D7.1

Definition of Requirements for derivation and attestation of mobile IDs

Document Identification	
Date	22.02.2017
Status	Final
Version	Version 1.0

Related WP	WP 2	**Related Deliverable(s)**	D2.1
Lead Authors	F.-M. Kamm	**Dissemination Level**	PU
Lead Participants	G&D	**Contributors**	ATOS, TUBITAK, OIX, FHG, TUG
Reviewers	Sebastian Mödersheim (DTU), Rachelle Sellung (USTUTT)		

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

1. Executive Summary

The overall focus of the LIGHTest project is to develop a lightweight trust infrastructure providing parties of electronic transactions with automatic validation of trust based on their individual trust policies. Most of the electronic transactions considered in this context are somehow related to electronic identities. Since LIGHTest has a focus on person related identities, this requirements document also focuses on person related identities and their needs to establish a continuous trust chain over the identity lifecycle.

As the use of mobile devices is more and more dominating the landscape of electronic transactions, WP7 concentrates on defining and realizing a system of mobile electronic identities that can be used for a large group of use cases like identification, authentication and signing of transaction data. This background immediately suggests several trust schemes with their respective trust publication authorities that are interrelated and require a mutual coordination as well as a propagation of trust-related information. For defining the requirements, the ultimate trust-related question of the derived mobile ID scheme is for the relying party how to assess the overall Level of Assurance (LoA) of the presented mobile ID. Consequently, the challenge of the requirements work is to define a scheme in which the relying party can obtain and verify all information required to assess the overall LoA and trust level of the presented mobile ID.

This deliverable documents the requirements for the ID derivation, the credential storage the device attestation and the propagation of trust information. To approach the complex scenario in a structured way this deliverable will focus on relatively generic requirements on the architecture level.

Section 5 focusses on the requirement of the ID derivation process in which derived credentials are generated based on a primary ID. Section 6 will address the requirements for credential storage on the mobile device taking into account the security properties of the storage environment. The requirements for device attestation will be documented in section 7 followed by the requirements for trust propagation in section 8 allowing for a propagation of trust information along the lifecycle steps of the mobile ID.

2. Document Information

2.1 Contributors

Name	Partner
Frank-Michael Kamm	G&D
Elif Ustundag Soykan	TUBITAK
Edona Fasllija	TUBITAK
Lorenzo Rosa	Atos
Alberto Crespo	Atos
Heiko Roßnagel	FHG
Peter Lipp	TUG
Sue Dawes	OIX

2.2 History

Version	Date	Author	Changes
0.1	14.12.16	F.-M. Kamm	Initial document
0.2	10.01.2017	F.-M. Kamm	Chapter 4 and 6 added.
0.3	02.02.2017	E.Ustundag Soykan, E. Fasllija	Chapter 5.2 added.
0.4	06.02.2017	L. Rosa	Chapter 8 added.
0.5	08.02.2017	F.-M. Kamm	Consolidation of requirements
0.9	09.02.2017	F.-M. Kamm	Finalisation of internal review draft.
1.0	22.02.2017	F.-M. Kamm	Integration of reviewer comments.

3. Table of Contents

3.1 Table of Figures

3.2 Table of Acronyms

BLE	Bluetooth Low Energy
CA	Certificate Authority
DAA	Direct Anonymous Attestation
DNS	Domain Name System
ECC	Elliptic Curve Cryptography
eID	Electronic Identity
eSE	Embedded Secure Element
EU	European Union
FIDO	Fast Identity Online
GSMA	Global System for Mobile Communications Association
ID	Identity
IETF	Internet Engineering Task Force
IoT	Internet of Things
LoA	Level of Assurance
PKI	Public Key Infrastructure
SE	Secure Element
TEE	Trusted Execution Environment
TPM	Trusted Platform Module

4. Introduction

4.1 Background

The overall focus of the LIGHTest project is to develop a lightweight trust infrastructure providing parties of electronic transactions with automatic validation of trust based on their individual trust policies. By using an existing infrastructure of the global Domain Name System (DNS) for publication, querying, and cross-jurisdiction translation of information relevant to make such decisions, including levels of assurance, LIGHTest wants to enable the use of truly “global trust lists”. With this approach LIGHTest will basically provide an infrastructure to enable the most important principles and driving factors of eIDAS on a global level.

Most of the electronic transactions considered in this context are somehow related to electronic identities. In a more general view these identities could be eID related personal identity data (like name, date of birth, etc.) as well as other person related credentials like a cryptographic key used to authorize a payment transaction. Extending this concept further to the Internet of Things (IoT) even device related identities like the identity of a connected car or an industrial machine could be considered. All of these entities can perform transactions that require a certain trust level into the authenticity and integrity of the transaction data and the entity triggering the transaction.

LIGHTest has a focus on person-related identities. Therefore, this requirements document will also focus on person-related identities and their needs to establish a continuous trust chain over the identity lifecycle. However, the approach of defining requirements will start as generic as possible to potentially allow transferring the concept also to purely device-related identities at a later stage.

As the use of mobile devices is more and more dominating the landscape of electronic transactions WP7 will focus mainly on defining and realizing a system of mobile electronic identities that can be used for a large group of use cases like identification, authentication and signing of transaction data. Since these identities are typically related to a primary identity (e.g. a government issued eID card) the focus will be on derived mobile IDs that have been generated after a process of initial identification and a procedure of deriving credentials. These credentials are linked to the primary identity and can be securely stored on mobile devices. The primary ID in this scenario acts as a root of trust for the derived credentials.

This model automatically implies several trust schemes with their respective trust publication authorities that are interrelated and require a mutual coordination as well as a propagation of trust-related information. The situation is depicted in Figure 1. As a basis of ID derivation the issuer of the primary ID has its own trust scheme which can be a government owned scheme for a national ID card as an example. In most cases the issuer of a derived mobile ID will also have its own trust scheme although in a special case this could also be the same as the scheme of the primary ID. A third trust scheme that needs to be considered is the attestation scheme of the mobile device since it provides assurance of the environment used for authentication and

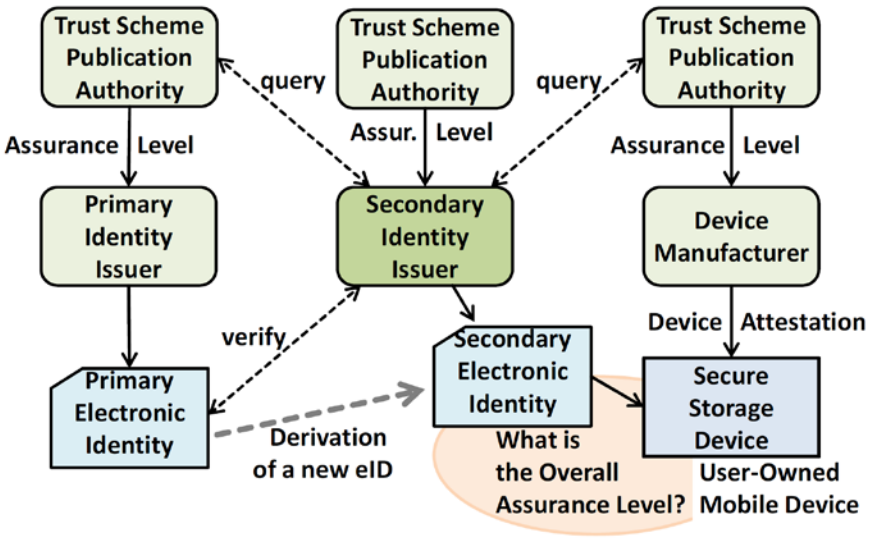

Figure 1: Relation of trust schemes in the case of derived mobile IDs. (Source: DoW).

storage of the mobile ID credentials. In addition, the relying party (not shown in Figure 1) could operate in a fourth trust scheme. To establish a continuous chain of trust these schemes have to query and verify each other and therefore have to access a corresponding trust infrastructure. While the primary and secondary ID issuer may come from the same or similar trust domain (e.g. the eIDAS domain within Europe) the device manufacturer will typically come from a separate domain (e.g. Asia). Thus, even the relatively simple three party relations can immediately create the need for a global trust infrastructure as envisioned by LIGHTest.

For defining the requirements, the ultimate trust-related question of the derived mobile ID scheme is for the relying party how to assess the overall level of assurance of the presented mobile ID. This level is determined by taking into account several boundary conditions along the lifecycle of the derived ID, as shown in Figure 2.

For the process of initial identification, the type of initial ID credential/document and the process of ID verification (e.g. in-person verification or remote verification) are of relevance. When creating the derived credentials, the question will be how strongly these can be linked to the primary ID (e.g. via a cryptographic link) and how well the revocation status of the primary and secondary ID are synchronized. After the derived credentials have been generated they need to be securely stored on the mobile device or some kind of mobile token. Accordingly, the security of the environment used for storage will influence the overall assurance level. Strongly related to this aspect is the existence and type of a device attestation scheme that gives assurance of the integrity of the device authenticator used. Depending on the quality of the attestation (e.g. whether it is a self-claimed attestation of the device manufacturer or an independently verified attestation) the overall assurance level may be influenced.

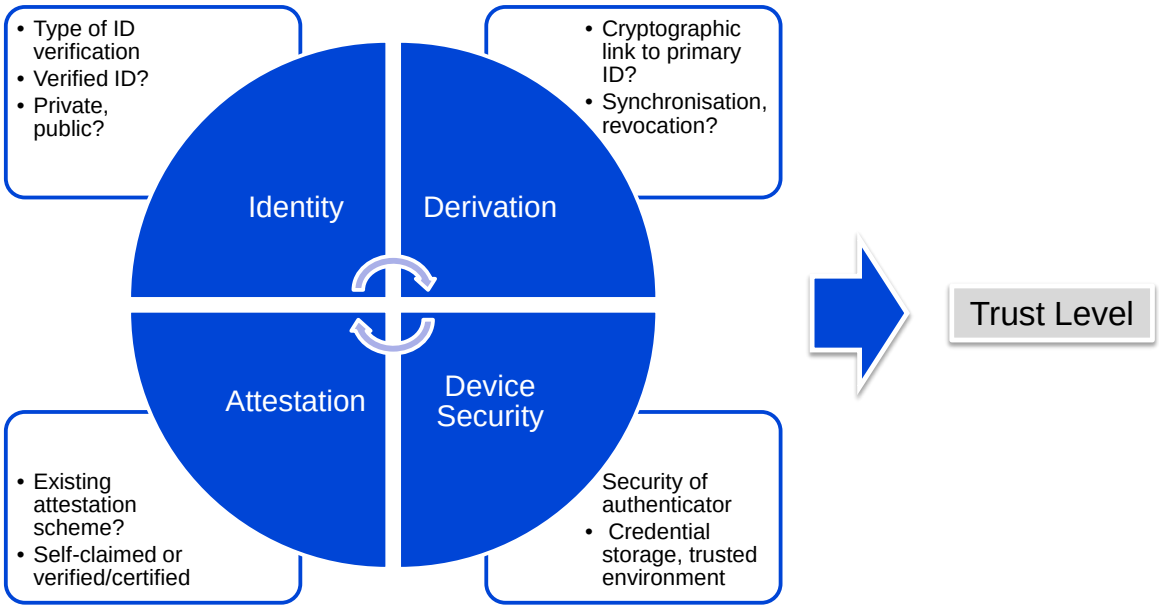

Figure 2: Parameters influencing the overall trust level along the different process steps of derived mobile IDs.

Thus, it will be the challenge of the requirements work to define a scheme in which the relying party can obtain and verify all information required to assess the overall assurance and trust level of the presented mobile ID.

Since LIGHTest will offer the flexibility to integrate different trust schemes, it shall also be possible to create different trust domains. These domains could be regional domains (e.g. Europe, North America, Asia, etc.) as well as application sector domains (e.g. government, payment, industry). In addition, a hierarchical structure is possible like for example a separate trust domain for electronic payment in Europe in contrast to government applications in Europe.

Applied to the use cases of mobile derived IDs in conjunction with a device attestation scheme the following situation should become possible. A specific mobile device coming from a device manufacturer of a certain region may be regarded as applicable for electronic payment applications within Europe while it may not provide sufficient security for governmental mobile IDs in Europe. In North America, where other regulations are effective, the same device might be applicable for mobile ID applications but only up to a certain trust level. As a consequence, a relying party must be able to obtain all required information about the type of mobile identity as well as the type of mobile device authenticator to query the respective trust domain and its corresponding policies. Based on the result the relying party can either accept or reject the specific device type for the respective application.

For the requirements definition it is therefore essential to keep such a scenario in mind and to shape the corresponding requirements accordingly.

4.2 Goal of this deliverable

As outlined in the previous section, the ultimate goal for the derived mobile ID scheme is to establish a continuous chain of trust and to enable the corresponding propagation of trust information along the lifecycle steps of the mobile ID. The relying party shall be enabled to assess the overall trust and assurance level of a mobile ID based on the information obtained during the authentication step and based on the defined policies of the respective trust scheme or trust domain.

This deliverable documents the requirements for the ID derivation, the credential storage the device attestation and the propagation of trust information, taking into account the scenarios and the background described in section 4.1. To approach the complex scenario in a structured way, this deliverable will focus on relatively generic requirements on the architecture level. In a second step, documented in deliverable D 7.2, these generic requirements will be narrowed down to a more concrete scheme taking into account more specific existing mobile ID or mobile authentication schemes like FIDO or GSMA MobileConnect (see deliverables D 2.1 and D 2.2 for an overview of inventories) and their possible extension. This stepwise approach will also allow for a better alignment with the overall requirements work of WP2.

Section 5 focusses on the requirement of the ID derivation process in which derived credentials are generated based on a primary ID. Section 6 will address the requirements for credential storage on the mobile device taking into account the security properties of the storage environment. The requirements for device attestation will be documented in section 7 followed by the requirements for trust propagation allowing for a propagation of trust information along the lifecycle steps of the mobile ID.

5. Requirements for ID derivation

5.1 Introduction

Within the trust chain of derived mobile IDs the ID derivation step is the initial step in which credentials are generated and derived from an existing primary identity. As shown in Figure 1 this is done by the secondary identity issuer which could be for example a private organisation like a bank or a mobile network operator. After verifying the user identity based on a primary ID (like a national eID card) the secondary issuer generates credentials which can be stored in a mobile device and which are by some means linked to the primary ID. Depending on the actual scheme this could be either a direct cryptographic link (e.g. including a key derivation and/or certificate issuance) or an indirect link (e.g. via a user database).

To ensure that ID derivation is carried out effectively and reliably, it is vital that there is a continuous trust chain - from the initial identification to credential generation, provisioning and usage of the identity. This section therefore defines the generic requirements of the derivation step to lay the foundation for further propagation of trust information through the identity lifecycle. These requirements shall be the basis for the next stage of the development and creation of an architecture model that is trusted on a broad range of mobile devices.

The ID Derivation work that is proposed should be co-ordinated with four International bodies:

- IETF,
- GSMA,
- FIDO Alliance and the
- Open ID Foundation.

Co-ordinating the LIGHTest efforts with these International standards bodies is a critical success factor of the global adoption and interoperability of the LIGHTest effort. The goal of the project team is to promote the early awareness and influence on both the LIGHTest project leadership and the appropriate committees within those organisations. We will look to the Advisory Board to provide guidance for the appropriate amount of information sharing, the official liaison relationships and other matters as necessary to ensure positive relation and success of this collaboration

5.2 Requirement definition

Identifier	Level	Description
R_MID_IDev_1	MUST	The Secondary ID Derivation Service MUST provide functionalities for the Creation/ Deletion/ Revocation of the derived ID credentials.
R_MID_IDev_2	MUST	The ID Derivation Service of the Secondary ID Issuer MUST provide functionalities for the Activation/ Deactivation of the derived ID credentials.

Identifier	Level	Description
R_MID_IDev_3	SHOULD	The Secondary ID Derivation Service SHOULD be able to generate derived ID credentials from different primary eID cards.
R_MID_IDev_4	MUST	The Secondary ID Derivation Service MUST be able to derive multiple derived ID Credentials from the selected primary eID credential.
R_MID_IDev_5	MUST	The Secondary ID Derivation Service MUST provide means for the visualisation of the content of the derived ID credential that is to be generated (i.e. which attributes are included in the derived ID credential)
R_MID_IDev_6	MUST	The Secondary ID Derivation Service MUST provide means for the renewal of the validity period of the derived ID credential.
R_MID_IDev_7	MUST	The Secondary ID Derivation Service MUST authenticate itself to its users before the ID derivation process is carried out.
R_MID_IDev_8	MUST	The derived ID credentials MUST be valid only for a limited period of time.
R_MID_IDev_9	SHOULD	The derived ID credentials SHOULD be suitable to be used as replacement of the primary eID credentials for identification, authentication and authorization steps depending on the LoA of the primary eID credential.
R_MID_IDev_10	MUST	The derived ID credentials MUST be stored securely on the mobile device. The level of security may depend on LoA requirements set by the corresponding trust scheme.
R_MID_IDev_11	MUST	The Secondary ID Derivation Service MUST ask for the user's consent on the attributes to be transferred to the derived ID credential.
R_MID_IDev_12	MUST	A minimum set of attributes that are required by the trust scheme of the Secondary ID Issuer to be contained in the derived ID credentials MUST be determined.
R_MID_IDev_13	MUST	The Secondary ID Derivation Process MUST include an identity proofing phase followed by a derived ID issuing phase.
R_MID_IDev_14	MUST	The Secondary ID Derivation Service MUST synchronize the lifecycle and status of the derived ID credential with the primary ID credential.
R_MID_IDev_15	SHOULD	The Secondary ID Derivation Service SHOULD allow for both remote and local derived ID credential provisioning schemes.
R_MID_IDev_16	MUST	End-to-end security MUST be ensured between the primary ID card and the mobile device in the local provisioning case.
R_MID_IDev_17	MUST	A proof of possession of the derived ID credential by the owner MUST be ensured.
R_MID_IDev_18	SHOULD	The Secondary ID Derivation Service SHOULD be able to choose among different available options of security environments on mobile devices, based on the required security level.
R_MID_IDev_19	MUST	The primary ID used for ID derivation MUST have a known and verifiable level of assurance (LoA) within the trust scheme of the primary ID issuer.

6. Requirements for credential storage

6.1 Introduction

Every mobile ID system uses some kind of cryptographic credentials that need to be stored securely in the mobile device or on some kind of token. If an attacker is able to extract, clone or compromise the credentials then he will also be able to compromise or misuse the corresponding identity. Therefore, it is essential to ensure a well-defined security level of the credential storage environment.

The actual absolute security level is not so relevant (except for some minimum security properties) as long as it is well-known and is embedded into the device attestation scheme. For the purpose of trust propagation (see chapter 8) it is essential to have a well-defined security level and to provide the required attestation (see chapter 7) to the relying party. In the context of scalable security it is certainly allowable to support also environments with limited security as long as the resulting impact on overall trust and assurance level is transparent for the relying party. However, these environments with a limited security level must at least provide some measures against extraction and cloning of the credentials.

As an example, secure storage environments can be a SIM/UICC, a contactless or dual interface smart card addressable via NFC, an embedded Secure Element (eSE), an external USB or BLE token, a Trusted Execution Environment (as defined by Global Platform), or a software-secured environment (e.g. cryptographic container secured by Whitebox Crypto). All of these environments differ significantly in security and availability. For applications that require a high or medium level of security (typically hardware-based environments and Trusted Execution Environments) the range of usable mobile devices will be limited. On the other hand, software-based environments provide better scalability but limited security. This trade-off needs to be considered when designing the derived ID system.

To define the requirements of the storage environments it seems reasonable to follow the lifecycle of the identity credentials:

- **Derivation**: when the credentials are derived from a primary ID the credential generation must either occur in a secure environment on the mobile device without the private key leaving the environment or it must be generated in a remote secure environment and exported into the mobile device.
- **Provisioning**: in case that the storage environment on the mobile device does not allow for a secure credential generation, the derived credentials need to be provisioned via an end-to-end secured channel between the credential generation environment and the secure storage on the mobile device. If no end-to-end security is established, the chain of trust will be broken and the trust level cannot be defined anymore within the trust propagation scheme.

- **Usage/Attestation**: When using the credentials it must be ensured that only authorized users can access them and can trigger events like an authentication or transaction signing. This is typically ensured by some kind of access control mechanism. The authenticity and integrity of the secure storage environment must be provable by an attestation scheme with the attestation key being stored in the respective environment.
- **Termination/Revocation**: When the mobile identity is terminated or revoked, the corresponding credentials must be deleted in a reliable and secure way.

As a consequence, the following general requirements have been defined for the storage environments.

6.2 Requirement definition

Identifier	Level	Description
R_MID_CrSt_1	MUST	The mobile device MUST have at least one storage environment with well-known security properties that is part of a device attestation scheme.
R_MID_CRSt_2	MUST	The storage environment MUST contain at least one cryptographic key that can be used for the attestation of the type of security environment.
R_MID_CRSt_3	SHOULD	The mobile device SHOULD support scalable security by providing several storage environments with different but known levels of security.
R_MID_CRSt_4	MUST	If a mobile device has several credential storage environments, each of these environments MUST be integrated into the same attestation scheme.
R_MID_CRSt_5	SHOULD	The mobile device SHOULD have at least one storage environment that is based on hardware-supported security.
R_MID_CRSt_6	SHOULD	The security properties of the credential storage environment(s) SHOULD have been reviewed and evaluated by an independent security expert entity.
R_MID_CRSt_7	MUST	Pure software-based storage environments MUST apply measures to prevent extraction and cloning of secret credentials.
R_MID_CRSt_8	MUST	The storage environments MUST provide an access control mechanism to allow access by authorized users only.
R_MID_CRSt_9	SHOULD	The secure storage environment SHOULD be able to generate cryptographic credentials in a secure way and to export the public part of the credentials.
R_MID_CRSt_10	MUST	In case that the environment does not support key generation it MUST provide a mechanism to securely import cryptographic credentials over an end-to-end protected channel.
R_MID_CRSt_11	MUST NOT	The security environments MUST NOT allow the transfer of secret/private ID credentials to other environments that reach only a lower LoA.

7. Requirements for device attestation

7.1 Introduction

Since derived ID credentials are stored on the mobile device in some kind of security environment (see chapter 6) it is essential to understand the security level and integrity of this environment. This is typically achieved by attestation and a corresponding attestation scheme. Attestation is dynamic measuring of the integrity of the entity that is being attested and is based on building a trust chain from the manufacturer to the device. The aim of attestation is providing reliable evidence to the consumer of the attestation about the state of software running on a system. Only known software (presumably written or at least endorsed by the manufacturer) should be running on the device, software that is considered intact and trustworthy.

During attestation, code that is to be executed on the device is measured applying cryptographic hashing techniques. The attestation data is signed by a hardware root of trust (Secure Element/TPM, ARM CryptoCell [TRUSTZONE], Samsung Device Root Key [SAMSUNG], Trustonic Key Provisioning Host (KPH)) on the device. The public key is certified by a certification authority, usually run by the device manufacturer. The hardware root of trust can either be a dedicated piece of hardware, like the TPM, or a feature of the processor, providing hardware-assisted isolated execution, usually called Trusted Execution Environment (TEE).

To decide whether the software running on the device is trustworthy, a list of measurement values corresponding to released versions of the software needs to be known. The more often patches or updates are released, the more “trustworthy” measurement values exist. The question, whether to trust an older version of the software also needs to be considered. When the hardware element on the device gets compromised, revocation on the device level becomes an issue. When privacy and anonymity are relevant, special attestation protocols based on zero-knowledge-proofs are available. [DAA, SDAA]

As an example, FIDO and GSMA-Mobile-Connect use both the concept of an authenticator. However, only FIDO supports the concept of attestation. GSMA-Mobile-Connect however accepts FIDO-Authenticators as one of the authentication options. In FIDO, the hardware root of trust is part of the FIDO-Authenticator, which is responsible for user verification and maintaining the cryptographic material required for the relying party authentication. The authenticator will in practice be implemented by one of the above listed forms of the root of trust. In the FIDO UAF context, attestation is how authenticators make claims to a Relying Party during registration that the keys they generate, and/or certain measurements they report, originate from genuine devices with certified characteristics. [FIDO-UAF]

FIDO 2.0 specifies multiple attestation models: [FIDO-KAF]

- **Full and Surrogate Basic Attestation**: the device does not have a unique key; all devices of the same model typically share the same private attestation key.

- **Privacy CA**: The device owns a specific key; a trusted third party – the Privacy CA – issues an attestation certificate. This improves privacy but requires a Privacy CA to be run.
- **Direct Anonymous Attestation (DAA)**: The device receives DAA credentials from a single DAA-Issuer. These DAA credentials are used along with blinding to sign the attestation data.

The GSMA [GSMA] specifies four levels of assurance (LoA) that an authenticator according to ISO/IEC 29115 can provide. STORK [STORK] also defines levels of assurance including quality levels of robustness for credentials used, which however is specified in terms of quality of the certificates used and not as direct requirements on the hardware.

- Level 1 - Low: Little or no confidence (Out-of-scope)
- Level 2 – Medium: Some confidence (1 Factor Authentication)
- Level 3 – High: High confidence (2 Factor Authentication)
- Level 4 – Very high: Very high confidence (2 factor Authentication + PKI (Step 2))

Taking into account these existing attestation mechanisms and attestation schemes the following requirements for device attestation are derived within the LIGHTest context.

7.2 Requirement definition

Identifier	Level	Description
R_MID_DevAt_1	SHOULD	The device SHOULD support hardware level attestation.
R_MID_DevAt_2	MUST	The device MUST at least provide software level attestation
R_MID_DevAt_3	MUST	The private key of the device MUST be used to sign data during the attestation process.
R_MID_DevAt_4	SHOULD	The private key of the device SHOULD be unique.
R_MID_DevAt_5	SHOULD	The attestation scheme used SHOULD provide privacy, e.g. by using a Privacy CA or a scheme like ECDAA
R_MID_DevAt_6	MUST	The device MUST provide a mechanism for device level revocation.
R_MID_DevAt_7	SHOULD	The device SHOULD provide secure memory for key storage.
R_MID_DevAt_8	SHOULD	A policy on how old versions are handled SHOULD be provided.

8. Requirements for Derived ID LoA propagation

8.1 Introduction

In the most general case of a derived mobile ID scheme the primary identity issuer, the secondary identity issuer, the device manufacturer, and the relying party may all be working in a different trust scheme. Since the secondary identity issuer may not know for which relying party the mobile ID will be used, the trust propagation to the relying party also has to work across trust scheme boundaries. Thus, in general four different scenarios should be distinguished:

- The relying party operates within the same trust scheme as the secondary ID issuer,
- The relying party can translate trust information (like the LoA) from the secondary ID issuer trust scheme to the relying party trust scheme via a trust translation scheme,
- The relying party trusts the secondary ID issuer trust scheme without trust translation,
- The relying party wants to assess the LoA level independently, based on the LoA of the primary ID, the LoA of the secondary ID and/or the device attestation level.

In the first three cases the task is to enable the secondary ID issuer to determine the achievable LoA of the derived ID within his own trust scheme. For the last case, as much as possible trust relevant information has to be passed on to the relying party. The assumption for defining the requirements on trust propagation is that the first three cases shall be regarded as mandatory cases while the last case is more regarded as optional.

The following subsection lists the requirements for derived ID LoA propagation, which allow the trust information to be securely propagated along the steps of the mobile ID lifecycle, establishing and maintaining a continuous chain of trust. The requirements make sure that the user is informed about and can assess any changes to the overall trust and LoA of the mobile ID, giving consent where necessary for the propagation steps to be performed.

8.1 Requirement definition

Identifier	Level	Description
R_MID_TrPr_1	MUST	The derived ID credentials MUST contain the LoA that can be reached by the derived ID within the trust scheme of the Secondary ID Issuer.
R_MID_TrPr_2	SHOULD	The derived ID credentials SHOULD contain the LoA of the primary ID that was achieved in the primary ID issuer trust scheme.
R_MID_TrPr_3	SHOULD	The derived ID credentials SHOULD contain a reference to the authenticator used during ID derivation and to the attestation key of the authenticator.
R_MID_TrPr_4	MUST	The LoA propagation to the relying party MUST employ open standard protocols and data formats to ensure interoperability.
R_MID_TrPr_5	MUST	Specific consent MUST be given by the user for any registration

Identifier	Level	Description
		or authentication step that involves propagation of the personal ID data across borders.
R_MID_TrPr_6	SHOULD	When no other rule is mandated to the relying party to determine the LoA for a Derived ID resulting from a combination of derivation, storage, and attestation trust elements, the LoA of the Derived ID to be propagated to the relying party SHOULD be the minimum of the LoAs of the combined trust elements.
R_MID_TrPr_7	SHOULD	Trust elements considered for determining resulting LoA to be propagated SHOULD consider the elements of technical specifications and procedures contained in the Annex of the eIDAS Regulation Implementing Act 2015/1502 of 8/9/2015, which determines the reliability and quality of enrolment, electronics verification means management, authentication, and management and organization, as applicable to mobile ID.
R_MID_TrPr_8	Must	The user MUST be informed whenever a LoA propagation process involves a reduction in the LoA of the Derived ID, communicated using language that is clear and understandable to the user.

9. Conclusions

The requirements definition for the trust propagation of derived mobile IDs has shown that a complex scenario has to be taken into account. The ID lifecycle and the involved entities can stretch over various trust schemes, from the primary ID to the ID derivation step, the device attestation and the relying party. Thus, it has to be assumed that these trust schemes are either related by implicitly trusting each other or via a trust translation scheme or that the relying party has to be enabled to make its own assessment of the achieved LoA.

In addition to the complex cross-border trust relation there also several components from the ID system that have to be taken into account for assessing the overall LoA. These components include the ID derivation process, the credential storage, the device or authenticator attestation, as well as the trust propagation. Consequently, the requirements have been structured along these components or process steps.

Since it is impossible to consider all specific properties of each trust scheme and each authentication and ID scheme, the requirements were kept as generic as possible. By further narrowing down the options to concrete trust schemes and ID schemes in the course of the LIGHTest project the resulting system architecture and technical requirements will be derived.

10. References

[DAA]Brickell; Camenisch; Chen (2004). "Direct Anonymous Attestation" (PDF). *ACM Conference on Computer and Communications Security*: 132–145.

[SDAA] *Brickell; Chen; Li (2009). "Simplified security notions of Direct Anonymous Attestation and a concrete scheme from pairings" (PDF). International Journal of Information Security.* ***8*** *(5): 315–330. doi:10.1007/s10207-009-0076-3.*

[SAMSUNG] Technotes, Hardware Root of Trust, https://kp-cdn.samsungknox.com/bb91024cad9080904523821f727b9593.pdf, retrieved Feb. 2nd 2017.

[TRUSTZONE] ARM Trustzone, https://developer.arm.com/technologies/trustzone, retrieved Feb. 2nd 2017.

[KKPH] TRUSTONIC Kinibi Key Provisioning Host (KPH), https://www.trustonic.com/products/kinibi-kph, retrieved Feb. 2nd 2017.

[FIDO-KAF] FIDO 2.0: Key Attestation Format, https://www.w3.org/Submission/2015/SUBM-fido-key-attestation-20151120/

[FIDO-UAF] FIDO UAF Architectural Overview, https://fidoalliance.org/specs/fido-uaf-v1.1-rd-20161005/fido-uaf-overview-v1.1-rd-20161005.pdf

[GSMA] CPAS04 Authenticator Options Version 1.0, 11 November 2015 http://www.gsma.com/latinamerica/wp-content/uploads/2016/06/techdoc-MC-Authenticator_Options-1.pdf

[STORK] D2.3 - Quality authenticator scheme, https://www.eid-stork.eu/dmdocuments/public/D2.3_final._1.pdf

11. Project Description

LIGHT^{est} 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 LIGHT^{est} 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 LIGHT^{est} 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 LIGHT^{est} open source software to easily query this trust information to verify trust in simple signed documents or multi-faceted complex transactions.

The three-year LIGHT^{est} 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 LIGHT^{est} consortium consists of 14 partners from 9 European countries and is coordinated by Fraunhofer-Gesellschaft. To reach out beyond Europe, LIGHT^{est} attempts to build up a global community based on international standards and open source software.

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.

The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.