This form of customer-managed relationships is called VRM (Vendor Relationship Management).

4.2.5 SecureKey Concierge™ Canada Trust Framework

General Description

The SecureKey Concierge (SecureKey, 2016) service is a cloud-based, Relying Party (RP) and Credential Provider (CP) neutral, online authentication service that enhances the security of online authentication transactions between Users and Relying Parties (RPs) through a network of trusted Credential Providers (CPs).

How the framework is being used practically

SecureKey Concierge uses a set of standards and technology to formalize the participation of its users through contractual relationships. The governance structure ensures that the ecosystem continually develops and enhances.

Users are able to sign in to Government of Canada services using their profile from their financial institution, bank or credit card instead of a username and password.

Technical description

Of particular importance to this scheme was that the underlying platform would have privacy built in. Therefore, they have developed Meaningless But Unique Identifiers and Persistent Anonymous Identifiers.

The SecureKey Concierge also uses a triple-blind privacy model where RPs are blind to the user’s selected CP, CPs are blind to the RP the user is accessing and SecureKey has no access to the user’s personal identifiable information.

Document name:	Inventories (2)	Page:	25 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



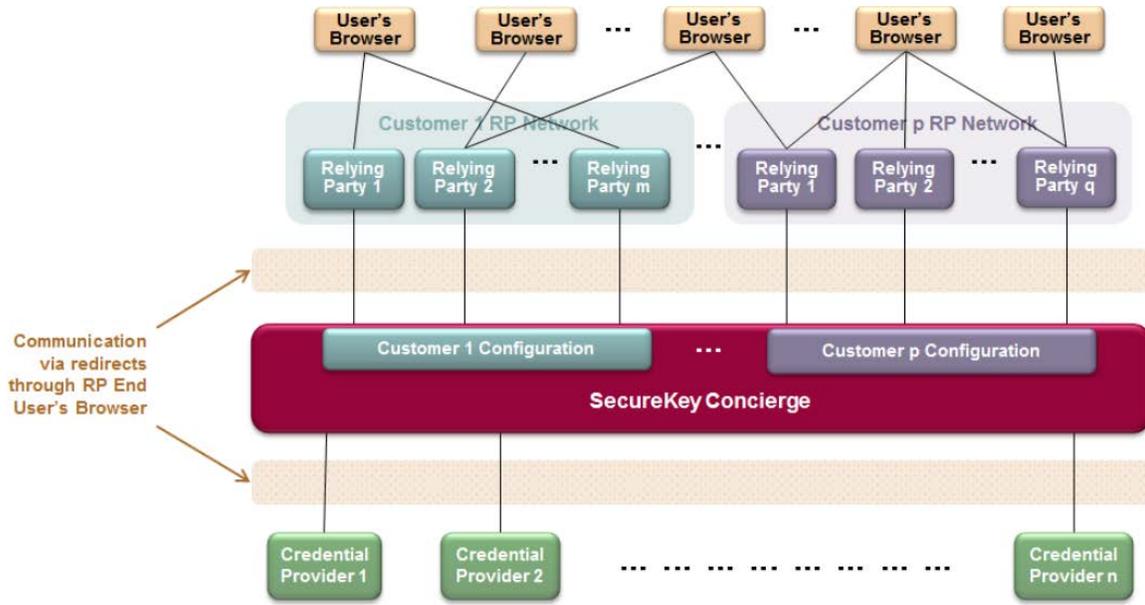


Figure 4 SecureKey Concierge service (SecureKey, 2015)

4.2.6 tScheme

General description

tScheme (tScheme, 2016) is an independent, industry-led and self-regulatory scheme which uses strict assessment criteria to approve trust services. tScheme itself does not run trust schemes or trust frameworks, its role is to define profiles for such schemes against which organisations can be independently assessed by a UKAS assessor.

As *tScheme* has such strict criteria, it provides a level of assurance to individuals and businesses who are using or relying upon e-business transactions. Due to this commitment to industry-led self-regulation rather than government-led legislation, *tScheme* is proving popular across Europe, and their objective is to continue to be the preferred option for fulfilling Part I of the UK's Electronic Communications Act 2000.

Types of organisations that tScheme is working with

- Schemes (trust frameworks) Authorities
 - organisations or groups of organisations seeking the development of a specific set of profiles or the addition of an auditable specification to an existing set of profiles to support one or more trust schemes they wish to operate and have any participant independently assessed with approved UKAS tScheme Assessors. For example, GOV.UK Verify
- Applicants

Document name:	Inventories (2)	Page:	26 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- organisations who seek to become approved to operate under one or more schemes. They are charged an applicant fee and such organisations need to be assessed by an independent UKAS approved tScheme assessor. Organisations included: Verizon, Experian, Digidentity, BT
- Independent Assessors
 - Organisations who employ assessors to undertake audit and inspection of Applicants under one or more schemes for example KPMG, LRQA.
- tScheme Members
 - organisations who are committed to delivering trust based services and see the value in supporting tScheme as an entity operate and develop an independent approvals body. Example members of tScheme are Mydex, BT, Experian, Payments UK, Cabinet Office

A technical example

The Cabinet Office runs a service called GOV.UK Verify that is used by government departments. Those government service providers rely on Identity Providers (IDP) who carry out a process of identity assurance to ensure that the relying party knows that the person visiting their digital front door to access a service is the person they claim to be.

The Identity Providers are subject to approval under the "Verify Scheme" which defines ways they must operate. Within the Verify Scheme organisations are required to get tScheme approval for delivering services against specific Profiles in accordance with a rule book from the scheme called GPG45.

- Base Approval Profile tSd0111 3.00
- Approval Profile for Identity Registration Services tSd0108 2.06
- Approval Profile for an Identity Provider tSd0112 1.00
- Approval Profile for Credential Management Services tSd0113 1.00

To get approved the identity provider must go through the process of being an approved applicant, producing a series of documents and then being independently assessed by a UKAS approved assessor who then writes a report which is submitted to the tScheme approvals The final decision to allow them go live is with the GDS who are the Verify Scheme Authority.

4.2.7 Pan Canadian Trust Framework (PCTF)

General Description

The PCTF launched in September 2016 and is not yet operational, however there are lessons that can be learnt from their policy frameworks and as of January 2017, the private and public sector in Canada are heavily involved.

The PCTF is a collaborative initiative of the public and private sectors and has been developed through collaborating with the Digital ID and Authentication Council of Canada (DIACC) and the Pan-Canadian Identity Management Sub-Committee (IMSC) of the Joint Councils of Canada.

Document name:	Inventories (2)	Page:	27 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



The PCTF will be applied across industries and subject to the laws and regulations of Canada. The idea is to allow PCTF to enable an ecosystem of trusted services as a foundation for digital interactions.

How the framework will be used practically

The PCTF is designed to allow digital identification, online credential, electronic authentication and authorization systems to provide services to government, citizens and businesses.

Stakeholders including, federal and provincial governments, financial institutions, telecoms, identity networks etc.

Technical description

In June 2016, Andrew Hughes undertook a presentation (Hughes, 2016) for the Kantara Initiative that described trust frameworks of which his main points are listed below.

Lots of different needs and expectations as well as operational modes.

DIACC Framework:

- Person identity proofing
- Credential management
- Authorization policy
- Access control (PEP)
- Authentication of credentials (verifier)
- Establishment of government authoritative identity records

Tools and Rules

- Technical protocols
- Software/servers
- Cryptography
- Communication protocols
- Standards
- Policies or proof of identity; levels of certainty
- Privacy policy
- Operations practices
- Designated authorities

Also in June 2016, Andrew Hughes presented at the Cloud Identity Summit (Brennan, 2016) with the following points mentioned:

Business value of a trust framework:

- Enables a whole of government approach for seamless e-service delivery
- Improves client experience and user convenience by supporting a 'tell us once' approach
- Enables jurisdictions to trust and leverage each other's identity management and assurance processes.

Document name:	Inventories (2)	Page:	28 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- Reduces the risk that the individual is not who they claim to be
- Reduces identity-related administration costs
- Strengthens program integrity

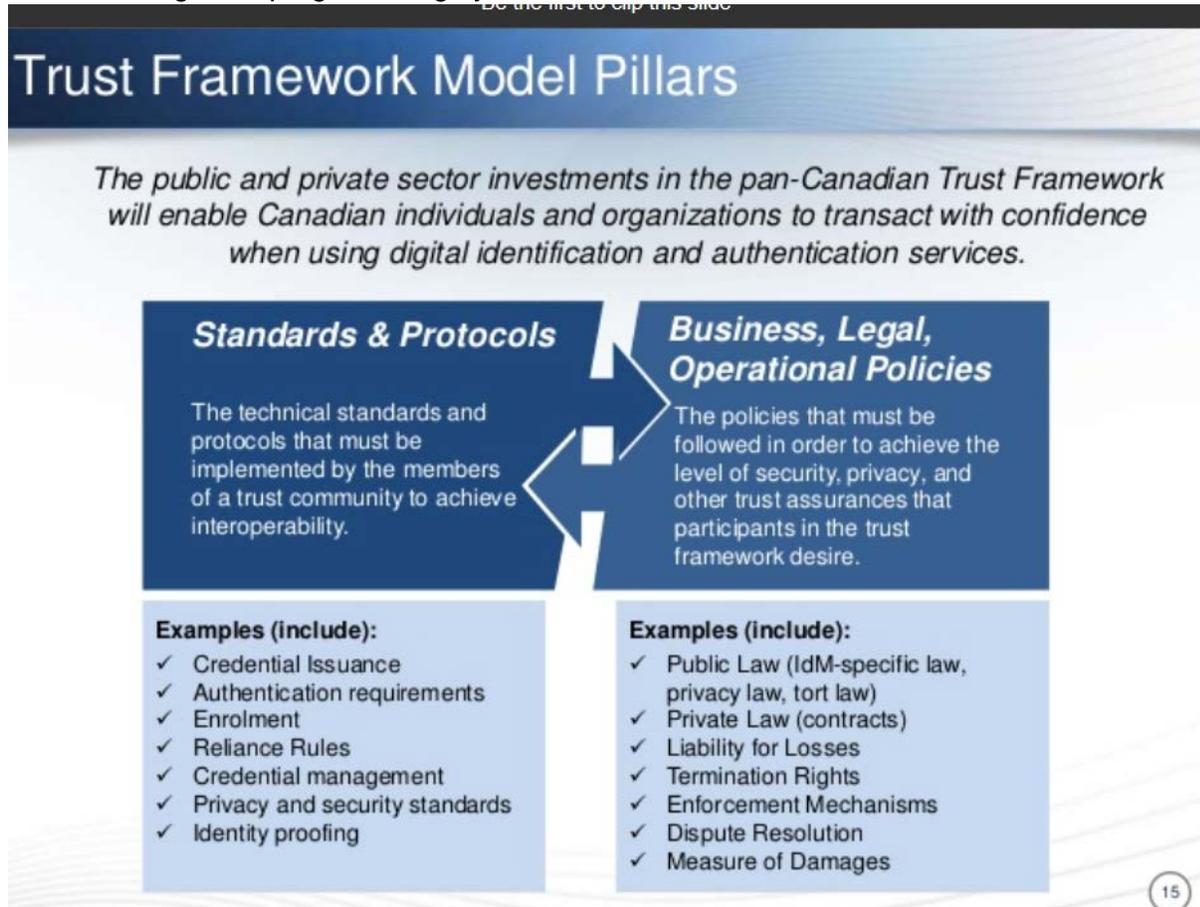


Figure 5 Trust Framework Model Pillars (Brennan, 2016)

4.2.8 ID.me

General description

The ID.me service provides end-to-end identity proofing and credential management service for veterans across North America, first responders, and members of other designated groups. The digital ID card allows for a single sign-on technique to verify their identities remotely, for online transactions, which doesn't expose their personally identifiable information.

This service allows individuals to bind specific characteristic attributes to their primary identity, enabling them to gain a broad range of customized services and benefits across multiple sectors.

Document name:	Inventories (2)	Page:	29 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



How this framework is being used practically

As an example, this scheme is being used by military personal, both active and veterans, to allow them to verify their military credentials at a number of retail partners and government agencies. This allows them to get discounts at various retailers without having to show their social security number.

Technical description

ID.me issues password-based single and multi-factor credentials across Assurance Levels 1, 2 and 3. To enroll, consumers apply through the ID.me website, fill in some of their personal information such as name and zip code, and then fill in a secret field that varies according to the organisation and benefit value. For example, in a military context this could be a full or partial social security number. In the back-end, ID.me then compares the applicant’s information with authoritative databases such as a bank or university. Any organisation that uses the technology to prevent fraud is charged up to \$1 for the verification response.

ID.me uses SAML protocol to return a response from government agencies. To ensure the security of all sensitive information, ID.me uses RSA 2048 encryption for data in transit and AES 256-bit encryption for data at rest.

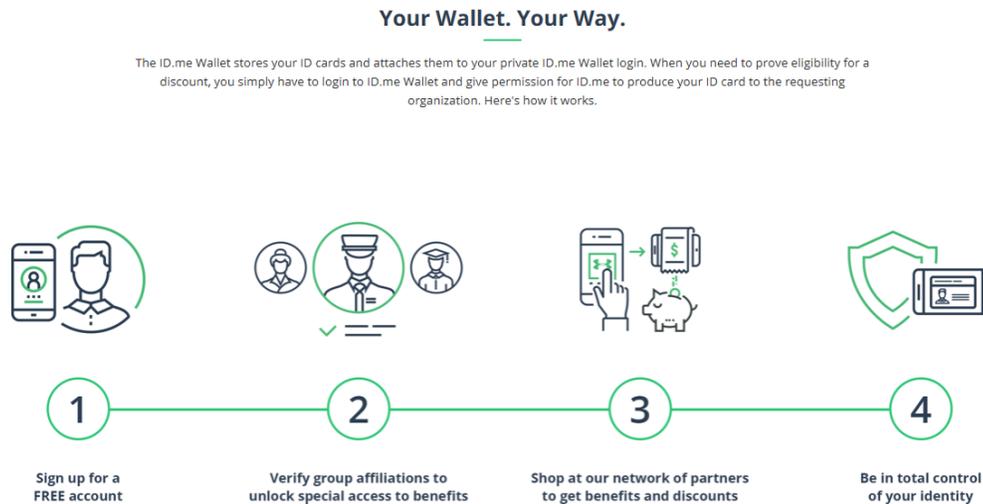


Figure 6 ID.me (ID.me, 2016)

Document name:	Inventories (2)	Page:	30 of 170	
Dissemination:	PU	Version:	2.5	

5. Existing Device Attestation Schemes

This section focuses on elaborating on the existing device attestation schemes in an academic and industry aspect. With regards to the academic side, there is an introduction to what an attestation scheme is and a deeper insight to hardware, software, and hybrid types of device attestation schemes. With regards to the industry side, there is insight to various existing security models and standards regarding existing device and attestation schemes.

5.1 Academic Perspective

5.1.1 Introduction to Attestation

This section provides a brief and forward introduction to attestation schemes. For instance, while working at a refinery, you open your remote monitoring dashboard at <http://intranet/monitoring.php> and receive the following message:

```
{  
    "name" : "centrifuge speed",  
    "value" : "90%",  
    "timestamp" : "153327822.3"  
}
```

What does it mean to you?

Would there be a difference, if you had received the same data over an authenticated, integrity-protected communication channel?

In the first case, it seems that the speed is within allowed range. Or that the sensor has actually failed and is displaying the last value indefinitely. Or that the sensor has been replaced by accident with another model that actually scales values to 20-80%. Or an adversary has replaced the part or penetrated the monitoring system and is feeding you false information on purpose.

Without secure device attestation, you might think that things are going well, but you wouldn't ever know for sure.

Verification of a local or remote system's integrity to ensure performing as expected is an important research problem in Computer Security field. Attestation defines the verification process of computer systems works fully operational and secure in both hardware and software layers. Computer systems are layered structures, and the integrity of a layer depends on the integrity of lower layers. Therefore, only a chain of attestation could guarantee the integrity of a system. An attestation process starts in computer booting at hardware and firmware level and continues on software level. In common understanding for attestation, *the prover* (the system

Document name:	Inventories (2)	Page:	31 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



that wishes to be evaluated for compliance) sends its current configuration to *the verifier* to declare it is a trustworthy system.

Remote attestation allows changes to the user's computer to be detected by authorised 3rd parties. Attestation starts when the prover, sends a report of its current configuration to the verifier, asking it to confirm that the prover is in an accepted state. (Asokan et al, 2015).

Stripped to basics, attestation is an interaction between two parties, the verifier and the prover, through which the verifier ascertains the current state and behaviour of the prover.

The two basic requirements of attestations are to:

1. Represent the real state of the system
2. Represent the current state

To achieve these requirements in practice, we need to be able to not just verify that the prover provides a truthful representation of its current state, but also to verify that the information hasn't been changed on its way to the verifier.

Trust can't be built on thin air, and therefore there are three approaches for the trust anchor:

1. Hardware-based (HWAT)
2. Software-based (SWAT)
3. Hybrid

The most secure attestation is achieved with specifically designed secure hardware, like TPM modules for private key storage and ARM's TrustZone for application storage. The TPM platform registers can store a cryptographic hash of the underlying platform in a chain, that can't be overwritten by any software, only extended.

Attestation based on secure hardware is most suitable for complex/expensive platforms, such as smartphones, tablets, laptops, and servers. The trade-off for the security is increased complexity: the additional hardware takes up space and power and both the hardware and the required software increase costs.

In contrast, software-based attestation requires neither secure hardware nor cryptographic secrets. Typically, the verifier sends the prover a request to verify its operation along with a nonce; the prover then runs a verifying application that returns a cryptographically signed report along with the signed nonce for timeliness. However, the verifier cannot guarantee that the prover runs any specific code. Therefore, security guarantees of software-based attestation methods rely on strong assumptions, such as the adversary being passive while the attestation protocol is executed and the applicability of the attestation algorithm and its implementation. They also rely on tight time constraints. Strict estimation of the round-trip time and the existence of an out- of-band authentication channel are required, as no secrets are shared between the prover and the verifier. Such assumptions are hard to achieve in practice, and they restrict the applicability of software-based attestation to the one-hop setting.

Document name:	Inventories (2)	Page:	32 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Hence, a secure and practical software attestation scheme requires minimal security features in hardware, such as write-protected memory like ROM or an MMU. (Francillon et al., 2014). A hybrid solution is to use a minimal amount of additional hardware for the trust anchor. For example, the verifying application and TLS keys could be stored in read-only memory, making the attestation stronger.

So far we haven't yet taken a look of the requirements of the other side of the attestation relationship, the verifier. Securing the verifier is just as important, as an adversary could otherwise impersonate the verifier to abuse attestation results or even launch a DoS attack against the resource-constrained nodes by repeatedly requesting attestation.

To prevent the abuse of attestation, the verifier must be authenticated to provers. Two-way TLS provides a well-known, strong method for this, but unfortunately asymmetric crypto is computationally expensive. Recognising this, in the past five years new ciphers have been developed for IoT applications, for example the Curve25519 for use with the elliptic curve Diffie-Hellman key agreement and the related Ed25519 digital signature scheme.

TLS alone will not protect against replay attacks. In order to detect replays of previous requests the prover can use nonces, counters or timestamps. The first two require integrity-protected storage for previous nonces/for the counted. The latter requires a trusted synchronised clock at the prover side.

LIGHTest aims to address the challenge of deriving identities in user-owned devices from existing trust identities, ensuring that the trust in government IDs can be properly propagated to mobile identities in user-owned devices. In this context, Device attestation schemes play a key role in determining a level of assurance of the derived credentials generated in this user-owned device. Depending on the environment where these credentials are generated (hardware-based or software-based security), a certain level of assurance of the user-owned device can be reached.

5.1.2 Hardware-based Attestation Schemes

Hardware based attestation methods rely on specialized hardware (e.g. an external TPM (Trusted Platform Module) chip or on the availability of special SoC integrated hardware to perform attestation, either statically (at system power-up) or dynamically, during normal operation of the system.

Secure Boot: In Secure Boot (Arbaugh et al., 1997), system integrity is verified at system startup: The root of trust is a cryptographic key buried in hardware, which is used to compute a hash of the boot loader, and compared to a signed hash stored in secure ROM. A device is only allowed to boot if the two hashes match. In the 60s and 70s, secure computing theories was built on OS security and based on the assumption of hardware and firmware are trustworthy. However, a trust decision based on the assumption of secure OS kernel bootstrap, which may be started by an untrusted process, is unreliable. One of the early studies in the field of device attestation published in 1997 (Arbaugh et al., 1997) to solve the unreliability of these highly

Document name:	Inventories (2)	Page:	33 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



axiomatic decisions by proposing a secure bootstrap process called AEGIS. They proposed a “chain of integrity checks” which starts from power-on to control transfer to the , independently hashing each layer.

TPM Attestation: A TPM module at boot time and send this checksum to be validated by a remote verifier. TPMs can also protect a limited amount of data against a compromised operating system, e.g. generate and store private keys. A TPM can store integrity measurements in PCRs in protected memory. Overall, security is based on two properties: (1) PCRs are accessible only via an API provided by the TPM and (2) measurements in the PCRs can only be extended, each new extension is computed using a cryptographic hash of the previous PCR value and the new measurement. The root of trust is the private key stored in firmware.

DAA Attestation: Direct Anonymous Attestation (DAA) (Chen, 2011) is a scheme developed by Brickell, Camenisch, and Chen, for remote authentication of hardware TPM module, while preserving the privacy of the user of the platform that contains the module. The DAA scheme was adopted by the Trusted Computing Group (TCG), an industry standardization body that aims to develop and promote an open industry standard for trusted computing hardware and software building blocks, and was included in TPM specification version 1.2. The concept is based upon group signatures with stronger anonymity guarantees; in particular, the identity of a signer can never be revealed, but signatures may be linked with the signer's consent, and signatures produced by compromised platforms can be identified. A DAA scheme considers a set of hosts, issuers, TPMs, and verifiers; the host and TPM together form a trusted platform or signer. DAA protocols proceed as follows. A host requests membership to a group provided by an issuer. The issuer authenticates the host as a trusted platform and grants an attestation identity credential (occasionally abbreviated credential). The host can now produce signatures using the credential, thereby permitting a verifier to authenticate the host as a group member and therefore a trusted platform. In (Brickell et al., 2009) the following properties for DAA are characterized:

- User-controlled anonymity.
 - o Deniability. The identity of a signer cannot be revealed from a signature.
 - o Unlinkability. Signatures cannot be linked without the signer's consent.
- User-controlled traceability.
 - o Event chainability. Signatures are linkable with the signer's consent.
- Non-frameability. An adversary cannot produce a signature associated with an honest TPM.
- Correctness. Valid signatures can be verified and, where applicable, linked.

Document name:	Inventories (2)	Page:	34 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



SPM : A recent hardware-based mechanism for process isolation is called SPM, (Strackx et al., 2010). It relies on a special vault module bootstrapped from a static root of trust. This vault bootstraps the SPM-protected programs, which gain an exclusive control over their own memory pages.

PUFatt (Embedded Platform Attestation Based on Novel Processor-Based PUFs): In this paper, (Kong et al., 2014) propose a hardware based device attestation technique which is based on ALU PUFs (A physically unclonable function based on the delays between two ALU units). In their protocol a server (V: verifier) emulates the PUF assuming that it knows the intrinsic delay of the PUF and runs a challenge response function on the emulator. Later using this response, the V runs a SWAT algorithm using the response as an input and obtains a result. The V sends the same challenge to the device (P: prover), which sends the challenge to the PUF and runs the same SWAT using the result of the PUF. Matching the two results on the server, V verifies the integrity of the software running on the P.

5.1.3 Software-based Attestation Schemes

Most of the existing software-based attestation techniques are based on challenge-response paradigm between the trusted verifier and the potentially compromised prover (the target device). The basic mechanism behind the SW based attestation is guaranteeing to get a response from a prover within a specific time frame and get the calculated checksum of the prover's current state. A verifier accepts the trustworthiness of a prover if and only if i) the checksum calculated by the prover is the same as the checksum calculated by the verifier, which verify the existence of the expected program within the prover and ii) the prover responds back within a time limit like an honest device would give which verifies the prover did not do additional computations such as hiding a malicious software etc.

The list for the well-known software-based attestation Schemas:

Pioneer: provides device attestation without relying on a secure co-processor or any specialized hardware. It computes a checksum of device memory using a function that includes side-effects (e.g., status registers) in its computation, such that any emulation of this function incurs a timing overhead that is sufficient to detect cheating (Seshadri et al., 2005).

Time-based Approaches: Attestation that relies on time-based checksums has also been adapted to embedded devices (Kovah et al., 2012) However, some assumptions that form the basis for these solutions have been challenged and several attacks on these (and similar) schemes have been proposed.

- SWATT (SoftWare-based ATTestation): This is a software based device attestation method that allows an external verifier to perform an equality check on the entire memory of the device. This is more like a state based integrity check (i.e. the current image looks good, but this does not make sure that a malicious execution will not take place). Also checking the entire memory might be a bit impractical because the external verifier might not have access to all the memory. (Seshadri et al., 2004)

Document name:	Inventories (2)	Page:	35 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- SCUBA (Secure Code Update by Attestation in Sensor networks): This is a protocol between a base station and sensor connected to this station, where the base station performs attestation and malicious code removal (i.e. untampered code update) on the sensor (Seshadri et al., 2006). They propose a protocol that guarantees that a firmware update executable is not harmed prior to, and during the malicious code removal. While the integrity of the executables are verified via check summing, they use a constructing a challenge response protocol called ICE (Indisputable Code Execution) and running an ICE verification function which sets up an atomic execution environment and does self-code check summing. After performing self-verification in an atomic manner, the ICE protocol runs the executable in three steps: 1) verify the integrity of the update executable, 2) set up an untampered execution environment for the executable (i.e. set up an atomic execution context that does not allow any other process to run during that time), 3) Invoke the executable to do the update and removal. They analyse various attacks (e.g. checksum forgery, speed up, impersonation attacks) and analyse their proposed method accordingly. SCUBA protocol either repairs the sensor memory by replacing the malicious code with an authentic firmware or the base station blacklists the sensor if the update takes too much time, assuming that a malicious code is interfering the update. They assume that the attacker's hardware devices are not present in the network during repair which is a drawback.
- VIPER (Software based attestation of the peripherals): (Li et al., 2011) proposes a software based attestation scheme to verify the integrity of the firmware running on the peripherals of a device. The problem to be addressed is that the peripherals of a system (mainly a computer system) might be vulnerable to malicious codes during firmware upgrades. They also provide, some example attacks from the literature. (e.g. (Triulzi et al., 2010) have demonstrated that a malicious code running on a Broadcom Tigon NIC can deploy malicious code to the GPU, Chen has demonstrated that the Apple keyboard update tool has a vulnerability that allows a malign code can be injected to the keyboard). They state the fact that peripherals might communicate each other via the Southbridge completely undetected by the hardware attached to the Northbridge (CPU, memory...), and a weak peripheral (i.e. a slow 8-bit microcontroller) might use a strong peripheral for expensive operations like check summing and hashing (called Proxying). They propose a method that assumes a reliable operating system running a reliable verification tool that has the checksum and hash values of the firmware running on the peripherals. The verification tool requests the values from the peripherals and compares them to what it has to fulfil the attestation process. They solve the proxying problem by starting the verification with the most powerful peripheral to the least powerful one. In addition, they state that it is important to keep the verification procedures of the peripherals busy until the completion of the verification of all the peripherals, so that, a malicious code cannot use a more powerful peripheral for check summing and hashing during the full attestation process. Please refer to the paper for the details about their experiments and results.

Non-time based Approaches: Alternative (non-time-based) approaches rely on filling the entire memory of the prover with random data to ensure absence of malicious code. Although timing is not essential here, this approach is still limited to one-hop attestation since it lacks the means to authenticate a remote prover (Perito et al., 2010).

Document name:	Inventories (2)	Page:	36 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



5.1.4 Hybrid Attestation Schemes

SMART: – a hardware-based scheme for establishing a dynamic root of trust in embedded devices. Its focus is on low-end microcontrollers (MCUs) that lack sophisticated features such as specialized memory management or protection features. SMART requires small changes to the MCUs but no additional hardware (Eldefrawy et al., 2012).

5.2 Industry Perspective

Device attestation has obtained renewed interest with the raise of the Internet of Things (IoT). Indeed, Intel suggests its Enhanced Privacy ID (EPID) protocol (which is a variant of DAA) as the industry standard for authentication and attestation for IoT.

5.2.1 Security Models

In spite of the large scale deployment and the long body of work on the subject, a sound security model was only given this year (Camenisch, et al., 2016). Let us thus briefly summarize the state of the art here. There exist a number of security definitions using the simulation-based and property-based paradigms. In the simulation-based paradigm, a single ideal functionality is specified that needs to be implemented by a protocol. The security and functional property of which are typically easily derived from that specification and thus inherited by the protocol if it implements the functionality correctly. In the property-based paradigm, a number of independent properties are stated by security games and it is then proven that a protocol satisfies each of these properties separately.

Unfortunately, all security definitions for DAA (Camenisch, et al., 2016) have rather severe shortcomings such as allowing completely broken schemes to be proven secure. This was recently discussed by Bernhard (Bernhard, et al., 2013) who provided an analysis of existing security notions and also proposed a new DAA model. In a nutshell, the existing simulation-based models that capture the desired security properties in form of an ideal functionality either miss to treat signatures as concrete objects that can be output or stored by the verifier (Brickell, et al., 2004) or are unrealizable by any instantiation (Chen, et al., 2008) (Chen, et al., 2008)

Another line of work therefore aimed at capturing the DAA requirements in the form of property-based security games (Brickell, et al., 2009) (Chen, 2010) (Bernhard, et al., 2013) as a more intuitive way of modeling. However, the first attempts (Brickell, et al., 2009) (Chen, 2010) have missed to cover some of the expected security properties and also have made unconventional choices when defining unforgeability (the latter resulting in schemes being secure that use a *constant* value as signatures).

Realizing that the previous models were not sufficient, Bernhard et al. (Bernhard, et al., 2013) provided an extensive set of property-based security games. The authors consider only a simplified setting which they call pre-DAA. The simplification is that the host and the TPM are considered as single entity (the platform), thus they are both either corrupt or honest. For properties such as anonymity and non-frameability this is sufficient as they protect against a corrupt issuer and assume both the TPM and host to be honest. Unforgeability of a TPM

Document name:	Inventories (2)	Page:	37 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



attestation, however, should rely only on the TPM being honest but allow the host to be corrupt. This cannot be captured in their model. In fact, shifting the load of the computational work to the host without affecting security in case the host is corrupted is one of the main challenges when designing a DAA scheme. Therefore, a DAA security model should be able to formally analyze this setting of an honest TPM and a corrupt host. This is also acknowledged by Bernard et al. (Bernhard, et al., 2013) who, after proposing a pre-DAA secure protocol, argue how to obtain security in the full DAA context. Unfortunately, due to the absence of a full DAA security model, this argumentation is done only informally. This argumentation is actually somewhat flawed: the given proof for unforgeability of the given pre-DAA proof cannot be lifted (under the same assumptions) to the full DAA setting (Camenisch, et al., 2016). This highlights the fact that an “almost matching” security model together with an informal argument of how to achieve the actually desired security does not provide sound guarantees beyond what is formally proved. As a consequence, all schemes except the recent ones by Camenisch et al. (Camenisch, et al., 2016) (Camenisch, et al., 2016)

Number theoretic assumption

The attestation scheme in the literature are all based on number theoretic assumption that will not withstand a quantum computer. Thus, further research is needed towards finding attestation schemes that are based on assumptions that are believe to be secure also against quantum computers.

5.2.2 Standards

From an industry perspective, it is important that an attestation scheme be standardized. In the following we review the most relevant standards.

Trusted Computing Group and TPM standards: The TCG specified a number of mechanisms for attestation. The first one was using traditional certificates together with a third party (called Privacy CA). Here, the TPM would first generate an ephemeral attestation key pair and then send the public key of that pair to the Privacy CA together with the endorsement key (the long-term certificate of the TPM). The Privacy CA would validate the endorsement key, then certify the ephemeral public key, and send that certificate back to the TPM. The TPM can then use the attestation key pair to attest to its state and then the attestation together with the certificate from the Privacy CA to the verifying party. As such a Privacy CA is clearly a bottleneck and also be able to break privacy, the TPM 1.2 specified direct anonymous attestation as a better protocol. That protocol was based on RSA and hence implementations were slow. With the TPM 2.0 specification, the RSA-based scheme was dropped in favour of a set of elliptic curves based protocols. The initial TPM 2.0 specification contained some flaws, preventing a security proof for the new protocol. This flaw has been fixed in the most recent version (late 2016).

ISO/IEC: ISO/IEC 20008-8 specifies anonymous signatures which include a number of direct anonymous attestation scheme (in particular the DAA scheme from TCG TPM 1.2 and version of the schemes based on elliptic curves). However, some of these scheme (in particular the elliptic curve ones do have security flaws (Camenisch, et al., 2016) (Camenisch, et al., 2016).

Document name:	Inventories (2)	Page:	38 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Intel/EIPD/SGX (quasi standard): Intel has put forth what is called Software Guard Extensions that is a set of CPU instructions to form a safe software compartment. It also features remote attestation that a secure enclave has been established and results of the execution of an enclave. The attestation is based on EPID.

Document name:	Inventories (2)	Page:	39 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



6. Relevant delegation Schemes

Using electronic means such as electronic mandates to satisfactorily express these delegations in an interoperable, cross-domain and even cross-border manner has been identified as a domain integral to LIGHTest scope, given that one of its tangible outcomes will consist in infrastructure (open-source client and server tools useful for constituent entities of the LIGHTest architecture like Delegation Publishers) supporting different types of publication and querying of delegations (including new forms of delegation such as DNS-enabled delegation of some of their own capacities by under signers with formal verification of those capacities). Trust verification mechanisms of LIGHTest will also query and apply rules based on processing of delegations data (including mandate chains which also express chains of trust) and the automatic processing of delegations/mandates is part of the scope of LIGHTest e-Procurement pilot as well (enabling applications to use delegations so that employees can be authorized to i.e. issue invoices). Analysis of relevant schemes identified here (and extended in subsequent Inventories deliverable) will be relevant to subsequent tasks for other tasks of both “Requirements, Concepts and Evaluation” and “Infrastructure for the Publication and Querying of Delegations” Work Packages. Other sources of a legal nature on delegations will be addressed more extensively in the context of Task 5.5 “Ensuring Cross-Border Legal Compliance and Validity of Delegation”.

6.1 Academic Perspective

6.1.1 Overview

More and more, empowering (in a legally recognized way) a person to be authorized to conduct a certain transaction or carry out a representation on behalf of another person is becoming a common need in everyday business cases. In the context of electronic transactions, electronic forms of empowerment and representation are needed to express authorizations explicitly. A brief overview is given here.

6.1.1.1 Delegation schemes

A legal mandate can be defined as the authority to perform well-defined legal actions on behalf of another entity, and is conferred through delegation. The mandate only provides the legal ability to perform the actions, but does not necessarily configure an obligation. As an example, the Belgian ‘Tax-on-Web’ application’s main delegation options are delegated administration (which is a technical kind of mandate) and agency (which configures a legal contract). (Alsenoy, et al., 2009)

Spain issues special digital certificates to companies, that give the holder absolute power to represent the company in any situation. Special certificates, however, as well as attributes added to certificates in order to enable a specific kind of representation, are too inflexible to be useful beyond simple delegation cases. (SpringerLink, 2009)

Document name:	Inventories (2)	Page:	40 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



The Austrian e-ID system empowers electronic representation by using XML-based electronic mandates. Electronic mandates are important as they are the electronic equivalent of conventional mandates for empowering a person, in which a proxy acts for another person (the mandatory), and also because they serve to close the gap between private persons and legal entities. Since Austrian Citizen Cards, useful to electronically identify a person in front of Austrian e-Government applications, are only issued to natural persons, electronic mandates allow legal entities to actively participate in Austrian e-Government. (SpringerLink, 2009)

In order to introduce delegation and mandates in the STORK framework, the STORK 2.0 project implemented a new function which permits to add attributes to specify legal and representation powers, extending the identification to legal persons, and permitting one entity to authenticate on behalf of another. The mandates are typically derived from an authoritative source, for example a Business Register, establishing criteria to assign a LoA to the attribute to establish its authoritativeness. Attributes can also be specific to certain domains, for examples the identification on health care providers in the eHealth domain. (Leitold, et al., 2014)

6.1.1.2 Delegation management

In the past, most identity management systems used roles to specify user privileges. Under this model, a role comprises a set of actions which an entity that has assumed that role is allowed to perform. This set of 'permitted actions' is also referred to as the 'privileges' of a particular user. (Alsenoy, et al., 2009)

In case of delegation, the mandate holder's privileges need to be extended to include the authority bestowed upon him. The downside of an entirely role-based approach is that when the privileges of one particular entity need to be extended or suspended, a new role must be created. (Alsenoy, et al., 2009)

In advanced identity and information management systems, use is made of so-called (security) tokens to achieve more flexible user and access management. A security token is a digital representation of a claim or set of claims which has been certified by a particular entity. More generally speaking, a security token can be any piece of information (data) which has been attested by a particular entity, typically an attribute. Tokens are therefore also often referred to as 'assertions' or 'vouchers'. (Alsenoy, et al., 2009)

In Austria, a unique personal identifier known as Source Personal Identification Number (sourcePIN) and derived from the Central Register of Residents, serves as the basis for electronic identification and delegation in Austrian e-Government, and is created during the Citizen Card issuing process. This process and all required secrets, i.e. the secret key used during the creation process, are under the control of the so called Source-PIN Register Authority which is governed by the Austrian Data Protection Commissioner. Due to privacy reasons, it is forbidden by law to use this sourcePIN within e-Government applications directly. Instead, Austrian e-Government applications have been divided into a number of application sectors and for each application sector a different Sector-Specific Personal Identification Number (ssPIN) has to be created. (SpringerLink, 2009)

Document name:	Inventories (2)	Page:	41 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



6.1.1.3 Delegation publishing and querying

Since 2007 Belgian 'Tax-on-Web' mandates are managed through a generic application which allows civil servants to register, modify, consult and delete mandates through a web-interface. The mandate registrations and modifications are then uploaded to a logical entity of which the primary purpose is to confirm, when requested, whether or not a particular user (in this case: an accountant) has in fact been issued the appropriate mandate (and whether or not it is still valid). In this sense the logical entity in question acts as what is commonly referred to in identity management literature as an 'authoritative source'. (Alsenoy, et al., 2009)

In particular, this logical entity acts as an authoritative source with regards information concerning mandates within the system. The local administrator can detail which applications should be made accessible to which user, but the authorization policies themselves are still managed by the relevant governmental agencies. (Alsenoy, et al., 2009)

In Austria, electronic mandates are issued by the Source PIN Register Authority only. Therefore, this authority provides a web-application with which citizens can apply for electronic mandates based on an existing authorization (empowerment). This means, that the empowerment must be already established, e.g. based on paper mandates or entries in official registers (e.g. the register of commerce). In order to foster the take up of electronic mandates in the field of e-Government applications, the Austrian e-Government initiative provides open-source software modules for providers and developers of e-Government services, which automatically verify electronic mandates—including chain verification—and provide e-Government applications the unique electronic identity of the mandator and the proxy. (SpringerLink, 2009)

6.1.1.4 LoAs of mandates

The protocol between the relying service provider and an Authoritative Source of Attribute Information (ASAI) is similar to the protocol between the relying service provider and the Mandate Authority: when confronted with an entity alleging a mandate, the relying service provider will query the relevant Authoritative Source to find out whether this entity in effect has the prerequisite profession or capacity. If such is the case, the Authoritative Source will respond by way of an attribute assertion (which also takes the form of a security token), provided that the entity requesting confirmation is authorized. Mandate assurance based on attributes such as LoAs implies that the relying party has implemented a set of policies clearly specifying which attributes give rise to which (apparent) authority. (Alsenoy, et al., 2009)

6.1.1.5 Existing data formats

Token types are commonly specified using the Security Assertion Markup Language (SAML) standard, allowing assertion of identity, attributes, and entitlements of a subject from one entity to other entities (OASIS, 2010), developed by the Organization for the Advancement of Structured Information Standards (OASIS). (Alsenoy, et al., 2009)

On a technical level, an electronic mandate in Austria is a specific XML structure which must be electronically signed by an issuing authority, i.e. the Source-PIN Register Authority. The issuing

Document name:	Inventories (2)	Page:	42 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



authority just asserts that the electronic representation bases on an existing and already established authorization. (SpringerLink, 2009)

6.1.2 Electronic mandates and representations

While earlier studies like MODINIS partially address mandates and delegation aspects (modinis, 2005), (Alsenoy, et al., 2009) and their categorization -like IDABC (European Commission, 2009)-, most recent conclusions stem from studies in STORK 2.0 project (STORK 2.0, 2014), (Leitold, et al., 2014), which indicate that while mandates and electronic representation of legal entities are of great importance, there appears to be relatively little maturity in this field. (Alsenoy, et al., 2009) study under the name Delegation and digital man- dates: Legal requirements and security objectives, considers both legal and technical aspects of mandates. The input received in that project from participating countries (STORK 2.0, 2015) shows that there are a significant number of relevant factors that determine whether a mandate to represent a legal entity is available to third parties and whether it is legally valid, including the type of legal entity, type of action, restrictions in the act of association/charter of the company, and type of agent designated. Unfortunately there is no general and harmonized legal or policy framework for mandates in Europe: this issue is still left to national legislations which are not always consistent between each other.

A very important issue concerns the possibility for third parties to know with a great degree of certainty which person has the mandate to represent a legal entity, given that there exists also no harmonization at the European level as regards publication in the commercial register of agents with the power to represent and manage legal entities. Such publications are not universally available. Even if they would be available, barriers would still arise in practice when a legal representative of a legal person acts in another country due to language issues and semantic divergences, provided that original information about mandates (including any applicable restrictions to the mandate, e.g. a requirement for joint signatures) in the commercial register are in the language of the country of the legal person. The basic requirement of STORK 2.0 to produce an electronic SAML 2.0 assertion and token to capture the essence of the powers of representation is not explicitly authorised or compatible with the schemes of many countries. The national laws provide for traditional company certificates, but not for web service “micro-transactions” which moreover use the STORK 2.0 powers taxonomy to describe the company powers. More details on this are given in (STORK 2.0, 2015) and (STORK 2.0, 2016).

Therefore, in this section we focus mostly on the pioneering work of STORK 2.0 on electronic mandates and representation (in particular in the field of cross-border authentication) and on its extended AQAA (Attribute Quality Authentication Assurance) model, inasmuch it supports the extension of levels of assurance to attribute providers which also provide information relevant for delegation and can thus be considered part of pan-European delegation scheme of STORK 2.0. This is an important starting point for LIGHTest as a way to consider different levels of assurance of delegations (applicable to empowerment based on Constitutive Registers or Competent Authorities) as an element for overall assessment of trustworthiness in a way that promotes global acceptance of the LIGHTest approach. Furthermore, STORK 2.0 also provided

Document name:	Inventories (2)	Page:	43 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



common specifications and reference implementation for electronic mandates and for their use to extend electronic authentication to natural persons acting on behalf of legal persons (STORK 2.0, 2016). We also offer an example of a national delegation scheme, which is working currently in Austria (see 6.2.1 Austria: MOA/MOA-ID (Vollmachtenservice)), relying on XML-based electronic mandates as the vehicle to achieve empowerment and representation with flexibility for addressing scenarios beyond simple scenarios (covered in other countries with special types of certificates or adding identifiers to digital certificates that express a certain type of representation). Belgium also has a systematic electronic mandates scheme (other countries in the EU have more ad-hoc solutions covering specific applications/service types).

6.1.3 Attribute Quality Authentication Assurance (AQAA) model

STORK 2.0 implies the integration of legal entities and mandates (both mandates to represent legal entities and contractual mandates to represent specific natural persons). STORK 2.0 included technical activities defining the structure of the electronic mandate and the procedures for handling the corresponding SAML token (STORK 2.0, 2015) or the validation of powers stored at service providers, as well actions addressing the organisational-semantic-legal issues involved in achieving cross-border interoperability of this information (STORK 2.0, 2015). It is implicit in the very logic of a mandate or a chain of mandates that the final representative will be acting on behalf of persons not present or directly involved in the transaction.

STORK 2.0 provided solutions for the integration of legal entities and mandates (both mandates to represent legal entities and contractual mandates to represent specific natural persons) in pan-European ecosystem for interoperable electronic identity (and trust services). In bridging the few national islands where such services currently exist, STORK 2.0 achieved significant results, by evolving STORK 2.0 specifications to include attributes for legal persons and representation powers and mandates, and by adapting the procedures implemented in the common building blocks to allow cross-border transfer of this kind of information integrated in real eGovernment processes. Its Report on Mandate/Attribute Management (STORK 2.0, 2015) presents an overview of the problems linked to the cross-border use of mandates and roles and of the possible legal solutions to assure their smooth usability in international contexts. In particular it assesses how mandates can be used in another participating country based on the existing EU, international and national legal framework. The aim of this Deliverable was not that of providing a full overview of legal tools such as national laws that apply to the issue (since an analysis of all legislations of participating countries is cumbersome and out of the scope of STORK2.0) but rather to deliver methods, rules and techniques to apply to each specific case. Based on questionnaires filled in by STORK 2.0 participating countries, it addresses legal rules in each country covering key concepts, establishment of mandates (form, content and notary intervention), validation obligations by the recipient of a mandate, legal limitations, term and revocation, use of sub mandates, and of course the establishment of mandates using electronic means (including the need for eSignatures).

The analysis pointed out that mandates topic is governed by national law, and that it would be necessary to assess in each case which law applied, which type of mandate was being given

Document name:	Inventories (2)	Page:	44 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



under national law, and what the relevant requirements would be. The use of affirmative declarations by mandate givers/mandate holders can be useful as a risk mitigation approach.

STORK 2.0 noted that the national frameworks on mandates are largely unaligned, and often contain specific exceptions (linked to the type of legal entity, the type of transaction conducted, corporate statutes, etc.). There isn't a shared European taxonomy about representation powers and mandates, what prevents powers/mandates information originated in one country from being directly machine processable in other. Representation is complex and the national solutions are often too much focused on country specific details.

For legal entities, the main challenge continues to be the integration of business registers as attribute providers in such a way that natural persons identified through STORK can be reliably linked to a legal entity. Then, for establishing whether legal entities are competent to represent that legal entity for the specific envisaged transaction, a functional and sufficient approach implies creating an ontology of mandates that are most commonly used (which STORK 2.0 did and where this is expected to be maintained through ISA² Programme (European Commission, 2016), in particular Core Person and Core Business vocabularies). STORK 2.0 approach then requires a matching of this ontology against the know relationship that the identified person has with a legal entity (i.e. 'does person x with function y in company z have the mandate in this ontology'), and requiring a confirmation on this point.

STORK 2.0 has thus produced a high-level ontology of likely and common mandates, covering both the scenarios of representation of legal entities and use cases in which one natural person would be authorized to represent another person. Powers are classified as General (or Prokura), Commercial, Human Resource, General services, Financial, Public interest representation and Health (more details on this ontology including description of these categories of mandates and examples can be found in the Consolidated Legal Entities Report, referenced above).

One of the primary outputs of the STORK project was the QAA (Quality Authentication Assurance) model (STORK, 2012), which permitted quality levels to be assigned to various eID solutions, based on some of their main characteristics. As a part of the expanded scope of STORK 2.0, a QAA Status report was drafted that expanded upon the original QAA, allowing it to be applied to attribute providers (to ensure that quality ratings can be assigned to attributes as well) and legal entities (to ensure their identification can be covered as well) (STORK 2.0, 2015). The report recommends to retain the QAA model when comparing it to the then emerging ISO/IEC FDIS 29115 standard given the unfinished status of this standard and it is not being "adjusted to the specific characteristics of many EU eID systems". Implementing Regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of eIDAS Regulation, explicitly references STORK:

Recital (4) notes that "*Therefore, the Large-Scale Pilot STORK, including specifications developed by it, and the definitions and concepts in ISO/IEC 29115 should be taken into the utmost account when establishing the specifications and procedures set out in this implementing act.*" (European Commission, 2014).

Document name:	Inventories (2)	Page:	45 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



And – despite containing only 3 levels of identity assurance versus the 4 levels within STORK – also it draws upon much of the elements that were also present within the QAA. It contains requirements in relation to enrolment (covering application and registration, identity proofing and verification and the binding between the electronic identification means of natural and legal persons), in relation to electronic identification means management (covering electronic identification means characteristics and design; issuance, delivery and activation; suspension, revocation and reactivation; renewal and replacement), and in relation to authentication mechanisms. The same Implementing Regulation acknowledges that while it has taken into account ISO/IEC 29115 for specifications and procedures it sets out, eIDAS differs from it “*in relation to identity proofing and verification requirements, as well as to the way in which the differences between Member State identity arrangements and the existing tools in the EU for the same purpose are taken into account.*”

A new Attribute Quality Authentication Assurance (AQAA) framework is proposed, covering the cross-border use of attributes and external attribute providers. A QAA policy for attribute assertions is provided, which builds upon the STORK1 QAA policy but amends it to address the specific characteristics of external attribute providers (which may be public or private sector entities). It is furthermore explained how this scheme could be applied to the representation of legal entities in a logically consistent manner. Criteria are based strongly on the existing QAA with small changes to account for the unique characteristics of Attribute Providers compared to Identity Providers.

Given that, in practical terms, the mandate can be considered as a collection of attributes in relation to the mandate giver (represented) and the mandate holder (representative), that is, if a person has the mandate to represent company X, then that mandate can be described as an attribute of its holder, the AQAA framework can thus be properly used to extend the notion of levels of assurance to the domain of delegation schemes, powers and representation. Thus, a single Attribute Quality Authentication Assurance AQAA scheme was created, which could be applied both to mandate providers (such as business registers) and to other attribute providers. In fact, eIDAS Regulation approaches electronic identification of legal persons as a variation of electronic identification of natural persons, which may rely on supporting information drawn from authoritative sources (such as business registers). To achieve broader support for attribute providers as well, longer term legal revisions can be expected (by expanding the scope of the eIDAS Regulation and the Implementing Regulation to more explicitly support attributes providers in general and to assess their quality, like the STORK 2.0 AQAA does).

The AQAA model addresses three crucial aspects:

1. Validating the link between a STORK eID and an attribute (including a mandate), which includes the possible interaction of the eID holder and the attribute/mandate provider in this validation process (the criterion of physical appearance does not occupy an equally crucial role for attribute providers as often –but not always- they can rely on externally established eIDs to register, and in some cases as well to later provide, attributes);

Document name:	Inventories (2)	Page:	46 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



2. The quality of the attribute or mandate (the factual accuracy at the time of registration, periodic verification/review schemes and availability of attribute verification mechanisms for relying parties) and
3. The quality of the attribute provider itself, i.e. to what extent can a service provider rely on its statements.

(See more details on legal and liability lessons learned for use of mandates in STORK 2.0 in section 5.3.3 of D5.3.5 eGov4Business Final Report, (STORK 2.0, 2016).

The main challenge explained in AQAA framework is the linking between eID and attribute information at the time of authentication. The AQAA criteria include validation of the link between the eID and the attribute (both at the time of registration and when authenticating), the validation of the quality of the attribute, and the quality of the attribute provider itself. For instance, it is possible (but unlikely in practice) that the Attribute Provider (AP) uses the STORK eID to retrieve attribute information (either because the user uses his eID to authenticate towards the AP, or because it uses a SAML assertion from an eIDAS Node to retrieve attribute information). In that case, use of STORK ID would allow attributes to be retrieved with perfect reliability. When not using STORK ID, fuzzy logic could be used (based on matching name, date of birth, nationality, etc.), but the quality of the attribute assertion would suffer significantly. Criteria to assess this negative impact are proposed in the AQAA. If the AP requires re-authentication using its own (non-STORK supported) credentials, STORK cannot provide any statement on the quality of the attribute assertion, because the quality of the AP's credentials is unknown. Impact of attribute aggregators would be another area for further refinement and update of AQAA model since their role and impact could only be assessed in a limited manner in STORK 2.0 pilots.

As stated in the AQAA Cookbook Addendum to the D3.2 QAA Status Report of STORK 2.0 (STORK 2.0, 2015), "the AQAA allows quality levels to be assigned to attribute assertions, comparable in intent and set-up to the original QAA. Thus, two types of quality statements can be made on the basis of STORK 1 and STORK 2.0 outputs:

- An assertion of quality of the eID under the QAA, ranging from level 1 to 4;
- An assertion of quality of specific attributes or attribute sets under the AQAA, ranging from level 1 to 4.

This also implies that certain choices must be made when identity information combines eID information and attribute information, whenever quality rated identity information is provided and combined into a single assertion with a single quality statement, the lowest quality level should be assigned to this assertion." The report recommends "to at least keep eID quality statements and attribute quality statements distinct, since the QAA and AQAA criteria are not directly comparable, and the AQAA is still largely untested in practice" (STORK 2.0, 2015). This Cookbook is meant to assist both Attribute Providers to determine what the quality of their attributes is and Service Providers to decide which quality level is appropriate for their service. The Cookbook has been used to help business registers to determine their AQAA level in six STORK 2.0 countries (Estonia, Greece, Iceland, Italy, The Netherlands and Slovakia), whereas it had been used by service providers in five countries (Estonia, Greece, Iceland, Italy and Slovakia) to decide which quality level is appropriate for their service.

Document name:	Inventories (2)	Page:	47 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



It provides illustrative example of use cases for delegation of authentication (so called in STORK 2.0 “Authentication on behalf of” procedure) where in a basic cross-border scenario, a natural person in Member State A who has a mandate from a different person to act on their behalf and where they use STORK to log on to an application in Member State B, whereby this representative sends the mandate information to the service provider, which includes information both on the mandate giver and themselves as mandate holders. Trust in the STORK/eIDAS network allows the service provider in MS B to be sure that these powers have been provided by an appropriate authority in MS A, with the consent of the end-user:

Because users may represent more than one company some flexibility was already built-in through a single sign-on feature, allowing the service provider to check the user’s powers to represent other companies, always with the consent of the user, without forcing the user to repeat the authentication process of providing a new password or PIN for each check.

This presupposes the availability of Attribute Providers (Business Register or other authority) furnishing the evidence of user’s powers of representation of specific companies (statutory powers of company representatives). In general terms the act of incorporation or the charter of the legal person states who has the power to act as agent and to represent and manage the company.

Thus, in STORK 2.0, an important new class of Attribute Provider was introduced, the Business Identity Provider or B-IDP. Being usually the national Business Register (but also Commerce and Mercantile Registers), the B-IDP handles and authenticates the eID of legal persons in the same way that the IDP is the authoritative source for personal eID information. The B-IDP is also often the source for mandate information, official information regarding the representation of one person (e.g., a company) by another (the authorised representative). In some countries a specific Mandate Authority exists to register delegation of powers of representation: such is the case of Austria, The Netherlands and Portugal, where separate agencies and services dealing with mandates and/or company roles provide such information (STORK 2.0, 2015). In many countries the electronic certification of powers of representation has not been defined by law or is defined in specific ways limited to certain forms of transaction and delivery. The main functional and data specifications for integrating the B-IDP were developed as part of the eGov4Business pilot specifications.

Thus, in STORK 2.0 mandates were included as SAML tokens that carry information about a person’s power to represent or act on behalf of another person, legal or natural. Their current status lies somewhere between fundamental eID information and specialized domain attributes. The cross-border legal status of the mandate is in some cases unclear which is due to the fact that the legal status of the original declaration in the country of origin may be uncertain and also because the SP itself may require certain guarantees beyond the STORK 2.0 SAML assertion. Moreover, while eIDAS covers natural persons acting on behalf of legal persons, this is limited to the link between the legal person and the natural person. The actual mandate is out of eIDAS scope, in particular STORK 2.0 semantically rich mandate content is not covered by eIDAS.

Document name:	Inventories (2)	Page:	48 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



While eIDAS sets out requirements concerning the minimum set of attributes for both natural and legal person, explicit information about the link between legal and natural person together with mandate content is not present. The legal basis and the security of the mandate information are fundamental aspects for the STORK 2.0 delegation approach to be widely adopted and used in practice.

Despite the practical validation of mandates in STORK 2.0, it is important to note that one of the findings was that “representing the type of power that the mandates describe is a difficult question which would require a complex ontology to describe and to harmonise. The many factors used to describe the powers of a person to represent a company create an enormous richness of expression involving functional limitations, temporal or economic constraints and even organisational conditions (in the case of joint powers). STORK 2.0 has developed a Powers Taxonomy and a mandate structure (STORK 2.0, 2015) that can capture a good degree of this richness, but in practical terms few countries are able to exploit the structure. Some of the attributes used in modelling the powers of representation include: TypeOfPowers (expressed in terms of a taxonomy based on business functions), timeRestriction (period of validity), transactionLimitRestriction (monetary constraint), isJoint and isChained. To provide a greater degree of legal value, the STORK 2.0 mandate assertion includes a general attribute, the originalMandate, which can be used to store a digital version of a full certificate or the full natural language text of the original mandate as produced by the national authority. Such information would necessarily require back-office processing, but was expressly requested by several MS as a necessary element in case of liability claims.

The typeOfPower attribute of the STORK 2.0 mandate token expresses, in a simplified, but agreed-upon form, a brief taxonomy of role-oriented company powers. Since there is no EU-wide legal basis for these values – no standard description or ontology exists - each national infrastructure had to create a suitable mapping from the national system of powers to the STORK 2.0 model.

We note that the implementation of the eIDAS Regulation does not make explicit use of a model of different representation powers: the juxtaposition of two persons is used to indicate that one person represents (with presumably full powers) the other. In fact, clause 2 of Art. 11 reads, “A minimum data set for a natural person representing a legal person shall contain the combination of the attributes ... for natural persons and legal persons when used in a cross-border context”. The fact that the implementation of mandates and the “authentication on behalf” operation itself exceed the eIDAS specifications creates a risk that these functions will not be completely supported by some national eIDAS nodes thus limiting the convergence between project results and the future CEF eID building block and risking to lose some degrees of cross-border interoperability that were achieved by STORK 2.0 MS. This risk is being addressed by the STORK 2.0 partners involved in e-SENS and CEF and ISA² initiatives.

The feasibility of the developed delegation approach was verified by means of the STORK 2.0 pilots, in which use cases that require cross-border access to information about representation capabilities have been successfully tested. Besides that STORK did add the concept of role

Document name:	Inventories (2)	Page:	49 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



based mandates. Within STORK 2.0, the eGov4Business pilot (STORK 2.0, 2016) was much more concerned with all aspects of mandate implementation than other pilots. This included the technical and semantic issues of data modelling and standardization of attribute values, the organisational aspects of integrating appropriate Attribute Providers (Business Registers) and the legal aspects of validity of cross-border mandates and trust schemes for AQAA and the legal basis and constraints for cross-border service provision. In order to have a basis for interoperability, that is for the automatic exchange and processing of “powers to represent”, the eGov4Business Pilot chose a strong simplification of the possible types of powers which will be recognised as the minimum set: full powers or no powers. In reality a third value indicating “other powers” is also used to indicate that a person may be the authorised representative but this cannot be fully determined automatically. Six SPs (from AT, EE, GR, IT, LT and SK) successfully implemented the new STORK 2.0 procedure for the “authentication of a person on behalf of” (AUB) a company (or other legal person) based on mandates, and this procedure was successfully tested across borders of 8 of the 13 MS participating in the Pilot (AT, EE, GR, IS, LT, IT, SI and SK). The eight MS involved in testing the AUB procedure all successfully integrated a business or trade register or, alternatively, a Mandate Provider capable of issuing a STORK Mandate token for qualified businesspersons.

With the STORK 2.0 approach to delegation, the AQAA-labelled Legal Person identity attributes and mandate attributes supplied by one government agency – the Business register or B-IDP – to another eGovernment service portal represents an official communication of information with a precise legal value. One of the strengths of the STORK 2.0 approach was the flexibility of verification of legal person or company credentials offered in the Authentication-on-behalf procedure. One aspect of flexibility is the possibility for the SP to request and receive the Attribute Quality Authentication Assurance level (AQAA) for attributes describing the company (Legal Person attributes) and the end-users powers to represent the company (mandate attributes). The SP can then evaluate whether the level of trust in the received information is sufficient to grant the user access to the SP application. Different Services or different operations may require different assurance levels so a goal was set to verify at least two different AQAA values in different AUB procedures, which was achieved.

While not implementing in practice solutions for all of them, STORK 2.0 acknowledged as well more advanced delegation topics such including complex chains of mandates (i.e. verifying the continued validity of powers of people different from the current end-user linked in a mandate chain and usually not online at the moment the verification is needed), the representation of joint powers and the legal and organisational instruments necessary to extend the STORK 2.0 authentication on behalf of legal persons process to broader eGovernment use cases, in particular extensions of Powers Validation use case when chains of mandates are involved and when the requested service involves back-office procedures when the end-user is no longer in session. The possibility for SPs to verify a mandate (or potentially other attributes) without the user being in session provides significantly more flexibility to the service providers and to end-users. E.g. an accountant of a company (who has a power of representation) would be able to continue to use an accounting service without requiring the manager of a company to log on to the service as well. However STORK 2.0 explored associated data protection risks for the

Document name:	Inventories (2)	Page:	50 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



implementation of such facility (in particular related to authorization to SPs to access relevant attribute sources in the future.

The Powers Validation use case presents itself when the service provider stores the STORK powers of representation credentials in a local user profile. The service provider does this to make it easier for the end-user to manage their own roles when accessing services on behalf of different companies. Before granting the end-user access to the requested service, the service provider may need to verify the current validity and accuracy of the previously registered powers with the original authority in MS A. In this case, there is no need to disturb the end-user for further information or consent.

An important opportunity for these advanced cases arises for LIGHTest, considering what is expressed in section 2.3 of STORK 2.0's Consolidated Legal Entities Report referenced above: "infrastructure needs to be engineered to be able to recognize which service providers are permitted to check mandates via STORK (eIDAS) without user involvement. STORK (or at least the attribute providers) must be able to recognize service providers that are granted this authority, and/or the definition of specific criteria on the basis of which such service providers are recognized by other Member States. To give a practical example: if a service provider is given this authority in Spain, then this provider must be on a Spanish trusted list, which must also be recognized by all other Member States, so that when the Spanish service provider approaches e.g. the Belgian business register to validate a mandate for a Belgian company, the Belgian register does not block or deny this request. This requires the political will to open up certain attribute information sources (such as business registers) to certain service providers in other Member States". Considering the on-going work in the context of CEF, ISA² and bodies like the eIDAS Expert Group (where the need for service providers of having powers/mandates information together with the data regarding the represented and representing persons, in order to properly assess the scope of the transactions that the representing person is allowed to perform on behalf of the represented one, has been steadily highlighted), allows to expect a strengthening of the support to delegation schemes based on approaches like STORK 2.0, with the support of the Member States, the EC and interested stakeholders, namely businesses with a need for everyday use of electronic powers of representation.

6.2 Industry Perspective

6.2.1 Austria: MOA/MOA-ID (Vollmachtenservice)

Most information provided here on national scheme for delegation (natural person representing another natural person or else a legal person) comes from the paper "Empowerment through Electronic Mandates – Best Practice Austria" (SpringerLink, 2009) by T. Rössler (T.U. Graz), which acknowledges that "the European Union undertakes tremendous efforts to enforce the support of e-services for businesses and service providers, e.g. through the EU Service Directive" and consequently the urgent need by business and service providers "for being able to express all the various kinds of representations by electronic means". Electronic mandates were introduced into the Austrian electronic identification schema in 2006 (Austria Government, 2016). They satisfy the need for bilateral authorization for certain actions typically involving

Document name:	Inventories (2)	Page:	51 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)

company/association representatives (EGIZ, 2012). Professional representation (by accountants, lawyers as official representatives) is also covered in Austria.

On a technical level, an electronic mandate in Austria is a specific XML structure which must be electronically signed by an issuing authority, e.g. the Source-PIN Register Authority. The issuing authority just asserts that the electronic representation bases on an existing and already established authorization. The concept of electronic mandates requires that electronic mandates are held by the proxies or representatives. Every time a representative makes use of a mandate, she has firstly to use her e-ID (i.e. Citizen Card) to prove her own identity. Additionally, she has to declare to the e-Government application that she is rightfully acting in the name of the mandator by presenting the electronic mandate with the following structure:

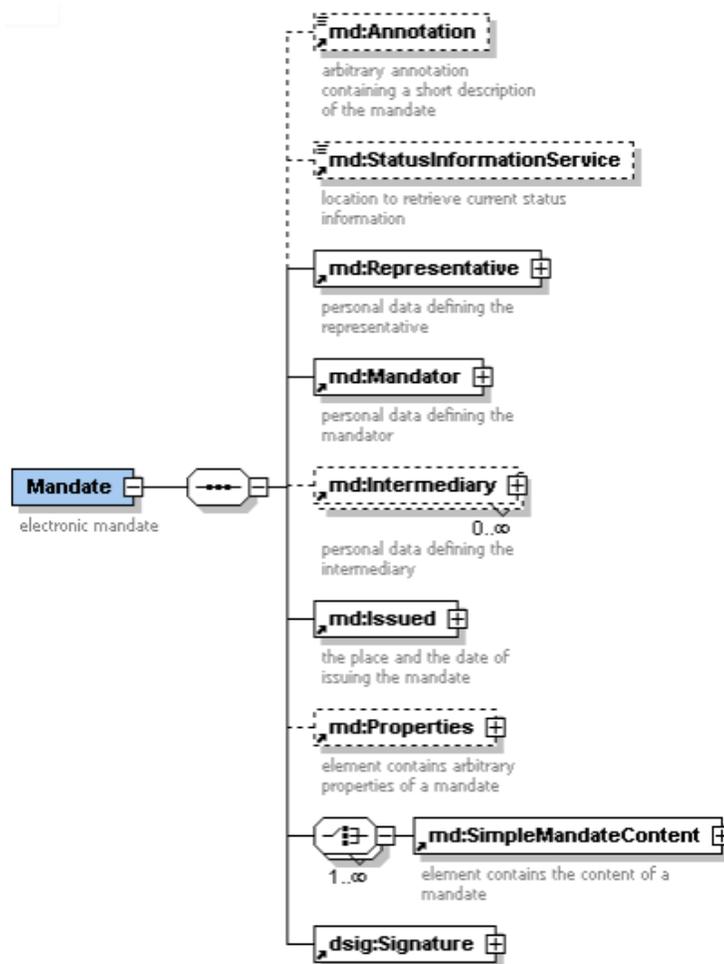


Figure 7: Basic layout of electronic mandates (XML schema) in Austria

(The figure above has been extracted from (Rössler & Hollos, 2006).)

Document name:	Inventories (2)	Page:	52 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Stakeholders for delegation representation (see paper above for more types of representation):

- The mandatory (Machtgeber or Vertretene) is the person on whose behalf an action is performed. The mandator is in original possession of the rights and roles respectively.
- The representative (Machthaber or Vertreter / Bevollmächtigte) is the person acting on behalf of the mandator. The rights or roles have been transferred to the representative via mandate. The transfer of this rights (roles) does not change them for the mandator.
- The intermediary (Intermediär or Mittler) is the person acting as a broker between the mandator and the representative within the process of transferring rights between these two parties. Due to Austrian law, every electronic mandate has to be signed by the issuing Source PIN Register Authority. This also applies to bilateral mandates.

Electronic mandates are tokens asserting that the representative is empowered to act in the name of another entity and can prove it in front of any application. Applications can then verify this information, easing the management of authorizations. Similar to conventional mandates, an electronic mandate should hold:

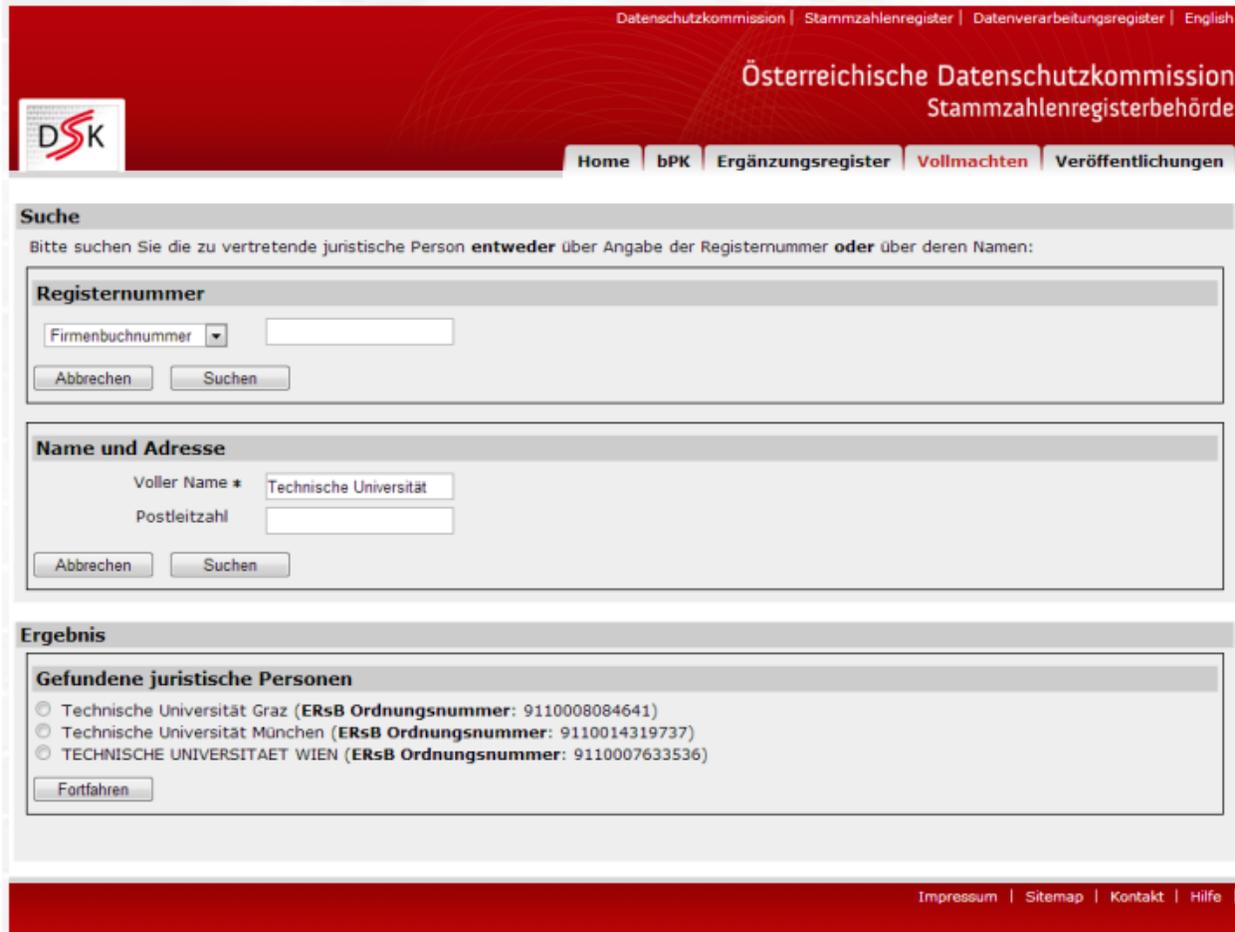
- identity of the mandator
- identity of the proxy
- date and place of issuing
- content and concern of the mandate (scope of empowerment)
- optional restrictions (in time, in amount for financial transactions, etc.)
- Electronic signature by mandator or issuing authority

Electronic mandates are issued and signed by the Source PIN Register Authority only. Therefore, this authority provides a web-application with which citizens can apply for electronic mandates based on an existing authorization (empowerment). This means, that the empowerment must be already established, e.g. based on paper mandates or entries in official registers (e.g. the register of commerce). In order to foster the take up of electronic mandates in the field of e-Government applications, the Austrian e-Government initiative provides open-source software modules for providers and developers of e-Government services, which automatically verify electronic mandates—including chain verification—and provide e-Government applications (for instance, electronic delivery which was one of the first applications in Austria which accepted electronic mandates) the unique electronic identity of the mandator and the proxy. Mandates are especially important for the Austrian electronic delivery service since legal entities are only able to register for electronic delivery with the use of electronic mandates (this means that a private person has to act in the name of a legal entity).

Since 2010 (EGIZ, 2014, pp. 30-73), the electronic mandate system has evolved to a central, user-friendly, on-line mandates model, with access to fresh information from constitutive registers (Business Registers for legal mandates, Business Service Portal for delegated mandates and Register of bilateral mandates between natural persons) and with Just-In-Time mandate generation with a Mandate Issuing Service (MIS). Production system is operational at (Austria Government, 2016). A test environment exists at (EGIZ, 2016).

Document name:	Inventories (2)	Page:	53 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final





Datenschutzkommission | Stammzahlenregister | Datenverarbeitungsregister | English

Österreichische Datenschutzkommission
Stammzahlenregisterbehörde

Home | bPK | Ergänzungsregister | Vollmachten | Veröffentlichungen

Suche

Bitte suchen Sie die zu vertretende juristische Person **entweder** über Angabe der Registernummer **oder** über deren Namen:

Registernummer

Firmenbuchnummer

Abbrechen Suchen

Name und Adresse

Voller Name *

Postleitzahl

Abbrechen Suchen

Ergebnis

Gefundene juristische Personen

- Technische Universität Graz (ERsB Ordnungsnummer: 9110008084641)
- Technische Universität München (ERsB Ordnungsnummer: 9110014319737)
- TECHNISCHE UNIVERSITAET WIEN (ERsB Ordnungsnummer: 9110007633536)

Fortfahren

Impressum | Sitemap | Kontakt | Hilfe

Figure 8: Legal Person Representation at Austrian Online infrastructure for delegation

(The above figure has been extracted from (EGIZ, 2014, p. 80).)

For authentication based on mandates (Authentication on behalf of, also piloted in STORK), the process flow is:

1. Mandator selects „in Vertretung anmelden“ and selects the Citizen Card or the mobile phone signature
2. The next step is a standard citizen card login which includes Displaying the data to be signed (DTBS).
3. MOA-ID contacts the MIS and forwards Identity Link, Signature certificate, RedirectURL (User to be redirected after selection), Reference value (revision/audit), Allowed mandates
4. The MIS returns a session-ID that is used by MOA-ID for fetching the selected mandate.
5. The MIS starts a search for active mandates within the source registers based on the data received from MOA-ID (using as identifier for the search ssPIN of the representative).

Document name:	Inventories (2)	Page:	54 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



6. For natural persons bilateral mandate register is consulted and for legal persons/legal mandates the Business register (containing companies register, central register of associations, supplementary register for others concerned) is consulted. In case of delegated mandates for legal persons, Business service portal is used.

7. Representative is forwarded to a MIS GUI where they can select mandate: MIS will create and sign the electronic mandate.

8. MOA-ID fetches the signed mandate (session-ID of step 4 has to be included in request)

9. MOA-ID forwards the SAML Assertion to the application (besides the identity data of the mandator, assertion contains identity data of representative).

In Austria, so called professional representatives (Organwalter), e.g. lawyers, tax advisors, etc., are not required to provide an explicit mandate if they want to act in the name of their clients (Berufsmäßige Parteiververtretung). For them it is sufficient to prove that they are professional representatives. Their Citizen Cards (or to be more precise their qualified certificates), hold a special object identifier (OID, according to ISO/IEC 9834-1, the Austrian Federal Chancellery has reserved an OID-sub tree that defines these OIDs on an international level) (Digital-Austria, 2009) identifying them being a professional representative. As a result, professional representatives are not required to present explicit electronic mandates; instead e-Government applications just verify whether the digital certificate of the representative contains the OID defined for Austrian professional representatives.

Finally, an important aspect addressed in the model is the revocation (service) of electronic mandates, allowing the functionality of providing current revocation status corresponding to a given unique serial number (electronic mandates needs to be registered with this service), within the process of verifying an electronic mandate. Indeed, in Austria, the Source PIN Register Authority runs a mandate revocation service accessible via an HTTP-protocol and currently all existing electronic mandates in Austria are registered with this registration service per default.

6.2.2 Katso service

Implementing the characteristic processes/components of identity management, authentication and authorization within the “online-services-relationship” between government organizations and organizations, and between government organizations and citizens, the National Board of Taxes and the social Insurance of Finland, created the Katso system platform.

Technically Katso works with high international standards by using Oasis SAML 2.0. to guarantee the highest level of authentication, which is necessary for the online services interactions.

The Katso system, does work as “one of the largest successful deployments of outsourced delegated identity management, authentication and attribute distribution solutions in the world.” It says that “all of the Finnish companies in practice need to have a Katso ID” (Nowadays 95% monthly user rates). (Ihalainen, 2007)

Document name:	Inventories (2)	Page:	55 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



The following explanation refers on a Case Study done by the Liberty Alliance (Liberty Alliance Project, 2016) and the VeroSkatt Homepage (Skatt, 2017)

The Identity and Delegation model in Katso

Katso identities are divided into three categories, where the Master user can create lower level identities and authorize them to act on behalf of the organization where the Master user belongs. Authorization can be given to other companies as well. This feature essentially outsources the identity management to an organization that needs to use a service which is protected by Katso.

The organization that delivers services integrated with Katso can create roles that are tied to the service in question and these roles can be assigned to Katso identities by the master users in the organizations utilizing Katso.

Katso utilizes standards such as SAML for Web based authentication enabling organizations to implement Katso authentication across the application landscape. Katso delivers basic attributes about the user to the applications upon authentication. These attributes can be configured so that almost anything available through the Katso system can be delivered upon authentication. This makes it easy to implement application level authorization functions. (Liberty Alliance Project, 2016) (Skatt, 2017)

Authentication

E-government services require a certain level of trust and some of the services require strong authentication of users. There were several proprietary authentication methods available for government on-line services and one of the Katso requirements was to get rid of the old authentication options and harmonize the authentication infrastructure for organizations.

Through the IDP, other authentication methods can be used, so that in the future new authentication methods can be deployed to the services within seconds.

The new Finnish Trust Network, which is based on EIDAS (see section about that), will link KATSO with EIDAS. (Liberty Alliance Project, 2016) (Skatt, 2017)

Authorization

Katso is not just about authentication and identity management. One of the strongest parts in Katso is the ability to authorize other organizations or individuals, that is, to perform delegation or issue mandates to other organizations or individuals. The Board of Taxes and Social Insurance Institute needed a system, where organizations themselves can authorize other organizations to act on behalf of them and maintain these authorizations themselves, thus reducing the workload the government institutes even further. Hence the Katso concept has a cross-organization delegation of authorizations and mandates. The requirement was that authorization should be flexible, and at the same time maintain security aspects, i.e. privacy. (Liberty Alliance Project, 2016) (Skatt, 2017)

Document name:	Inventories (2)	Page:	56 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Identity Management

The Katso system now covers more than 320 000 organizations nationwide, which is approx. 97% coverage of the organizations (mostly companies, but also some registered associations) in the national business registry. The amount of users is close to a million, and this kind of user and business-identities base cannot be maintained by the government organizations. Hence also the life cycle management of users has been delegated to the organizations themselves, by the delegation means of the system.

Katso was from the start developed as a delegated solution, where the both the service infrastructure and the identity life cycle management processes are both outsourced and delegated. Management of the identities, roles and the attributes in Katso is delegated to and maintained by the registered organizations themselves, that is, not by the government officials. (Skatt, 2017)

Role based identity as base for delegation of authorizations

Government organizations have a large numbers of online services available for the population and for businesses. A single service can offer several different levels of doing business with the government. The confidentiality level varies between the services and functionalities within a service. Therefore it was required that the authorization of Katso users was based on roles, with respect to service content and levels. A given role defines your ability conduct your online businesses in the government services Possession of a role may give you authorization to delegate that role further to other organizations or other individuals. (Skatt, 2017)

Katso design and specification refinement

One of the most complex refinements in Katso was to determine the relationships where different authorizations and delegations could take place. A fundamental requirement for Katso was the ability to authorize other entities in the Katso system that is to delegate a role or an attribute to another entity. This authorization created a web of different relationships between users, private sector organizations and government organizations. (Skatt, 2017)

Transferring the admin account to a new person

In a corporate world nothing is constant. People leave their organizations for other companies or they take on new challenges within the same organization. For this reason, the admin account privileges must be transferred to a new person when the current account holder is leaving. For those cases the same delegated mechanism in Katso are used as described above. (Skatt, 2017)

Creating Katso sub-accounts

Once there's a company and an administration account in the Katso system, it becomes possible to create Katso sub accounts within the organization. Only a few roles are available for

Document name:	Inventories (2)	Page:	57 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



these accounts and they are intended for authentication of a representative of an organization, not individuals. The Katso sub-account concept is a quick way to delegate day-to-day tasks to the personnel of the company. All transactions that are done as a Katso sub account represent corporate transactions, as the Katso sub-account does not authenticate individuals, but organizations. (Skatt, 2017)

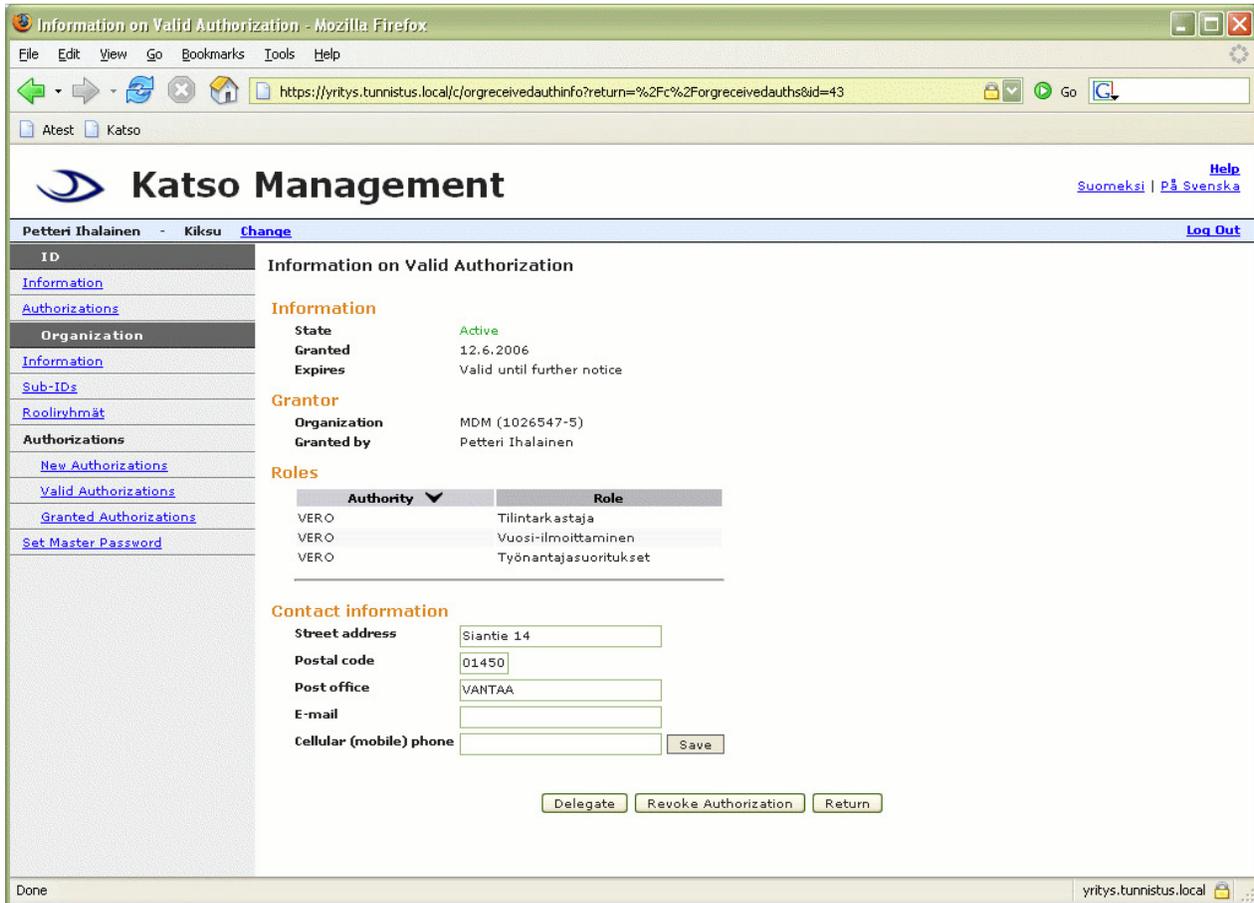


Figure 9 Katso Management

Authorizing organizations in Katso

Small and medium size companies don't have the resources to handle tax issues by themselves, so they delegate accountant firms to help them sort out the taxation issues.

In Katso a company can authorize (delegate) other companies to act on their behalf in certain tasks. In e.g. taxation corporations can authorize an accountant company to do their taxes. The Katso admin creates an authorization in the Katso system and assigns the required roles to the authorization.

This authorization (delegation of duties) is assigned to a specific entity in the Katso system, i.e. another company within the system (accountant firm). Once the assignment is done and the

Document name:	Inventories (2)	Page:	58 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



correct roles are tied to the authorization, it is forwarded to the receiving company, namely to the Katso admin of the receiving party.

The authorization can be revoked at any time. It can also have a certain starting date and expiry date associated with it. This way companies can create temporary authorizations within the system.

The receiving party Katso admin can either accept or reject the authorization. If the receiving company decides to accept the authorization, it must be delegated to a Katso account or a Katso sub account so that the actual authorization becomes usable. (Skatt, 2017)

Authorizing Katso accounts

Authorizations are useless in the Katso system unless they are assigned to a Katso ID or a Katso sub ID. Katso admins can delegate and authorize (grant roles) to Katso IDs within their organization or to a Katso ID located in another organization. The process of authorizing Katso IDs in another organization is similar to the organizational level authorization, but the delegation has been done already as the authorizing party is assigning the authorization to a specific Katso ID.

Authorizations within the organization can be either internal or assignments of received authorizations from another organization. In either case the Katso admin is responsible for delegating the received authorization, or creating a new authorization that is assigned to a Katso ID within the organization. (Skatt, 2017)

Authorizing Katso sub-accounts (sub-IDs)

The process of authorizing Katso sub-IDs is identical to the Katso ID authorization. The most notable exception is that not all roles can be assigned to a Katso sub-ID. Some of the roles require personal authentication, and therefore can't be delegated to Katso sub-IDs which only authenticate a representative of an organization. (Skatt, 2017)

Public authority authorization for Katso organizations or Katso accounts

The most typical authorization use cases are described above. But sometimes there is a need to create authorizations by the public authorities. These are special cases, but quite common in the government. A good example could be a situation, where the receiving party is a Katso entity, a company or a Katso ID, and where the actual authorization is delegated to be done by the public authorities on behalf of someone else. This could happen if someone is declared incapable, corporation goes to bankruptcy, or a company is assigned to care of the assets of an estate of a deceased person.

Public authority authorization characteristic is that there is no authorization party, but the authorization is created by a third party. For the receiving Katso admin this authorization is just like any other received authorization. But most of the times public authorities will assign these type of authorization to Katso IDs directly. (Skatt, 2017)

Document name:	Inventories (2)	Page:	59 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Accessing e-government services using Katso

There's a clear need to offer more government online services to organizations and citizens as the cost savings are undeniable. There are however many types of services available and the confidentiality requirements vary. Even in a single service there are functions that can't be available to every authenticated entity.

The Katso system provides a common platform for delegation of roles that specify which resources are available. But the first step accessing the government online services is authentication with the right LoA, accordingly. (Skatt, 2017)

6.2.3 Energy sector trust delegation use case - Helen

Helen Ltd (formerly Helsinki Energy) is a leading energy sector company in Southern Finland, serving both residential and business customers in the Helsinki metropolitan area. (Helen Ltd. , 2016). As Helen has a comprehensive online service, which encompasses the following advanced features related to trust and delegation based on trust experience of:

- Strong authentication of both residential and business customers
- Delegated user management for business customers
- Mandate-based credential management for both residential and business customers
- Federated identities: B2B customers can login using existing consumer credentials and see their own usage in addition to company usage from the same session. A user may have several business accounts and/or domestic accounts

Strong authentication

Knowing the parties involved is the first step in the signing up for an energy contract. Helen is platform agnostic and accepts user and organization authentications based on the criteria defined for strong authentication in the law. The trust rests ultimately on strong authentication of the individual and also on the social order, that is, that a person or corporation violating the law e.g. if signing an energy distribution contract without having authorization to do so, can be successfully challenged in a court of law (Helen Ltd. , 2016).

Delegated user management

In B2B use cases concerning energy contracts for business customers, there used to be typical obstacles for Helen in their online-services of knowing which persons working for a particular Company should or should not have access to its service. Therefore a solution for delegation of user management to the respective organisations has been implemented. While Helen still doesn't know about the internal workings of the Company in question, the authorized and authenticated contact person does. Therefore, Helen first gives a limited administrator role to the contact person of the Company whose name is on the signed contract – and based on the trust

Document name:	Inventories (2)	Page:	60 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



formed by the signed contract, initially delegates the Company's user management with respect to the Helen e-services to the person who signed the contract with them.

That person may then either continue manage their internal Company users himself/herself, or alternatively further delegate that responsibility to one or more other persons that she trusts. Those other person's may be other employees of the Company, or external 3rd party users to who then get a mandate to act according to that delegation, on behalf of the company towards Helen services.

This concept of delegation also breaks down the scalability problem into multiple chunks, each of which can be further sub-divided until the individual chunks are e.g. small enough to be handled by a single person.

Mandate-based credential management

A common situation in a commercial e-service is that access management is strictly user-based: the only way to share access is to physically give my credentials to another person, granting him or her full power to act in my name.

Mandates provide a way to provide controlled access to persons or groups of my choosing, enabling varying levels of trust to translate into varying rights to act in my name – or in the name of the organization I'm myself authorized to act for.

This differs from delegated user management in the way that each individual person or organisation still have their private access credentials to the service, they simply are now additionally authorized to commit acts in another person's or organization's name. With Helen these mandates range from the right to see detailed energy consumption statistics to even making new legally binding contracts concerning energy-related services with Helen.

Often combined with delegated user management, the trust chains can grow very long and wide. The key enabler is that each individual link in the chain is only responsible for the adjacent links.

Document name:	Inventories (2)	Page:	61 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



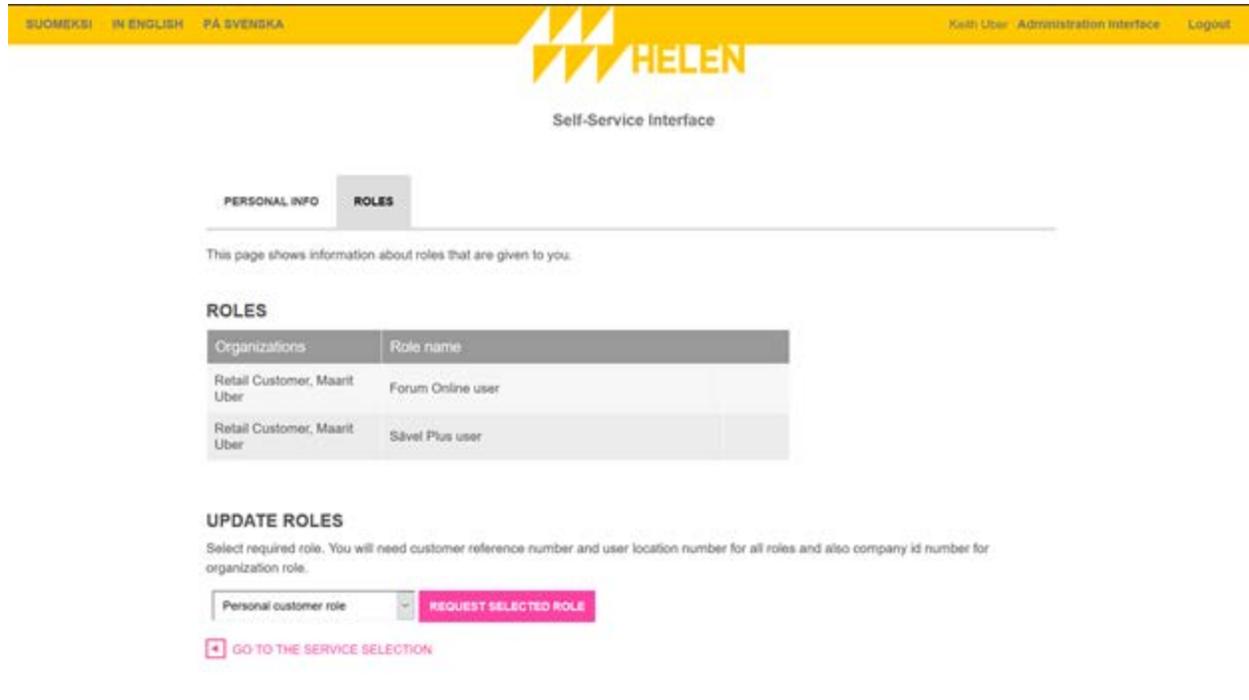


Figure 10 Helen Self-Service Interface

Identity profiles based on Roles and delegated Roles

A common issue in the corporate world is that business identities and trust chains do not follow a person out of the office.

For example, one individual person, a Helen private sector customer, call her Maarit, could towards Helen also at the same time represent and administering energy contracts for the company she works for, in addition to having her personal account for her own domestic use.

Federated identities merge different trust domains together. On an individual user level, this may also mean that the individual's different roles and the trust related to those may merge in one session of that individual user. When Maarit logs in with her personal credentials, she can now manage both her domestic and her company's contracts without having to log out and then in again using her workplace credentials. This trust relationship doesn't have to be, and often isn't, two-way. Logging in using her workplace credentials, she would only see and manage work-related contracts and services. But if logged in, strongly authenticated as the individual, and thereby identified as Maarit, she may then act using both or several of her profiles. Some profiles could be available based on her verified personal identity, others based on trust and authorizations that have been specifically delegated to her through mandates. For instance, she could be managing her own contractual issues; or those of her employer; or further those of yet another, e.g. if being an authorized representative of an association which also has an energy contract with Helen.

Document name:	Inventories (2)	Page:	62 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Elaborating this further, if Maarit then delegates and authorizes her husband, Keith, to act on behalf of her towards Helen in certain contractual issues, then he would still not through that one delegation get any of the other mandates and delegated authorizations that Maarit herself possesses based on e.g. her profession and employment.

Document name:	Inventories (2)	Page:	63 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



7. Relevant Trust Policies and Policy Languages

In section seven, there is a deeper insight to relevant trust policies and policy languages in both an academic and industry perspective. Within the Academic perspective, the definitions that LIGHTest follows are stated along with some reference suggestions of summaries of existing policy languages. Further, the academic section provides a summary and discussion of what would be needed in the terms of LIGHTest with regards to what trust policy language style would be the most relevant. Furthermore, a more complete version of the Trust Policy Language that is used within LIGHTest can be found in D2.14, the Reference Architecture.

7.1 Academic Perspective

A wide range of trust policy languages exists that have been proposed for a wide range of applications and contexts. Some of these are, for example, reviewed by De Coi et al.. For efficiency, the following discussion starts with a discussion of the needs of LIGHTest in order to be more focused on relevant languages only. This describes the elements of a trust policy that need to be expressible in a trust policy language. The inventory is then focused on relevant language elements only. (De Coi, 2008) provides a review on trust management, security and policy languages that could be a helpful source for LIGHTest. Further, this paper provides a collection of different policy languages, criteria to consider for each policy language, core policy properties, contextual properties, and a comparison.

7.1.1 Aspects useful for a LIGHTest Trust Policy Language

While considering important aspects to establishing a LIGHTest trust policy language, it is first necessary to define some of the concepts used by LIGHTest that specify the functionality and features required by a policy language. On this basis, the necessary language elements can be identified.

7.1.1.1 Definitions

The following definitions of concepts originate from an early version of the LIGHTest Glossary that will eventually be part of Deliverable 2.14. Only the definitions relevant for trust policy and policy languages are listed below:

Trust Policy

A Trust Policy is a recipe, expressed in a Trust Policy Language, that takes an Electronic Transaction and potentially multiple Trust Schemes, Trust Translation Schemes and Delegation Schemes as input and creates a single Boolean value (trusted [y/n]) and optionally an explanation (e.g., why not trusted) as output. In LIGHTest, a trust policy is evaluated by the Automatic Trust Verifier component.

Electronic Transaction

Document name:	Inventories (2)	Page:	64 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



An Electronic Transaction is the object in LIGHTest whose trustworthiness is evaluated by a verifier. The simplest possible electronic transaction is a single document that is cryptographically associated with an electronic identity, e.g., through the mechanism of electronic signature.

In the more general case, an electronic transaction is a container (of a given format) that contains several documents or sub-containers. Optionally, documents and containers are associated with an electronic identity, e.g., via electronic signature.

Both, documents and associated electronic identities contain specific data elements that are referred to in the trust policy. For example, a purchase order may have a “purchaser” and a “total amount”; an electronic identity may be associated with an “issuer”.

Trust Policy Language

A Trust Policy Language is a formal language with well-defined semantics that is typically based on a mathematical formalism and is used to express the recipe of a trust policy.

7.1.2 Trust Policy Language relevant to LIGHTest

In the LIGHTest context, a trust policy language needs to provide the following language aspects:

- A mechanism to uniquely identify trust schemes, trust translation schemes, and delegation schemes on a global scale.
- A mechanism to refer to the data that a trust scheme expresses about a given entity.
- A mechanism to refer to translated trust schemes according to a given trust translation scheme.
- A mechanism to express that delegation is allowed and how many delegation steps are admissible.
- A mechanism to address the various parts within an electronic transaction (to express constraints on these parts)
- Mechanisms to refer to specific data values within a given part contained in an electronic transaction.
- Mechanisms to reduce a structured set of the above values to a single Boolean value (trusted [y/n]).

Inventories for these specific language elements are provided in the following.

The current suggestion within the LIGHTest consortium is to achieve this is a simple but powerful language in the style of Prolog/Horn clauses. Our arguments for this are:

- It is trivial to formalize all simple policies that are based on a kind of enumeration
- It offers us an easy mechanism to describe relations between concepts, e.g. what criteria need to be satisfied to fulfill a certain standard, logical combinations of policies (and/or/not)

Document name:	Inventories (2)	Page:	65 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- It is ideal for concepts like delegation and black-listing (for this reason for instance the access control policy languages like SECPAL and DKAL by Microsoft are based similarly on Horn clauses)
- The language comes directly with a clear formal meaning including an evaluation procedure, i.e., our specifications are directly "executable".
- We can be sure that the language is powerful enough because it is Turing complete (every computable policy can be expressed)
- The evaluation can be made to directly trigger necessary queries to servers, e.g., using DNS (with DNSSEC validation), and process their answer; thus the bulk of the ATV can directly be encoded into the language, either as a prototype/testing reference or even as the final product.
- For the average users we can either provide design patterns for their policy or even interface to a simpler (possibly graphical) language that they can use more intuitively but that is limited in expressive power. In this way one may be able to use LIGHTest without any learning curve in 99% of all cases, but when one wants to express something really non-standard (the remaining 1% of cases), the language still allows that.

We illustrate the flavour of the language and what specifications could look like with a few examples. The language is based on Horn clauses that have the form

conclusion : –requirements

This loosely corresponds to a sentence of the form: “if the requirements on the right are all satisfied, I get the left-hand side conclusion as a result”. Consider as a specific example the sentence “I trust X if I trust someone that delegates to X”. This could be expressed as a Horn clause in the following way.

trust(X) : –trust(Y), delegate(Y, X).

In the above, : – should be read as “if” in the sense of a sufficient (but not necessary) condition, i.e., if the requirements on the right-hand side are not met, there may still be another clause to derive that I trust X. The comma between the requirements should be read as “and”. The clause should thus be read as “I trust X if I trust Y, and Y delegates to X”. Here the terms *trust* and *delegate* are not built-in parts of the (base) language, and the clause says nothing of their meaning in isolation, i.e. nothing is said of what it means to trust or delegate to something. However, we may consider having a library of the most important terms and concepts (so users do not have to start from scratch when specifying their own policy) and they may have also a distinguished meaning for our ATV.

The language would then consist of a set of such clauses, each having exactly one term (the *head* of the clause) before the : – (the “if”), and zero or more terms separated by commas (the *body* of the clause) after the : –. Expressing trust by a bounded number of delegations in this language could be done using the following two clauses.

trust(X, N) : – trust(X).

Document name:	Inventories (2)	Page:	66 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



$$\text{trust}(X, N): - N > 0, \text{delegate}(Y, X), \text{trust}(Y, N - 1).$$

The first clause should express that I trust X through at most N steps of delegation if I trust X directly (without considering delegation). The second clause says that I trust X through at most N steps of delegation if N is greater than zero, Y delegates to X, and I trust Y through N-1 steps of delegation.

One big advantage of using this language is that it happens to be valid Prolog code. It is then possible to use a Prolog environment to evaluate the policy against a prototype, which, conveniently, can also be specified as Prolog code. The following is a prototype meant to express that I trust *a*, *b*, and *c* (this could represent that I trust these because they are listed in some trust list), and that *c* delegates to *d*, which delegates to *e*.

$$\text{trust}(a).$$
$$\text{trust}(b).$$
$$\text{trust}(c).$$
$$\text{delegate}(c, d).$$
$$\text{delegate}(d, e).$$

With the two clauses with $\text{trust}(X, N)$ in the head loaded into a Prolog environment together with the above prototype, the query $\text{trust}(e, 2)$. will return true, and $\text{trust}(e, 1)$. will return false.

7.1.2.1 Inventories of Language Elements

Globally Unique Identification of Schemes

The LIGHTest trust policy language requires a mechanism to uniquely identify trust schemes, trust translation schemes, and delegation schemes on a global scale. Syntactically, this can be achieved trivially by a string that is very similar to a variable name in programming languages. More interesting is an inventory of the approaches that are possibly used in achieving a globally unique naming system that avoids conflict where the same name is used for different entities.

The Addressing in the ITU Standard X.400 (Union, 1999) created a hierarchical name space starting with “country” and “organization” and then further subdividing with “organizational units” down to leave nodes that represent actual entities. While this approach theoretically produced globally unique addressing, in practice the absence of collisions and conflicting naming could not be guaranteed due to the absence of a global registry system and the lack of control over who used which name. This shortcoming of X.400 addressing can for example be removed by using Internet domain names, URIs, or e-mail addresses in X.400 address elements (Cooper, 2008).

Really globally unique naming has only been achieved by the use of a globally operating registry service that guarantees the uniqueness of names. Possibly the best-known registry service—that also has by far the greatest practical relevance—is part of the Internet Domain Name

Document name:	Inventories (2)	Page:	67 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



System (DNS) (Mockapetris, 1987) (Mockapetris, 1983) under supervision of the Internet Corporation for Assigned Names and Numbers (ICANN).

The top-level domains, together with their subdivision into domain names of organizations, define a hierarchical name space that can be further subdivided to create globally unique names. E-Mail addresses that base on organization's domain names are a prime example (Postel, 1982), as are the World Wide Web's Uniform Resource Identifiers or URIs (Masinter, 2005). URIs even attempt to be a generic and extensible way for uniquely identifying any kind of resource, including, for example, e-Mail addresses.

From the point of view of LIGHTest, domain-name-based URIs are the approach to unique addressing of the most relevance. Since LIGHTest bases its infrastructure on the domain name system, Fully Qualified Domain Names (Mockapetris, 1983) are the most useful language element to uniquely identify schemes of various kinds.

Trust Scheme Data of an Entity

The LIGHTest trust policy language requires a mechanism to refer to the data that a trust scheme expresses about a given entity. This requirement is very specific to LIGHTest and is unlikely to be found in other trust policy languages. That said, it can be handled by a very simple syntactic construct. For example, for Boolean trust schemes, a Boolean valued function "inTrustScheme(<trust scheme id>, <entity id>)" would be sufficient. For an ordinal valued trust scheme, a function such as "LoA(<trust scheme id>, <entity id>)" would work. For a trust scheme that asserts generic tuples of attributes for each entity, a construct such as "getAttribute(<trust scheme id>, <attribute id>, <entity id>)" would work. Since these constructs are so simple, they are not further reviewed.

Translation of Trust Schemes

LIGHTest requires a mechanism to refer to translated trust schemes according to a given trust translation scheme. Similarly to above, this is highly specific to LIGHTest and it is very unlikely to find an existing language mechanism that fits. Again, this required language element can be satisfied with simple constructs. For example, a "native" trust scheme could be constructed by a function such as "translate(<foreign trust scheme id>, <translation scheme id>)"

Support for Delegation

LIGHTest requires a mechanism to express that delegation is allowed and how many delegation steps are admissible. Consider for example a purchase order that needs to be signed by the company that issues it. If the purchase order is signed by an electronic seal of the company, the policy language must state that the entity that signed the purchase order must be the same as the entity issuing the purchase order. This could be done with a language construct similar to the following: identical(getAttribute(<part id of purchase order>, "issuer"), associatedEntity(<part id of purchase order>, "subject.DN.CN")). Here, the association mechanism is assumed to be electronic signature and the "subject.DN.CN" is part of the certificate used for the signature. The "identical" function verifies that the two values it takes as arguments are indeed equivalent.

Document name:	Inventories (2)	Page:	68 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



The above case without delegation renders it easier to understand the case with delegation. What is different is that identity does not compare two entities but allows chains of entities that are based on delegation. The language mechanism must be able to specify which delegation publishers are trusted to verify the chain of delegation present in a given electronic transaction. While in most cases, a single step of delegation will be present, it may be chosen to support longer delegation chains. In that case, the language would also have to express the maximal possible length of the chain.

For an inventory of the possible mechanisms, we refer to section 6 on delegation schemes.

7.2 Industry Perspective

This section will give a brief insight to how the Spanish Government and Public Administration has utilized different e-services and trust policies. During the last years, the Spanish Government and the Public Administration developed advanced trust policy as a driving force to reinforce citizen relations with the administration (national, autonomous regions and municipalities)

Reasons to develop these services are that citizens have developed new behaviors patterns and expectations in their use of e-services, the way they relate to business and their interaction with public administrations, looking for efficiencies and improvements in services.

In this new context, the Administration have been capable to adapt to new demands in a changing environment without prejudice to security assurance, offering e-services and information through wide range channels (web, apps...) and making them available anywhere at any time, developing new ways of interacting with citizens, contributing to create opportunities and doing business in a productive way.

One important milestone into the administration transformation is the publication of the 11/2207 on Citizen's Electronic Access to Public Services Law. This law gave impulse to the modernization of the Spanish Administration, guaranteeing citizens' right to interact with the Administration through digital channels. Introduced, on the main time, the corresponding obligation for the Administration to make electronic means available for the various stages of those administration procedures that involve interaction with citizens.

Recently (last October), one important legal change has been the provisions of the Bills of Law on Common Administrative Procedures in the Public Administration and on the Legal Regime of the Public Sector (Respectively, Law 39/2015, of October 1, the Common Administrative Procedure Public Administration and Law 40/2015, of 1 October, the Legal Regime of the Public Sector were taken into account.

This new legislation to reform the functioning of the government implements a fully electronic, interconnected, and transparent and with a clear and simple structure Administration.

This reform is based on two complementary areas: the external relations of the administration with citizens and businesses through the Law on the Common Administrative Procedure of

Document name:	Inventories (2)	Page:	69 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Public Administration; and the organization and internal relations within each administration and between different administrations through the Law on the Legal Regime of the Public Sector is concerned.

For reference, one can find the legal framework related to electronic administration and the trust policies needed to provide the public services from this source (Digital, 2016).

Some public services have been developed during last years in order to help citizens do things in other European countries in regard to moving, living, studying, working, shopping or travelling abroad. Groups of services for citizens are in travel, work and retirement, vehicles, residence formalities, education and youth, health, family, consumers, taxes, benefits, pensions, etc.

Private industry uses in this context are different than citizens. Each company has developed internal trust policies to provide their eServices to clients and to secure IT infrastructure in order to avoid cyber-attacks. In Spain, some companies have been involved in the development of eDNI in their online services (Mapfre, 2016). Further information on how the postal sector industry has deployed various eServices in the UPU member countries can be found in this report (Corredera, 2015)

Document name:	Inventories (2)	Page:	70 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



8. Existing Trust Translation Schemes

This section elaborates on the Trust Translation Schemes that are existing in both an academic and industry perspective. For the academic perspective, it elaborates on a general interpretations of trust translation schemes and their purpose. Further, it points out that there is a gap in research regarding trust translation schemes but points out related aspects that would be beneficial for trust translation schemes. The industry perspective gives a deeper insight into a lot of the legal aspects regarding trust translation schemes.

8.1 Academic Perspective

8.1.1 Purpose of Trust Translation Schemes

The world of trust schemes is heterogeneous: different organizations like business and government institutions have developed often quite different standards of how they assess and specify trust, making it hard to interoperate across the boundaries of such standards. This has of course often historical or political reasons, but also it may be that different organizations have different needs (that may be incompatible with each other). To allow for interoperability requires thus first to come to agreements between different communities how to translate between their concepts, e.g., to translate from a trust scheme with levels {1,2,3} to one with levels {A,B,C,D}. This may be first and foremost a legal question: can we for instance legally recognize an e-signature of level 2 in one jurisdiction to be just as good as a level-B signature in the other?

Once a policy is defined (and legally accepted) for translating between the trust schemes, it is of course not desirable to hard-code this translation into the respective software systems: this would make it harder to observe (since one has to look up the source code), in-transparent (if the code is not open source), and most importantly hard to change and maintain. As in other areas of trust, access control and security in general, it is preferable to have a simple language to describe such trust translation schemes. The files that are written in this language are a kind of configuration files that can either be published (so everyone can see how the trust translates) or it could also remain closed (to be visible only within an organization). Either way, the software that makes the trust decision will then base its decision on the given trust translation scheme, rather than having this translation hard coded.

8.1.2 A Gap in Research

There is not much research at present that deals with trust translation, in particular in the formal methods community, we have not found a single paper that deals exactly with this issue. A reason may be that, from a purely theoretical view point, one may regard trust translation as a problem that should be solved by international standardization: if one could obtain a common terminology, rating, standards, quality criteria and the like, then we would not need any translations anymore. In fact, almost all formal methods papers seem to assume such an underlying generally-agreed standard. Such a common standard does not exist in practice and is hard to be achieved, since different organizations have developed in a heterogeneous way

Document name:	Inventories (2)	Page:	71 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



and have different needs and focusses. In fact, LIGHTest should help to facilitate solutions that bridge over the gap of the different standards. Since a large part of the literature does not consider the problem in the first place, there are relatively few works on formalisms (languages) that allow to describe how to translate between different trust schemes. We give an overview of the few works that even discuss the problem, and also discuss the solutions to similar problems in related domains like access control that may help to fill the gap in the future. However, it seems we do not have to start from scratch here, but in fact, trust schemes and their translation share many traits with classical access control languages and mechanisms, so the solutions to the challenges and requirements of this domain may indeed borrow from this field. We therefore discuss in the following also a few formalisms that may seem a bit far away (in their application domain and content) but could indeed be helpful for LIGHTest.

8.1.3 Existing work in Electronic Identity

The STORK project involves trust translation and defines the QAA model for mapping assurance levels. This is discussed in more detail below in section 10.2. There are scientific papers on STORK such as (A. Crespo, 2011).

The FutureID project also – at least indirectly -- deals with the translation between different kinds of credentials, namely through broker services. Although this is not directly on trust levels, but on attributes of credentials, this is a similar problem. There is no general translation scheme language for FutureID, but a formalization of a semantic criterion by (O. Almousa, 2016) for the issuing that could be the formal basis also for LIGHTest trust translation schemes. A similar idea was first used in the formalization of general identity management systems by (J. Camenisch, 2010).

The idea of these two works is that every credential is a sequence of attribute-values that are signed by the issuer together with a credential type. The formal meaning (semantics) of such a credential can be expressed as a statement about the bearer of the credential. We can express this statement as a formula with function and predicate symbols like "firstname", "lastname" or "dateOfBirth" and either fix a model for such symbols or characterize them axiomatically. Then we can make logical implications, e.g., if a bearer is over 21 years old then he or she is also over 18. In the work by Camenisch et al., this was used to define the acceptance condition of a credential: a server accepts a credential if the condition it requires on the user is logically implied by the condition proved by the user. Similarly, in Almousa et al., a broker service can issue a credential B for a user who has shown a credential A, if the statement of A implies the statement for B. For instance, A can be a credential containing name and date of birth, while B is only asserting that the bearer is over 18.

In general, this approach seems directly applicable for trust translation schemes and reasoning about their correctness. We can formalize similarly by formulas that a particular certificate, signature, etc., has a certain property, e.g., being on a level of assurance 2 in schema X, and have as an axiom a mapping from schema X with levels {1,2,3} into another schema Y with levels {A,B,C,D}, for instance that 2 in X is at least as good as B in Y. Similarly we can give axiom about the relationship of the trust levels, for instance: $A > B > C > D$, and $3 > 2 > 1$. So if for a

Document name:	Inventories (2)	Page:	72 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



certain transaction level C (in scheme Y) is sufficient, we can logically derive that the level 2 (in scheme X) is also sufficient.

Moreover, this logical approach allows us to leave open the precise definition of the levels of the two schemata, for instance what precise requirements one has to fulfill to reach level 2 in schema X. This is desirable because some requirements may not be of a technical nature, hard to formally express, and even irrelevant for the trust translation. However, whenever we can characterize relationships between trust levels of different schemata, we can do so with the additional benefit that some translations do not have to manually stated, but can be logically derived from our characterization. This could reduce the manual work (of specifying out many special cases individually) and errors that can occur from them. Finally, also changing a trust translation scheme becomes easier through such an approach.

The sketched approach leaves open two questions:

- The concrete language/format for describing the translation; we have just argued on the semantic level (logical implications). The precise language must be balanced between expressiveness (especially for reasoning about trust and trust translation) and practical implementability (not all formalisms are decidable or have feasible complexity).
- How to relate the statements made by several entities in a system (e.g., delegation or chains of certificate) and when these are not persistent, but may change over time.

There is some literature about similar problems that we consider them in the following sections.

8.1.4 Description Logics

Description logics have been proposed for expressing knowledge and especially to formalize ontologies in the semantic web, see for instance (F. Baader, 2007) et al. for an introduction. They are a compromise between the limited expressivity of Boolean logic and the undecidability of full first-order logic. They are tailored to problems like the ones that we can encounter in trust translation, e.g., that criterion A is fulfilled if B and C are fulfilled and that C is a special case of D. Then, if criterions B and D are fulfilled, also A is. We can certainly draw from this field and actually may use some existing ontologies.

8.1.5 Logics of Belief

Burrows, Abadi and Needham introduced a logic, often called BAN-logic after the authors' initials, for reasoning about the belief of participants (M. Burrows, 1990). BAN logic relates the statements that each participant believes in with the messages that they transmit (e.g., electronic signatures), the knowledge about involved keys (e.g., that a public key belongs to a particular party), and predicate that can be used to model trust, namely "P has jurisdiction over X" (where X can be again any formula). It is a modal logic that allows one to nest statements with the modal operators, e.g. "A believes B says C believes D has the jurisdiction over ...". This is in contrast to classical logic and characterizing several worlds (since the beliefs of the different participants are not necessarily consistent). This seems certainly an inspiring approach for

Document name:	Inventories (2)	Page:	73 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



reasoning about trust, but it should be seen with a grain of salt: while it is based on a number of intuitive deduction rules, BAN logic has actually no semantical foundation and in fact was used to prove the security of some protocols that later turned out to be flawed. For this reason, BAN will not play a role in LIGHTest, and is here only mentioned as a historically important concept.

8.1.6 Access Control Policy Languages

Since trust translations are essentially policies, one may look at other policy languages, especially from the field of access control. They share also literally many concepts with trust schemes such as the reasoning about delegation. While this is mostly relevant to chapter 7, we also briefly discuss this here for trust translation.

There are several languages possibly XACML being one of the most popular. XACML is a fine-grained approach that defines user access by evaluating detailed policies derived from the attributes of sources. It illustrates a problem of semi-formal language design and implementation (i.e., the language does not get a precise formal semantics, but is defined by a set of natural language descriptions and the tools that work on it). The attempt to give it a precise meaning reveals the real complexity of such a language that results out of positive and negative default values (C. Ramli, 2014).

8.1.7 Trust and Domain Theory

Several works have pointed out the relation between trust and domain theory, e.g. (M. Carbone, 2003). The insight is that aspects like delegation and the availability of information mean a regression on the trust relation in a system, and one can derive the actual trust through a fixed-point computation. Carbone et al. do not consider the translation between heterogeneous parts of the system per se, but the general view of semantic domains allow for an integration of translation schemes in their setting.

While these approaches are only considering a positive fixed-point, i.e., no negative changes as in the following example: an employee leaves a company and thereby the privileges granted by the company no longer apply. To overcome the limitation of "persistent" permissions and delegations (that cannot be revoked) the AVANTSSAR project proposed the language ASLan (D. v. Oheimb, 2010): here one can model a state transition system with dynamic properties, e.g. the membership in a group or delegations can change during transitions, and one can specify access rights, delegation, trust—and we believe also trust translation—by Horn clauses over the dynamic properties. This allows only to specify the conditions positively (e.g. that all members of a group have access to some resource, and that every delegate of somebody who has access to the resource also has access) avoiding any contradiction and hard-to-read specification and limit negation to the dynamicity of the system (e.g. revocation, blacklisting).

8.2 Industry Perspective

In this section we focus on the compilation of (legal and standardization) sources at European and international levels which, either refer to trust translation schemes which are already being used (i.e. mapping of national levels of assurance for electronic identification means to EU

Document name:	Inventories (2)	Page:	74 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



levels—QAA/AQAA models—such as those carried done in STORK and STORK 2.0 Large Scale Pilot projects or, more importantly, the levels of assurance for electronic identification means under Article 8 of the eIDAS Regulation and for which the Implementing Regulation (EU) 2015/1502 has set out minimum technical specifications and procedures) or, in the absence of such translation frameworks, we offer a comprehensive overview of the main sources which could allow in the future to set up such trust translation schemes based on the formats and properties which can allow to categorize different types of electronic services, with particular focus on eIDAS Trust Services (e.g. electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services, certificates for website authentication) into levels from a trust perspective.

For each Trust Service in the eIDAS Regulation we provide:

- Definitions and concepts
- European Landscape: Relevant Legal Provisions and Relevant Standards
- International Landscape: Relevant Legal Provisions and Relevant Standards
- Conclusions

In order to ensure the security and legal validity of an electronic transaction in cross-border scenarios (as at national level), the eSignature has been certainly very important but not sufficient. As said in (European Commission, 2016), other trust services are needed to ensure:

- *“Time stamping: The date and time on an electronic document which proves that the document existed at a point-in-time and that it has not changed since then.*
- *Electronic seal: The electronic equivalent of a seal or stamp which is applied on a document to guarantee its origin and integrity.*
- *Electronic delivery: A service that, to a certain extent, is the equivalent in the digital world of registered mail in the physical world.*
- *Recognition of the legal admissibility of electronic documents that provide sufficient assurances of their authenticity and integrity.*
- *Website authentication: Trusted information on a website (e.g. a certificate) which allows users to verify the authenticity of the website and its link to the entity/person owning the website.”*

While many sources are related to Standards or EU legal texts, they are included in this “Industry Perspective” subsection because it can be considered that the security and electronic services industry shall be following these norms in order to produce services, products and solutions which are interoperable and standards-based in order to satisfy the expectations of their customers and comply, at least in Europe, with the legal framework that regulate their activity (i.e. in the case of Trust Service Providers).

Document name:	Inventories (2)	Page:	75 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Policy provisions and technical requirements could be aligned on multiple levels of assurance (LoA) relevant for trust assessment:

	ESig	ESeal	Time-Stamp	Digitised Data	Digital Certificate	RED	RED receipt	I.P. Archive	IAA	SCD/ACD	Signature Validation Assertion
Qualified (LoA4)	AdESig + QC + SSCD	AdESeal + QC + SSCD	QTST	QDD	QC (corresponds to QCP+ certificate policy)	QRED	QREDreceipt	QIPA	QIAA	SSCD/SACD	QSVA
	Equivalent to Handwritten signature	Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty
LoA3	AdESig _{QC}	AdESeal _{QC}			(corresponds to QCP certificate policy)						
LoA2	AdESig	AdESeal			(corresponds to NCP+ or NCP certificate policy)						
LoA1	ESig	ESeal			(corresponds to LCP certificate policy)						

Figure 11 Different levels of assurance for several trust schemes

(The above figure has been extracted from (DLA Piper; PriceWaterhouseCoopers; SEALed; SGA; TimeLex, 2013).)

Broadly speaking we consider a distinction between *authoritative* and *reputation based trust translation schemes*. The first refer to schemes where a standard or legal norm determines (authoritatively) how a translation (or mapping) of trust or identity assurance should be carried out between two different schemes (examples of this are STORK QAA/AQAA models, ISO 29115 standard for LoAs or eIDAS specifications and procedures used to specify the assurance level of the electronic identification means issued under a notified electronic identification scheme by determining the reliability and quality of certain elements). In the most basic approach under eIDAS, trust service providers and their services can be broadly classified between “Qualified” and “non-qualified” when they respectively are granted that status by a supervisory body and meet the requirements laid down in the Regulation. The second refer to schemes where reputation of a given service (or its provider) is determined by different means (including by rating mechanisms accessible to stakeholders involved in the use of the services) and made public, allowing for comparison and thus, also potential mapping across different providers and countries.

Two main gaps are identified which will need to be addressed: the lack of (explicit) trust translation schemes in some cases due to the lack of maturity of the referred services (demanding schemes to ensure comparability and interoperability on a global market scale), and the difficulty in certain cases to find sources on applicable standards and legal norms (for Trust Services) in non-EU countries as it does seem the case that, for most of these services, Europe is indeed the most advanced area of the world in terms of the efforts being made, both on the technical and legal fronts, to foster and achieve interoperability and uptake of eID and Trust Services.

We anyhow expect to provide a more complete inventory of sources in the final iteration of this deliverable. More advanced topics, including more general trust translation schemes applicable in complex scenarios where it is needed to compose trust levels of individual trust services in the

Document name:	Inventories (2)	Page:	76 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



context of other services which combine different types of trust services and/or trust services from different providers in the same or different countries, will be addressed.

While the current scope of this part of the inventory is on existing trust translation schemes, given the gap identified on lack of such schemes for many of the Trust Services relevant for LIGHTest (and therefore also for other more general services and solutions built upon these Trust Services), there is a wide opportunity to establish fruitful dialogues with policy and decision makers (political level) and, with standards developing organizations and the industry to develop frameworks for implementing trust translation schemes at an international level.

This relates well to the “International aspects” addressed in Art. 14 of the eIDAS Regulation which refers to agreements to be concluded between the EU and third countries or international organisations allowing to recognize trust services provided in that third country or international organization (and, conversely, the recognition of EU trust services abroad).

The main authoritative legal references used in this part of the inventory refer to the eIDAS Regulation (European Commission, 2014) and Secondary Legislation related to its implementation:

On electronic identification:

- Commission Implementing Decision (EU) 2015/296 of 24 February 2015 on procedural arrangements for MS cooperation on eID (European Commission, 2015):

Member States shall cooperate in order to reach interoperability and security of electronic identification schemes. The decision establishes the methods for exchange of information and creates the Cooperation Network to facilitate cooperation on the subject.

- Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework (European Commission, 2015):

The regulation creates the platform enabling practical connectivity between eID means from different Member States, to foster interoperability.

- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means (European Commission, 2015):

The main goal of the eID mutual recognition is to enable EU citizens to do cross-border interaction with their own national eID means. Since each Member State has a separate system to manage electronic identities, a mechanism is needed to make them comparable and interoperable. The Commission Implementing Regulation on levels of assurance includes detailed criteria which allow Member States to map their eID means against a benchmark (low, substantial and high) and thus to compare each other.

Document name:	Inventories (2)	Page:	77 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification (European Commission, 2015):

Notification of electronic identification schemes by Member States is a prerequisite of mutual recognition of electronic identification means. The decision ensures uniform use of the notification form.

On electronic trust services:

- Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 on the form of the EU Trust Mark for Qualified Trust Services (European Commission, 2016):

The objective of the regulation is to foster transparency in the market. The trust mark clearly differentiates qualified trust services from other trust services; the aim is to foster confidence in and of essential online services, for users to fully benefit and consciously rely on electronic services.

- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists (European Commission, 2015):

Trusted lists are essential for ensuring certainty and building trust among market operators as they indicate the status of the service provider at the moment of supervision. The decision also aims at fostering interoperability of qualified trust services by facilitating the validation of e-signatures and e-seals.

- Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies (European Commission, 2015):

by ensuring continuity with the principles adopted under the Service Directive (European Commission, 2009), the decision facilitates cross-border transactions with public sector bodies in a different Member State. It also ensures technological neutrality by setting a method for the use of non-standardised formats.

- Commission Implementing Decision (EU)2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices (European Commission, 2016):

The decision lists the standards for the security assessment of qualified signature and seal creation devices.

8.2.1 Electronic Identity

8.2.1.1 Definitions and Concepts

(The following definitions can be found at (European Commission, 2016).)

Document name:	Inventories (2)	Page:	78 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Electronic Identification (e-Identification, eID)

The process of determining a person/entity's identity by using electronic means. In Europe many Member States provide their citizens with electronic IDs via smart cards, mobile phones, or other technologies: some Member States combine an e-ID with the function of an identity card used also as a travel document, others have a citizen card to access public online services, others work with mobile devices, or a combination of card and phone.

Electronic Identity Card (e-ID)

The electronic identity card (eID) is an official electronic proof of one's identity. It also enables the possibility to sign electronic documents with a legal signature.

Authentication

Electronic authentication is the process of confirming a person/entity's identity.

Authentication and Authorisation Infrastructure (AAI)

The Authentication and Authorisation Services, components for Identity and Privilege Management and the entities responsible for these services - constitute an Authentication and Authorisation Infrastructure (AAI). In research networks federated AAIs containing multiple Identity Providers, trusted by the members of the federation are common.

In 2014, the Regulation No 910/2104, called **eIDAS Regulation**, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC was adopted. Formal definitions of 'electronic identification', 'electronic identification means', "person identification data", "electronic identification scheme", 'authentication' and 'relying party' provided in Art. 3 of the eIDAS Regulation should also be considered and are provided below.

8.2.1.2 European Landscape

Relevant Legal Provisions

(eIDAS) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market

eIDAS regulation on assurance levels for electronic identification means is generated by taking into consideration the international standard "ISO/IEC 29115 Entity Assurance Framework". eIDAS specification on LoA starts with some definitions as stated below. An Authoritative Source is a nationally trusted source that provides data, information or evidence for proving an identity. An identity evidence/information proves an identity as known to an Authoritative Source and it can be evaluated as an identity proof as long as it can be confirmed as original.

The definitions of levels of trust/assurance and certificates contain the sets of criteria useful to define the equivalences and translation criteria with other legislations and jurisdictions. In particular, see **Chapter I Art. 3 and Chapter II Art. 6.1 and Art. 8.2 of eIDAS for the exact definitions.**

Relevant Initiatives

Document name:	Inventories (2)	Page:	79 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



STORK - Levels of Assurance - Review of QAA

STORK developed a Quality Authentication Assurance (QAA) model (STORK 2.0, 2015), (STORK 2.0, 2015) to map national levels of assurance of electronic identification means to a common security level scheme. The QAA has been developed in early project stages. I.e., it is about five years old and remained unchanged since. Given that and given technological progress, some uncertainty existed, if the original QAA still fits MS practices. With the advent of the eIDAS Regulation, a review has been carried out by some Member States. This document reports on that review.

The eIDAS Regulation defines Assurance Levels in article 8. An implementing act shall set out minimum technical specifications where, acc. to recital (16) STORK QAA and ISO 29115 should be taken into account.

The STORK QAA, however, has been finalised in 2009 and since remained unchanged. MS processes and technology changed, as well as experience has been gained through piloting and through mapping MS existing eID schemes to QAA. STORK 2.0 therefore collected comments and suggestions for updates through the MS Council (the MS representatives in the STORK 2.0 project). Comments have been received by AT, CH, CZ, ES, LU, NL, SE, UK.

This summary limits itself to the STORK QAA core technical specifications, i.e. sections 2.3, 2.4, and 2.5 of the original STORK QAA on the registration phase and the authentication phase. Comments received by MS on these sections have been incorporated. This as the document shall serve as a concise overview of the STORK QAA core (STORK, 2014).

8.2.1.3 International Landscape

Relevant Legal Provisions

NSTIC (US, 2011)

In April 2011, the White House issued its "National Strategy for Trusted Identities in Cyberspace - Enhancing Online Choice, Efficiency, Security and Privacy" (hereinafter "Strategy").

This document (The White House, 2011) aims at securing online transactions for businesses and individuals, and introduces the concept of an "**Identity Ecosystem**". This implies an online environment where individuals and organisations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities — and the digital identities of devices.

The Identity Ecosystem is designed to securely support transactions that range from anonymous to fully-authenticated and from low to high-value. It will offer, but will not mandate, stronger identification and authentication while protecting privacy by limiting the amount of information that individuals must disclose. The Identity Ecosystem is built around four guiding principles, namely:

- the enhancement of privacy and support of civil liberties;

Document name:	Inventories (2)	Page:	80 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- identity solutions must be secure and resilient;
- ensure policy and technology interoperability among identity solutions;
- the Identity Ecosystem must be developed from identity solutions that are cost-effective and easy to use.

NSTIC has funded pilot projects to develop, deploy, and adopt NSTIC-aligned technology, guidance, and policy, establishing an identity marketplace of solutions leveraged by both public and private sectors. More information on the pilots: (NIST, 2016) and (NIST, 2015).

In its Strategy, the White House indicates the key players within the Identity Ecosystem:

Draft NISTIR 8149: Developing Trust Frameworks to Support Identity Federation

Of particular relevance for LIGHTest can be the Draft NISTIR 8149: Developing Trust Frameworks to Support Identity Federation (NIST, 2016). This document provides an informational look at trust frameworks and explains what they are, what their components are, and how they relate to the concept of identity federation. It covers all the critical topics of trust frameworks, including roles and responsibilities, framework components and rules, legal structures (including risk and liability), and establishing and recognizing conformance. It aims to educate communities interested in pursuing federated identity management as they try to establish the agreements that will make up the framework. It includes guidance on determining roles in an identity federation, what to consider from a legal standpoint, and understanding the issues of establishing and recognizing conformance.

Other technical resources can be found in this list:

Draft NISTIR 8112: Attribute Metadata (NIST, 2016)

Draft Special Publication 800-63-3, Digital Authentication Guideline (NIST, 2016)

Draft NISTIR 8062: Privacy Risk Management for Federal Information Systems (NIST, 2015)

NISTIR 8103: Advanced Identity Workshop on Applying Measurement Science in the Identity Ecosystem: Summary and Next Steps (NIST, 2016)

Attribute Metadata and Confidence Scoring (NIST, 2015) and Attribute metadata project charter (NIST, 2016)

Measuring Strength of Authentication (NIST, 2015)

Strength of Function for Authenticators - Biometrics (SOFA-B): Discussion Draft (NIST, 2015) (NIST, 2016)

Measuring Strength of Identity Proofing (NIST, 2015)

Document name:	Inventories (2)	Page:	81 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



International Government Assurance Profile (iGov) Working Group Draft Project Charter (OpenID Foundation, 2016)

More details at the official site of NSTIC (NIST, 2016).

8.2.1.4 Relevant Standards

ISO/IEC 29115:2013

This standard (ISO, 2013), provides a framework for managing entity authentication assurance in a given context. Together with STORK (QAA model) it is referenced by the eIDAS Regulation, however the Implementing Regulation on Assurance Levels states “International standard ISO/IEC 29115 has been taken into account for the specifications and procedures set out in this implementing act as being the principle international standard available in the domain of assurance levels for electronic identification means. However, the content of Regulation (EU) No 910/2014 differs from that international standard, in particular in relation to identity proofing and verification requirements, as well as to the way in which the differences between Member State identity arrangements and the existing tools in the EU for the same purpose are taken into account.”

In particular, this standard:

- specifies four levels of entity authentication assurance;
- specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance;
- provides guidance for mapping other authentication assurance schemes to the four LoAs;
- provides guidance for exchanging the results of authentication that are based on the four LoAs; and
- provides guidance concerning controls that should be used to mitigate authentication threats.

ITU Standards

The ITU standards X.1250-X.1279 are about Identity management:

- **X.1250** (ITU, 2009): Baseline capabilities for enhanced global identity management and interoperability.
- **X.1251** (ITU, 2009): A framework for user control of digital identity.
- **X.1252** (ITU, 2010): Baseline identity management terms and definitions.
- **X.1253** (ITU, 2011): Security guidelines for identity management systems. This Recommendation proposes security guidelines for identity management (IdM) systems. The security guidelines provide how an IdM system should be deployed and operated for secure identity services in NGN (Next Generation Network) or cyberspace environment. The security guidelines focus on providing official advice how to employ various security guidelines provide how an IdM system should be deployed and operated for secure

Document name:	Inventories (2)	Page:	82 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



identity services in NGN (Next Generation Network) or cyberspace environment. The security guidelines focus on providing official advice how to employ various security mechanisms to protect a general IdM system and it also provides proper security procedures required when two IdM systems are interoperated.

- **X.1254** (ITU, 2012): Entity authentication assurance framework.
- **X.1255** (ITU, 2013): Framework for discovery of identity management information.
- **X.1275** (ITU, 2010): Guidelines on protection of personally identifiable information in the application of RFID technology.

Recommendation ITU-T X.1275 recognizes that radio frequency identification (RFID) technology renders information pertaining specifically to the merchandise worn or carried by individuals open to abuse even as it greatly facilitates access to and distribution of such information for useful purpose. The abuse can manifest as tracking the location of the individual or invasion of his or her privacy in another malfeasant manner. For this reason, this Recommendation provides guidelines regarding the RFID procedures that can be used to enjoy the benefits of RFID while attempting to protect personally identifiable information.

8.2.1.5 Conclusions on Electronic Identity

Electronic identity is perhaps governed by the most highly developed trust schemes in the world. As a consequence, there are some trust translation schemes already defined, at least in the European industry.

The three levels of assurance defined in eIDAS have their corresponding ones in (A)QAA models and the specific technical specifications and procedures in the Annex of Implementing Regulation (EU) 2015/1502 allow to map national levels of assurance for electronic identification means to those three levels of assurance. Mapping of the eIDAS LoAs to international levels defined for example in ISO/IEC 29115:2013 could be more complex to achieve as there seems to be no direct/binary equivalence or correspondence between the criteria used in both norms.

LIGHTest supports various different trust schemes including trust schemes that assign Levels of Assurance (LoA)s to each identity. An identity's level of assurance depicts the confidence of an identity provider on a user is who she says she is. Each country or organization determines.

8.2.2 Electronic Signatures

8.2.2.1 Definitions and Concepts

Electronic Signature

The following information has been extracted from (ETSI, 2016), CEF eSignature Digital Service Infrastructure (European Commission, 2016) . building block (European Commission, 2016), and eSignature goals (European Commission, 2016).

An electronic signature is essentially the equivalent of a hand-written signature, with data in electronic form being attached to other electronic subject data (Invoice, Payment slip, Contract, etc.) as a means of authentication.

Document name:	Inventories (2)	Page:	83 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Both electronic signatures and electronic seals can be supported technically by digital signatures which are data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

With first the European Commission e-sign Directive (1999/93/EC) and now with the **Regulation (EU) No 910/2014**, electronic signatures and electronic seals have legal effect. **Similar effect is provided by the June 2000, U.S. government E-sign bill.**

On 28 November 2008 the European Commission adopted an 'Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market' (COM(2008) 798).

On 22nd December 2009, the European Commission issued a standardization mandate on electronic signatures (M/460) for the definition of a rationalized standardization framework.

In 2014, the Regulation No 910/2104, called eIDAS Regulation, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC was adopted.

The eSignature building block helps public administrations and businesses to accelerate the creation and verification of electronic signatures. The deployment of solutions based on this building block in a Member State facilitates the mutual recognition and cross-border interoperability of eSignatures. This means that public administrations and businesses can trust and use eSignatures that are valid and structured in EU interoperable formats.

eSignature in context: CEF Digital

CEF eSignature's main goal is to ensure that Public Administrations and Businesses can create and validate electronic signatures across borders. This means contributing to the creation of a EU single market which is fit for the digital age.

eSignature is a building block in the eidentification and eSignature DSI and is needed in key application domains and policy contexts. The provision of nearly all online public-sector services requires exchange of documents whose signature can be recognised across border. It therefore constitutes a key building block for European core service platforms.

CEF eSignature supports public authorities in automating the validation of interoperable eSignatures and eSeals coming from any EU Member State, based on the Member States' "Trusted Lists" (the public lists of supervised qualified trust service providers – including those issuing qualified certificates – and the qualified trust services they provide).

The eSignature building block therefore foresees Administration to Business communication (A2B). However, CEF eSignature can also be used to enable Administration to Administration (A2A) and Administration to Citizen (A2C) communication.

The CEF eSignature building block consists of advisory services managed by the European Commission.

The solution is primarily based on the following services:

- The Digital Signature Services (DSS) application for the creation and validation of e-signatures (European Commission, 2016). Releases are published as well (European Commission, 2016).

Document name:	Inventories (2)	Page:	84 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- Complementary service, called Trusted Lists (TL) Manager, that enables the creation, editing and maintenance of a Trusted List in a standard, machine-readable format (European Commission, 2016).

8.2.2.2 European Landscape

Relevant Legal Provisions:

(eIDAS) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (European Commission, 2014)

The definitions of levels of trust/assurance and certificates contain the sets of criteria useful to define the equivalences and translation criteria with other legislations and jurisdictions.

In particular, see Chapter I Art. 3, Chapter III Section 4 Art. 25.2, Art. 26, Art. 27.3, Art. 32.1, and Annex I.

Other legal provisions (including the now superseded eSignature Directive of 1999 but also the eServices Directive and Commission Decisions related to cross-border processing of eSignatures and those related to the publication of Trusted Lists) are described in CEFDIGITAL (European Commission, 2016)."

Relevant Initiatives:

STORK 2.0

D4.9 Final version of Functional Design

The Functional design (STORK 2.0, 2015) describes the data and processes resulting of the requirement analysis which will cover the needs of the Member States within the scope of STORK 2.0. The processes are authentication on behalf of and powers for signature validation for STORK 2.0, in both cases there are natural persons acting on behalf of other persons, especially SMEs. A third process for people acting on behalf of others is the powers validation, which supports the validation of powers stored at service providers. This document also describes an extension of STORK1 process flows with domain-specific attributes, as well as support processes like signatures, version control and anonymity. Furthermore it includes a description of available data.

D4.10 Final version of Technical Design

This document describes the final architecture (STORK 2.0, 2015) of the systems that compose the common functionalities of the STORK 2.0 platform. This description is made from various points of view, conforming to the RUP methodology. The relevant points of view are applied to each of the two systems: PEPS and Virtual IDP. The deliverable also describes "commodities", which are software components discovered to be useful in several places. Finally detailed software design is provided, describing class diagrams for each module and interface specification for each package.

Document name:	Inventories (2)	Page:	85 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



CROBIES study

This study (CROBIES, 2010) analyses the requirements and establish a general strategy for cross-border use of QES and AES based on QC *within* the existing legal framework set by the eSignatures Directive, and provided some of the inputs that were taken into account for the drafting of the eIDAS Regulation.

The CROBIES study concluded that a recast of the existing legal, standardization and trust frameworks related to ES, supported by appropriate promotional and educational efforts, is essential to improve interoperability and cross-border use of ES. However CROBIES focused in five working packages (WP) on several “quickwin” actions that could improve some very specific aspects of the interoperability, cross-border use and mutual recognition of QES and AES based on QC *within* the current legal framework.

Relevant Standards:

The following standards can be found at (ETSI, 2016).

ETSI EN 319 122 (CAAdES)

- ETSI EN 319 122-2 V1.1.1 (2016-04) Published

Electronic Signatures and Infrastructures (ESI); CAAdES digital signatures; Part 2: Extended CAAdES signatures

- ETSI EN 319 122-1 V1.1.1 (2016-04) Published

Electronic Signatures and Infrastructures (ESI); CAAdES digital signatures; Part 1: Building blocks and CAAdES baseline signatures

ETSI EN 319 132 (XAdES)

- ETSI EN 319 132-2 V1.1.1 (2016-04) Published

Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures

- ETSI EN 319 132-1 V1.1.1 (2016-04) Published

Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures

ETSI EN 319 142-2 (PAdES)

- ETSI EN 319 142-2 V1.1.1 (2016-04) Published

Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles

Document name:	Inventories (2)	Page:	86 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Rationalised structure for Electronic Signature Standardisation (version 09/2013):

The above are electronic signature formats for binary, XML and PDF documents but are not expressing 'levels' (like QES, AdES, AdESQC do).

This document (AFNOR Group, 2014) proposes a rationalised framework for electronic signature standardisation providing a coherent basis for selection of standard appropriate to business needs. An inventory of existing standardisation at the International, European and national/sector level is also available (AFNOR Group, 2014).

Joint CEN and ETSI Response to Mandate M460 (European Commission, 2013)

As of today the electronic signatures standardization landscape is rather complex and does not offer a clear mapping with the requirements of directive 1999/93/EC on a community framework for electronic signatures. The current multiplicity of standardisation deliverables together with the lack of usage guidelines, the difficulty in identifying the appropriate standards and lack of business orientation is detrimental to the interoperability of electronic signatures. Also because many of the documents have yet to be progressed to full European Norms, their status may be considered uncertain. (AFNOR Group, 2013)

It resulted in a lack of truly interoperable e-signature applications and in a lack of trust in the existing framework. We particularly face problems with the mutual recognition and cross-border interoperability of electronic signatures. A few interoperability events have been held. These have yet to be developed to the extent that they provide full conformance tests and cover all areas of standardization.

On the other hand, the ESOs have initiated work to partially update the standardization framework derived from EESSI in such way that existing new materials have to be incorporated in a rational way into the new framework. Moreover, CEN/TC224 has to complete the conversion as ENs of the CWAs referenced in the 2003/511/EC Decision in order to allow the European Commission to publish a new release of this Decision.

The definition of a rationalised framework (European Commission, 2009) for electronic signature standards will overcome those issues and will allow business stakeholders to easily implement and use products and services based on electronic signatures. Latest comments to ETSI drafts for review can be found at (ETSI, 2016).

8.2.2.3 International Landscape

Relevant Legal Provisions

PIPEDA (Canadian)

In this Canadian federal law (Office of the Privacy Commissioner of Canada, 2008):

(1) An electronic signature is "a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document";

Document name:	Inventories (2)	Page:	87 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



(2) A secure electronic signature is as an electronic signature that

(a) is unique to the person making the signature;

(b) the technology or process used to make the signature is under the sole control of the person making the signature;

(c) the technology or process can be used to identify the person using the technology or process; and

(d) the electronic signature can be linked with an electronic document in such a way that it can be used to determine whether the electronic document has been changed since the electronic signature was incorporated in, attached to or associated with the electronic document.

US law regulations

In the US, a number of legal instruments provide a regulatory framework for electronic signatures. Apart from these federal laws, each State can proclaim state legislation regarding the subject. What follows is a brief summary of each of the most relevant US acts regarding electronic signatures.

ESIGN

The **Electronic Signatures in Global and National Commerce Act** (US Government, 2000) , enacted on 30 June 2000, is a federal acts facilitating the use of electronic records and electronic signatures in both interstate and foreign commercial transactions by attributing the validity and legal effect to contracts entered into electronically. This act lays out the guidelines for interstate commerce, and assimilates electronic signatures and records with their paper equivalents.

Although every state has at least one law pertaining to electronic signatures, it is the federal law that lays out the guidelines for interstate commerce. The general intent of the ESIGN Act is spelled out in the very first section (101.a), that a contract or signature “may not be denied legal effect, validity, or enforceability solely because it is in electronic form”. This simple statement provides that electronic signatures and records are just as good as their paper equivalents, and therefore subject to the same legal scrutiny of authenticity that applies to paper documents.

In the Act Sec 106 (US federal law):

(5) **ELECTRONIC SIGNATURE-** *The term ‘electronic signature’ means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.*

Federal Reserve (US Government, 2017) 12 CFR 202 (US federal regulation) refers also to the ESIGN Act.

Document name:	Inventories (2)	Page:	88 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



UETA

The **Uniform Electronic Transactions Act** (US, 1999), which has been adopted by 48 US states, aims at aligning the differing state laws over areas such as retention of paper records and the validity of electronic signatures, and supports the validity of electronic contracts as a viable medium of agreement.

In Sec 2 (US state law):

(8) "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

SEAL

National and state governments in many jurisdictions have enacted laws governing the use of digital signatures for various types of transactions. In 1998, the US Congress passed the Digital Signature and Electronic Authentication Law (SEAL), which amended the Bank Protection Act (1968) to allow use of digital signatures to facilitate the use of electronic authentication by financial institutions. (See section about **Relevant Legal Provisions**

SEAL (US) for more information.)

GPEA

The **Government Paperwork Elimination Act** (Bowman, 2003), requires federal agencies to use electronic forms, electronic filing and electronic signatures (when practicable) to conduct official business with the public.

In its Sec 1710 (US federal law):

(1) ELECTRONIC SIGNATURE.—the term "electronic signature" means a method of signing an electronic message that—

(A) identifies and authenticates a particular person as the source of the electronic message; and

(B) indicates such person's approval of the information contained in the electronic message.

Commodity Futures Trading Commission

In the Commodity Futures Trading Commission (US Government, 2016) 17 CFR Part 1 Sec. 1.3 (US federal regulations):

(tt) Electronic signature means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

Document name:	Inventories (2)	Page:	89 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Food and Drug Administration

The Food and Drug Administration (US Government, 2017) 21 CFR Sec. 11.3 (US federal regulations) says:

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

United States Patent and Trademark Office

The United States Patent and Trademark Office (USPTO, 2015) 37 CFR Sec. 1.4 (federal regulation) states:

(d)(2) S-signature. An S-signature is a signature inserted between forward slash marks, but not a handwritten signature ...

(i) The S-signature must consist only of letters, or Arabic numerals, or both, with appropriate spaces and commas, periods, apostrophes, or hyphens for punctuation...

(e.g., /Dr. James T. Jones, Jr./)...

(iii) The signer's name must be:

(A) Presented in printed or typed form preferably immediately below or adjacent the S-signature, and

(B) Reasonably specific enough so that the identity of the signer can be readily recognized.

ZertES (Swiss law)

ZertES (Criptomathic, 2003) is a Swiss Federal law that regulates the conditions under which trust service providers may use certification services with electronic signatures. Additionally, this law provides a framework that outlines the provider's obligations and rights as they apply to providing their certification services. 2003. (Advanced and qualified signatures). Qualified signature is equivalent to eIDAS definition.

Electronic Signature Law of the People's Republic of China

In the Electronic Signature Law of the People's Republic of China (China, 2005), the stated purposes include standardizing the conduct of electronic signatures, confirming the legal validity of electronic signatures and safeguarding the legal interests of parties involved in such matters.

Federal Law of Russian Federation about Electronic Signature

The Federal Law of Russian Federation about electronic digital signature (Russia, 2011) was proclaimed in 2011. The "E-Signature Law" (or the "Law"), sets forth the legal framework for the use of e-signatures in electronic document flows. The Law is based on the following principles (The e-Signature Law Journal, 2005):

Document name:	Inventories (2)	Page:	90 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



1. The e-signature is recognized to be equivalent to the handwritten signature subject to the conditions provided in the Law;
2. The government supervises commerce in products and services involving e-signatures, by way of certification of e-signature means; and
3. Information systems are divided into common-use and corporate systems, differing in the degree of government supervision.

Under the E-Signature Law, the e-signature forms a part of an electronic document that is intended to protect the document against forgery. It is generated by cryptographic transformation of the information using a private key, permitting the holder of the e-signature key certificate to be identified, and ascertain the absence of distortion of information from the electronic document.

The procedure of electronic signing provides that three components must be present: two keys, private and public, and the certificate of the signature key. The Law defines them as follows:

- The private key is a unique series of symbols known only to the holder of the certificate of the signature key;
- The public key is a unique series of symbols corresponding to the private key available to any user of the information system and intended for the verification of the e-signature in the electronic document; and
- The certificate of the signature key is a hardcopy or softcopy document electronically signed by an authorized officer of a certification center, which contains the public key and is issued to the user of the information system to verify the e-signature and the identity of the signatory.

The certificate must contain, in particular, the period of its validity, the name of the issuing center, the full name or pseudonym of the holder of the certificate, the public key, other details as may be requested by the certificate holder, and the details of transactions in which electronically signed documents will be legally valid. The latter provision does not appear to be entirely clear. The Law expressly states that it applies to relations arising “upon the execution of transactions under civil law and in other cases provided for by the laws of the Russian Federation”. This provision of the Law may presumably apply to the types of transactions under civil law as are provided for in the Civil Code. But the reference to “other cases opens” a wide scope of relations including various areas where public and private law apply.

A substantial difference between the E-signature Law from a number of its foreign counterparts consists in an attempt to divide all information systems into corporate and common-use systems and establish different legal treatment for each system.

UNCITRAL

The United Nations Commission on International Trade Law (UNCITRAL) emitted the UNCITRAL Model Law on Electronic Signatures in 2001 (UNCITRAL, 2001), (UN, 2016). It aims

Document name:	Inventories (2)	Page:	91 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



to enable and facilitate the use of electronic signatures by establishing criteria of technical reliability for the equivalence between electronic and hand-written signatures. Thus, the MLES may assist States in establishing a modern, harmonized and fair legislative framework to address effectively the legal treatment of electronic signatures and give certainty to their status.

Relevant Standards

ISO/IEC 15945:2002

Specification of Trusted Third Parties services to support the application of digital signatures (ISO, 2002).

This Recommendation | International Standard will define those TTP services needed to support the application of digital signatures for the purpose of non-repudiation of creation of documents. It will also define interfaces and protocols to enable interoperability between entities associated with these TTP services.

Definitions of technical services and protocols are required to allow for the implementation of TTP services and related commercial applications.

This Recommendation | International Standard focuses on:

- implementation and interoperability;
- service specifications; and
- technical requirements.

This Recommendation | International Standard does not describe the management of TTPs or other organizational, operational or personal issues. Those topics are mainly covered in ITU-T Rec. X.842 | ISO/IEC TR 14516, Information technology — Security techniques — Guidelines on the use and management of Trusted Third Party services.

NIST FIPS 186-4

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. DSA is a variant of the ElGamal Signature Scheme. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and **FIPS 186-4** in 2013 (NIST, 2013).

OASIS Digital Signature Services TC

The goal of OASIS Digital Signature Services (DSS) TC is to define an XML interface to process digital signatures for Web services and other applications. References used (OASIS, 2016) and (OASIS, 2007).

Document name:	Inventories (2)	Page:	92 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



A paper submitted to the EEMA ISSE 2006 conference describing DSS is available (courtesy of EEMA) (Cruellas & Pope, 2006).

In particular the technical work of the Committee is available in this site (OASIS, 2016) and of particular relevance are:

- Digital Signature Services v1.0 (OASIS, 2007)
- DSS Advanced Electronic Signature Profiles (OASIS, 2007)
- DSS Signature Gateway Profile (OASIS, 2007)

8.2.2.4 Conclusions on eSignature

No trust translation scheme has been found currently, however the European regulations distinguish the following levels of assurance:

- Electronic signature: non-qualified eSignature
- Advanced electronic signature: non-qualified eSignature
- Qualified electronic signature

More analysis should be done in a next iteration of this inventory to address how these levels relate to technical standards in actual use in Third Countries outside the EU.

8.2.3 Electronic Seals

8.2.3.1 Definitions and Concepts

Electronic seals are defined according to eIDAS (European Commission, 2014), Art. 3.

There are two major differences between electronic seal and electronic signature (DLA Piper; PriceWaterhouseCoopers; SEALed; SGA; TimeLex, 2013):

- Nature of the creator
 - Legal person or public sector body for electronic seal / Natural person for electronic signature
 - No pseudonym allowed for electronic seal
- Functionality (legal effect)
 - equivalence to handwritten signature for electronic signature
 - presumption of integrity of the data and of correctness of the origin of that data to which the seal is linked

Electronic documents

Electronic documents are *linked to electronic seals* in the following way in eIDAS Regulation: “*Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document’s origin and integrity.*” (Recital 59). Therefore the trust service of electronics seals can be used to ensure authenticity and integrity of electronic documents and, in that way, their legal admissibility.

Document name:	Inventories (2)	Page:	93 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



According to eIDAS, an electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

Actually, even though there is a definition of 'electronic document' in Art. 3 paragraph 35 ('electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording), and although it is mentioned as a key enabler in recitals 6 (and 63 to highlight their importance for further development of cross-border electronic transactions in the internal market) and it is listed in Art.1 alongside electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services and certificate services for website authentication, the fact is that in Art. 3 para 16 -definition of 'trust service'-, 'electronic document' is *not* listed as a trust service in that definition:

“(16) ‘trust service’ means an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services;”

Furthermore, it is not listed in the page of the EC for trust services (European Commission, 2016). Indeed, electronic documents are regulated by a separate Chapter IV of the eIDAS Regulation, following and separate from the Chapter III on Trust Services. Thus, while electronic documents are a key use case for trust services, they are clearly not considered as a trust service in their own right under the eIDAS Regulation.

The Regulation speaks about electronic documents in order to ensure “the legal admissibility of electronic documents to ensure their authenticity and integrity” (European Commission, 2016) as indicated in Recital 63 the principle that “an electronic document should not be denied legal effect on the grounds that it is in an electronic form in order to ensure that an electronic transaction will not be rejected only on the grounds that a document is in electronic form”. Also Art. 46: “An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.”

Thus, it seems it is not pertinent to investigate on standards, formats or possible trust levels for electronic documents as for trust services.

8.2.3.2 European Landscape

Relevant Legal Provisions

See eIDAS references at 8.2 Industry Perspective. Also interesting this reference (ENISA, 2016).

Document name:	Inventories (2)	Page:	94 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



European Regulation (EU) No 910/2014 (eIDAS)

Formats of advanced electronic signatures and seals (2015/1506) are specified in Art. 27.5 & 37.5. See *COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals*, below in this document.

Standards for the security assessment of qualified signature and seal creation devices (2016/650) are defined in Art. 30.3 & 39.2. See *COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices*, below in this document.

About qualified validation and preservation of Advanced and Qualified Electronic Seals the eIDAS Regulation says:

Art.37(5) - defines reference formats of advanced electronic seals in public services or reference methods where alternative formats are used. Adopted as CID 2015/1506/EU

Art.39(3) - defines formats and procedures applicable for the purpose the notification by Member States to the Commission of information on qualified electronic seal creation devices that have been certified by their designated bodies and information on electronic seal creation devices that are no longer certified (Art.31(1)).

EC is not empowered to define the technical requirements and specifications:

Art.37(4) - reference numbers of standards for advanced electronic seals (in public services).

Art.38(6) - reference numbers of standards for qualified certificates for electronic seals.

Art.39(1) - reference numbers of standards for qualified electronic seal creation devices

Art.39(2) - a list of standards for the security assessment of information technology products included in the list of qualified electronic seal creation devices whose conformity with the requirements laid down in Annex II of the Regulation has been certified by appropriate public or private bodies designated by Member States.

Art.40 - reference numbers of standards for the validation of qualified electronic seals, for qualified validation service for qualified electronic seals, and for the qualified preservation service for qualified electronic seals.

Requirements for QTSPs providing qualified validation services for QESig/QESeal laid down in:

Art.33.1(a) with regard to the validation process to be provided in compliance with Art.32.1. ((a) to (h)).

Art.33.1(b) for the provision of the validation result in an automated manner that needs:

Document name:	Inventories (2)	Page:	95 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- to provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues (in conjunction of Art.32.2);
- to be reliable and efficient; and
- to bear the advanced electronic signature or advanced electronic seal of the QTSP providing the qualified validation service.

Requirements for QTSPs providing preservation service for QESig/QESeal laid down in:

Art.34.1 for making use of procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals

Advanced electronic signatures and advanced electronic seals are similar from the technical point of view. Therefore, the standards for formats of advanced electronic signatures should apply *mutatis mutandis* to formats for advanced electronic seals.

This *mutatis mutandis* means:

Art 35 4 Electronic seals in public services. The underlying technologies are the same – the referred standards should be adapted to consider nature of:

- creator and
- the functionality

Art 35 5 Reference formats of advanced electronic seals or reference methods (in public services):

- the format of the digital signatures is in no way affected by the nature of the signature
- formats that Member States shall recognize are the same

Art 38 reference numbers of standards for the validation and preservation of qualified electronic seals:

- signature validation should include the verification of the fact that a received digital signature is a seal or a signature

Member States requiring an advanced electronic seal or an advanced electronic seal based on a qualified certificate as provided for in Article 37(1) and (2) of Regulation (EU) No 910/2014, shall recognise XML, CMS or PDF advanced electronic seal at conformance level B, T or LT:

Levels of conformance for digital signatures:

- B-Level – Profiles both signed and some unsigned properties of a signature at the time it is created.

Document name:	Inventories (2)	Page:	96 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- T-Level – Generates a trusted token to prove the signature was created on a certain date and time.
- LT-Level – Incorporates all material that is required to validate the signature and allow for the long term availability of the signed document.

Also, it is possible to use an associated seal container where those comply with the technical specifications listed in the Annex (see the **Fehler! Verweisquelle konnte nicht gefunden werden.** below, extracted from (European Commission, 2015), Annex).

List of technical specifications for XML, CMS or PDF advanced electronic seals and the associated seal container

Advanced electronic seals mentioned in Article 3 of the Decision must comply with one of the following ETSI technical specifications, with the exception of clause 9 thereof:

XAdES Baseline Profile	ETSI TS 103171 v.2.1.1
CAdES Baseline Profile	ETSI TS 103173 v.2.2.1
PAdES Baseline Profile	ETSI TS 103172 v.2.2.2

Associated seal container mentioned in Article 3 of the Decision must comply with the following ETSI technical specifications:

Associated Seal Container Baseline Profile	ETSI TS 103174 v.2.2.1
--	------------------------

Figure 12 Specs for AES and the associated seal container

(For the above standards, you can see (ETSI, 2012), (ETSI, 2013), (ETSI, 2013).)

In relation to the electronic seal validation, the seal validation possibilities shall be indicated in the sealed document, in the electronic seal or in the electronic document container. The seal validation possibilities shall confirm the validity of a provided advanced electronic seal.

COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices

The standards for the security assessment of information technology products that apply to the certification of qualified electronic signature creation devices or qualified electronic seal creation devices are (European Commission, 2016):

ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security, Parts 1 to 3 as listed below:

— ISO/IEC 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1. ISO, 2009.

— ISO/IEC 15408-2:2008 — Information technology — Security techniques — Evaluation criteria for IT security — Part 2. ISO, 2008.

Document name:	Inventories (2)	Page:	97 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



— ISO/IEC 15408-3:2008 — Information technology — Security techniques — Evaluation criteria for IT security — Part 3. ISO, 2008,

—ISO/IEC 18045:2008: Information technology — Security techniques — Methodology for IT security evaluation, and

—EN 419 211 — Protection profiles for secure signature creation device, Parts 1 to 6 — as appropriate — as listed below:

— EN 419211-1:2014 — Protection profiles for secure signature creation device — Part 1: Overview

— EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation. This document specifies a protection profile for an SSCD that performs its core operations including the generation of signature keys in the device. This profile may be extended through extensions specified in other parts.

— EN 419211-3:2013 — Protection profiles for secure signature creation device — Part 3: Device with key import. This document specifies a protection profile for an SSCD that performs its core operations including import of the signature key generated in a trusted manner outside the device.

— EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application. This document specifies an extension protection profile for an SSCD with key generation that support establishing a trusted channel with a certificate-generating application. This profile may be extended through extensions specified in other parts.

— EN 419211-5:2013 — Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application. This document specifies an extension protection profile for an SSCD with key generation that additionally supports establishing a trusted channel with a signature-creation application.

— EN 419211-6:2014 — Protection profiles for secure signature creation device — Part 6: Extension for device with key import and trusted channel to signature creation application. This document specifies an extension protection profile for an SSCD with key import that additionally supports establishing a trusted channel with a signature-creation application. Additional protection profiles or other form of security certification and security evaluation processes may be required, to ensure that they offer the relevant level of security, for other types of devices such as, e.g.:

- Mobile phones with hardware-based security (TEE, MTM, etc.).
- HSM being recognised as an SSCD.
- SSCD used for mass signing operations (e.g. for signing a series of documents).

Document name:	Inventories (2)	Page:	98 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Relevant Standards

Signature standards that also cover Seals

Some QSignature standards have been drafted to also cover QSeals:

- ETSI TS 119 101: Policy and Security Requirements for Electronic Signature Creation and Validation (ETSI, 2016)
- ETSI EN 319 102: Procedures for Signature Creation and Validation
- CEN EN 419 111: Protection Profiles for Signature Creation & Validation Applications
- ETSI EN 319 441 Policy & Security Requirement for TSPs providing Signature Validation Services
- ETSI EN 319 442 Profiles for TSPs providing Signature Validation Services

Assurance level based on the ETSI Normalized Certificate Policy (NCP)

NCP (Normalised Certificate Policy) level means that the certificates are governed by a Certificate Policy in compliance with the ETSI TS 102 042 standard (ETSI, 2004) for NCP or a similar standard. NCP relates to an ETSI TS 102 042 defined certificate policy which offers the same quality as that offered by the Qualified Certificate Policy (QCP) as defined in TS 101 456 but without the legal constraints implied by Directive 1999/93/EC and without requiring the use of a Secure Signature Creation Device (SSCD). ETSI TS 102 042 also defines an extended Normalized Certificate Policy (NCP+) which offers the same quality as that offered by the Qualified Certificate Policy (QCP) as defined in TS 101 456 but without the legal constraints implied by the Electronic Signature Directive (1999/93/EC) and, instead of requiring the use of a Secure Signature Creation Device, requires the use of a 'secure user device'. (SEALED, 2010)

On the other hand, QCP (Qualified Certificate Policy) level are certificates governed by a Certificate Policy in compliance with the ETSI TS 101 456 standard for QCP or a similar standard.

According to the type of the certificate provided (qualified or not) and the electronic seal provider itself (qualified or not) , the electronic seal can be classified:

- Advanced electronic seal (AdES): a non-qualified eSeal provider is signed by a non-qualified certificate provider.
- Advanced electronic seal supported by qualified certificate (AdES-qc): a non-qualified eSeal provider is signed by a qualified certificate provider.
- Qualified Electronic Seal: a qualified eSeal provider is signed by a qualified certificate provider.

Document name:	Inventories (2)	Page:	99 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Differences among QES, AdES-qc, and AdES are shown in the next figure:

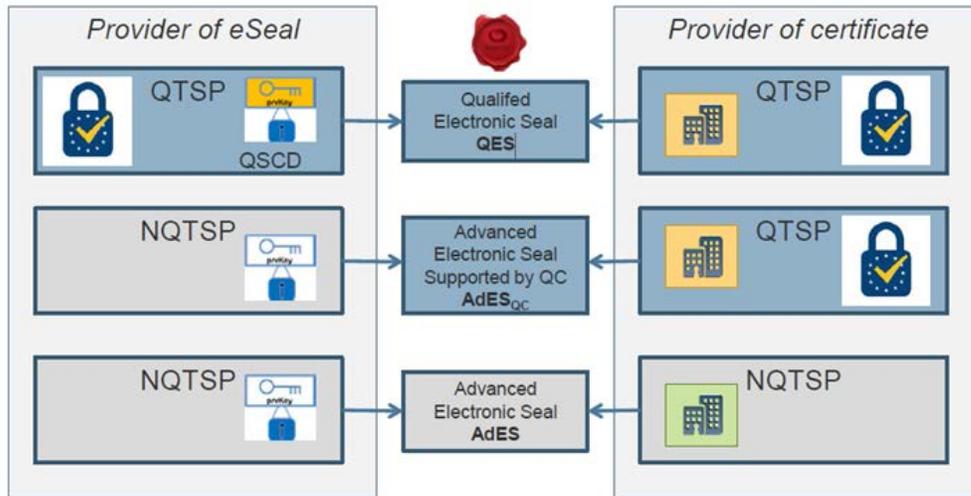


Figure 13 Level of Assurance for eSeals

(The figure above was extracted from (BuyPass, 2016).)

8.2.3.3 International Landscape

Relevant Legal Provisions

SEAL (US)

National and state governments in many jurisdictions have enacted laws governing the use of digital signatures for various types of transactions.

In 1998, the US Congress passed the **Digital Signature and Electronic Authentication Law** (US Government, 2013), which amended the Bank Protection Act (1968) to allow use of digital signatures to facilitate the use of electronic authentication by financial institutions.

Section 6 of the SEAL states the electronic authentication may be used if an agreement to use them was made by all parties.

(a) ELECTRONIC AUTHENTICATION OF DOCUMENTS, INFORMATION, AND IDENTITY-

(1) IN GENERAL- A financial institution may use electronic authentication in the conduct of its business if it has entered into an agreement regarding the use of electronic authentication with any counterparty, or if it has established a banking, financial, or transactional system using electronic authentication.

GPEA

(See also this Act in a former section about *the electronic document*.)

US law regulations)

Document name:	Inventories (2)	Page:	100 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



The Government Paperwork Elimination Act - GPEA, (Bowman, 2003), Pub.L. 105–277 Title XVII- requires that, when practicable, Federal agencies use electronic forms, electronic filing, and electronic signatures to conduct *official business* with the public by 2003. In doing this, agencies will create records with business, legal and, in some cases, historical value. This guidance focuses on records management issues involving records that have been created using electronic signature technology.

Relevant Standards

ISO/IEC 15408

Information technology — Security techniques — Evaluation criteria for IT security, Parts 1 to 3 as listed below:

— ISO/IEC 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1. ISO, 2009.

— ISO/IEC 15408-2:2008 — Information technology — Security techniques — Evaluation criteria for IT security — Part 2. ISO, 2008.

— ISO/IEC 15408-3:2008 — Information technology — Security techniques — Evaluation criteria for IT security — Part 3. ISO, 2008,

ISO/IEC 18045:2008

Information technology — Security techniques — Methodology for IT security evaluation

OASIS DSS Entity Seal Profile

Belonging to the OASIS Digital Signature Services TC.

See also previous section about

OASIS Digital Signature Services TC.

8.2.3.4 Conclusions on Electronic Seals

No trust translation scheme has been found currently, however the European regulations distinguish the following levels of assurance:

- Electronic seal: non-qualified eSeal
- Advanced electronic seal: non-qualified eSeal
- Qualified electronic seal

Other classification would be based on the provider of the certificate, whether it is qualified or not, and on the provider of the seal, whether it is qualified or not.

- Advanced electronic seal (AdES)
- Advanced electronic seal supported by qualified certificate (AdES-qc)

Document name:	Inventories (2)	Page:	101 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- Qualified Electronic Seal

So, four possible levels of assurance have been detected in the European industry:

- Electronic seal
- Advanced electronic seal
- Advanced electronic seal supported by qualified certificate
- Qualified electronic seal

More analysis should be done in a next iteration of this inventory. For example, levels for electronic seals in other parts of the world have not been studied yet in depth to assess potential trust translation scheme with potential levels in the EU.

8.2.4 Electronic Time-stamps

8.2.4.1 Definitions and Concepts

Electronic time-stamps are defined according to eIDAS (European Commission, 2014), Art. 3.

There are many time stamping schemes with different security goals:

- PKI-based – timestamp token is protected using PKI digital signature.
- Linking-based schemes – timestamp is generated such a way that it is related to other timestamps.
- Distributed schemes – timestamp is generated in cooperation of multiple parties.
- Transient key scheme – variant of PKI with short-living signing keys.
- MAC – simple secret key based scheme, found in ANSI ASC X9.95 Standard.
- Database – document hashes are stored in trusted archive; there is online lookup service for verification.
- Hybrid schemes – the linked and signed method is prevailing, see X9.95

Only the PKI covers the 3 of them, the *RFC 3161*, *X9.95* and *ISO/IEC 18014*.

Scheme	RFC 3161	X9.95	ISO/IEC 18014
PKI	✓	✓	✓
Linked		✓	✓
MAC		✓	
Database			✓
Transient key		✓	
Linked and signed		✓	

Figure 14 Trusted Timestamping

Document name:	Inventories (2)	Page:	102 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



8.2.4.2 European Landscape

Relevant Legal Provisions

European Regulation (EU) No 910/2014 (eIDAS)

Qualified time-stamps

Requirements for QTSPs issuing qualified electronic time stamps (referring to Art.42) are these requirements applicable and common to all TSPs, and the following requirements laid down in:

Art.42.1 for qualified electronic time stamps:

- to bind the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
- to be based on an accurate time source linked to Coordinated Universal Time; and
- to be signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method

As of Art.42.2 the Commission may, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. (ENISA, 2016).

EESSI

Regarding with the requirements for QTSPs issuing qualified electronic time stamp:

EESSI Conformity Assessment Guidance - Part 8 - Time-stamping Authority services and processes (CEN CWA 14172-8), Published, Assessment (European Commission, 2016).

EESSI is an IT system that will help social security bodies across the EU exchange information more rapidly and securely – as required by EU regulations on social security coordination. At the moment there is no EU-wide system and most exchanges are still paper-based.

How will it work? All communication between national bodies on cross-border social security files will take place using structured electronic documents. These documents will be routed through the EESSI (hosted centrally by the European Commission) to the correct destination in another EU country. Staff in social security bodies will be able to find the correct destination in another EU country using a directory of national bodies.

ANSSI

From *Agence nationale de la sécurité des systèmes d'information* (ANSSI, 2016) (in English: National Cybersecurity Agency of France), some regulations related to the requirements for QTSPs issuing qualified electronic time stamp are listed:

Document name:	Inventories (2)	Page:	103 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



ANSSI DCSSI-PP 2008/07: Time-stamping System (CC3.1), Published, TST trustworthy product. It is currently the only evaluated Common Criteria protection profile for a timestamping system.

ANSSI RGS A5: Politique d'Horodatage Type, Published, Assessment (ANSSI, 2012)

Relevant Standards

prCEN/EN 419 231

Protection Profile (PP) for trustworthy systems supporting time stamping. This is a new standard by ETSI that is under approval.

ETSI EN 319 42x

There is a set of ETSI standards related to Electronic Signatures and Infrastructures (ESI) generating trusted time-stamps.

(See M460-Overview of standards-Dec2014.pdf at (European Commission, 2016), (European Commission, 2009))

ETSI EN 319 421 V1.1.1 (ETSI, 2016)

Policy & security requirements for trust service providers issuing time-stamps (replacing Policy requirements for time-stamping authorities ETSI TS 102 023) TS: July 2015 -EN: March 2016. Assessment, trustworthy systems, time management.

ETSI EN 319 422 V1.1.0 (ETSI, 2016)

Time-stamping protocol and time-stamp token profiles ETSI EN 319 422 (**replacing TS 101 861**) TS: July 2015 - EN: March. Assessment, trustworthy systems.

ETSI EN 319 423

Conformity assessment for TSPs providing time-stamping services

Other European standards related to trust time-stamping

Following, other standards related to trust time-stamping are collected:

ETSI TS 119 401/EN 319 401 (ETSI, 2012)

General Policy Requirements for Trust Service Providers.

ETSI TS 101 861 V1.4.1 (ETSI, 2007)

Electronic Signatures and Infrastructures (ESI); Time stamping profile

Document name:	Inventories (2)	Page:	104 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Abstract: A Time Stamp Protocol (TSP) has been defined by the IETF. The present document limits the number of options by placing some additional constraints.

Scope: The present document is based on the Time Stamp Protocol (TSP) from RFC 3161 (IETF, 2001) including optional ESSCertIDv2 update in RFC 5816 (IETF, 2010). It defines what a Time Stamping client must support and what a Time Stamping Server must support.

ETSI TS 102 023 V1.2.2 (ETSI, 2008) *Replaced by EN 319 421-422 under the M460!*

Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities

Scope: The present document specifies policy requirements relating to the operation of Time-stamping Authorities (TSAs). The present document defines policy requirements on the operation and management practices of TSAs such that subscribers and relying parties may have confidence in the operation of the time-stamping services.

8.2.4.3 International Landscape

Relevant Standards

There are three main protocols related to trusted time-stamps:

IETF RFC 3161 Time Stamp Protocol

August 2001

*Internet X.509 Public Key Infrastructure
Time-Stamp Protocol (TSP)*

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

According to the RFC 3161 (IETF, 2001) Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), a **trusted timestamp** is a timestamp issued by a trusted third party (TTP) acting as a Time Stamping Authority (TSA). It is used to prove the existence of certain data before a certain point (e.g. contracts, research data, medical records, etc.) without the possibility that the owner can backdate the timestamps. Multiple TSAs can be used to increase reliability and reduce vulnerability.

IETF RFC 3628

Policy Requirements for Time-Stamping Authorities (IETF, 2003)

Document name:	Inventories (2)	Page:	105 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Policy Requirements for Time-Stamping Authorities (TSAs)

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This document defines requirements for a baseline time-stamp policy for Time-Stamping Authorities (TSAs) issuing time-stamp tokens, supported by public key certificates, with an accuracy of one second or better. A TSA may define its own policy which enhances the policy defined in this document. Such a policy shall incorporate or further constrain the requirements identified in this document.

ANSI ASC X9.95

The newer ANSI ASC X9.95 Standard for **Trusted Time Stamps** (ANSI, 2016), (ANSI, 2005), augments the RFC 3161 standard with data-level security requirements to ensure data integrity against a reliable time source that is provable to any third party. This standard has been applied to authenticating digitally signed data for regulatory compliance, financial transactions, and legal evidence.

This standard specifies the minimum security requirements for the effective use of time stamps in a financial services environment. Within the scope of this Standard the following topics are addressed: Requirements for the secure management of the time stamp token across its life cycle, comprised of the generation, transmission and storage, validation, and renewal processes. The requirements in this Standard identify the means to securely and verifiably distribute time from a national time source down to the application level; Requirements for the secure management of a Time Stamp Authority (TSA); Requirements of a TSA to ensure that an independent third party can audit and validate the controls over the use of a time stamp process; Techniques for the coding, encapsulation, transmission, storage, integrity and privacy protection of time stamp data; Usage of time stamp technology.

ISO on trust time-stamping

Some ISO standards could be analysed for trust time-stamping:

ISO/IEC 18014

ISO/IEC 18014 (2009) Information technology — Security techniques — Time-stamping services. (ISO, 2013)

It is an international standard that specifies time-stamping techniques. It comprises three parts:

- Part 1: Framework

Document name:	Inventories (2)	Page:	106 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- Part 2: Mechanisms producing independent tokens
- Part 3: Mechanisms producing linked tokens

ISO/IEC 18014-3:2004 describes time-stamping services producing *linked tokens*, that is, tokens that are cryptographically bound to other tokens produced by these time-stamping services. It describes a general model for time-stamping services of this type and the basic components used to construct a time-stamping service of this type, it defines the data structures and protocols used to interact with a time-stamping service of this type, and it describes specific instances of such time-stamping services.

ISO 8601:2004

Data elements and interchange formats – Information interchange – Representation of dates and times is an international standard covering the exchange of date and time-related data. (ISO, 2016)

ISO 7498-2

Information processing systems — Open Systems Interconnection— Basic Reference Model— Part 2: Security Architecture (ISO, 2016)

ITU X509

In cryptography, X.509 (ITU, 2016) is an important standard for a public key infrastructure (PKI) to manage digital certificates and public-key encryption and a key part of the Transport Layer Security protocol used to secure web and email communication. An ITU-T standard, X.509 specifies formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

OASIS DSS XML Timestamping Profile

Belonging to the OASIS Digital Signature Services TC (OASIS, 2007), (OASIS, 2016).

More initiatives on time-stamping authority

TrueTimeStamp.org: Open and free time-stamping authority utilizing linked time-stamps, trusted certificates, and an online database of timestamps. (Radiology Universe Institute, 2015)

OriginStamp.org: Anonymous and free trusted time-stamping service utilizing the Bitcoin blockchain for timestamp storage and verification. (Gipp & Gernandt, 2014)

Decentralized Trusted Timestamping (DTT) using the Crypto Currency Bitcoin: This paper presents a trusted time-stamping concept and its implementation in form of a web-based service that uses the decentralized Bitcoin block chain to store anonymous, tamper-proof timestamps for digital content. The service allows users to hash files, such as text, photos or videos, and store the created hashes in the Bitcoin block chain. Users can then retrieve and verify the timestamps that have been committed to the block chain. The non-commercial service enables anyone, e.g.,

Document name:	Inventories (2)	Page:	107 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



researchers, authors, journalists, students, or artists, to prove that they were in possession of certain information at a given point in time. (Gipp, et al., 2015)

Analysis of a Secure Time Stamp Device: This paper discusses the design of a Secure Time Stamp device used to securely timestamp digital data, such as computer documents, files, and raw binary data of arbitrary format. Thus, the device is used to prove two facts: Existence: That a file existed on a given date & time and Data Integrity: That the file was not altered since the time it was stamped. (SANS Institute Reading Room, 2001)

FreeTSA: Free Time-Stamping Authority using the RFC 3161 Protocol. (busilezas, 2015)

8.2.4.4 Conclusions on Electronic Timestamp

No trust translation scheme has been found currently, however the European regulations distinguish the following levels of assurance:

- Electronic time-stamp: non-qualified time-stamp
- Qualified time-stamp

International standards define trusted and non-trusted time-stamps.

More analysis should be done in a next iteration of this inventory in particular on electronic time-stamps in other parts of the world to assess how they can be mapped in terms of levels of trust to qualified / non-qualified time-stamps defined in eIDAS Regulation.

8.2.5 Electronic Registered Delivery Services

8.2.5.1 Definitions and Concepts

eDelivery

Infrastructure for the transfer of documents (or data) between two entities or systems electronically. (European Commission, 2016)

The infrastructure provides for safe and traceable transfer of information. It can also include additional services such as acknowledgement of receipt. In collaboration with DIGIT (European Commission's Directorate-General for Informatics) with the financial support from CEF (Connecting Europe Facility), the Commission is launching an eDelivery cross border service reusable in multiple contexts. The eDelivery building block (Digital Service Infrastructure) helps public administrations to exchange electronic data and documents with other public administrations, businesses and citizens, in an interoperable, secure, reliable and trusted way. Through the use of this building block, every participant becomes a node in the network using standard transport protocols and security policies. eDelivery is based on a distributed model, allowing direct communication between participants without the need to set up bilateral channels.

Several models are enabled:

Document name:	Inventories (2)	Page:	108 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- Administration communication (A2A) to ensure that Public Administrations can exchange any type of data and documents across borders and contributing to the creation of an EU single market which is fit for the digital age.
- eDelivery can also be used in Administration to Business (A2B) and Business to Administration (B2A) scenarios as proven by the PEPPOL implementation of eDelivery in the eProcurement domain.
- When behind a web-portal, eDelivery can also enable the interconnection of Public Administrations with Citizens (A2C and C2A). For example, eDelivery enables the eJustice portal to talk with other information systems. The latter shows that the communication between Citizens (C2C) is out of scope of eDelivery building block (but private eDelivery services may target this segment).

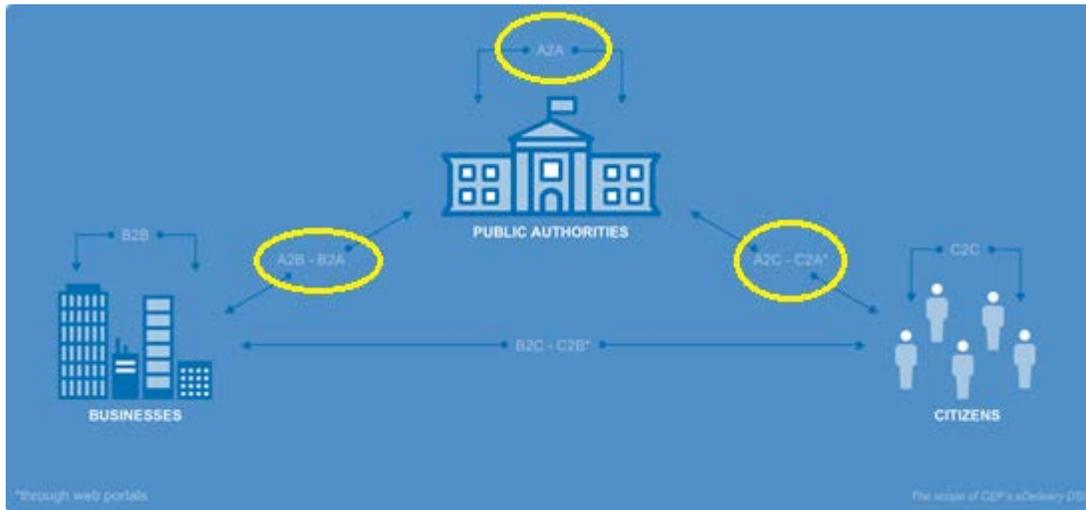


Figure 15 eDelivery Building Block Scope

The figure above has been taken from (European Commission, 2016). The *Building Block* only covers use cases with an 'A' component (so no B2B, C2C, or B2C). This is in fact the main differences between the eDelivery Building Block (which has only 'A' component use cases) and the registered delivery service as defined in eIDAS (which has no restriction and can cover all use cases, including those without any administration).

Electronic Registered Delivery Services are defined according to eIDAS (European Commission, 2014), Art. 3.

8.2.5.2 European Landscape

Relevant Legal Provisions

European Regulation (EU) No 910/2014 (eIDAS)

In the Article 44, the requirements for qualified electronic registered delivery services are detailed.

Document name:	Inventories (2)	Page:	109 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



In relation to the requirements for QTSPs providing qualified electronic registered delivery service (referring to Art.44) are these requirements applicable to all TSPs, these requirements common to all QTSPs, and the following requirements laid down in:

- Art.44.1 on the definition of the qualified electronic registered delivery service which may be offered by one or more QTSP.

As of Art.44.2 the Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data.

In Article 43 the legal effect of an electronic registered delivery service is established:

(1.) Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.

(2.) "Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service."

Furthermore Article 46 establishes the legal effects of electronic documents:

(1.) "An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form."

eDelivery supports this fundamental principle of the Digital age by promoting the alignment between its technical specifications and the eIDAS regulatory framework.

CEF Digital

The CEF eDelivery building block can be found at (European Commission, 2016) and a summary of this building block is provided at (European Commission, 2016)

More details on its architecture, interoperability and technical specifications can be found at (European Commission, 2016), (European Commission, 2016).

An overview of eDelivery benefits and goals can be found at (European Commission, 2016), (European Commission, 2016).

The Large Scale Pilots that were sponsored by the ICT Policy Support Programme (ICT PSP) to pilot eDelivery in several policy domains are introduced here (European Commission, 2016).

The conformant services and software related to eDelivery CEF DSI are also available:

- Self-assessment tool (European Commission, 2016)
- Access Point software (European Commission, 2016)

Document name:	Inventories (2)	Page:	110 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- SML software (European Commission, 2016)
- SML service (European Commission, 2016)
- SMP software (European Commission, 2016)
- PKI service (European Commission, 2016)

Testing services for eDelivery are conformance testing (European Commission, 2016), and connectivity testing (European Commission, 2016).

Relevant Standards

ETSI SR 019 530

Study on standardisation requirements for e-delivery services applying e-signatures (30.4.2014) (ETSI, 2014).

ETSI/CEN Framework for Standardisation

Trust application service providers: covering trust service providers offering value added services applying digital signatures and that relies on the generation/validation of electronic signatures in normal operation. This includes namely registered mail and other e-delivery services, as well as data preservation (long term archiving) services.

SR 019 050 provided a proposal for a rationalized framework of standards for electronic registered delivery services, as defined by the eIDAS Regulation 2014/910/EU; the current structure of the framework documents covering these services is the one published in TR 119 000. (ETSI, 2015), (ETSI, 2015).

ETSI/CEN for trust application service providers

EN 319 521 Policy & security requirements for electronic registered delivery service providers(new). Undefined date.

Policy & security requirements for registered electronic mail (REM) service providers (replaces TS 102 640). Undefined date.

ETSI/CEN for Technical specifications

EN 319 522 Electronic registered delivery services: - Part 1: Framework and architecture - Part 2: Semantic contents - Part 3: Formats - Part 4: Bindings. (new). Undefined date.

EN 319 532 Registered electronic mail (REM) services: - Part 1: Framework and architecture - Part 2: Semantic contents - Part 3: Formats - Part 4: Interoperability profiles (replaces TS 102 640). Undefined date.

ETSI/CEN for Testing Conformance & Interoperability

TS 119 504 General requirements for technical conformance and interoperability testing for trust application service providers and the services they provide. Undefined date.

Document name:	Inventories (2)	Page:	111 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



TS 119 524 Testing conformance and interoperability of electronic registered delivery services: - Part 1: Testing conformance - Part 2: Test suites for interoperability testing of electronic registered delivery service providers. Replaces TR 103 071. Undefined date.

TS 119 534 Testing conformance & interoperability of registered electronic mail services. Undefined date.

- Part 1: Testing conformance

- Part 2: Test suites for interoperability testing of providers using same format and transport protocols

- Part 3: Test suites for interoperability testing of providers using different format and transport protocols.

TS 102 640 series

The standardisation work on electronic registered delivery services will leverage on the existing multipart *TS 102 640* series addressing standardisation of registered electronic mail (REM) and align these specifications to the requirements of Regulation (EU) No 910/2014 on electronic registered delivery services. Effective production of such REM specifications and more general specifications addressing all other types of electronic registered delivery services has not been planned yet and is likely **not to be finalised in 2016**.

Part 1: Architecture (ETSI, 2010)

Part 6: Interoperability profiles (ETSI, 2011)

Part 2: Data requirements, Formats and Signatures for REM (ETSI, 2010)

Part 3: Part 3: Information Security Policy Requirements for REM Management Domains (ETSI, 2010)

Part 4: REM-MD Conformance Profiles (ETSI, 2010)

ETSI for the QTSP providing electronic registered delivery service

ETSI EN 319 511: Policy and security requirements for registered electronic mail (REM) service providers

ETSI EN 319 512: Registered electronic mail (REM) services

ETSI TS 119 514: Testing compliance and interoperability of REM service providers

ETSI EN 419 221, parts 1-5: Protection profiles for TSP Cryptographic modules. (DIN, 2016)

ETSI EN 419 241, parts 1-3: Security requirements for trustworthy systems supporting server signing (signature generation services)

Document name:	Inventories (2)	Page:	112 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Other Initiatives

e-SENS

Electronic Simple European Networked Services (e-SENS) is a large-scale project to provide an easy access to public European administration and services online, and ensure interoperability across different national systems. eDelivery results from several European Large Scale Pilot projects are part of this initiative:

- **SPOCS** (Simple Procedures Online for Cross-Border Services) uses the solution for the cross border use of natural persons eID developed by STORK. Furthermore it also builds on document transport concepts developed by STORK. It has used the Virtual Company Dossier (VCD) concept of *PEPPOL* for document containers and has generalized it into a container format for eDocuments (OCD) to package company information for transmission to Points of Single Contact in other countries. (SPOCS, 2012)
- **e-CODEX** (e-Justice Communication via Online Data Exchange) will build on and make necessary changes to deliverables from SPOCS and the other pilots in order to meet its objectives of improving the cross-border access of citizens and businesses to legal means in Europe as well as to improve the interoperability between legal authorities within the EU. (e-codex, 2016)
- **PEPPOL** (Pan-European Public Procurement Online) has developed and implemented technology standards for European governmental public electronic procurement. (PEPPOL, 2016)

8.2.5.3 International Landscape

Relevant Legal Provisions

US law

Digital Distribution is a distribution method in which content is delivered without the use of physical media, normally by downloading from the internet straight to a consumer's home. Digital distribution overrides conventional physical distribution methods, like paper or DVDs. A consumer can log on to an approved website that offers preview samples, singles or full albums online for download. It is transferred from the internet web server to the individual user's computer hard drive. Distribution programs are being improved to offer more secure on-line transactions, consumer licensing, and anti-piracy measures. (US Legal Inc., 2016)

The **Digital Millennium Copyright Act** (DMCA) is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures (commonly known as digital rights management or DRM) that control access to copyrighted works. It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet (US government, 1998).

Document name:	Inventories (2)	Page:	113 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Canadian law

Some laws could be interesting:

Bill C-60, 38th Canadian Parliament, first Session: (Canadian Government, 2005)

Bill C-61, 39th Canadian Parliament, second Session: (Canadian Government, 2006)

Bill C-32, 40th Canadian Parliament, third Session: (Canadian Government, 2010)

Digital Economy Act 2010 (United Kingdom)

The Digital Economy Act 2010 (c. 24) is an Act of the Parliament of the United Kingdom. The act addresses media policy issues related to digital media, including copyright infringement, Internet domain names, Channel 4 media content, local radio and video games. Introduced to Parliament by Lord Mandelson on 20 November 2009, it received Royal Assent on 8 April 2010. It came into force two months later, with some exceptions: several sections - 5, 6, 7, 15, 16(1) and 30 to 32 - came into force immediately, whilst others required a Statutory Instrument before they would come into force. However some provisions have never come into force since the required statutory instruments were never passed by Parliament and considered to be "shelved" by 2014, and other sections were repealed. (UK Government, 2010)

DADVSI (France)

DADVSI (generally pronounced as dadsi) is the abbreviation of the French *Loi sur le Droit d'Auteur et les Droits Voisins dans la Société de l'Information* (in English: "law on authors' rights and related rights in the information society"). It is a bill reforming French copyright law, mostly in order to implement the 2001 European directive on copyright (known as EUCD), which in turn implements a 1996 WIPO treaty. (French Government, 2006)

Most of the bill focused on the exchange of copyrighted works over peer-to-peer networks and the criminalizing of the circumvention of digital rights management (DRM) protection measures. Other sections dealt with other matters related to copyright, including rights on resale of works of art, copyright for works produced by government employees and exceptions to copyright for education and the handicapped, among other issues.

Relevant Standards

Universal Postal Union (UPU)

The delivery of services, whether electronic or not, is one of the key goals of the UPU, the Universal Postal Union (**UPU**), which is the second oldest international organization worldwide.

The UPU has developed some standards regarding interoperability aspects, the registered electronic mail, in collaboration with CEN, etc. (UPU, 2016), (Universal Postal Union, 2016)

S33 Interoperability framework for postal public key infrastructures

Document name:	Inventories (2)	Page:	114 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



The objective of this standard is to create a common Postal Public Key Infrastructure (PKI) to provide global certification and security services aimed at globally binding the identity of individuals and organisations with their public key. The framework itself and its first four elements (PKI structure, cryptographic algorithms, data formats and data dissemination protocols) are included.

S52 Functional specification for postal registered electronic mail

This standard defines the functional specification of a secure electronic postal service, referred to as the postal registered electronic mail or PReM service. PReM provides a trusted and certified electronic mail exchange between mailer, designated operators and addressee/mailee. In addition, evidence of corresponding events and operations within the scope of PReM will be generated and archived for future attestation.

xDTM (no standard yet)

In the U.S., the xDTM Standard Association (an independent non-profit organization) is on its way to define and advance requirements (the xDTM Standard), and create the framework for an associated certification program to ensure open, secure digital transactions. In the same spirit as the e-IDAS Regulation, the xDTM self-defined objective is to define an interoperable and widely accepted standard. The term Digital Transaction Management (DTM) denotes a category of cloud services that would enable companies to manage their document-based transactions digitally with the same legal value and acknowledgement as they have with paper-based transactions. (xDTM Standard Association, 2016)

First experiments with digital signatures in the U.S. were originated in the pharmaceutical industry and have achieved some success in that domain.

The xDTM Association has not yet released any standard

NIST SP 800-177

SP 800-177 – Computer security – trustworthy email

8.2.5.4 Conclusions on Electronic Registered Delivery Services

No trust translation scheme has been found currently, however the European regulations distinguish the following levels of assurance:

- Electronic registered delivery service: non-qualified electronic registered delivery service
- Qualified electronic registered delivery services

Following has been taken the analysis of the requirements for QTSPs providing qualified electronic registered delivery service (eIDAS Art.44), against some international standards (DLA Piper; PriceWaterhouseCoopers; SEALed; SGA; TimeLex, 2013):

Document name:	Inventories (2)	Page:	115 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Article 44 of the eIDAS Regulation requires the following on qualified electronic registered delivery services:

(a) they are provided by one or more qualified trust service provider(s);

ETSI TS 102 640 : That point is not addressed in the standards. Moreover, REM systems may forward messages to "regular e-mail" services, hence "unqualified" services providers.

UPU : That point is not addressed in the standards. In particular, issues regarding "cross-border scenarios" are explicitly not covered.

(b) they ensure with a high-level of confidence the identification of the sender;

ETSI/CEN TS 102 640 : In the standards, "choice of the authentication mechanism is left to the [trust service provider]". Specific requirements must hence be added to correctly reflect these of the eIDAS Regulation.

UPU : Same situation ("The act of physically authenticating individual calls to a SePS is outside the scope of this specification").

(c) they ensure the identification of the addressee before the delivery of the data;

ETSI/CEN TS 102 640 : That point is covered in the functional working of the protocol.

UPU : idem.

(d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;

ETSI/CEN TS 102 640 : the standards only "assume the usage of at least an Advanced Electronic Signature [...] issued with a Secure Signature Creation Device", in the sense of the EU Directive 1999/93/EC. Hence, this standard does not require such a signature, strictly speaking.

UPU : The standards contain no requirement on the level of the signatures.

(e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;

ETSI/CEN TS 102 640 : That point is not addressed in the standards.

UPU : idem.

However, that point could be deemed inapplicable to these standards, which do not consider that one could alter the sent data in any way.

Document name:	Inventories (2)	Page:	116 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



(f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.

ETSI/CEN TS 102 640 : That point is not addressed in the standards.

UPU : The electronic PostMark is a "superset of a standard timestamp", and several European post services are already providing ETSI 102 023-certified services. More analysis should be done in a next iteration of this inventory.

Summary:

Overall, the existing standards are technical and were written before any existing regulation. It is not surprising, then, that they do not try to strongly enforce specific properties. In particular, they contain very few strict requirements on the services.

Future ETSI standardisation work on electronic registered delivery services will leverage on the existing multipart TS 102 640 series addressing standardisation of registered electronic mail (REM) and align these specifications to the requirements of Regulation (EU) No 910/2014 on electronic registered delivery services. Effective production of such REM specifications and more general specifications addressing all other types of electronic registered delivery services has not been planned yet and is likely not to be finalised in 2016.

The standards could be used as a basis for a technical definition of the qualified electronic registered delivery services, under additional requirements (service profiles) covering the above elements. For instance, the requirement that sent data must be signed/sealed according to (d).

8.2.6 Electronic Website Authentication

8.2.6.1 Definitions and Concepts

Website authentication

Trusted information on a website (e.g. a certificate) which allows users to verify the authenticity of the website and its link to the entity/person behind the website. (European Commission, 2016)

Electronic Website Authentication is defined according to eIDAS, Art. 3. (European Commission, 2014)

Since the market is leading mature solutions related to this trust service, some concepts are now presented, coming from the real world: (Qualified Website Authentication Certificates have been taken from (ENISA, 2016).

Stakeholders on website authentication (creation, verification and validation of certificates related to them)

- Trust service providers (TSPs) issuing website authentication certificates, commonly known as *Certificate Authorities* (CAs).

Document name:	Inventories (2)	Page:	117 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- The *owners of websites* play a critical role in the market for website authentication certificates as primary consumers.
- *Web browsers* also perform critical tasks in the chain of trust that website authentication certificates create between users and online content. They help determine the trustworthiness of trust service providers. The five most widely used web browsers all contain strictly moderated and monitored lists of root TSPs, which must follow a set of guidelines in order to prove the identity of intermediary TSPs and certificates they authorise and to ensure security is maintained within the system. After a root TSP is designated *trustworthy*, browsers can automate a number of security decisions, while at the same time indicating the level of security to users via their interface⁶, with visual cues such as a green padlock icon.
- The '*end-user*' refers to natural persons (including citizens, residents and consumers), and legal entities (including businesses, non-profit organizations, and governmental agencies and institutions) that *access an online service which employs a website authentication certificate*.

Two main classifications can be established regarding types of commercial certificates, based (i) on the verification procedure of the applicant's data and (ii) on the number of domains/servers the certificate is intended to secure.

Classification according to the data validation level

When a trust service provider issues a website authentication certificate, it is acting as an independent trusted third party; performing the authentication of the applicant, as well as the verification of the certificate data. The effort taken for the proper authentication and data verification usually is reflected in the quality level of the certificate (as well as in the price for the customer). According to this parameter, a common terminology has been adopted in the market to differentiate the types of website authentication certificates:

- **Domain Validated (DV)**: This is an entry-level type certificate with a low level of trust. The only procedural check that is made by the issuing TSP is that the prospective owner of the certificate actually owns the domain that it will authenticate. DV certificates are available nowadays at a very low price or even for free. There are no checks that the owner organisation is a valid business entity or any other validation of the owner organisation.
- **Organization Validated (OV)**: Also called 'subject identity validated' or 'fully authenticated'. This certificate has detailed validation checks performed by the issuing TSP that the prospective owner of the certificate is a registered legal entity, registration is valid, it is the owner of the domain, which it will authenticate, and indeed that the applicant has the authority to apply for such a certificate.
- **Extended Validation (EV)**: This certificate includes additional information on the owner of the certificate, and additional checks are made by the issuing TSP to ensure that the owner of the domain which it will authenticate, is validated, and that the applicant has indeed the authority to apply for such a certificate. Overall, these aspects are validated

Document name:	Inventories (2)	Page:	118 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



(the issuance process of EV SSL Certificates is strictly defined in the EV Guidelines, as formally ratified by the CA/Browser forum in 2007):

- The legal, physical and operational existence of the entity
- The identity of the entity matches official records
- The entity has exclusive right to use the domain specified in the EV certificate
- The entity has properly authorized the issuance of the EV certificate

When consumers visit a website secured with an Extended Validation certificate, the address bar at the top of the browser becomes green and details of the genuine owner of the website and the certificate provider are shown. This works on many of the commonly available browsers.

Finally, it should be noted that some certificates, meant to be used internally within private networks, are not issued by publicly trusted third party providers. These *self-signed website authentication certificates* are created and signed internally by an organisation and are not trusted outside of that organisation network. They do not hold the same weight as a publicly trusted certificate created by a trust service provider, and may or may not conform to some form of certificate policy. Self-signed certificates are not meant to be used publicly, as there is no third party who can attest to the veracity of the information contained in the certificate, therefore they should be created for strict internal use only.

Classification according to the number of domains secured

Another distinction that can be made among types of website authentication certificates relates to the number of domains that are secured by the certificate:

- **Single domain:** Single domain certificates are used to secure a single domain. They are the most adequate for small organizations. Single domain certificates are available as Domain Validated, Organization Validated or as Extended Validation.
- **Wildcard:** Wildcard certificates (e.g. issued to *.example.com) are used to secure an unlimited number of first level subdomains in a single domain. Subdomains added subsequently will automatically be secured. This adds flexibility to customers, however it can introduce some security risks. Wildcard certificates are available as Domain Validated or as Organization Validated, but not as Extended Validation.
- **Multi Domain:** Multi Domain certificates are used to secure multiple domain names or servers across multiple domains in one certificate. They are the most adequate for large organizations and usually allow typically up to 100 domains to be included in one certificate. Multi domain certificates are available as Domain Validated, Organization Validated or as Extended Validation.

The next figure shows a cross-classification of possible combinations of commercial types of certificates based on both kind of attributes, identity validation and number of domains.

Document name:	Inventories (2)	Page:	119 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



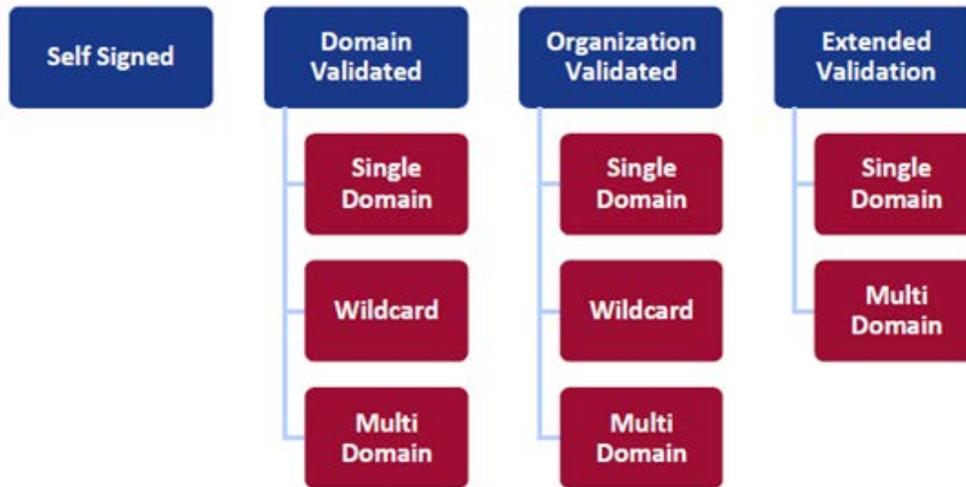


Figure 16 Classification of existing types of commercial WACs

(The figure above has been extracted from (ENISA, 2016).)

8.2.6.2 European Landscape

Relevant Legal Provisions

European Regulation (EU) No 910/2014 (eIDAS)

Qualified certificates for website authentication (QWAC) present a particular case among the new trust services defined in the eIDAS Regulation. They will need to enter in an already mature, global and unregulated market.

Art.45(2) - reference numbers of standards for *qualified certificates for website authentication*:

- It sets the requirements to fulfill but does not establish how it must technically and operationally be implemented by trust service providers. In light of the above, the minimum requirements for QWAC certificates are defined in Article 45 and annex IV of the Regulation.
- Article 45 sets the requirement for trust service providers issuing qualified website authentication certificates of being qualified, which implies that all requirements for QSTPs described in the previous section will be applicable.
- Annex IV defines the content of qualified certificates for website authentication.

Regarding with the requirements for QTSPs issuing *qualified certificates*:

- Contents of qualified certificates:
 - Annex III for qualified certificate for electronic seals (Art.38.1)

Document name:	Inventories (2)	Page:	120 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



- May include non-mandatory attributes, not affecting interoperability or recognition (Art.28.3, Art. 38.3, also applying to QC for WSA when special case of QC for electronic seals – Recital (65))
- Revocation of qualified certificates is definitive (Art.28.4, Art. 38.4, also applying to QC for WSA when special case of QC for electronic seals – Recital (65))
- Temporary suspension of QC for electronic seals and for electronic signatures may be specified on a national basis (Art.28.5, Art.38.5)

Relevant Standards

ETSI EN 319 4xx

ETSI has released four public drafts of standards relevant to QWAC certificates, which are **under the process of approval**: (taken from ETSI Certification Authorities and other Trust Service Providers portal (ENISA, 2016))

EN 319 401 General Policy Requirements for Trust Service Providers (ETSI, 2015)

EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements (ETSI, 2015).

The Extended Validation Certificate Policy (mentioned as a base for the qualified website authentication certificate policy), is defined in the standard EN 319 411-1, which concerns all TSPs issuing public certificates. The EVCP is a policy for “TLS/SSL/TLS certificates offering the level of assurance required by CA/Browser Forum for EVC. The requirements for this certificate policy are built on the normalized policy requirements for the issuance and management of Normalized Certificate Policy certificates, enhanced to refer to requirements from Extended Validation guidelines.”

EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. Note: Extends requirements in part 1 with specific requirements for EU qualified certificates (ETSI, 2016).

This standard, which sets requirements for trust service providers issuing EU qualified certificates, states as its objective, in what concerns qualified website authentication certificates, to define “A policy for EU qualified web certificate offering the level of quality defined in Regulation (EU) N° 910/2014 for EU qualified certificates (requiring or not the use of a secure cryptographic device) used in support of web authentication. The requirements for this certificate policy include all the Extended Validation certificate policy (EVCP) requirements, plus additional provisions suited to support EU qualified certificates issuance and management as specified in Regulation (EU) N° 910/2014.”

EN 319 412-4: Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organizations (ETSI, 2015).

Document name:	Inventories (2)	Page:	121 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



8.2.6.3 International Landscape

Relevant Standards

CA/Browser Forum Extended Validation (EV) Guidelines

The most relevant, market-led, harmonization activities in the area of website authentication certificates have been conducted by the CA/Browser Forum, a voluntary consortium which groups more than fifty TSPs and browsers, among them the largest market players.

Organized in 2005, it is a voluntary group of certification authorities (CAs), vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS and code signing. It was created to provide greater assurance to Internet users about the web sites they visit by leveraging the capabilities of SSL/TLS certificates.

The CA/Browser Forum began as part of an effort among certification authorities and browser software vendors to provide greater assurance to Internet users about the web sites they visit by leveraging the capabilities of SSL/TLS certificates. In June 2007, the CA/Browser Forum adopted version 1.0 of the **Extended Validation (EV) Guidelines**. EV certificates are issued after extended steps to verify the identity of the entity behind the domain receiving the certificate. Internet browser software displays enhanced indication of that identity by changing the appearance of its display (i.e. colors, icons, animation, and/or additional website information).

Currently the CA/Browser Forum continues work on Internet security issues such as the distribution of digitally signed code, revocation/certificate-validity checking, the domain name system, and other issues of common interest to CAs, Internet software providers, website owners, and Internet users. (CABForum, 2016)

8.2.6.4 Conclusions on Website Authentication

No trust translation scheme has been found currently, however the European regulations distinguish the following levels of assurance:

- Electronic certificate: non-qualified certificate
- Qualified certificate

There is a lack of standards related to requirements for QCs for website authentication: they are under development. However there are some initiatives (like CabForum's EV Guidelines):

EV certificate

highest level of identity assurance
identity – legal entity of site owner

OV certificate

medium level of identity assurance
identity – domain and site owner

DV certificate

lowest level of identity assurance

Document name:	Inventories (2)	Page:	122 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



identity – domain only

Single domain, multiple domain, and wildcard (less used).

When we try to compare to the different types of certificates, the rationale is that QWAC certificates are meant to be high quality certificates, and therefore should have comparable requirements to high quality types. As described before, the most relevant criterion for the classification of website authentication certificates concerns the level of validation of identity of the certificate requester.

A series of standards are being prepared to facilitate compliance of QTSPs with the eIDAS Regulation. These standards are following an approach of achieving compatibility of QWAC certificates with EV certificates, easing for QTSPs to be compliant with both schemes. The goal is that issuers of QWAC certificates that comply with the ETSI standard EN 319 411-2, will also be compliant with EV guidelines requirements.

Partial coverage

The CAB Forum documents are an industrial standard on the Internet, used by all the mainstream web browsers, but their requirements, which aim at strongly ensuring a site's identity and that of its owner, do not fully match these of a « qualified certificate for website authentication », as defined in the eIDAS Regulation.

ETSI EN 319 412-4 (“Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates”) is an expected candidate for referencing by Art.45(2).

8.2.7 Other trust translation schemes

All the above paragraphs in this section 8.2 Industry Perspective, are referred to trust schemes based on authority regulations. The current section is related to **trust schemes based on reputation**, where we present some trust frameworks which are not necessarily based on compliance with legal norms and standards but also on reputation-based approaches.

It is important to notice which the criteria to assign levels of trust within a trust framework are. The community of interest defines the terms and conditions of the multiparty contract that instantiates the legal, technical and business interoperability requirements of participating organizations.

There is a critical necessity for trust translation to be clearly articulated within a framework in order to insure technical interoperability, assign liabilities and promote adoption among participants and other stakeholders. The necessity for trust translation between trusts frameworks are determined by the communities of interest.

Transparency drives trust and that transparency is provided by the registration of a frameworks business, legal and technical requirements and its availability to all stakeholders.

Document name:	Inventories (2)	Page:	123 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



8.2.7.1 OIXnet

OIXnet is a registry (OIXnet, 2016). It is an official online and publicly-accessible repository of documents and information relating to identity systems and identity system participants. Referred to as a “registry”, it functions as an official and centralized source of such documents and information, much like a government-operated recorder of deeds. That is, individuals and entities can register documents and information with the OIXnet Registry to provide notice of their contents to the public, and members of the public seeking access to such documents or information can go to that single authoritative location to find them.

The aim is the development of a centralized global registry of trust frameworks at OIXnet.org.

More information on OIXnet can be read in section 4.2 in the current document.

Minors Trust Framework
Mydex Trust Framework
NATE Blue Button for Consumers (NBB4C) Trust Bundle
OpenID Certification Program
Respect Trust Framework
SAFE-BioPharma Bridge Certification Authority (PKI Bridge CA)
SAFE-BioPharma FICAM Trust Framework Provider Program
SAFE-BioPharma Global Trust Framework Program
SecureKey Concierge
tScheme

Figure 17 Available registries in OIXnet

(The above figure has been taken from (OIXnet, 2016).)

Documentation on how a variety of trust frameworks develop and require trust translation can be found in Open Identity Exchange White Papers (OIX, 2016). A new paper on Trust Frameworks is expecting by March (during the first LIGHTest technical meeting).

8.2.7.1 OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) Committee

The OASIS Trust Elevation TC (OASIS, 2017) works to define a set of standardized protocols that service providers may use to elevate the trust in an electronic identity credential presented to them for authentication. The Trust Elevation TC is intended to respond to suggestions from the public sector, including the U.S. National Strategy for Trusted Identities in Cyberspace (NSTIC). The Trust Elevation TC promotes interoperability among multiple identity providers--

Document name:	Inventories (2)	Page:	124 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



and among multiple identity federations and frameworks--by facilitating clear communication about common and comparable operations to present, evaluate and apply identity [data/assertions] to sets of declared authorization levels.

The Trust Elevation Technical Committee will identify methods being used currently to authenticate electronic identities by online relying parties and service providers, and similar methods in development or identified in theoretical models. By comparison and factoring of those methods, the TC will propose and describe a set of standardized protocols that service providers may use to elevate the trust in an electronic identity credential presented to them for authentication, at levels of identity assurance or risk mitigation, representing increasing degrees of authentication certainty.

The Trust Elevation TC will collect information on trust elevation techniques, or risk mitigation techniques, being standardized, marketed and implemented in the public or private sector and will perform analyses of them and their approaches, assessing their effectiveness at assuring the identity of the electronic claimant, and working towards creating a general model of how effective the trust elevation / risk mitigation efforts are in creating trusted online transactions. Once the initial collection and analyses have been completed, the TC will correlate the results with various other trusted credential and trusted transaction models. The more widely-recognized and adopted these standardized protocols are, the more useful they will be to governments, businesses and individuals engaged in eGovernment and eCommerce.

The Trust Elevation TC is intended to respond to the suggestions of several governments, including the US government's NSTIC strategy document (NIST, 2017) that national and global identity infrastructures can be developed and supported by private sector cooperation among providers, users and subjects of trusted identity systems. The EIC-TEM documentation from this TC should promote interoperability among multiple identity providers, and among multiple identity federations & frameworks, by facilitating clear communication about common and comparable operations to present, evaluate and apply identity [data/assertions] to sets of declared authorization levels.

8.2.8 Conclusions

A main distinction can be made between **authoritative and reputation-based trust translation schemes**. In the first case, a standard or legal norm determines (authoritatively) how a translation (or mapping) of trust or identity assurance should be carried out between two different schemes (examples of this are STORK QAA/AQAA models, ISO 29115 standard for LoAs, and eIDAS specifications). In the second case, we have schemes where the reputation of a given service (or its provider) is determined by different means (including by rating mechanisms accessible to stakeholders involved in the use of the services) and made public, allowing for comparison and thus, also potential mapping across different providers and countries.

Document name:	Inventories (2)	Page:	125 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Under eIDAS, **trust service providers and their services** can be broadly classified between “Qualified” and “non-qualified” when they respectively are granted that status by a supervisory body and meet the requirements laid down in the Regulation.

We ultimately aim for general trust translation schemes applicable in complex scenarios, where it is needed to **compose trust levels** of individual trust services in the context of other services, which combine different types of trust services and/or trust services from different providers in the same or different countries.

In the **electronic identity** case, the three levels of assurance defined in eIDAS have their corresponding ones in (A)QAA models, and the specific technical specifications and procedures in the Annex of Implementing Regulation (EU) 2015/1502 allow to map national levels of assurance for electronic identification means to those three levels of assurance.

Mapping of the eIDAS LoAs to international levels defined for example in ISO/IEC 29115:2013 could be more complex to achieve as there seems to be no direct/binary equivalence or correspondence between the criteria used in both norms.

In the **eSignature** case, no trust translation scheme has been found currently, however the European regulations distinguish three levels of assurance: Electronic signature, Advanced electronic signature, and Qualified electronic signature. The first two levels are non-qualified in the eIDAS framework. More analysis is required to relate these levels to international standards.

In the **eSeal** case, no trust translation scheme has been found currently, however four possible levels of assurance have been detected in the European industry: Electronic seal, Advanced electronic seal, Advanced electronic seal supported by qualified certificate, and Qualified electronic seal. More analysis is required to relate these levels to international standards.

In the **eTime-stamp** case, no trust translation scheme has been found currently, however the European regulations distinguish between qualified and non-qualified time-stamps. International standards define trusted and non-trusted time-stamps, requiring further analysis to establish a comparison.

In the **eDelivery** case, the existing standards are technical and were written before any existing regulation, therefore they do not try to strongly enforce specific properties and contain very few strict requirements on the services, however they could be used as a basis for a technical definition of the qualified electronic registered delivery services.

Future ETSI standardisation work on electronic registered delivery services will leverage on the existing multipart TS 102 640 series addressing standardisation of registered electronic mail (REM) and align these specifications to the requirements of Regulation (EU) No 910/2014 on electronic registered delivery services, but this is currently not planned yet and therefore not available in the short term.

In the **website authentication** case, no trust translation scheme has been found currently, however the European regulations distinguish between qualified and non-qualified LoAs. The

Document name:	Inventories (2)	Page:	126 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



most relevant criterion for the classification of website authentication certificates concerns the level of validation of identity of the certificate requester.

There is a lack of standards related to requirements for qualified certificates for website authentication: they are under development. However there are some initiatives, like **CabForum's EV Guidelines** distinguishing three certificate levels: DV, OV, and EV (in ascending scale of identity assurance).

Open questions that come from the work on the deliverable regard the research gaps we encountered and that need to be addressed in the project:

- The **lack of trust translation schemes**, in some cases due to the lack of maturity of the services with regard to comparability and interoperability on a global market scale.
- The difficulty in certain cases **to find sources** on applicable standards and legal norms (for Trust Services) **in non-EU countries**, as it does seem the case that, for most of these services, Europe is indeed the most advanced area of the world in terms of the efforts being made, both on the technical and legal fronts, to foster and achieve interoperability and uptake of eID and Trust Services.
- We aim to establish a fruitful dialogue, on the one hand, with policy and decision makers (political level) and, on the other hand, with *SDOs (Service Delivery Organizations)* and the industry to develop frameworks for implementing trust translation schemes at an international level.
- We aim to give particular attention to the “**International aspects**” addressed in Art. 14 of the **eIDAS Regulation**, which refers to agreements to be concluded between the EU and third countries or international organisations allowing to recognize trust services provided in that third country or international organization (and, conversely, the recognition of EU trust services abroad).

Document name:	Inventories (2)	Page:	127 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



9. Best Practice Derivation Schemes for Mobile Identities

This section takes into consideration various best practice derivation schemes for mobile identities from both the academic and industry side. The academic side elaborates on previous EU research projects that have had experience with derivation schemes for mobile identities. The industry side shows a perspective of other projects that have had experience that could be relevant to learn from for LIGHTest.

9.1 Academic Perspective

This section will explore how derivation schemes for MobileID have been applied in real world situations, whether this implies in government or in companies. It will further explore the current situation in regards to an academic perspective. Further, the basic goal of this section is to understand what 'best uses' or 'best methods' have been observed and analyzed in research regarding these derivation schemes particularly with Mobile ID's and other forms of ID's.

This section will address some of the main applications that lead in the industry perspective, however, in an academic point of view. With respect to the academic perspective, this implies reviewing some of the previous or ongoing research projects that relate to these topics. Further, this section will look deeper into research projects that take a larger consideration into mobile electronic identity solutions, cloud computing infrastructures, and mobile Identity schemes in government.

9.1.1 SSEDIC 2020

This research project is a follow up project from the original SSEDIC project. SSEDIC stands for "Scoping the Single European Digital Community", where it has a community of over 200 international experts in digital identity (Michael Kubach, 2015). However, the SSEDIC 2020 project has committed to exploring more in the direction Mobile Identity. Their goal is to address some of the challenges that the public and private sectors face with mobile identities or more specifically, Mobile eID (Michael Kubach, 2015). The research project, SSEDIC 2020 aspires to develop a global solution for mobile identities. In this global vision, which is similar to LIGHTest, SSEDIC 2020 goal is to encourage global standardization and interoperability for mobile identity (Michael Kubach, 2015). More specifically, SSEDIC 2020 has created four categories that it wants to make an impact in. SSEDIC 2020 wants to explore into mobile identity, attribute usage, authentication, and liability (Michael Kubach, 2015) .

In greater detail to mobile Identity, SSEDIC aspires to lead towards the direction of creating a large acceptance of mobile eIDs for important tasks such as, being a notifiable credential for eGov, which would also allow access to other eGov services with mobile devices (Michael Kubach, 2015). Further, this exchange could be done regardless what mobile provider the user has and would be considered a public service like emergency calls (Michael Kubach, 2015) . While including mobile eID solutions on government is progress, there needs to be greater efforts in creating more interoperable mobile eID standards that utilize the advantages of mobile

Document name:	Inventories (2)	Page:	128 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



authentication. Overall, SSEDIC 2020 looks to assisting in progress of mobile identity in government, interoperable standards, and utilizing the overall authentication advantages of mobile identities (Michael Kubach, 2015). They have similar goals to LIGHTest, such as, leading towards finding global solutions and in developing best practices for mobile identity schemes. For greater detail on the SSEDIC 2020 project, please refer to (Michael Kubach, 2015) and (M. Talamo, 2014).

9.1.2 SKIdentity

“Skidentity- Trusted Identities for the Cloud” is a research project funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) in the “Trusted Cloud” Program (Cloud, 2015). The project aspires on creating a stable connection between eID cards and existing and emerging cloud computing infrastructures (Project, 2015) (Michael Kubach, 2015). The project ended at the end of 2015, however can help assist in some advantageous insight in “Cloud Identities”, which are cryptographically secured and can provide pseudonymous authentication or self-determined identity proofing (Project, 2015). Further the Cloud identities are `mobilized` as they are able to be managed by the user and can be transferred to almost any smartphone device to be used in mobile applications. Further, service providers can register with SkIDentity and us their services to securely identified (Michael Kubach, 2015).

9.1.3 FutureID

FutureID- Shaping the Future of Electronic Identity, was an EU funded research project that aspired on supporting and developing the practical aspects of Mobile eIDs. The research project included the integration of mobile identity and access in some of their use cases. Further, the project concluded that the practical world of identity management relies on progress of mobile electronic identity management in order to have secure and trustworthy digital devices (FutureID, 2015) For the LIGHTest Project, it could be beneficial to review how FutureID has integrated mobile identity and further used mobile eID access in their pilots.

Overall, there has been many EU projects that have successfully integrated mobile eID solutions. Further, it is expected that eIDAS regulation will include a roll-out to e-signature solutions and mobile eIDs that will be used for government applications (Michael Kubach, 2015). Further, it would be in LIGHTest interest to keep in mind the progress and results of the prior mentioned research projects with respect to the developments of mobile identities.

9.2 Industry Perspective

This section discusses some of the most relevant Mobile ID and ID derivation schemes from an industry perspective and thus with a relevant basis of active subscribers or at least a future perspective of a significant user base. To structure the landscape of existing schemes a little bit, it will be distinguished between different degrees of linking the (derived) mobile ID and its respective credentials to the original (primary) identity. In none of the schemes there is a direct cryptographic link between primary and derived identity credentials but there are schemes which at least include the registration with a primary ID and the creation of derived credentials as part of the overall process.

Document name:	Inventories (2)	Page:	129 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



9.2.1 Personal Identity Verification (PIV) derived credentials

The Personal Identity Verification (PIV) derived credentials are based on the special publication 800-157 of the National Institute of Standards and Technology (NIST) in the U.S. (H. Ferraiolo, 2014) This recommendation provides technical guidelines for the implementation of public key infrastructure (PKI) based identity credentials that are issued by Federal departments and agencies to individuals who possess and prove control over a valid PIV Card. The document includes requirements for initial issuance and maintenance of these credentials, certificate policies and cryptographic specifications, technical specifications for permitted cryptographic token types and the command interfaces for the removable implementations of such cryptographic tokens.

Document name:	Inventories (2)	Page:	130 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Originally, the PIV standard was introduced 2005 as a common standard for federal agencies allowing physical and logical access control with a smart-card form factor token. This system requires card readers on doors (physical access) and computing devices (logical access) which was commonly available during the time of publication. With the introduction of mobile devices

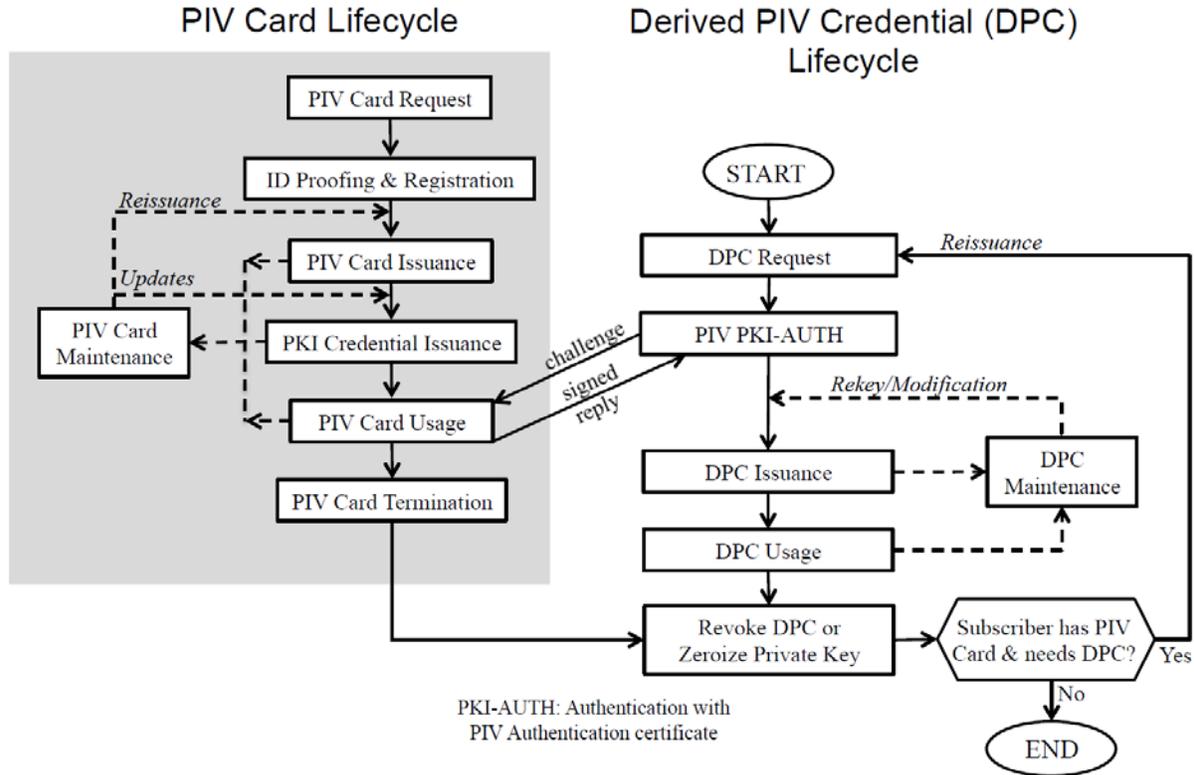


Figure 18: Principle of PIV derived credentials flow and lifecycle management (right). The figure also illustrates the relation to the card-based PIV credentials (left) and their lifecycle. From (H. Ferraiolo, 2014).

not supporting card readers the derived credential concept was developed in order to support the mobile infrastructure as well. Derived PIV Credentials are based on the general concept of derived credentials in SP 800-63-2, which leverages identity proofing and vetting results of current and valid credentials (W. E. Burr, 2013). Instead of repeating the identity proofing and vetting process the user proves possession of a valid PIV card to receive a derived credential. The general principle of PIV derived credentials is shown in Figure 16. After derived credentials have been requested in the initial process step (DPC Request) the card holder needs to authenticate with an existing and valid PIV card. The type of required authentication depends on the level of assurance (LoA) of the original PIV card. For a LoA-3 card a remote authentication is sufficient, while a LoA-4 card requires in-person authentication with biometric verification. After successful authentication derived credentials are issued based on classical X509-certificate PKI. The use of classical PKI certificates ensures interoperability with the existing reader/terminal infrastructure for physical access and existing protocols for logical access.

Document name:	Inventories (2)	Page:	131 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



One important aspect of the PIV derived credential system is the link between the lifecycles of the primary ID (PIV card) and the derived ID. In case of termination of the primary PIV card the derived credentials will be automatically revoked. Thus, the derived credential issuer has to ensure that the revocation status of the primary ID is checked regularly and that the certificate status of the derived credentials is adapted accordingly.

Overall, the PIV derived credential concept is currently the only existing real derivation scheme with practical relevance. Even without a direct cryptographic link between the primary and the derived credentials the synchronisation of ID lifecycles establishes a strong link between the primary and derived ID and thus a high trust into the validity of the derived credentials.

9.2.2 GSMA Mobile Connect

The Mobile Connect ecosystem is based on industry specifications issued by the GSMA. These specifications are not public and are only available to GSMA members. The goal of Mobile Connect is to position Mobile Network Operators (MNOs) to become providers of authentication and identity services to 3rd parties. It leverages the backbone of the existing security infrastructure under MNO control, namely the SIM (UICC) card in mobile devices. With its security properties as a Secure Element (SE) and the link to the International Mobile Subscriber Identity (IMSI) the UICC provides a unique identifier that can be linked to the customer identity in the MNO identity management or customer relationship management (CRM) system.

While the landscape of mobile devices is strongly fragmented into feature phones and smartphones, into various smartphone operating systems (e.g. Android and iOS) and device capabilities (with/ without NFC, Trusted Execution Environments, embedded SEs,...) the UICC together with the SIM toolkit typically is the smallest common denominator of almost all mobile devices with a mobile subscription. By using this infrastructure for strong authentication the system can be used by a broad user base of more than 2 billion users, according to the GSMA.

In general, the Mobile Connect ecosystem comprises two main components (see Figure 19). The MNOs operate a federation gateway (identity gateway) that can accept 3rd party requests based on the Open ID Connect protocol. For this purpose, the MODRINA (Mobile Operator Discovery Registration and Authentication) working group of the Open ID Foundation has defined an appropriate Open ID Connect profile (OpenID MODRINA WG, 2016). After receiving the request, the MNO performs a strong authentication with the end customer based on

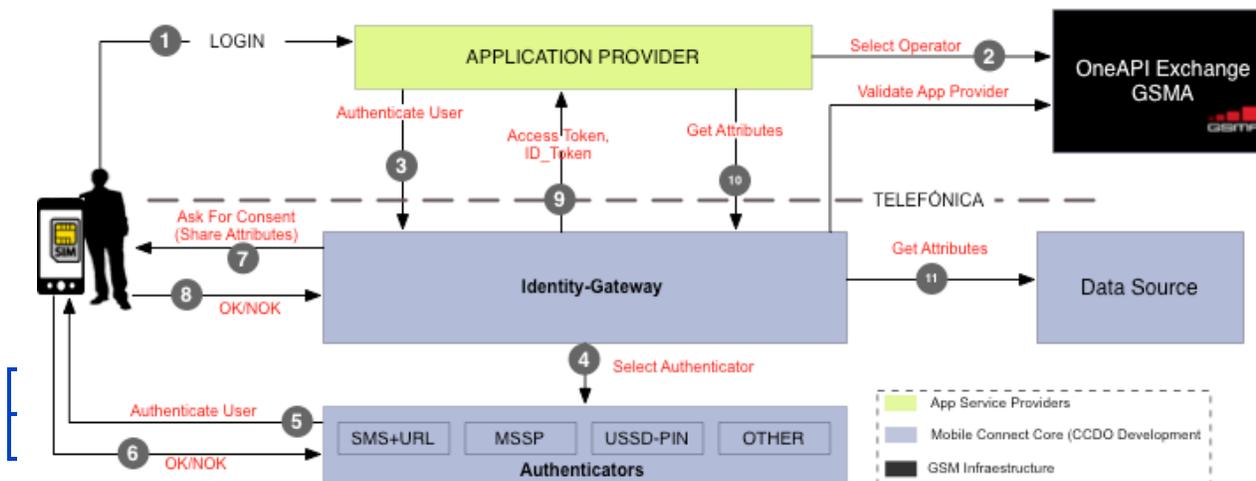


Figure 19: Principle of the GSMA Mobile Connect authentication and attribute sharing flow. Source: (Eleven Paths, 2015).

credentials stored in the UICC. After successful authentication the federation gateway issues an assertion within the Open ID Connect response. This assertion may also include verified attributes (e.g. for age verification) and/or identity data. Thus, the MNO cannot only offer authentication as a service but also identity as a service to relying parties. Technically, the system can also support legally binding signature services based on credentials in the UICC.

Depending on the level of authentication, Mobile Connect can support different Levels of Assurance (LoAs) comparable to those defined in ISO/IEC 29115. A LoA-2 authentication requires the user to confirm the authentication by just pressing “o.k.” when prompted by the SIM toolkit (one-factor authentication by possession of the UICC) while a LoA-3 authentication also requires to enter a PIN (two-factor authentication, including knowledge of PIN). LoA-4 is provided by additionally introducing PKI with a private key that is used to sign a challenge and a certificate that can be verified by the relying party or another verification provider.

While the mobile device containing the UICC is used for strong authentication there is, at least for LoA-2 and LoA-3, no direct cryptographic link between the authentication and the identity data. The ID management is performed by the MNO which also establishes the link between the mobile device and the customer identity via the ID management or CRM database. The lifecycle management of the mobile credentials is thus based on the lifecycle of the relationship between the end customer and the MNO, rather than on the lifecycle of the underlying identity. Nevertheless, since the MNO controls the mobile ID infrastructure (i.e. the UICC) and its lifecycle, it can be assumed that a strong link of lifecycles exists. The trust into the actual identity data however is unclear and is only implicitly given by the trust in the initial identification/onboarding process performed by the MNO. The quality of this process is not standardized and may depend on the MNO and its existing infrastructure (.e.g branch store, virtual MNO only,...) For some type of subscriptions, especially pre-paid cards, there were even gaps in the identification process which have been closed recently by many European countries as part of anti-terror legislation.

9.2.3 Fast Identity Online (FIDO) Alliance

The Fast Identity Online (FIDO) alliance is an industry specification group with now more than 200 members that aims to define an interoperable specification for mobile authentication to overcome existing fragmentation and silos. Technically, FIDO concentrates only on authentication and explicitly excludes identity and ID federation. It can however be embedded into identity schemes and combined with ID federation, although not directly supported by the FIDO protocol. Since FIDO is also an authentication option for other schemes, like GSMA Mobile Connect, and since it also provides an attestation scheme for authenticators, it discussed here.

FIDO has originally two flavours of the protocol, the U2F-protocol for two-factor authentication and the UAF-protocol for password-less authentication (e.g. using biometrics) and transaction signing (see in Figure 20 below). Both protocol versions exist under the FIDO 1.x specifications (FIDO Alliance, 2016) and are currently unified in the upcoming FIDO 2.0 (formerly UFS-protocol) specification.

Document name:	Inventories (2)	Page:	133 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



PASSWORDLESS EXPERIENCE (UAF standards)



SECOND FACTOR EXPERIENCE (U2F standards)



Figure 20 User experience of the two FIDO protocol versions UAF (left) for password-less authentication and transaction signing and U2F (right) for two-factor authentication. Source: (FIDO Alliance, 2016).

The principle of FIDO is based on simple challenge-response protocols using asymmetric keys. In contrast to previous PKI-based systems FIDO wants to explicitly reduce complexity by restricting PKI to the absolute minimum. As a consequence, the user-centric registration triggers the generation of the FIDO key pair and exports the public key to the service provider while the private key is kept on the user side. No further PKI is used in the registration and authentication step.

A lightweight PKI is used for device attestation where the authenticator proves its integrity with a self-signed certificate of the authenticator manufacturer that is published in a metadata database. Again, the PKI is restricted to the absolute minimum and is only integrated due to the need to identify the type of authenticator that is used. Attestation is required due to the open nature of the FIDO authenticator landscape. In principle, every authenticator that complies with the FIDO protocol specifications can be used on the client side. As a consequence, there will be a large variety of authenticators with significantly different security levels. The range can include pure software implementations as well as TEE-based authenticators or hardware-supported devices (smart cards, μ SD cards, USB tokens...). In order to enforce certain security policies, the relying party needs to know which type of authenticator is available and how trustworthy this can be. With the attestation certificates the relying party could restrict the range to only known authenticators.

As a consequence, when FIDO is integrated into a mobile ID scheme there is no direct link between identity data and authentication credentials in the current version of the FIDO protocol. However, there have been proposals to enhance FIDO by issuing certificates for the public key after identity verification and user registration. While this can be performed for one specific relying party supporting this enhancement it contradicts to the FIDO principle of user-centric and privacy-friendly generation of individual key pairs for each relying party (and the resulting non-traceability).

Nevertheless, due to its flexibility, widespread industry support, high usability (e.g. mobile device biometrics), existing links to other mobile ID schemes, an existing attestation mechanism and the option to integrate FIDO into an identity scheme, the protocol is of high interest for the LIGHTest applications.

Document name:	Inventories (2)	Page:	134 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



9.2.4 UICC-based PKI Schemes for Mobile Identities

Beyond the existing standards and industry specifications mentioned above there are also commercial proprietary solutions for mobile identities rolled out in several countries, like Finland, Estonia, Turkey, Norway, Iceland and others. Many of them are based on a mobile ID solution by Valimo, now acquired by Gemalto. The principle of these systems that are used for mobile ID, mobile authentication and/or mobile signature is comparable to the GSMA Mobile Connect LoA-4 solution, as described in 9.2.2. A SIM/UICC is used as the secure element, containing the private key credentials. For the public key, a PKI-backed certificate is issued that can be verified by the relying party.

Besides establishing a functioning PKI that is accessible to all involved parties, these system typically also require the cooperation of several (at least the most important) MNOs in the specific country. The feasibility of such a solution therefore depends on the specific MNO market structure in the respective country and may be subject to high entrance barriers in other countries. This is one of the reasons for developing a global standard like Mobile Connect from the GSMA.

9.2.5 Cloud-based Systems

Since cloud computing has gained more and more popularity in recent years and the implementation of "...as a service"-offerings has gained widespread acceptance there are several examples of cloud-based Identity as a Service (IaaS) offerings. One example is the SkIDentity project, which has been publicly funded by the German BMBF (Huehnlein, 2016). This service acts as an identity broker, accepting requests from relying parties via federation protocols like SAML or OpenID Connect. The initial identity is provided by an eID card like the German eID card (nPA) or other governmental cards (e.g. health card).

SkIDentity is also capable of "exporting" an identity to a mobile device. This is done by copying a URL or scanning a QR code containing session data of the active authentication session. A real credential generation in the sense of cryptographic credentials that are used for strong authentication and which are stored on the mobile device is not available yet. However, combining such a cloud-based federation system with a mobile authentication technology like FIDO or GSMA Mobile Connect is an attractive option for a mobile ID system that supports the full lifecycle fully online, from on-boarding/identification via eID to the credential registration, authentication and ID federation.

Document name:	Inventories (2)	Page:	135 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



10. Best Practices of Interaction Design

This section explores some practices in interaction design from both a research side and within the industry. This helps gain a broader perspective on interaction design, usability and user interface.

10.1 Academic Perspective

This section will observe some academic contributions to the “Best Practices of Interaction Design”. This will include exploring some of the methodologies used in the topic of Interaction Design, Usability, and User Interface. In general, Interaction Design can be referred to as design-oriented practices of Human Computer Interaction (HCI) (Kristina Hook, 2012). However, it can be argued that Interaction Design differs from Human-Computer Interaction by focusing completely on a “design discipline”, which implies that the main goal is to create a better more efficient interactive system (Fallman, 2008). Interaction Design research is a topic of multi-disciplinary interest. Further, as it is a growing topic in both interest and scope. This section will explore some of the existing methods and models in the field.

First off, (Fallman, 2008) elaborates that interaction design research can be modeled in three parts. He argues that in Interaction Design there are actual three external interfaces that need to be satisfied. These three external interfaces, differ in both tradition and perspective (Fallman, 2008). Further, it is argued that these three kinds of interaction design together create a balance and comprehensive concept for interaction design.

First, there is the interface for the industry, which has collaborations and exchanges with people (Fallman, 2008). This is also called Design Practice. Second, there is an interface for academics, which considers the research community in the topic (Fallman, 2008). Also, this is considered to be “Design Studies”. Third, it considers the interaction design interface for society as a whole, which observes the current and future impact of the interaction design (Fallman, 2008). Further, this is called Design Exploration. In figure 23, find a diagram of the model created by (Fallman, 2008). Further information on this model, can be found in the following paper (Fallman, 2008) and other works by Daniel Fallman.

Document name:	Inventories (2)	Page:	136 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



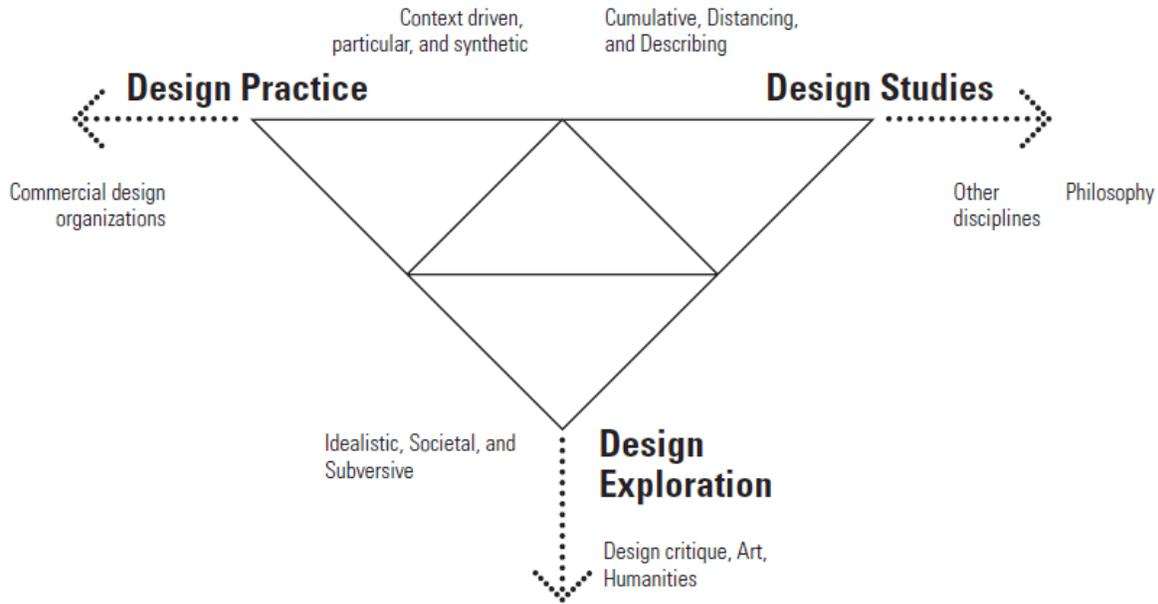


Figure 21 Model of Interaction Design Research by Daniel Fallman

Overall, it's undeniable that interaction design requires interdisciplinary insights in order to be successful. Further (Kristina Hook, 2012) discusses three strong concepts in interaction design research. The concepts cover insights relating to stages of design that are either broad and mature or tentative and experimental. Further, (Kristina Hook, 2012) argue that there are many concepts and practices in interaction design, however, it is more important to focus on the concepts that are used in interaction design solutions that are in between the technology and the people. Further, they state that strong interaction design concepts or practices should regard dynamic gestalts of design solutions (Kristina Hook, 2012). (Elizabeth Goodman, 2011) elaborate on the differences between HCI research and Interaction design. With that, they present a summary of different methods and theories used in both interaction design research and HCI research.

As for LIGHTest, it would be helpful to have a familiar understanding with the methods and models used in interactive design research as a foundation and structure. As interaction design is a field that is interdisciplinary and has many different faucets, choosing a methodology and structure, such as the model by (Fallman, 2008) could assist in leading to thorough results.

10.2 Industry Perspective

Trends in interaction design

In interaction design or IxD, there have been two underlying technical trends in the past decade. First is the onslaught of mobile devices and relevant use cases. The second is the emergence of high-DPI displays, which caught traditional, slow-moving UX kits by surprise and spurred a new generation of DPI-independent UI kits and design paradigms.

Document name:	Inventories (2)	Page:	137 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



In light of these two changes, traditional default UX-kit themed enterprise Java applications have aged very badly. They assume that the end-user has access to a pixel-perfect pointing device and a 4:3 aspect ratio 96DPI display. As the number of mobile users has already surpassed the number of desktop users, user interaction designers must not only keep mobile users in mind, but actually prioritise them over more traditional paradigms.

In addition to changed physical characteristics, also the end-users' perceptions and values have changed markedly in the past decade. Time, our 4th dimension is often forgotten in interaction design. It is no longer acceptable to have the end-user complete functions that the software could do for him, and the end-user places clear value on the time he spends on the interaction. Ideally, the system should respond to the user's experience and not the other way around. For example, instead of presenting the user multiple confirmation screen when doing a file delete operation, there could be a context-aware undelete functionality that becomes visible after the deletion. This way, the most common function of deletion function – actually deleting file(s) – becomes and a single operation while the much rarer branches can require an additional interaction.

As business practises become more automated, the users' interactions with the provided interfaces become the main surface between the customers and the service provider. When much of the supporting infrastructure is abstracted away from view, UX becomes a major differentiating factor between commercial offerings, and can make or break not only single cases, but the entire product line or even the whole company.

From an end-user perspective, the turmoil in UX trends is mostly a positive one. While the Wild West during the paradigm transition period can feel exhausting (great, yet another different UI to wade through), in the end we are heading towards a more reactive and flexible user experience.

Example of using role and user attributes to enhance user experience

A manufacturer of industrial products has very large volumes of content, eg product information and data. That content is as such not confidential in nature for the dealer, but the mere volume is so huge that presenting it as such without any pre-categorization or pre-processing would make the work of the dealer heavy, as he would drown down by the mere multitude of the content.

Typically roles and attributes have been seen as mechanisms in RBAC, to prevent unwanted access to information. That is, allowing only authorized users to have access. However roles and attributes can also be used as mechanisms for filtering data and content according to relevance. Hence, when the IDP and the identity services deliver identity information, they typically also can deliver additional attributes. Based on that the Service Provider or Relying Party may then present the user with only such content that is considered relevant; also based on, e.g., the actual task at hand and combined or in parallel with such categorization information about the content that the user has previously provided as, e.g., his areas of interest.

Document name:	Inventories (2)	Page:	138 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Example of mechanisms in use in industry that impact user experience: Http header enrichment in operator services

Http header enrichment (HHE) allows MNOs to address two issues: first, operators can append information into http traffic to enable attribute based provisioning of services, content and resources to specific users; analytics; improving performance; and access control as well as customization of user experience.

Also HHE is used by operators as enablers to revenue streams, through advertising etc.

HHE has consequences for mobile subscribers all over the world. Generally service providers should remove header enrichment at their network boundary to prevent privacy leaks. However, this does not necessarily remove injected http headers; thus, a web server visited with a mobile device could use this information, in addition for purposes that the end-user would typically allow and categorize as being part of good service practice; also for purposes against the user's interests like user discrimination and online tracking.

Document name:	Inventories (2)	Page:	139 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



11. References

Adobe, 2016. *Adobe's Approved Trust List (AATL)*. [Online]

Available at: <https://helpx.adobe.com/acrobat/kb/approved-trust-list2.html>

[Accessed 01 2017].

AFNOR Group, E. C. E. ..., 2014. *e-signatures standards: download form*. [Online]

Available at: <http://www.e-signatures-standards.eu/download-form?Ressource=1881>

[Accessed 2016].

AFNOR Group, E. C. E., 2013. *ationalised structure for Electronic Signature Standardisation version 09/2013*. [Online]

Available at: <http://www.e-signatures-standards.eu/reference-documentation/standardisation-mandate-and-framework/rationalised-structure-for-electronic-signature-standardisation-version-09-2013>

[Accessed 2016].

AFNOR Group, E. C. E., 2014. *e-signatures standards*. [Online]

Available at: <http://www.e-signatures-standards.eu/activities>

[Accessed 2016].

Alsenoy, B. et al., 2009. *Delegation and digital mandates: Legal requirements and security objectives*. s.l., Computer Law & Security Review 25, pp. 415-432.

Anon., 2016. *2016 Year in Review: (TIG-ing stock of) Innovation in the Identity Ecosystem*. [Online]

Available at: <http://imperialvalleynews.com/index.php/8-news/11657-2016-year-in-review-tig-ing-stock-of-innovation-in-the-identity-ecosystem.html>

[Accessed December 2016].

ANSI, 2005. *X9.95-2005*. [Online]

Available at: http://www.techstreet.com/standards/x9-x9-95-2005?product_id=1327239

[Accessed 2016].

ANSI, 2016. *ANSI ASC X9.95 Standard*. [Online]

Available at: <https://x9.org/standards/standards-store/>

[Accessed 2017].

ANSSI, 2012. *Plate-forme SUNNYSTAMP. POLITIQUE D'HORODATAGE*. [Online]

Available at: https://www.lex-marches.fr/fr/politiques/PH_Sunnystamp_v1.0-121101.pdf

[Accessed 2016].

ANSSI, 2016. *Agence nationale de la securite des systemes d'information*. [Online]

Available at: <http://www.ssi.gouv.fr/en/>

[Accessed 2016].

Document name:	Inventories (2)	Page:	140 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Austria Government, 2016. *Website of the Austrian Data Protection Authority*. [Online]
Available at: <http://archiv.dsb.gv.at/DesktopDefault.aspx?alias=dsken>
[Accessed 2016].

Barreira, e. a., 2013. *ENISA Guidelines for Trust Service Providers*. [Online]
Available at: <https://www.enisa.europa.eu/publications/tsp1-framework>
[Accessed 01 2017].

Bernhard, D. et al., 2013. Anonymous attestation with user-controlled linkability. *International Journal of Information Security* 12(3). *International Journal of Information Security*.

Bowman, I., 2003. *Government Paperwork Elimination Act*. [Online]
Available at: <http://www.isaacbowman.com/esign-laws-government-paperwork-elimination-act>
[Accessed 2017].

Brennan, J., 2016. *Kantara Workshop at CIS*, Unknown: Kantara.

Brickell, E., Camenisch, J. & Chen, L., 2004. *Direct Anonymous Attestation*. s.l.:s.n.

Brickell, E., Chen, L. & Li, J., 2009. Simplified security notions of direct anonymous attestation and a concrete scheme from pairings. *International Journal of Information Security*.

busilezas, 2015. *FreeTSA*. [Online]
Available at: https://www.freetza.org/index_en.php
[Accessed 2016].

BuyPass, M. H., 2016. *World e-ID & CyberSecurity - Digital Identity and Data Protection for Citizens and Businesses*. [Online]
Available at: <http://www.worlde-idandcybersecurity.com/session/new-trust-services-for-acceleration-of-the-digital-transformation>
[Accessed 2016].

CAB, 2016. *CAB Forum*. [Online]
Available at: <https://cabforum.org/>
[Accessed December 2016].

CABForum, 2016. *CA/Browser Forum*. [Online]
Available at: <https://cabforum.org/>
[Accessed 2016].

Camenisch, J., Drijvers, M. & Lehmann, A., 2016. Anonymous Attestation Using the Strong Diffie Hellman Assumption Revisited. TRUST. In: *Anonymous Attestation Using the Strong Diffie Hellman Assumption Revisited*. TRUST. s.l.:s.n., pp. 1-20.

Camenisch, J., Drijvers, M. & Lehmann, A., 2016. Universally Composable Direct Anonymous Attestation. *Public Key Cryptography (2)* . In: s.l.:s.n., pp. 234-264.

Document name:	Inventories (2)	Page:	141 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Canadian Government, 2005. *An Act to amend the Copyright Act (38th Canadian Parliament, 1st Session)*. [Online]

Available at:

<http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=2334015>

[Accessed 2017].

Canadian Government, 2006. *39th Canadian Parliament*. [Online]

Available at:

<http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=3188787>

[Accessed 2017].

Canadian Government, 2010. *An Act to amend the Copyright Act (40th Canadian Parliament, 3rd Session)*. [Online]

Available at:

<http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=4580265>

[Accessed 2017].

Celik, T. E. E. J. G. D. H. I. L. P. W. J., 2011. *Selectors Level 3 W3CF Recommendation 29 September 20177*, s.l.: W3C.

Chamberlin, D. M., 2004. *XML Path Language (XPath) 3.0.*, s.l.: W3C Consortium.

Chen, L., 2010. DAA Scheme requiring less tpm resources. In: *Information Security and Cryptology*. s.l.:s.n.

Chen, L., Morrissey, P. & Smart, N., 2008. *On proofs of security for DAA schemes Provable Security*. s.l.:s.n.

Chen, L., Morrissey, P. & Smart, N., 2008. *Pairings in trusted computing (invited talk)*. s.l.:s.n.

China, 2005. *People's Republic of China Electronic Signature Law*. [Online]

Available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=199526

[Accessed 2016].

Cloud, T., 2015. *Trusted Cloud*. [Online]

Available at: <http://trusted-cloud.de>

Congress, T. N. D. I. I. a. P. P. a. t. L. o., 2012. *Open Packaging Conventions (Office Open XML), ISO 29500-2:2008-2012*. [Online]

Available at: <http://www.digitalpreservation.gov/formats/fdd/fdd000363.shtml>

[Accessed 2016].

Cooper, D. S. S. S. B. S. H. R. P. W., 2008. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, s.l.: s.n.

Document name:	Inventories (2)	Page:	142 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Corredera, D. N., 2015. *Measuring postal e-Services development. A global perspective*, Berne, Switzerland: Universal Postal Union (UPU).

Criptomathic, 2003. *ZertES*. [Online]

Available at: <https://www.cryptomathic.com/news-events/blog/understanding-zertes-the-swiss-federal-law-on-electronic-signatures>

[Accessed 2017].

CROBIES, 2010. *Study on Cross-Border Interoperability of eSignatures 2010*. [Online]

Available at: <https://ec.europa.eu/digital-single-market/en/news/crobies-study-cross-border-interoperability-esignatures-2010>

[Accessed 2016].

Cruellas, J. & Pope, N., 2006. *Digital Signing without the Headaches*. [Online]

Available at: http://www.oasis-open.org/committees/download.php/22721/ISSE-DSS-full-final_b.pdf

[Accessed 2016].

De Coi, J. O. D., 2008 . A review of trust management, security, and policy languages. *Special Session on Trust in Pervasive Systes and Networks* .

Digital-Austria, 2009. *OID der öff*, Verwaltung: OID-T1 1.0.0.

Digital, P. o. E. A. M. o. F. a. P. F. G. S. o., 2016. *Legal framework of the digital administration in Spain*. [Online]

Available at:

https://administracionelectronica.gob.es/pae/Home/pae_Documentacion/pae_LegNacional/pae_NORMATIVA_ESTATAL_Legal_Provisions.html#.WLU6vFXytaR

DIN, 2016. *DIN Deutsches Institut für Normung e. V.*. [Online]

Available at: <http://www.din.de/en/getting-involved/standards-committees/nia/european-committees/68242/wdc-grem:din21:88827989!search-grem-details?masking=true>

[Accessed 2016].

DLA Piper; PriceWaterhouseCoopers; SEAled; SGA; TimeLex, 2013. *Feasibility study on an electronic identification, authentication and signature policy (IAS)*, at <https://ec.europa.eu/digital-single-market/en/news/feasibility-study-electronic-identification-authentication-and-signature-policy-ias-0>, EU: SMART.

e-codex, 2016. *e-codex: making justice faster*. [Online]

Available at: <http://www.e-codex.eu/>

[Accessed 2016].

EGIZ, 2012. *Leitfaden zur Integration und Verwendung von elektronischen Vollmachten in MOA-ID*. [Online]

Document name:	Inventories (2)	Page:	143 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Available at: <https://www.egiz.gv.at/files/download/Leitfaden-MOA-Vollmachten.pdf>
[Accessed 2016].

EGIZ, 2014. *AK IT-Security 1: Representation with electronic mandates*. [Online]
Available at:
http://www.iaik.tugraz.at/content/teaching/master_courses/e_government/slides/2014-11-05 - Electronic Mandates.pdf
[Accessed 2016].

EGIZ, 2016. *Test environment*. [Online]
Available at: <http://vollmachten.egiz.gv.at/>
[Accessed 2016].

Eleven Paths, 2015. *Introducing Mobile Connect – the new standard in digital authentication*. [Online]
Available at: <http://blog.elevenpaths.com/2015/09/introducing-mobile-connect-new-standard.html>
[Accessed 05 10 2016].

Elizabeth Goodman, E. S. R. W., 2011. *Understanding Interaction Design Practices*. CHI.

ENISA, 2016. *Analysis of standards related to Trust Service Providers. Mapping of requirements of eIDAS to existing standards*. [Online]
Available at: https://www.enisa.europa.eu/publications/tsp_standards_2015
[Accessed 2016].

ENISA, 2016. *ENISA Qualified Website Authentication Certificates*. [Online]
Available at: <https://www.enisa.europa.eu/publications/qualified-website-authentication-certificates>
[Accessed 2016].

Esther Makaay, D. T. a. S., March, 2017. *Trust Frameworks*, s.l.: Due to be published.

ETSI, 2004. *ETSI TS 102 042 V1.1.1 Policy requirements for certification authorities*. [Online]
Available at:
http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/01.01.01_60/ts_102042v010101p.pdf
[Accessed 2017].

ETSI, 2007. *ETSI TS 101 861 V1.4.1: Electronic Signatures and Infrastructures (ESI); Time stamping profile*. [Online]
Available at:
http://www.etsi.org/deliver/etsi_ts/101800_101899/101861/01.04.01_60/ts_101861v010401p.pdf
[Accessed 2016].

ETSI, 2008. *ETSI TS 102 023 V1.2.2: Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities*. [Online]
Available at:

Document name:	Inventories (2)	Page:	144 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



http://www.etsi.org/deliver/etsi_ts/102000_102099/102023/01.02.02_60/ts_102023v010202p.pdf
[Accessed 2016].

ETSI, 2009. *ETSI Technical Specification 102 231: Requirements for Trust Service Provider status information*. [Online]

Available at: <http://uri.etsi.org/02231/v3.1.2/>

[Accessed 01 2017].

ETSI, 2010. *ETSI TS 102 640-1 V2.1.1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_ts/102600_102699/10264001/02.01.01_60/ts_10264001v020101p.pdf

[Accessed 2016].

ETSI, 2010. *ETSI TS 102 640-2 V2.1.1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_ts/102600_102699/10264002/02.01.01_60/ts_10264002v020101p.pdf

[Accessed 2016].

ETSI, 2011. *ETSI TS 102 640-6-2 V1.1.1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6: Interoperability Profiles; Sub-part 2: REM-MD BUSDOX Interoperability Profile*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_ts/102600_102699/1026400602/01.01.01_60/ts_1026400602v010101p.pdf

[Accessed 2016].

ETSI, 2012. *Draft ETSI EN 319 401 V1.1.1: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_en/319400_319499/319401/01.01.01_20/en_319401v010101c.pdf

[Accessed 2016].

ETSI, 2012. *ETSI TS 103 171 V2.1.1: Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf

[Accessed 2016].

Document name:	Inventories (2)	Page:	145 of 170		
Dissemination:	PU	Version:	2.5		Status:

Inventories (2)



ETSI, 2013. *ETSI Technical Specification 119 612: Requirements for Trusted Lists (EU version of ETSI TS 102 231)*. [Online]

Available at: <http://uri.etsi.org/19612/v1.2.1/>

[Accessed 01 2017].

ETSI, 2013. *ETSI TS 103 172 V2.2.2: Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

[Accessed 2016].

ETSI, 2013. *ETSI TS 103 173 V2.2.1: Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf

[Accessed 2016].

ETSI, 2014. *ETSI SR 019 530: Study on standardisation requirements for e-delivery services applying e-signatures*. [Online]

Available at: http://docbox.etsi.org/ESI/Open/Latest_Drafts/sr_019_530_v000002-rf-for-e-delivery-stds-using-e-sign-stable-draft.zip

[Accessed 2016].

ETSI, 2015. *Draft ETSI EN 319 401 V2.0.0 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.00.00_20/en_319401v020000a.pdf

[Accessed 2016].

ETSI, 2015. *Draft ETSI EN 319 411-1 V1.0.0 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.00.00_20/en_31941101v01000a.pdf

[Accessed 2016].

ETSI, 2015. *Draft ETSI EN 319 412-4 V1.0.0 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organizations*. [Online]

[Online]

Available at:

http://www.etsi.org/deliver/etsi_en/319400_319499/31941204/01.00.00_20/en_31941204v01000a.pdf

[Accessed 2016].

Document name:	Inventories (2)	Page:	146 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



ETSI, 2015. *ETSI - SR 019 050: ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI); RATIONALIZED FRAMEWORK OF STANDARDS FOR ELECTRONIC REGISTERED DELIVERY SERVICES APPLYING ELECTRONIC SIGNATURES*. [Online]

Available at: <http://standards.globalspec.com/std/9933479/etsi-sr-019-050>

[Accessed 2016].

ETSI, 2015. *ETSI SR 019 050 V1.1.1 Electronic Signatures and Infrastructures (ESI); Rationalized framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_sr/019000_019099/019050/01.01.01_60/sr_019050v010101p.pdf

[Accessed 2016].

ETSI, 2016. *Digital Signature*. [Online]

Available at: <http://www.etsi.org/technologies-clusters/technologies/security/digital-signature>

[Accessed 2016].

ETSI, 2016. *ETSI EN 319 411-2 V2.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/en_31941102v020101p.pdf

[Accessed 2016].

ETSI, 2016. *ETSI EN 319 421 V1.1.1: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf

[Accessed 2016].

ETSI, 2016. *ETSI EN 319 422 V1.1.1: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf

[Accessed 2016].

ETSI, 2016. *ETSI Standards*. [Online]

Available at: [http://www.etsi.org/standards-](http://www.etsi.org/standards-search#page=1&search=&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2016-11-01&harmonized=0&keyword=&TB=&stdType=EN&frequency=&mandate=&sort=1)

[search#page=1&search=&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2016-11-](http://www.etsi.org/standards-search#page=1&search=&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2016-11-01&harmonized=0&keyword=&TB=&stdType=EN&frequency=&mandate=&sort=1)

[01&harmonized=0&keyword=&TB=&stdType=EN&frequency=&mandate=&sort=1](http://www.etsi.org/standards-search#page=1&search=&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2016-11-01&harmonized=0&keyword=&TB=&stdType=EN&frequency=&mandate=&sort=1)

[Accessed 2016].

Document name:	Inventories (2)	Page:	147 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



ETSI, 2016. *ETSI TS 119 101 V1.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation*. [Online]

Available at:

http://www.etsi.org/deliver/etsi_ts/119100_119199/119101/01.01.01_60/ts_119101v010101p.pdf

[Accessed 2016].

ETSI, 2016. *Open Latest Drafts*. [Online]

Available at: https://docbox.etsi.org/ESI/Open/Latest_Drafts/

[Accessed 2016].

European Commission, 2009. *Mandate M460: "Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the Field of Information and Communication Technologies Applied to Electronic Signatures"*. [Online]

Available at: [http://www.e-signatures-](http://www.e-signatures-standards.eu/content/download/9219/83899/version/2/file/m460.pdf)

[standards.eu/content/download/9219/83899/version/2/file/m460.pdf](http://www.e-signatures-standards.eu/content/download/9219/83899/version/2/file/m460.pdf)

[Accessed 2016].

European Commission, 2016. *CEF eSignature: TL Manager v5.0*. [Online]

Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/TL+Manager+v5.0>

[Accessed 2016].

European Commission, 2016. *Employment, Social Affairs & Inclusion: Electronic Exchange of Social Security Information (EESSI)*. [Online]

Available at: <http://ec.europa.eu/social/main.jsp?catId=869>

[Accessed 2016].

European Commission, 2016. *eSignatures: Standards*. [Online]

Available at: <http://www.e-signatures-standards.eu/activities>

[Accessed 2016].

European Commission, 2009. *Service Directive*. [Online]

Available at: http://ec.europa.eu/growth/single-market/services/services-directive/index_en.htm

[Accessed 2016].

European Commission, 2009. *Study on eID Interoperability for PEGS: Update of Country Profiles*, s.l.: IDABC Programme.

European Commission, 2013. *Digital Single Market: Standardisation aspects of eSignatures*. [Online]

Available at: <https://ec.europa.eu/digital-single-market/en/news/standardisation-aspects-esignatures>

[Accessed 2016].

European Commission, 2014. *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. [Online]

Document name:	Inventories (2)	Page:	148 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
[Accessed 19 October 2016].

European Commission, 2015. *Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electr.* [Online]

Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0005
[Accessed 2016].

European Commission, 2015. *Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regula.* [Online]

Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0006
[Accessed 2016].

European Commission, 2015. *Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic ident.* [Online]

Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_289_R_0007
[Accessed 2016].

European Commission, 2015. *Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament.* [Online]

Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1441782671426&uri=CELEX:32015D0296>
[Accessed 2016].

European Commission, 2015. *Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services.* [Online]

Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1441782373783&uri=OJ:JOL_2015_235_R_0001
[Accessed 2016].

European Commission, 2015. *Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the Eu.* [Online]

Document name:	Inventories (2)	Page:	149 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002
[Accessed 2016].

European Commission, 2016. *CEF Digital Signature Services (DSS)*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=23003381>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery Access Point software*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+software>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery Background*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Background>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery Conformance Testing*. [Online]
Available at:
<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Conformance+testing>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery Connectivity Testing*. [Online]
Available at:
<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Connectivity+testing>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery Goals*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Goals>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery Large Scale Pilots*. [Online]
Available at:
<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Large+Scale+Pilots>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery PKI service*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery self-assessment tool*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+self-assessment+tool>
[Accessed 2016].

Document name:	Inventories (2)	Page:	150 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



European Commission, 2016. *CEF Digital: eDelivery SML service*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+service>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery SML software*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+software>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery SMP software*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP+software>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery Technical Specifications*. [Online]
Available at:
<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Technical+Specifications>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eSignature Goals*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature+Goals>
[Accessed 2016].

European Commission, 2016. *CEF Digital: eDelivery Benefits*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Benefits>
[Accessed 2016].

European Commission, 2016. *CEF eSignature Digital Service Infrastructure: Discover eSignature*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature+Discover>
[Accessed 2016].

European Commission, 2016. *CEF eSignature: EU Legal Framework*. [Online]
Available at:
<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature+Legal+frameworks>
[Accessed 2016].

European Commission, 2016. *CEF Trusted Lists Manager (TLM) releases*. [Online]
Available at: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/TLM+--+releases>
[Accessed 2016].

European Commission, 2016. *Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament*. [Online]
Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.109.01.0040.01.ENG&toc=OJ:L:2016:109:TOC
[Accessed 2016].

Document name:	Inventories (2)	Page:	151 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



European Commission, 2016. *Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services (Text with EEA relevance)*. [Online]

Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1441782918257&uri=CELEX:32015R0806>
[Accessed 2016].

European Commission, 2016. *DG Connect - Building online trust and confidence: Electronic signatures, seals and trust services now valid throughout EU*. [Online]

Available at: <https://ec.europa.eu/digital-single-market/en/news/building-online-trust-and-confidence-electronic-signatures-seals-and-trust-services-now-valid>

[Accessed 2016].

European Commission, 2016. *Digital Service Market: Trust Services*. [Online]

Available at: <https://ec.europa.eu/digital-single-market/en/trust-services>

[Accessed 2016].

European Commission, 2016. *eSignature building block*. [Online]

Available at:

https://ec.europa.eu/cefdigital/wiki/download/attachments/23003331/Building%20Block%20DSI_IntroDocument%20%28eSignature%29%20%28v1.1%29.pdf?version=1&modificationDate=1475245253025&api=v2

[Accessed 2016].

European Commission, 2016. *Glossary*. [Online]

Available at: <https://ec.europa.eu/digital-single-market/glossary>

[Accessed 2016].

European Commission, 2016. *Introduction to the Connecting Europe Facility: eDelivery building block*. [Online]

Available at: https://ec.europa.eu/cefdigital/wiki/download/attachments/23003331/%28Building%20Block%20DSI_IntroDocument%29%28eDelivery%29%28v1.1%29.pdf?version=1&modificationDate=1475245253141&api=v2

[Accessed 2016].

European Commission, 2016. *The ISA² programme*. [Online]

Available at: http://ec.europa.eu/isa/isa2/index_en.htm

[Accessed 2016].

Fallman, D., 2008. The Interaction Design Research Triangle of Design Practice, Design Studies, and Design Exploration. *Design Issues, MIT*, 24(3).

FIDO Alliance, 2016. *FIDO Alliance*. [Online]

Available at: <https://fidoalliance.org/>

[Accessed 05 10 2016].

Document name:	Inventories (2)	Page:	152 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



French Government, 2006. *DADVSI*. [Online]

Available at: <http://www.assemblee-nationale.fr/12/dossiers/031206.asp>

[Accessed 2016].

FutureID, 2015. *FutureID Project*. [Online]

Available at: www.futureid.eu

Geant, 2016. *eduRoam/eduGAIN*. [Online]

Available at: http://www.geant.org/Services/Trust_identity_and_security/eduGAIN

[Accessed 01 2017].

Gipp, B. & Gernandt, A., 2014. *OriginStamp*. [Online]

Available at: <http://www.originstamp.org/>

[Accessed 2016].

Gipp, B., Meuschke, N. & Gernandt, A., 2015. *Decentralized Trusted Timestamping using the Crypto Currency Bitcoin*. [Online]

Available at: <http://www.gipp.com/wp-content/papercite-data/pdf/gipp15a.pdf>

[Accessed 2016].

H. Ferraiolo, e. a., 2014. *Guidelines for Derived Personal Identity Verification (PIV) Credentials, NIST Special Publication 800-157*, Gaithersburg, MD: National Institute of Standards and Technology (NIST).

Helen Ltd. , 2016. *Helen Ltd.*. [Online]

Available at: <https://www.helen.fi/en/helen--oy/>

[Accessed 2017].

Huehnlein, D., 2016. *SkIDentity*. [Online]

Available at: <https://www.skidentity.de/en/home/>

[Accessed 06 10 2016].

Hughes, A., 2016. *Trust Frameworks Explained*, Unknown: Kantara Initiative.

ID.me, 2016. *ID.me*. [Online]

Available at: <https://www.id.me/>

[Accessed December 2016].

IDEF, 2016. *Frequently Asked Questions*. [Online]

Available at: <https://www.idesg.org/About/FAQ>

[Accessed December 2016].

IDESG, 2016. *Identity Ecosystem Framework Registry*. [Online]

Available at: <https://www.idesg.org/The-ID-Ecosystem/Registry>

[Accessed December 2016].

Document name:	Inventories (2)	Page:	153 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



IETF, 2001. *RFC 3161 Internet X.509 Public Key Infrastructure*. [Online]
Available at: <https://www.ietf.org/rfc/rfc3161.txt>
[Accessed 2016].

IETF, 2003. *RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs)*. [Online]
Available at: <https://www.ietf.org/rfc/rfc3628.txt>
[Accessed 2016].

IETF, 2010. *RFC 5816 ESSCertIDv2 Update for RFC 3161*. [Online]
Available at: <https://www.ietf.org/rfc/rfc5816.txt>
[Accessed 2016].

IETF, 2010. *RFC5914: Trust Anchor Format*. [Online]
Available at: <https://tools.ietf.org/html/rfc5914>
[Accessed 01 2017].

IETF, 2010. *RFC5934: Trust Anchor Management Protocol (TAMP)*. [Online]
Available at: <https://tools.ietf.org/html/rfc5934>
[Accessed 01 2017].

IETF, 2010. *RFC6024: Trust Anchor Management Requirements*. [Online]
Available at: <https://tools.ietf.org/html/rfc6024>
[Accessed 01 2017].

Ihalainen, P., 2007. <https://joinup.ec.europa.eu/community/epractice/case/identity-management-authorization-and-authentication-platform>. [Online]
[Accessed 2017].

Ihalainen, P., 2007. <https://joinup.ec.europa.eu/community/epractice/case/identity-management-authorization-and-authentication-platform>. [Online]
Available at: <https://joinup.ec.europa.eu/community/epractice/case/identity-management-authorization-and-authentication-platform>
[Accessed February 2017].

Initiative, K., 2016. *Kantara Initiative*. [Online]
Available at: <https://kantarainitiative.org/trust-registry/ktr-status-list/>
[Accessed December 2016].

ISO, 2002. *ISO/IEC 15945:2002(en) Information technology — Security techniques — Specification of TTP services to support the application of digital signatures*. [Online]
Available at: <https://www.iso.org/obp/ui/#iso:std:iso-iec:15945:ed-1:v1:en>
[Accessed 2016].

ISO, 2008. *ISO/IEC 29500-2:2008*. [Online]
Available at:

Document name:	Inventories (2)	Page:	154 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51459
[Accessed 2016].

ISO, 2013. *ISO/IEC 18014*. [Online]

Available at: <http://www.iso.org/iso/search.htm?qt=18014&type=simple&published=on>
[Accessed 2017].

ISO, 2013. *ISO/IEC 29115:2013 Information technology -- Security techniques -- Entity authentication assurance*. [Online]

Available at: http://www.iso.org/iso/catalogue_detail.htm?csnumber=45138
[Accessed 2016].

ISO, 2016. *ISO 8601*. [Online]

Available at:

http://www.iso.org/iso/home/search.htm?qt=8601&published=on&active_tab=standards&sort_by=rel
[Accessed 2017].

ISO, 2016. *OSI Model*. [Online]

Available at:

http://www.iso.org/iso/home/search.htm?qt=7498&published=on&active_tab=standards&sort_by=rel
[Accessed 2017].

ITU, 2009. *X.1250 : Baseline capabilities for enhanced global identity management and interoperability*. [Online]

Available at: <https://www.itu.int/rec/T-REC-X.1250-200909-l>
[Accessed 2016].

ITU, 2010. *ITU-T X.1275 (12/2010) Guidelines on protection of personally identifiable information in the application of RFID technology*. [Online]

Available at: <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.1275>
[Accessed 2016].

ITU, 2010. *X.1252 : Baseline identity management terms and definitions*. [Online]

Available at: <https://www.itu.int/rec/T-REC-X.1252-201004-l>
[Accessed 2016].

ITU, 2011. *ITU-T X.1253 (09/2011) Security guidelines for identity management systems*. [Online]

Available at: <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11343&lang=en>
[Accessed 2016].

ITU, 2012. *X.1254 : Entity authentication assurance framework*. [Online]

Available at: <https://www.itu.int/rec/T-REC-X.1254-201209-l>
[Accessed 2016].

Document name:	Inventories (2)	Page:	155 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



ITU, 2013. X.1255 : *Framework for discovery of identity management information*. [Online]
Available at: <https://www.itu.int/rec/T-REC-X.1255-201309-l>
[Accessed 2016].

ITU, 2016. X.509. [Online]
Available at: <http://www.itu.int/rec/T-REC-X.509/en>
[Accessed 2017].

Kristina Hook, J. L., 2012. Strong Concepts: Intermediate-level Knowledge in Interaction Design Research. *ACM Transactions on Computer-Human Interaction*, 19(3).

Leitold, H., Lioy, A. & Ribeiro, C., 2014. *STORK 2.0: Breaking New Grounds on eID and Mandates*, s.l.: Proceedings of ID World International Congress.

Liberty Alliance Project, 2016.
http://www.projectliberty.org/liberty/content/download/417/2814/file/Finland_casestudyFINAL.pdf
. [Online]
Available at:
http://www.projectliberty.org/liberty/content/download/417/2814/file/Finland_casestudyFINAL.pdf
[Accessed 2017].

Liberty Alliance Project, n.d.
http://www.projectliberty.org/liberty/content/download/417/2814/file/Finland_casestudyFINAL.pdf
. [Online].

M. Talamo, M. L. B. D. M. a. C. S., 2014. *Global Convergence in Digital and Attribute Management: Emerging Needs for Standardization*. St. Petersburg, s.n.

Mapfre, 2016. *teCuidamos*. [Online]
Available at: <https://www.mapfre.es/oim/ValidarIdentificacionAction.do>

Masinter, L. B.-L. T. F. R., 2005. *Uniform resource identifier (URI): Generic syntax*, s.l.: s.n.

Michael Kubach, H. L. H. R. C. H. S. M. T., 2015. *SSEDIC.2020 on Mobile eID*. Bonn, Germany, Gesellschaft für Informatik.

Mockapetris, P. V., 1983. *Domain names: Implementation specification*, s.l.: s.n.

Mockapetris, P. V., 1987. *Domain names-concepts and facilities*, s.l.: s.n.

modinis, 2005. *Modinis study on identity management in eGovernment, 'Common Terminological Framework for Interoperable Electronic Identity Management'*. [Online]
Available at: <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf>
[Accessed 2016].

Document name:	Inventories (2)	Page:	156 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



NATE, 2016. *National Association for Trusted Exchange*. [Online]
Available at: <http://nate-trust.org/nbb4c-trust-bundle/>
[Accessed December 2016].

NIST, 2013. *FIPS PUB 186-4 Digital Signature Standard (DSS)*. [Online]
Available at: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>
[Accessed 2016].

NIST, 2015. *Draft NISTIR 8062: Privacy Risk Management for Federal Information Systems*. [Online]
Available at: http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf
[Accessed 2016].

NIST, 2015. *NSTIC Pilots: Catalyzing the Identity Ecosystem*. [Online]
Available at: <http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8054.pdf>
[Accessed 2016].

NIST, 2016. *Developing Trust Frameworks to Support Identity Federations*. [Online]
Available at: http://csrc.nist.gov/publications/drafts/nistir-8149/nistir_8149_draft.pdf
[Accessed 2016].

NIST, 2016. *Draft NISTIR 8112: Attribute Metadata*. [Online]
Available at: http://csrc.nist.gov/publications/drafts/nistir-8112/nistir_8112_draft.pdf
[Accessed 2016].

NIST, 2016. *National Strategy for Trusted Identities in Cyberspace*. [Online]
Available at: <https://www.nist.gov/itl/nstic>
[Accessed 2016].

NIST, 2016. *NISTIR 8149 (Draft) Developing Trust Frameworks to Support Identity Federation*. [Online]
Available at: <https://pages.nist.gov/NISTIR-8149/>
[Accessed 01 2017].

NIST, 2016. *NSTIC: Pilot Projects & Partners*. [Online]
Available at: <https://www.nist.gov/itl/nstic/pilot-projects>
[Accessed 2016].

NIST, 2017. *NIST: Information Technology Laboratory. Trusted Identities Group*. [Online]
Available at: <https://www.nist.gov/itl/tig>
[Accessed 2017].

OASIS, 2007. *Advanced Electronic Signature: Profiles of the OASIS Digital Signature Service (v. 1.0)*. [Online]
Available at: <http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-AdES-spec-v1.0-os.pdf>
[Accessed 2016].

Document name:	Inventories (2)	Page:	157 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



OASIS, 2007. *Digital Signature Service Core: Protocols, Elements, and Bindings (v. 1.0)*. [Online]
Available at: <http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf>
[Accessed 2016].

OASIS, 2007. *Digital Signature Service Overview*. [Online]
Available at: <http://www.oasis-open.org/committees/download.php/22725/oasis-dss-overview.pdf>
[Accessed 2016].

OASIS, 2007. *Signature Gateway Profile of the OASIS Digital Signature Service (v. 1.0)*. [Online]
Available at: <http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-SignatureGateway-spec-v1.0-os.pdf>
[Accessed 2016].

OASIS, 2007. *XML Timestamping Profile of the OASIS Digital Signature Services (v. 1.0)*. [Online]
Available at: <https://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-timestamping-spec-v1.0-os.pdf>
[Accessed 2016].

OASIS, 2010. *Security Assertion Markup Language (SAML)*. [Online]
Available at: <http://xml.coverpages.org/saml.html>
[Accessed 2017].

OASIS, 2016. *Digital Signature Services (DSS) TC: Defining an XML interface to process digital signatures for Web services and other applications*. [Online]
Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss
[Accessed 2016].

OASIS, 2016. *Technical Work Produced by the Committee*. [Online]
Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss#technical
[Accessed 2016].

OASIS, 2017. *OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC*. [Online]
Available at: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=trust-el
[Accessed 2017].

Office of the Privacy Commissioner of Canada, 2008. *PIPEDA Review*. [Online]
Available at: http://web.archive.org/web/20100813133308/http://www.priv.gc.ca/keyIssues/ki-gc/mc-ki-pipeda_e.cfm
[Accessed 2017].

OIX, 2016. *OIX.net*. [Online]
Available at: <http://oixnet.org/>
[Accessed December 2016].

Document name:	Inventories (2)	Page:	158 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



OIX, 2016. *Papers: Open Identity Exchange*. [Online]
Available at: <http://www.openidentityexchange.org/papers/>
[Accessed 2017].

OIXnet, 2016. *Minors Trust Framework*. [Online]
Available at: <http://oixnet.org/registry/minors-trust-framework/>
[Accessed 2016].

OIXnet, 2016. *Mydex Trust Framework*. [Online]
Available at: <http://oixnet.org/registry/mydex/>
[Accessed 2016].

OIXnet, 2016. *NATE Blue Button for Consumers (NBB4C) Trust Bundle*. [Online]
Available at: <http://oixnet.org/registry/nate-blue-button-for-consumers-nbb4c-trust-bundle/>
[Accessed 2016].

OIXnet, 2016. *OIXnet Registry*. [Online]
Available at: <http://oixnet.org/registry/>
[Accessed 2016].

OIXnet, 2016. *OpenID Certification Program*. [Online]
Available at: <http://oixnet.org/openid-certifications/>
[Accessed 2016].

OIXnet, 2016. *Respect Trust Framework*. [Online]
Available at: <http://oixnet.org/registry/respect-network/>
[Accessed 2016].

OIXnet, 2016. *SAFE-BioPharm Global Trust Framework Program*. [Online]
Available at: <http://oixnet.org/registry/safe-biopharma-global-ftp/>
[Accessed 2016].

OIXnet, 2016. *SAFE-BioPharma Bridge Certification Authority (PKI Bridge CA)*. [Online]
Available at: <http://oixnet.org/registry/safe-biopharma-pki-bridge-ca/>
[Accessed 2016].

OIXnet, 2016. *SAFE-BioPharma FICAM Trust Framework Provider Program*. [Online]
Available at: <http://oixnet.org/registry/safe-biopharma-ficam-ftp/>
[Accessed 2016].

OIXnet, 2016. *SecureKey Concierge Trust Framework*. [Online]
Available at: <http://oixnet.org/registry/securekey-concierge/>
[Accessed 2016].

OIXnet, 2016. *tScheme*. [Online]
Available at: <http://oixnet.org/registry/tscheme/>
[Accessed 2016].

Document name:	Inventories (2)	Page:	159 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



OpenID Foundation, 2016. *International Government Assurance Profile (iGov) Working Group Draft Project Charter*. [Online]

Available at: <http://openid.net/igov-wg-draft-charter/>
[Accessed 2016].

OpenID MODRNA WG, 2016. *OpenID MODRNA WG*. [Online]

Available at: <http://openid.net/wg/mobile/>
[Accessed 18 01 2017].

OpenID, 2016. *OpenID Certification*. [Online]

Available at: <http://openid.net/certification/>
[Accessed 2016].

PEPPOL, 2016. *Pan-European Public Procurement Online*. [Online]

Available at: <http://www.peppol.eu/>
[Accessed 2016].

Postel, J., 1982. Simple mail transfer protocol. *Information Sciences*.

Privo, 2016. *Privo*. [Online]

Available at: <https://privo.com/minors-trust-framework/>
[Accessed December 2016].

Project, S., 2015. *SkIdentity Project*. [Online]

Available at: www.skidentity.de

Radiology Universe Institute, 2015. *TrueTimeStamp*. [Online]

Available at: <http://truetimestamp.org/>
[Accessed 2016].

Regulation, e., 2014. *Regulation (EC) No 910/2014/EU Article 22*. [Online]

Available at: <http://data.europa.eu/eli/reg/2014/910/oj>
[Accessed 01 2017].

Respect Network, 2016. *Respect Network*. [Online]

Available at: <https://www.respectnetwork.com/>
[Accessed 2016].

Respect, 2016. *Respect Network: The Personal Cloud Network*. [Online]

Available at: <https://respectnetwork.wordpress.com/the-personal-channel/>
[Accessed December 2016].

Rössler, T. & Hollos, A., 2006. *Elektronische Vollmachten - Spezifikation 1.0.0*, s.l.: s.n.

Rusia, 2011. *FEDERAL LAW OF THE RUSSIAN FEDERATION About the digital signature*. [Online]

Document name:	Inventories (2)	Page:	160 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Available at: <http://cis-legislation.com/document.fwx?rgn=32989>
[Accessed 2016].

Russia, 2011. *FEDERAL LAW OF THE RUSSIAN FEDERATION About the digital signature.* [Online]

Available at: <http://cis-legislation.com/document.fwx?rgn=32989>
[Accessed 2016].

SAFE-BioPharma, 2016. *SAFE-BioPharma Infocenter.* [Online]

Available at: <https://www.safe-biopharma.org/infocenter.html>
[Accessed 2016].

SANS Institute Reading Room, 2001. *Analysis of a Secure Time Stamp Device.* [Online]

Available at: <https://www.sans.org/reading-room/whitepapers/vpns/analysis-secure-time-stamp-device-746>
[Accessed 2016].

SEALED, t. a. S., 2010. *CROBIES: Quality Classification Scheme for eSignature elements.* [Online]

Available at: http://users.skynet.be/fa283208/pdf/INFSO-CROBIES-DFC-WP5-2-SEALED-29032010_v1.pdf
[Accessed 2017].

SecureKey, 2015. *TRUST FRAMEWORK – SECUREKEY CONCIERGE IN CANADA*, Canada: SecureKey.

SecureKey, 2016. *SecureKey Concierge.* [Online]

Available at: <http://securekeyconcierge.com/>
[Accessed December 2016].

SecureKeyTechnologies, 2016. *SecureKey Technologies.* [Online]

Available at: <http://securekeyconcierge.com/>
[Accessed 2016].

Services, i. E. e., 2009. *eID Interoperability for PEGS: Update of Country Profiles study: Finnish country profile*, s.l.: s.n.

Skatt, V., 2017. [Online]

Available at: [https://www.vero.fi/en-US/Precise_information/eFiling/Katso_Identification/Users_guide/Katso_detailed_instructions\(14133\)](https://www.vero.fi/en-US/Precise_information/eFiling/Katso_Identification/Users_guide/Katso_detailed_instructions(14133))
[Accessed 2017].

Skatt, V., 2017. https://www.vero.fi/en-US/Precise_information/eFiling/Katso_Identification. [Online]

Document name:	Inventories (2)	Page:	161 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



Available at: https://www.vero.fi/en-US/Precise_information/eFiling/Katso_Identification
[Accessed February 2017].

SPOCS, 2012. *Simple Procedures Online for Cross-border Services*. [Online]

Available at: <http://www.eu-spocs.eu/>

[Accessed 2016].

SpringerLink, 2009. *Empowerment through Electronic Mandates – Best Practice Austria*. [Online]

Available at: http://link.springer.com/chapter/10.1007%2F978-3-642-04280-5_13#page-1

[Accessed 2016].

STORK 2.0, 2014. *Summary of D3.6 Legal Entities Identification Report*. [Online]

Available at: [https://www.eid-](https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=category&id=9&Itemid=175&limitstart=5)

[stork2.eu/index.php?option=com_phocadownload&view=category&id=9&Itemid=175&limitstart=5](https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=category&id=9&Itemid=175&limitstart=5)

[Accessed 2016].

STORK 2.0, 2015. *AQAA Guidelines*. [Online]

Available at: [https://www.eid-](https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=54:d32-addendum-aqaa-guidelines&Itemid=175)

[stork2.eu/index.php?option=com_phocadownload&view=file&id=54:d32-addendum-aqaa-guidelines&Itemid=175](https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=54:d32-addendum-aqaa-guidelines&Itemid=175)

[Accessed 2016].

STORK 2.0, 2015. *D2.1 Existing e-ID infrastructure analysis*. [Online]

Available at: [https://www.eid-](https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=3:d21-existing-e-id-infrastructure-analysis&Itemid=176)

[stork2.eu/index.php?option=com_phocadownload&view=file&id=3:d21-existing-e-id-infrastructure-analysis&Itemid=176](https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=3:d21-existing-e-id-infrastructure-analysis&Itemid=176)

[Accessed 2016].

STORK 2.0, 2015. *D3.2 - QAA Status Report*. [Online]

Available at: [https://www.eid-](https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=6:d32-qaa-status-report&Itemid=175)

[stork2.eu/index.php?option=com_phocadownload&view=file&id=6:d32-qaa-status-report&Itemid=175](https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=6:d32-qaa-status-report&Itemid=175)

[Accessed 2016].

STORK 2.0, 2015. *D3.2 Addendum. AQAA Guidelines*. [Online]

Available at: [https://www.eid-](https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=54:d32-addendum-aqaa-guidelines&Itemid=175)

[stork2.eu/index.php?option=com_phocadownload&view=file&id=54:d32-addendum-aqaa-guidelines&Itemid=175](https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=54:d32-addendum-aqaa-guidelines&Itemid=175)

[Accessed 2016].

STORK 2.0, 2015. *D3.2 QAA Status Report*. [Online]

Available at: [https://www.eid-](https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=6:d32-qaa-status-)

[stork2.eu/index.php?option=com_phocadownload&view=file&id=6:d32-qaa-status-](https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=6:d32-qaa-status-)

Document name:	Inventories (2)	Page:	162 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



[report&Itemid=175](#)

[Accessed 2016].

STORK 2.0, 2015. *D3.3 Mandate/Attribute Management Report*. [Online]

Available at: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=7:d33-mandateattribute-management-report&Itemid=175

[Accessed 2016].

STORK 2.0, 2015. *D3.5 Consolidated Legal Entities Identification Report*. [Online]

Available at: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=8:d35-legal-entities-identification-report&Itemid=175&start=5

[Accessed 2016].

STORK 2.0, 2015. *D4.10 Final version of Technical Design*. [Online]

Available at: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=71:d410-final-version-of-technical-design&Itemid=174

[Accessed 2016].

STORK 2.0, 2015. *D4.9 Final version of Functional Design*. [Online]

Available at: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=66:d49-final-version-of-functional-design&Itemid=174&start=5

[Accessed 2016].

STORK 2.0, 2015. *D4.9 Final version of Functional Design*. [Online]

Available at: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=66:d49-final-version-of-functional-design&Itemid=174

[Accessed 2016].

STORK 2.0, 2015. *D5.3.4 eGov4Business Pilot Progress Report*. [Online]

Available at: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=59:d534-egov4business-pilot-progress-report&Itemid=176&start=15

[Accessed 2016].

STORK 2.0, 2016. *D4.13 Final version of common building blocks*. [Online]

Available at: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=80:-d413-final-version-of-common-building-blocks&Itemid=174&start=10

[Accessed 2016].

Document name:	Inventories (2)	Page:	163 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



STORK 2.0, 2016. *D5.3.5 eGovernment Pilot Final Report*. [Online]
Available at: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=85:d535-egovernment-pilot-final-report&Itemid=176&start=15

[Accessed 2016].

STORK 2.0, 2016. *Public Services for Business Pilot*. [Online]
Available at: https://www.eid-stork2.eu/pilots/public_services/index.php/en/

[Accessed 2016].

STORK, 2012. *Related documents to STORK: D2.3-Quality authenticator scheme*. [Online]

Available at: https://www.eid-stork2.eu/index.php?option=com_content&task=view&id=366&Itemid=96

[Accessed 2016].

STORK, 2014. *STORK QAA revised 2014 MS Comments Summary as eIDAS Expert Group Input*, EU: STORK.

The e-Signature Law Journal, 2005. *Electronic signatures in Russian law*. [Online]

Available at: <http://www.russianlaw.net/files/law/english/ae08.doc>

[Accessed 2016].

The White House, 2011. *National Strategy for Trusted Identities in Cyberspace*. [Online]

Available at:

https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[Accessed 2016].

tScheme, 2016. *tScheme*. [Online]

Available at: <http://www.tscheme.org/>

[Accessed December 2016].

tScheme, 2016. *tScheme website*. [Online]

Available at: <http://www.tscheme.org/index.html>

[Accessed 2016].

UK Government, 2010. *Digital Economy Act 2010*. [Online]

Available at: <http://www.legislation.gov.uk/ukpga/2010/24/contents>

[Accessed 2017].

UN, 2016. *Official Document System*. [Online]

Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/490/26/PDF/N0149026.pdf?OpenElement>

[Accessed 2016].

UNCITRAL, 2001. *Model Law on Electronic Signatures*. [Online]

Available at:

Document name:	Inventories (2)	Page:	164 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html

[Accessed 2016].

Union, I. T., 1999. *Message Handling Recommendations this edition of ITU-T Recommendation F.400/X.400*, s.l.: ITU-T.

Universal Postal Union, 2016. *The UPU: Universal Postal Union*. [Online]

Available at: <http://www.upu.int/en.html>

[Accessed 2016].

UPU, 2016. *UPU Technical Standards*. [Online]

Available at:

http://www.upu.int/uploads/tx_sbdownloader/orderFormStandardsUpuTechnicalStandardsSingleCopyOrderFormEn_02.pdf

[Accessed 2016].

US government, 1998. *THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998*. [Online]

Available at: <http://www.copyright.gov/legislation/dmca.pdf>

[Accessed 2016].

US Government, 2000. *Electronic Signatures in Global and National Commerce Act*. [Online]

Available at: <https://www.gpo.gov/fdsys/pkg/BILLS-106s761enr/pdf/BILLS-106s761enr.pdf>

[Accessed 2017].

US Government, 2013. *Digital Signature and Electronic Authentication Law*. [Online]

Available at: <https://www.congress.gov/>

[Accessed 2017].

US Government, 2016. *Commodity Futures Trading Commission (CFTC)*. [Online]

Available at: <https://web.archive.org/web/20090506062234/http://www.cftc.gov/>

[Accessed 2017].

US Government, 2017. *Federal Reserve System*. [Online]

Available at: <https://www.federalreserve.gov/>

[Accessed 2017].

US Government, 2017. *Food and Drug Administration (FDA or USFDA)*. [Online]

Available at: <http://www.fda.gov/>

[Accessed 2017].

US Legal Inc., 2016. *Digital Distribution Law & Legal Definition*. [Online]

Available at: <http://definitions.uslegal.com/d/digital-distribution/>

[Accessed 2016].

US, 1999. *Uniform Electronic Transactions Act*. [Online]

Available at:

Document name:	Inventories (2)	Page:	165 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf
[Accessed 2016].

US, 1999. *Uniform Electronic Transactions Act*. [Online]

Available at:

http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf
[Accessed 2016].

USPTO, 2015. *Filing Papers With the U.S. Patent and Trademark Office*. [Online]

Available at:

<https://www.uspto.gov/web/offices/pac/mpep/s501.html#sect501%7Cpublisher=USPTO>
[Accessed 2016].

W. E. Burr, e. a., 2013. *Electronic Authentication Guideline, NIST Special Publication 800-63-2*, Gaithersburg, MD: National Institute of Standards and Technology (NIST).

wikipedia, 1988. *Digital Millennium Copyright Act*. [Online]

Available at: https://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act
[Accessed 2016].

wikipedia, 2003. *Government Paperwork Elimination Act*. [Online]

Available at: https://en.wikipedia.org/wiki/Government_Paperwork_Elimination_Act
[Accessed 2016].

wikipedia, 2003. *ZertES*. [Online]

Available at: <https://en.wikipedia.org/wiki/ZertES>
[Accessed 2016].

wikipedia, 2005. *An Act to amend the Copyright Act (38th Canadian Parliament, 1st Session)*. [Online]

Available at:

[https://en.wikipedia.org/wiki/An_Act_to_amend_the_Copyright_Act_\(38th_Canadian_Parliament,_1st_Session\)](https://en.wikipedia.org/wiki/An_Act_to_amend_the_Copyright_Act_(38th_Canadian_Parliament,_1st_Session))
[Accessed 2016].

wikipedia, 2006. *39th Canadian Parliament*. [Online]

Available at: https://en.wikipedia.org/wiki/39th_Canadian_Parliament
[Accessed 2016].

wikipedia, 2006. *DADVSI*. [Online]

Available at: <https://en.wikipedia.org/wiki/DADVSI>
[Accessed 2016].

wikipedia, 2010. *An Act to amend the Copyright Act (40th Canadian Parliament, 3rd Session)*. [Online]

Available at:

Document name:	Inventories (2)	Page:	166 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



[https://en.wikipedia.org/wiki/An_Act_to_amend_the_Copyright_Act_\(40th_Canadian_Parliament,_3rd_Session\)](https://en.wikipedia.org/wiki/An_Act_to_amend_the_Copyright_Act_(40th_Canadian_Parliament,_3rd_Session))

[Accessed 2016].

wikipedia, 2010. *Digital Economy Act 2010*. [Online]

Available at: https://en.wikipedia.org/wiki/Digital_Economy_Act_2010

[Accessed 2016].

wikipedia, 2013. *Digital Signature and Electronic Authentication Law*. [Online]

Available at: https://en.wikipedia.org/wiki/Digital_Signature_and_Electronic_Authentication_Law

[Accessed 2016].

wikipedia, 2013. *ISO/IEC 18014*. [Online]

Available at: https://en.wikipedia.org/wiki/ISO/IEC_18014

[Accessed 2016].

wikipedia, 2016. *ANSI ASC X9.95 Standard*. [Online]

Available at: https://en.wikipedia.org/wiki/ANSI_ASC_X9.95_Standard

[Accessed 2016].

wikipedia, 2016. *Commodity Futures Trading Commission (CFTC)*. [Online]

Available at: https://en.wikipedia.org/wiki/Commodity_Futures_Trading_Commission

[Accessed 2016].

wikipedia, 2016. *Electronic signatures and law*. [Online]

Available at: https://en.wikipedia.org/wiki/Electronic_signatures_and_law

[Accessed 2016].

wikipedia, 2016. *Electronic Signatures in Global and National Commerce Act*. [Online]

Available at:

https://en.wikipedia.org/wiki/Electronic_Signatures_in_Global_and_National_Commerce_Act

[Accessed 2016].

wikipedia, 2016. *Federal Reserve System*. [Online]

Available at: https://en.wikipedia.org/wiki/Federal_Reserve

[Accessed 2016].

wikipedia, 2016. *Food and Drug Administration (FDA or USFDA)*. [Online]

Available at: https://en.wikipedia.org/wiki/Food_and_Drug_Administration

[Accessed 2016].

wikipedia, 2016. *ISO 8601*. [Online]

Available at: https://en.wikipedia.org/wiki/ISO_8601

[Accessed 2016].

Document name:	Inventories (2)	Page:	167 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



wikipedia, 2016. *OSI Model*. [Online]
Available at: https://en.wikipedia.org/wiki/OSI_model
[Accessed 2016].

wikipedia, 2016. *Personal Information Protection and Electronic Documents Act*. [Online]
Available at: <https://en.wikipedia.org/wiki/PIPEDA>
[Accessed 2016].

wikipedia, 2016. *Trusted timestamping*. [Online]
Available at: https://en.wikipedia.org/wiki/Trusted_timestamping
[Accessed 2016].

wikipedia, 2016. *X.509*. [Online]
Available at: <https://en.wikipedia.org/wiki/X.509>
[Accessed 2016].

xDTM Standard Association, 2016. *xDTM: The Transaction Management Standard for an Open Digital World*. [Online]
Available at: <http://www.xdtm.org/>
[Accessed 2016].

Document name:	Inventories (2)	Page:	168 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



12. Project Description

LIGHTest project to build a global trust infrastructure that enables electronic transactions in a wide variety of applications

An ever increasing number of transactions are conducted virtually over the Internet. How can you be sure that the person making the transaction is who they say they are? The EU-funded project LIGHTest addresses this issue by creating a global trust infrastructure. It will provide a solution that allows one to distinguish legitimate identities from frauds. This is key in being able to bring an efficiency of electronic transactions to a wide application field ranging from simple verification of electronic signatures, over eProcurement, eJustice, eHealth, and law enforcement, up to the verification of trust in sensors and devices in the Internet of Things.

Traditionally, we often knew our business partners personally, which meant that impersonation and fraud were uncommon. Whether regarding the single European market place or on a Global scale, there is an increasing amount of electronic transactions that are becoming a part of peoples everyday lives, where decisions on establishing who is on the other end of the transaction is important. Clearly, it is necessary to have assistance from authorities to certify trustworthy electronic identities. This has already been done. For example, the EC and Member States have legally binding electronic signatures. But how can we query such authorities in a secure manner? With the current lack of a worldwide standard for publishing and querying trust information, this would be a prohibitively complex leading to verifiers having to deal with a high number of formats and protocols.

The EU-funded LIGHTest project attempts to solve this problem by building a global trust infrastructure where arbitrary authorities can publish their trust information. Setting up a global infrastructure is an ambitious objective; however, given the already existing infrastructure, organization, governance and security standards of the Internet Domain Name System, it is with confidence that this is possible. The EC and Member States can use this to publish lists of qualified trust services, as business registrars and authorities can in health, law enforcement and justice. In the private sector, this can be used to establish trust in inter-banking, international trade, shipping, business reputation and credit rating. Companies, administrations, and citizens can then use LIGHTest open source software to easily query this trust information to verify trust in simple signed documents or multi-faceted complex transactions.

The three-year LIGHTest project starts on September 1st and has an estimated cost of almost 9 Million Euros. It is partially funded by the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321. The LIGHTest consortium consists of 14 partners from 9 European countries and is coordinated by Fraunhofer-Gesellschaft. To reach out beyond Europe, LIGHTest attempts to build up a global community based on international standards and open source software.

Document name:	Inventories (2)	Page:	169 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final



Inventories (2)



The partners are ATOS (ES), Time Lex (BE), Technische Universität Graz (AT), EEMA (BE), G&D (DE), Danmarks tekniske Universitet (DK), TUBITAK (TR), Universität Stuttgart (DE), Open Identity Exchange (GB), NLNet Labs (NL), CORREOS (ES), IBM Danmark (DK) and Globalsign (FI). The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.

Document name:	Inventories (2)	Page:	170 of 170
Dissemination:	PU	Version:	2.5
		Status:	Final

