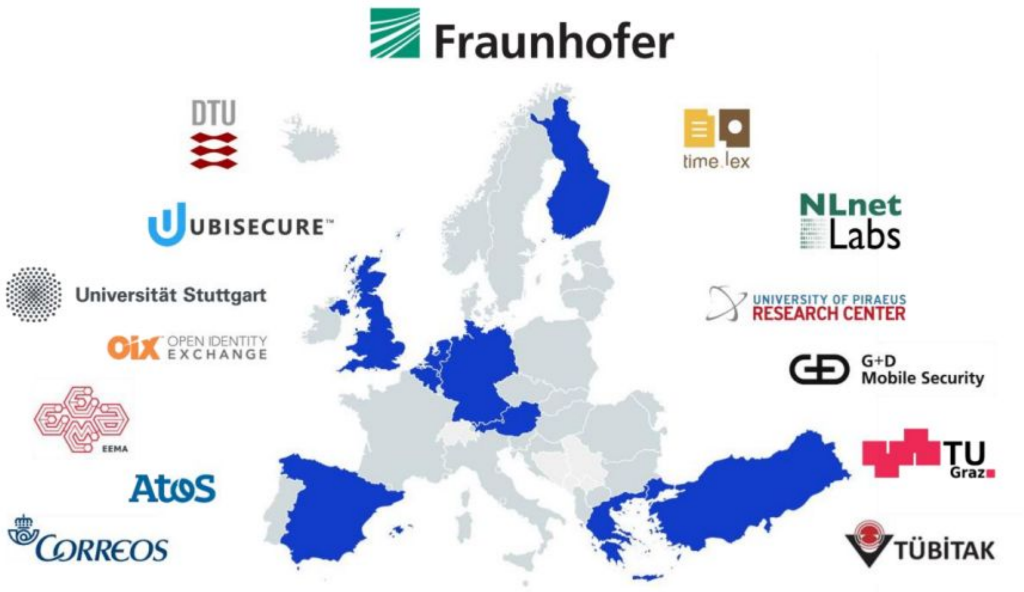
LIGHT^{est}

A Lightweight Infrastructure for Global Heterogeneous Trust Management



A LIGHT^{est} Delegation Overview

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Outline

1. **Intro**
2. Delegation basics
3. The 3 types of Delegations
4. Example Scenario
5. How it works in the Background
6. Delegation Authoring Tool

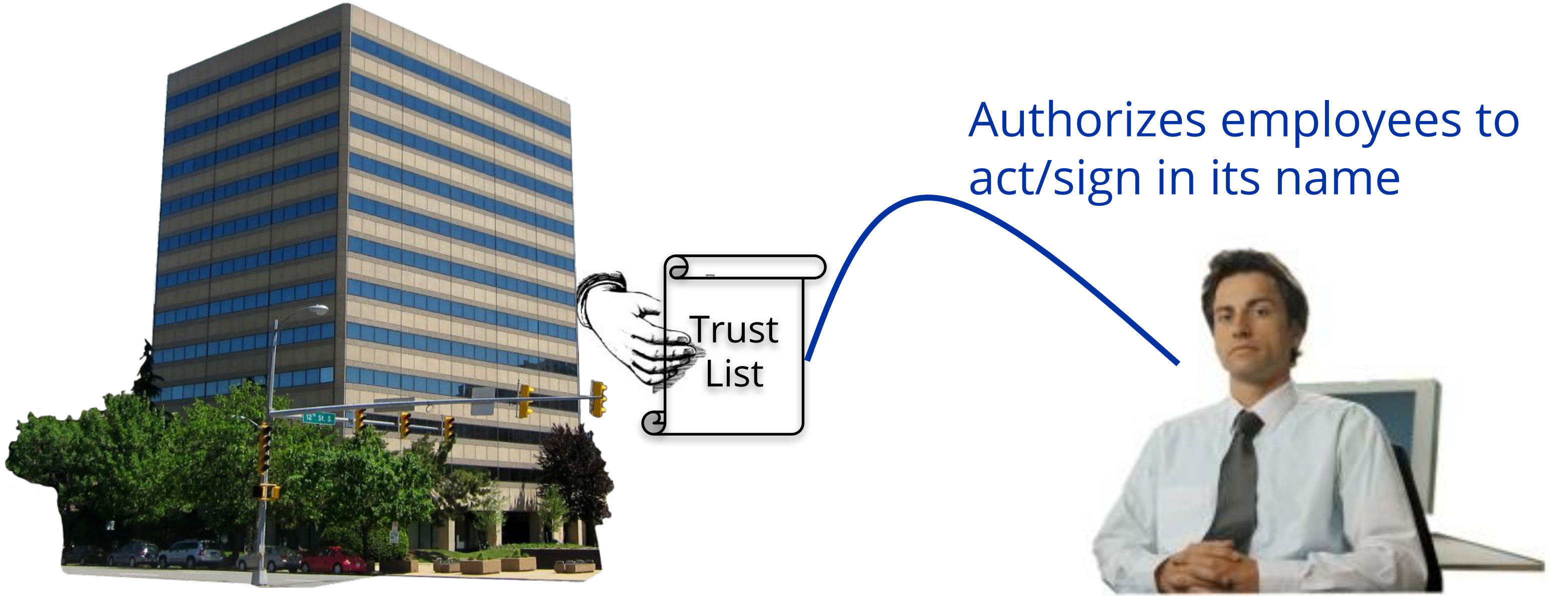
LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

What Delegation in LIGHT^{est} do?

Infrastructure for the Publication and Querying of Delegations

Delegation:

- Organization publishes Trust List on..
- ..who can sign/act in its name for which purposes

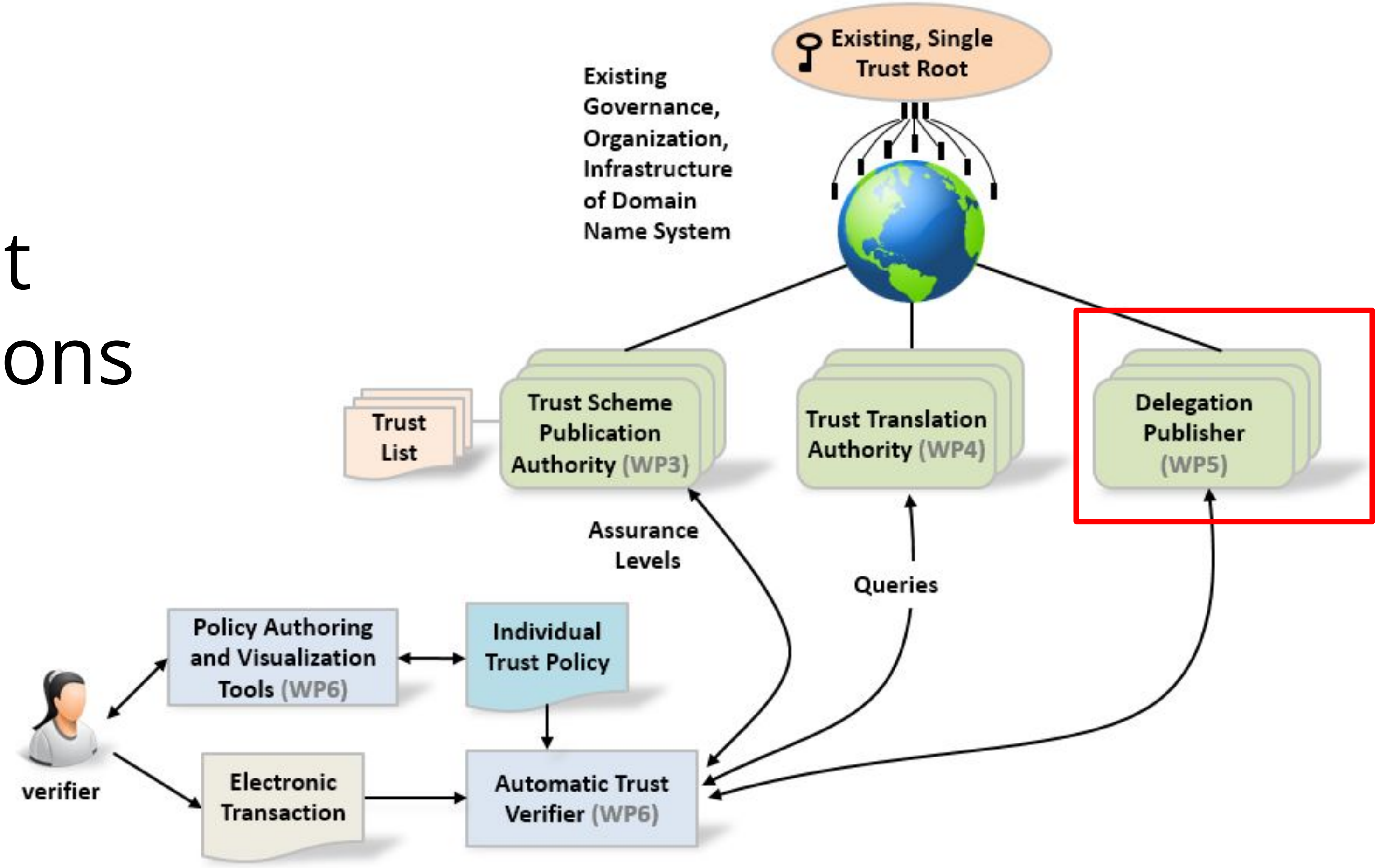


Authorizes employees to act/sign in its name

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

LIGHTest Architecture

LIGHTest Delegations


Existing, Single Trust Root
Existing Governance, Organization, Infrastructure of Domain Name System
Trust List
Trust Scheme Publication Authority (WP3)
Trust Translation Authority (WP4)
Delegation Publisher (WP5)
Assurance Levels
Queries
Policy Authoring and Visualization Tools (WP6)
Individual Trust Policy
verifier
Electronic Transaction
Automatic Trust Verifier (WP6)

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Outline

1. Intro
2. **Delegation basics**
3. The 3 types of Delegations
4. Example Scenario
5. How it works in the Background
6. Delegation Authoring Tool

LIGHT^est has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Definition

- Delegation is important in a wide variety of applications including authentication and digital signatures
- Basically: In a delegation an entity makes attributes available to another entity

- How can make good use of it:
  - Register of commerce (company register)
  - Competent Authorities (supervisory, surveillance, antitrust authorities)
  - Registries containing declaration of intent
  - Entities operating their own delegation provider (e.g. company internal)

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Terminology

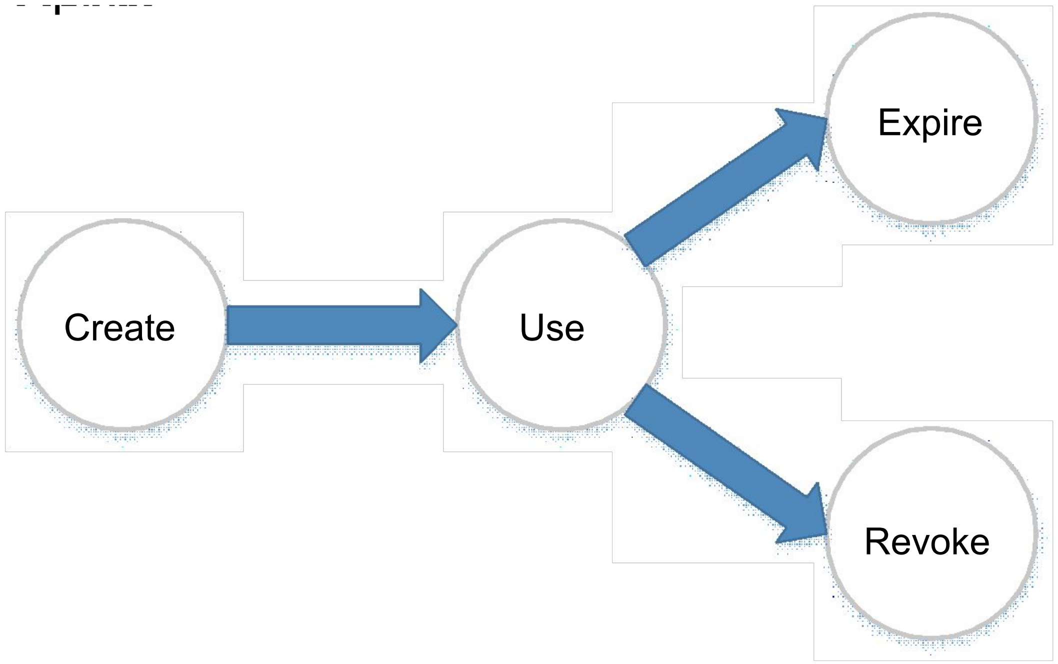
- Mandator
  - Person or entity empowering another person or entity to act on behalf of itself. The Mandator is the creator of delegations and publishes delegations at the Delegation Provider of his choice.
- Intermediary
  - Person or entity empowered by a Mandator to find another person or entity to act on behalf of the Mandator. The intermediary acts as a link between Mandator and Proxy in the selection process. The parameters of the delegation are provided by the Mandator.
- Proxy
  - Person or entity empowered by a Mandator to act on behalf of another person or entity. The Proxy is the person or entity executing the delegation.

LIGHT^est has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

The Delegation Lifecycle

- 4 States
  - Create
  - Use
  - Expire
  - Revoke
- All delegations follow this lifecycle.

- Delegations require a Mandator, and a Proxy.
- Mandator issues the delegation.
- Proxy receives the delegation



LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Outline

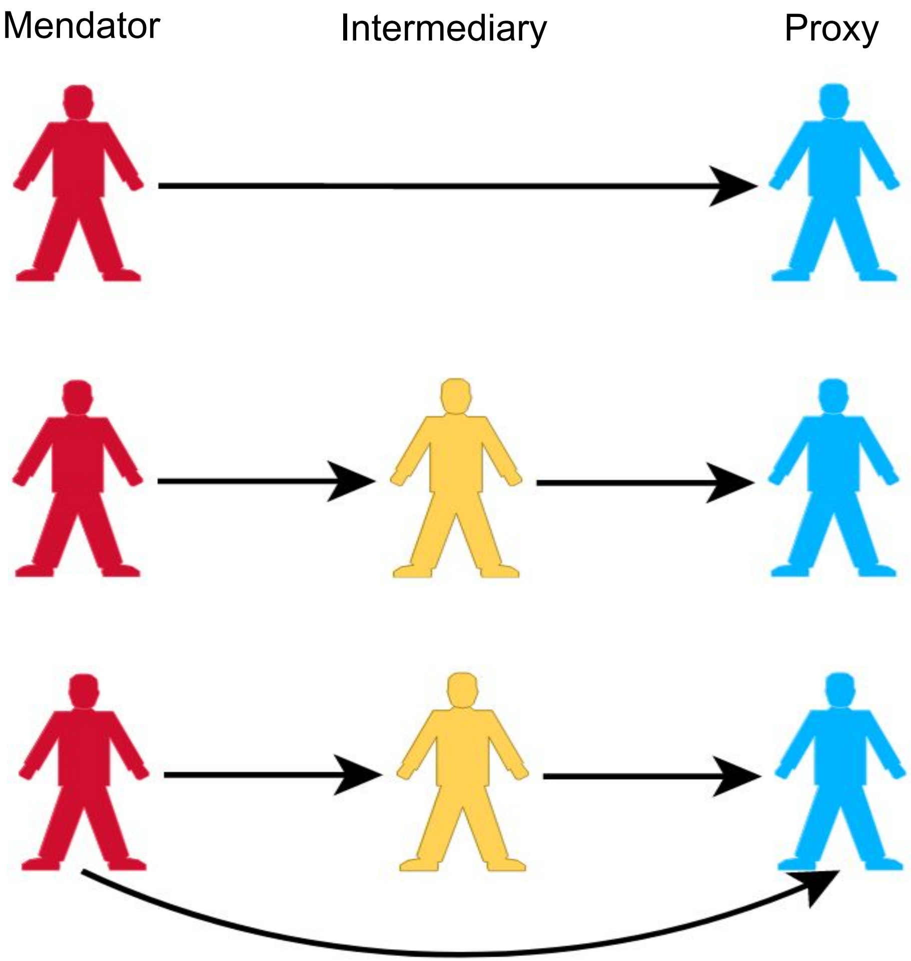
1. Intro
2. Delegation basics
3. **The 3 types of Delegations**
4. Example Scenario
5. How it works in the Background
6. Delegation Authoring Tool

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

The Types of Delegations

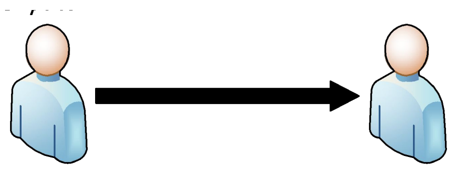
- Three basic types of delegations can be identified:
  - Bilateral Type
  - Substitution Type
  - Delegation Type

- They are the basic building blocks for more complex constructions



LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Types of Delegations:
The Bilateral Type

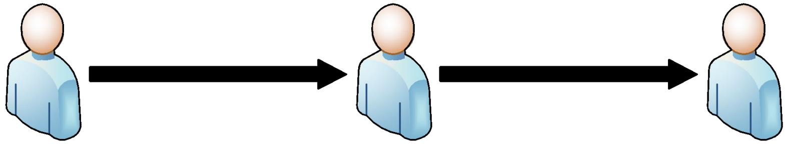


- Creation:
  - Mandator chooses Proxy
  - Mandator creates delegation for Proxy
  - Mandator publishes delegation at delegation provider

- Verification:
  - Discovery of delegation in transaction
  - Verification of link between Mandator and Proxy

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

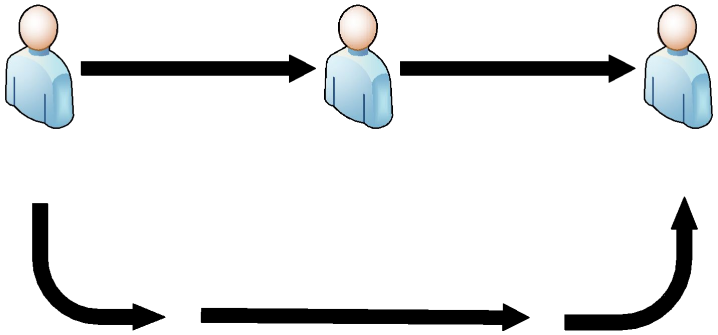
Types of Delegations: The Substitution Type



- Creation:
  - Mandator chooses Intermediary
  - Mandator create bilateral delegation for Intermediary and publishes it
  - Intermediary chooses Proxy
  - Intermediary creates bilateral delegation for Proxy based on previous delegation and publishes it
- Verification:
  - Discovery of delegation in transaction
  - Verification of link between Mandator and Intermediary
  - Verification of link between Intermediary and Proxy

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Types of Delegations: The Delegation Type



- Creation:
  - Mandator chooses Intermediary
  - Mandator create bilateral delegation for Intermediary and publishes it
  - Intermediary chooses Proxy
  - Intermediary creates bilateral delegation for Proxy based on previous delegation and publishes it

- Verification:
  - Discovery of delegation in transaction
  - Verification of link between Mandator and Proxy directly

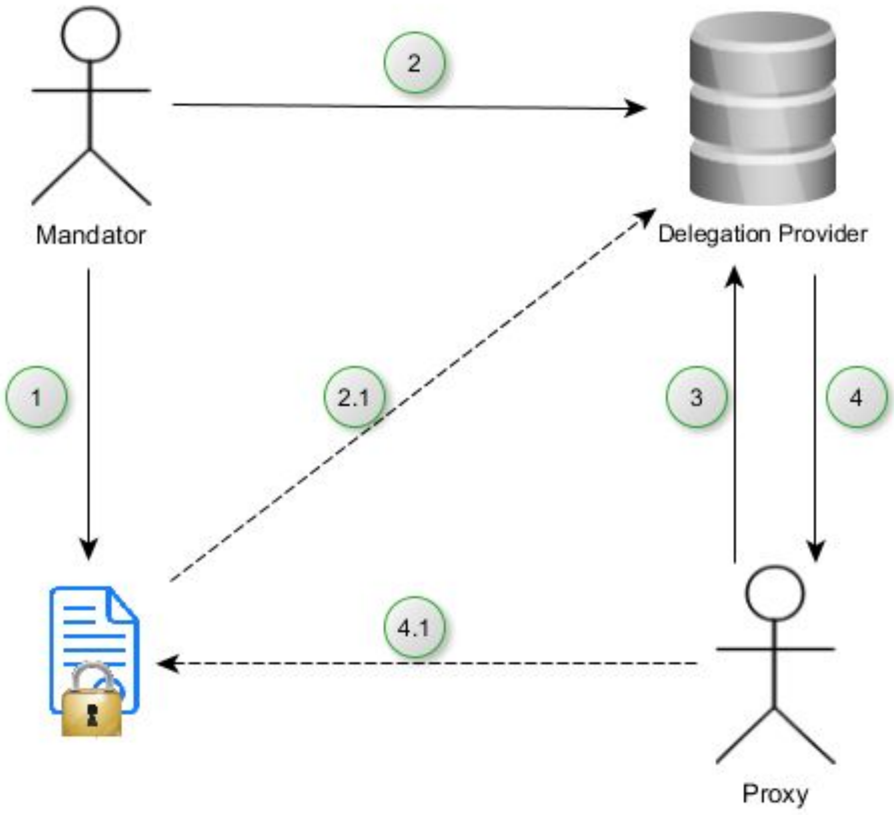
- Intermediary is only required to create the second bilateral delegation.
- Intermediary is not required for the verification

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Publication process of Delegations: Bilateral Type

1. Mandator creates the delegation
   - ○ Mandator signs and encrypts the delegation
2. Mandator uploads the delegation to the Delegation Provider
3. Proxy can query the Delegation Provider for the delegation
4. Delegation Provider provides the delegation to Proxy

- Delegations are encrypted to protect them from being stolen by an honest-but-curious Delegation Provider

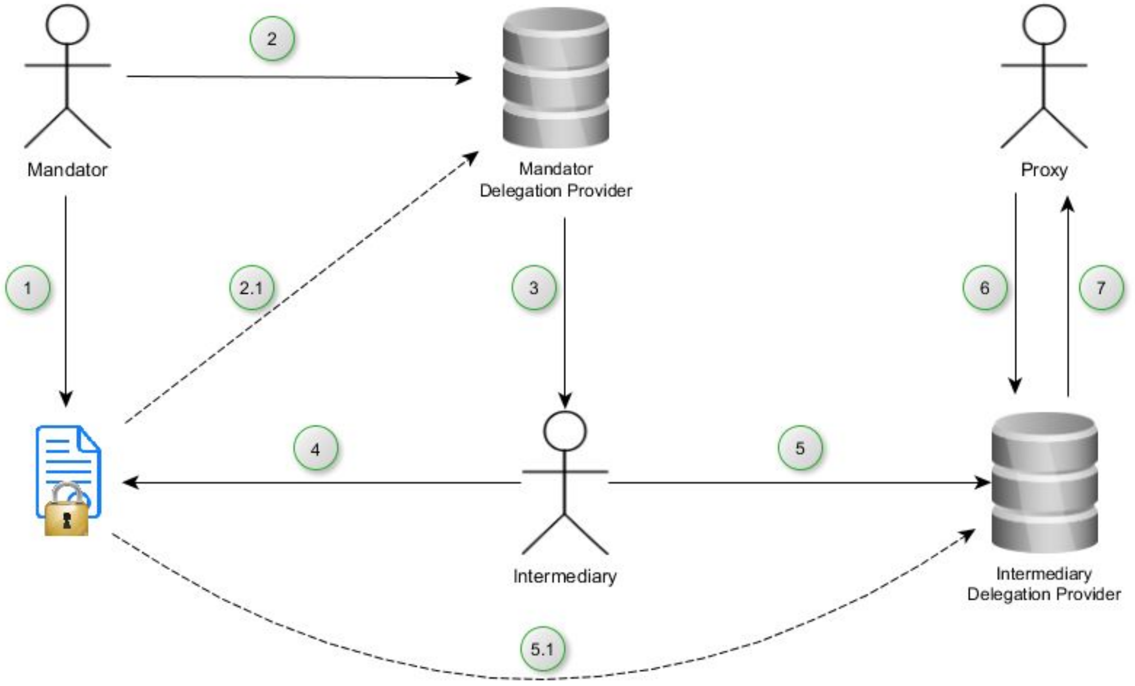


LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Publication process of Delegations: Substitution Type

- Steps 1-4 are similar to the bilateral type:
  5. Chooses Proxy and signs the delegation, then publishes it at the intermediary delegation provider
  6. Proxy can discover the delegation at intermediaries delegation provider
  7. Proxy receives delegation

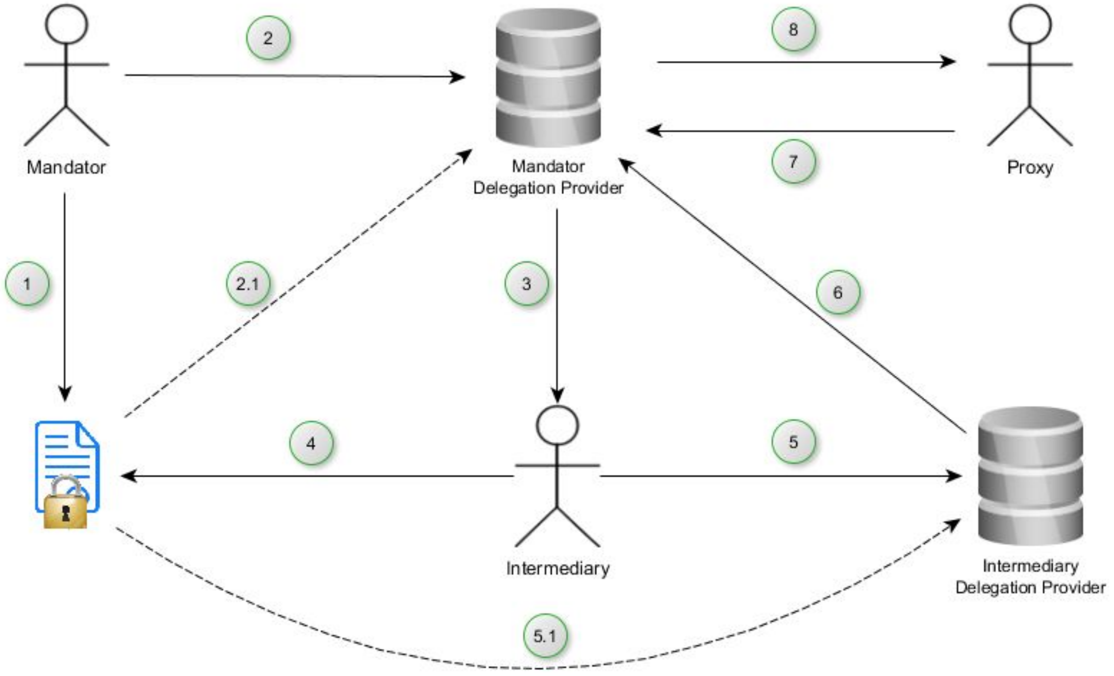
- The intermediary delegation provider can be the same as the mandators


Mandator
2
Mandator Delegation Provider
Proxy
1
2.1
3
6
7
4
5
Intermediary
Intermediary Delegation Provider
5.1

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

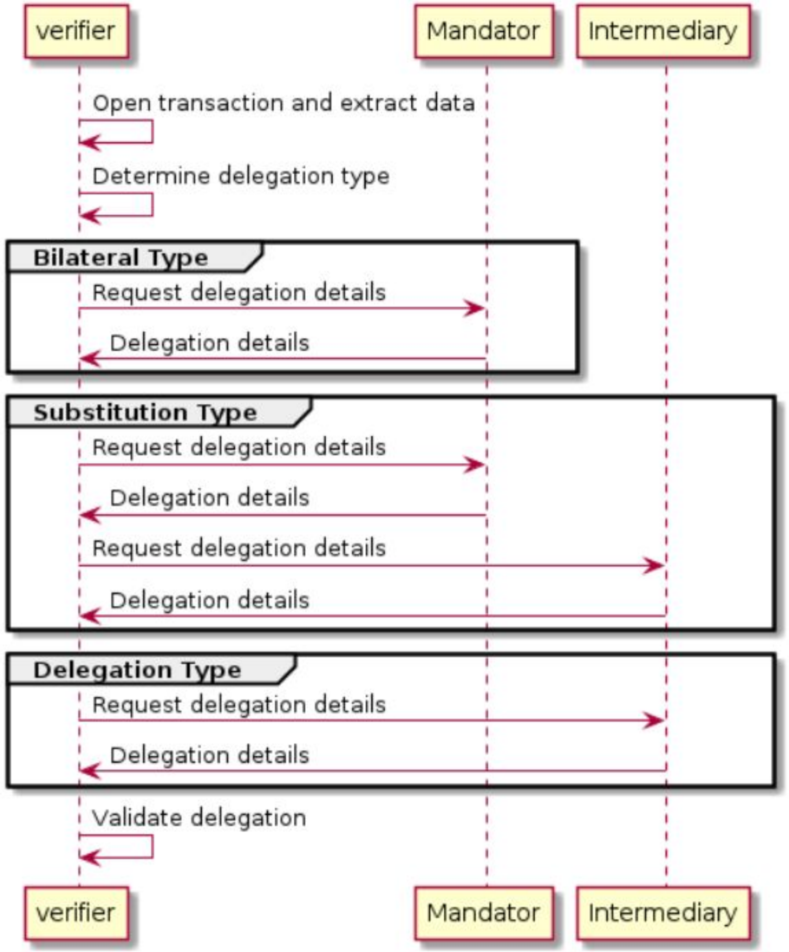
Publication process of Delegations: Delegation Type

- Basically the same as the substitution type, but:
  6. Additional step to send the data to the mandator delegation provider required
- Intermediary's delegation provider automatically updates the mandators delegation provider automatically
- Intermediaries delegation provider can be the same as the mandators delegation provider


Mandator
2
Mandator Delegation Provider
8
7
Proxy
1
2.1
3
6
4
5
Intermediary
Intermediary Delegation Provider
5.1

LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Verifying Delegations



LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Outline

1. Intro
2. Delegation basics
3. The 3 types of Delegations
4. **Example Scenario**
5. How it works in the Background
6. Delegation Authoring Tool

LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Delegation Scenario – The involved Persons

- Alice

  - CEO of a company
  - Very busy
  - Wants to do everything on her own
  - Time is her worst enemy

- Bob

  - New employee at Alice‘s company
  - Works in purchasing
  - Is only allowed to conduct purchases up to 100k€

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

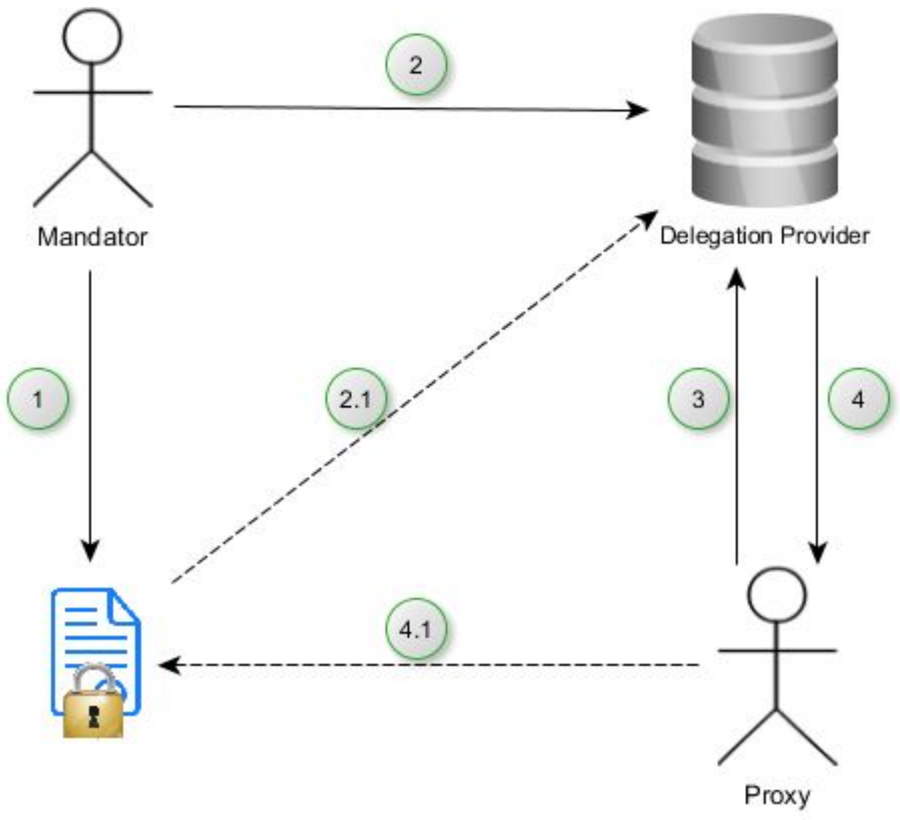
Scenario – The Scenario

- Alice finally has a new employee Bob for her purchasing department
- As Bob is new to the company he is only allowed to conduct purchases up to 100k€
- Purchases above 100k€ needs to be signed by Alice
- Alice has heard about a cool new project called LIGHTest that has the technology to help her with this task

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Scenario

- In a first step, Alice creates the new delegation
- The delegation is the signed and uploaded to the delegation provider
- At the delegation provider, Bob can download the delegation and verify it



LIGHT^est has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Outline

1. Intro
2. Delegation basics
3. The 3 types of Delegations
4. Example Scenario
5. **How it works in the Background**
6. Delegation Authoring Tool

LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

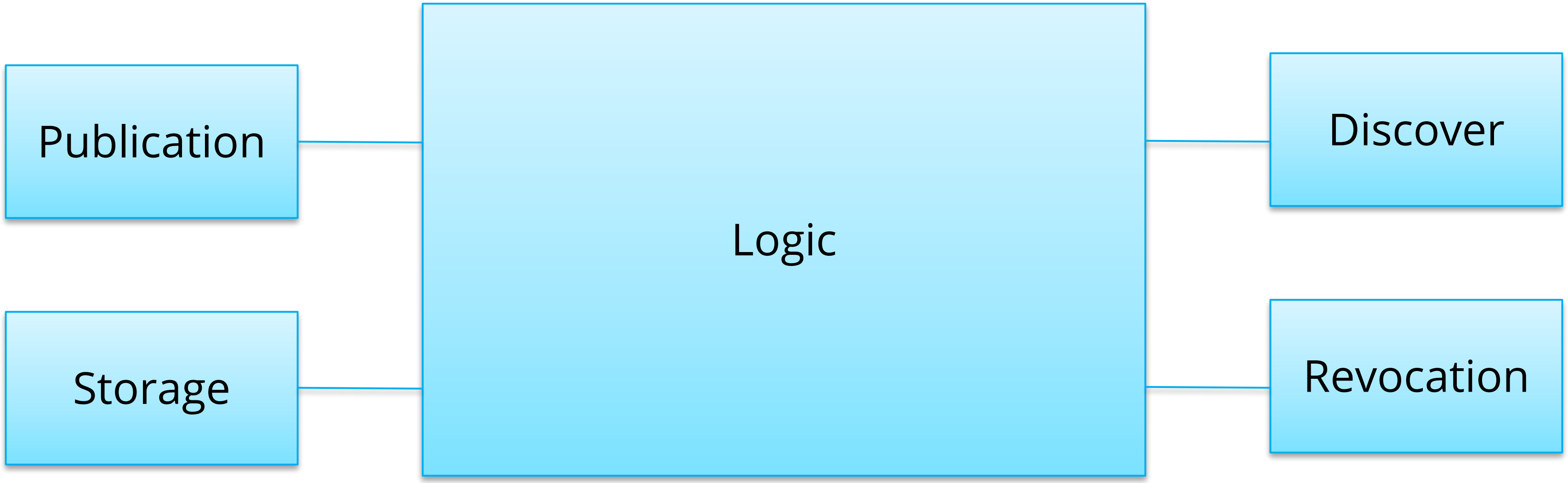
Delegation Infrastructure

- LIGHTest uses DNS infrastructure to store delegations
- DNS is used to find the Delegation Provider (DP)
- Delegation Provider is a web component
- All delegations can be queried in real time
- Competent Authorities and End Users can create their own delegations

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Delegation Provider

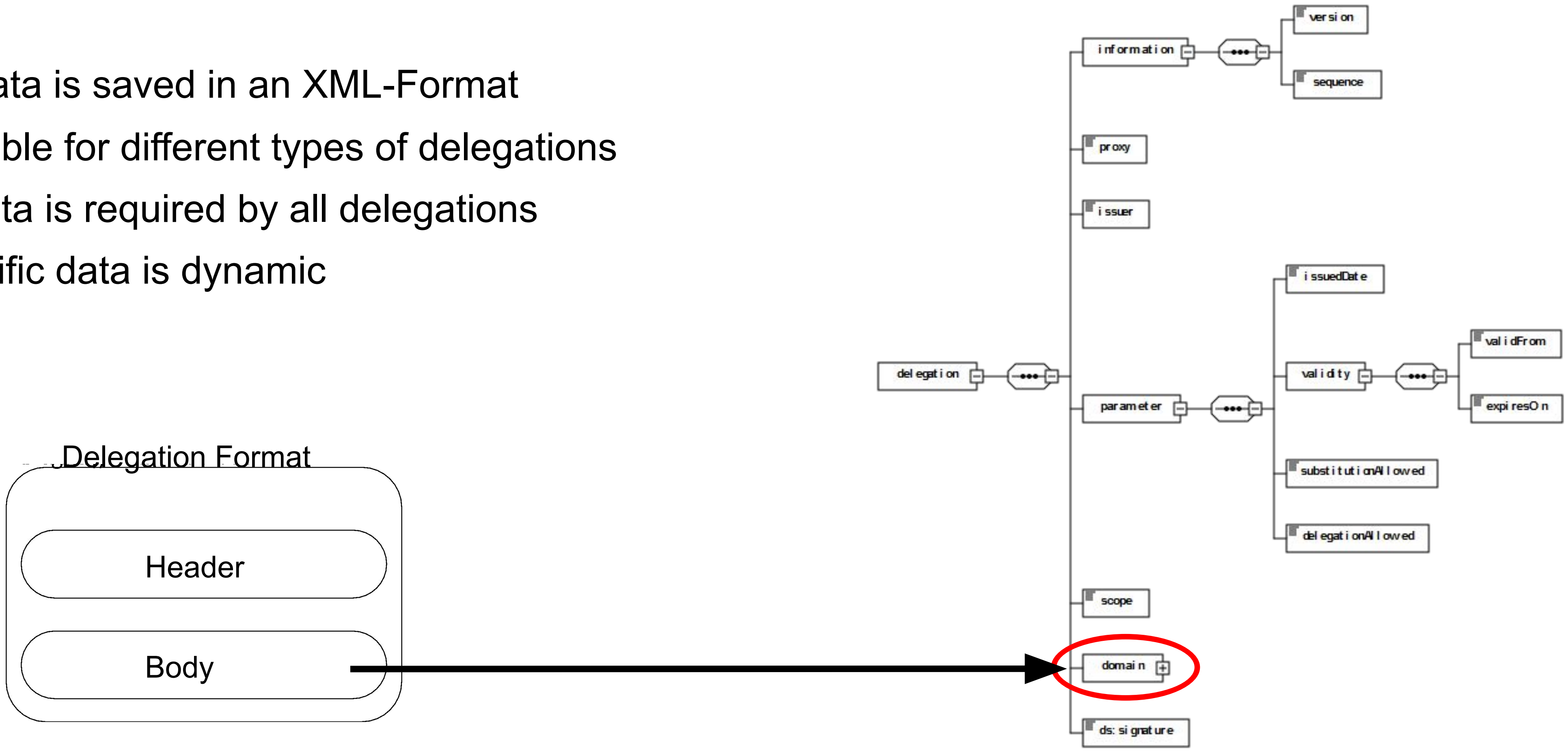
- The Delegation Provider provides a Restful API for the user to work with delegations (publish, use, revoke). Those endpoints are implemented as micro services.



LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Delegation Data Format

- Delegation Data is saved in an XML-Format
- Easily extensible for different types of delegations
- Mandatory data is required by all delegations
- Domain Specific data is dynamic

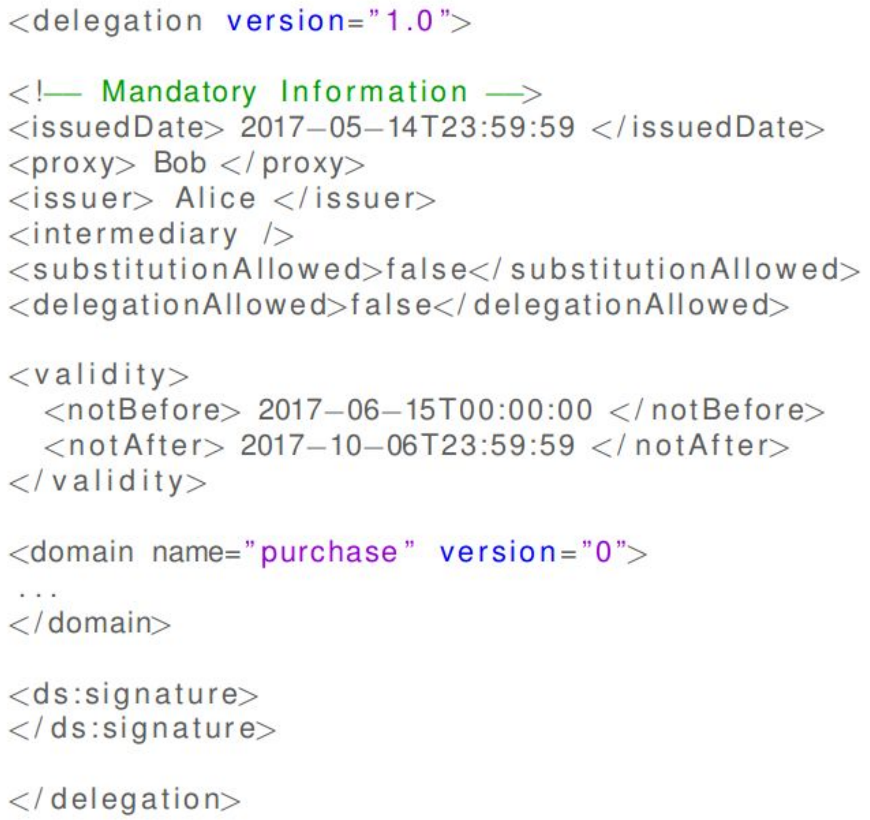


LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Delegation Fields

- information
  - version
  - sequence
- issuedDate
- proxy
- issuer
- intermediary

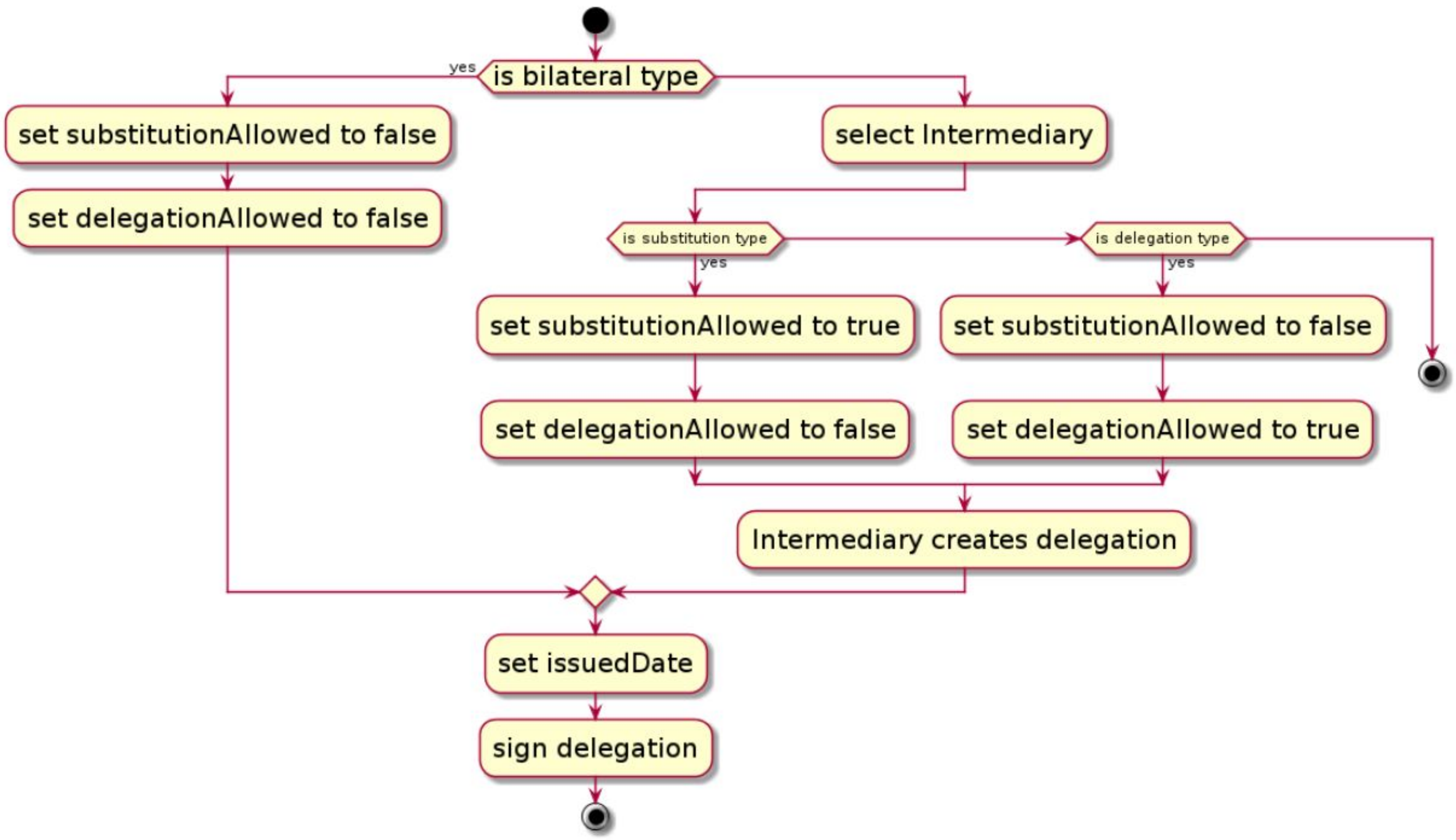
- substitutionAllowed
- delegationAllowed
- validity
  - notBefore
  - notAfter
- domain
- signature



```
<delegation version=”1.0”>

<!— Mandatory Information —>
<issuedDate> 2017–05–14T23:59:59 </issuedDate>
<proxy> Bob </proxy>
<issuer> Alice </issuer>
<intermediary />
<substitutionAllowed>false</substitutionAllowed>
<delegationAllowed>false</delegationAllowed>

<validity>
  <notBefore> 2017–06–15T00:00:00 </notBefore>
  <notAfter> 2017–10–06T23:59:59 </notAfter>
</validity>

<domain name=”purchase” version=”0”>
 ...
</domain>

<ds:signature>
</ds:signature>

</delegation>
```

LIGHT^{est} has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321

Substitution and Delegation Flag


is bilateral type
yes
set substitutionAllowed to false
set delegationAllowed to false
select Intermediary
is substitution type
yes
is delegation type
yes
set substitutionAllowed to true
set delegationAllowed to false
set substitutionAllowed to false
set delegationAllowed to true
Intermediary creates delegation
set issuedDate
sign delegation

LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

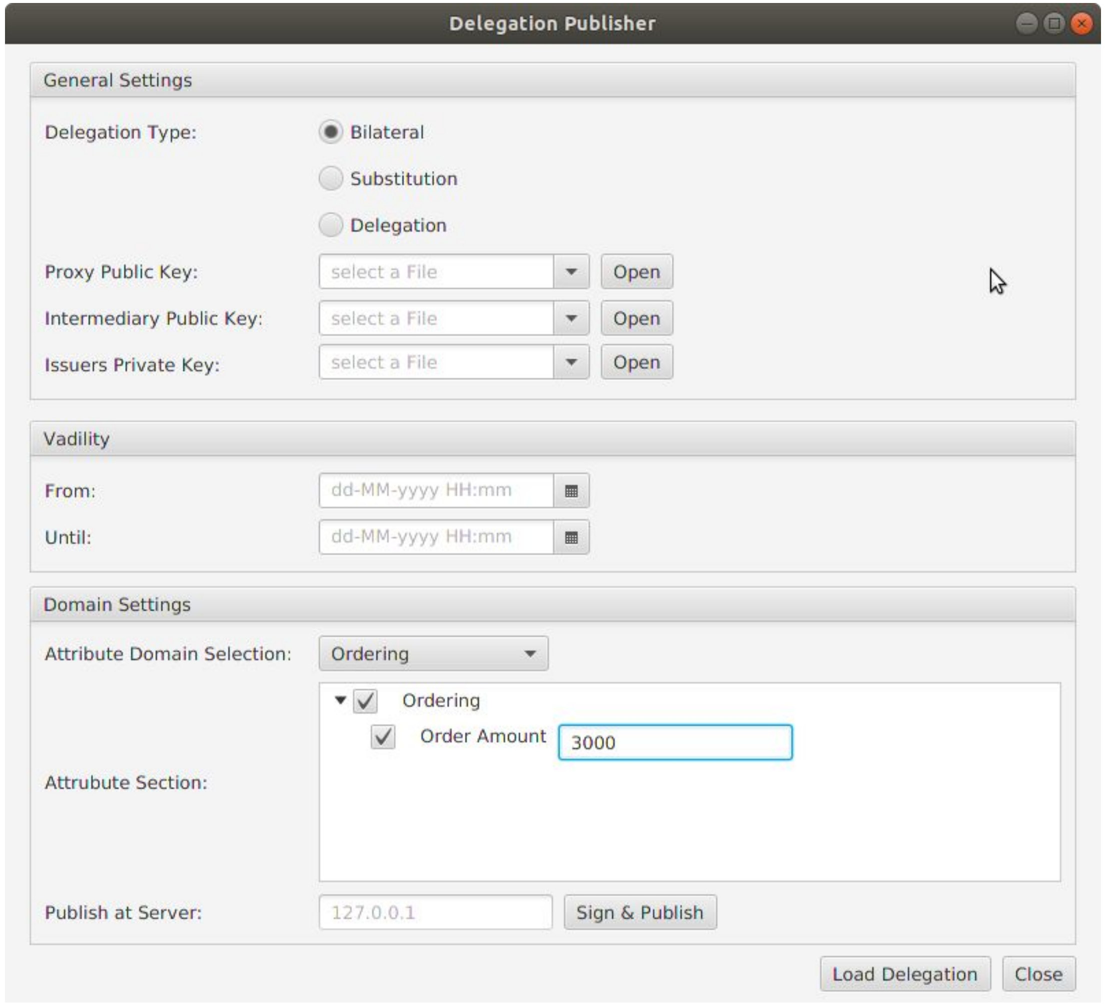
Outline

1. Intro
2. Delegation basics
3. The 3 types of Delegations
4. Example Scenario
5. How it works in the Background
6. **Delegation Authoring Tool**

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Delegation Authoring Tool

- User friendly way of creating a Delegation XML
- Direct publishing to the service Provider
- Loading saved or already published Delegations
- Two sections:
  - Delegation Header on first two views
  - Domain specific options in the last part
- Latter has a selector for the Domain
- Correspondent options are available in the attribute section


Delegation Publisher

General Settings

Delegation Type: ● Bilateral ○ Substitution ○ Delegation

Proxy Public Key: select a File

Intermediary Public Key: select a File

Issuers Private Key: select a File

Vadility

From: dd-MM-yyyy HH:mm

Until: dd-MM-yyyy HH:mm

Domain Settings

Attribute Domain Selection: Ordering

Attrubute Section: ☑ Ordering; ☑ Order Amount 3000

Publish at Server: 127.0.0.1

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Delegation Authoring Tool Plugins

- For Custom Domains
- Developer with Domain Knowledge builds it for the community (e.g. an IT Finance Engineer for a finance company)
- Procedure:
  - Write XSD
  - Generates JAXB classes
  - Implements the Plugin interface
  - Implements the Field interfaces

LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

The Electronic Transaction & where Delegations fit in

- 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

- Components of an electronic transaction are:

  - Electronic Transaction Data: This are other necessary information sent apart from the electronic signature in the process of the transaction, which are necessary to understand the will of the transaction

  - Electronic Delegation: This is the necessary information for the delegation. It contains the name of the Mandator and the Proxy. It is compared to the Transaction Data and the Electronic Signatures.

LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Questions & Answers

Thank you for your attention

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Bonus slide: API

what can I do and how? Why restful?

TODO: Maybe Deliverable, check...

LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321