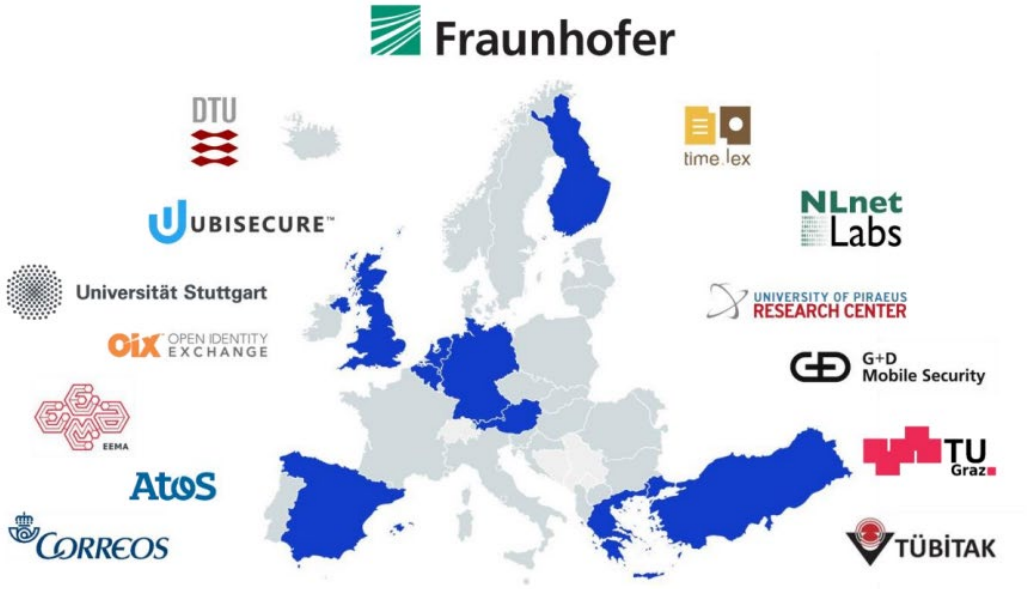
Trust establishment in Peppol using LIGHTest

A Lightweight Infrastructure for Global Heterogeneous Trust Management



Lightweight **I**nfrastructure for **G**lobal **H**eterogeneous **T**rust management in support of an open **E**cosystem of **S**takeholders and **T**rust schemes

Andriana Prentza, Jerry Dimitriou
UPRC

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

Agenda

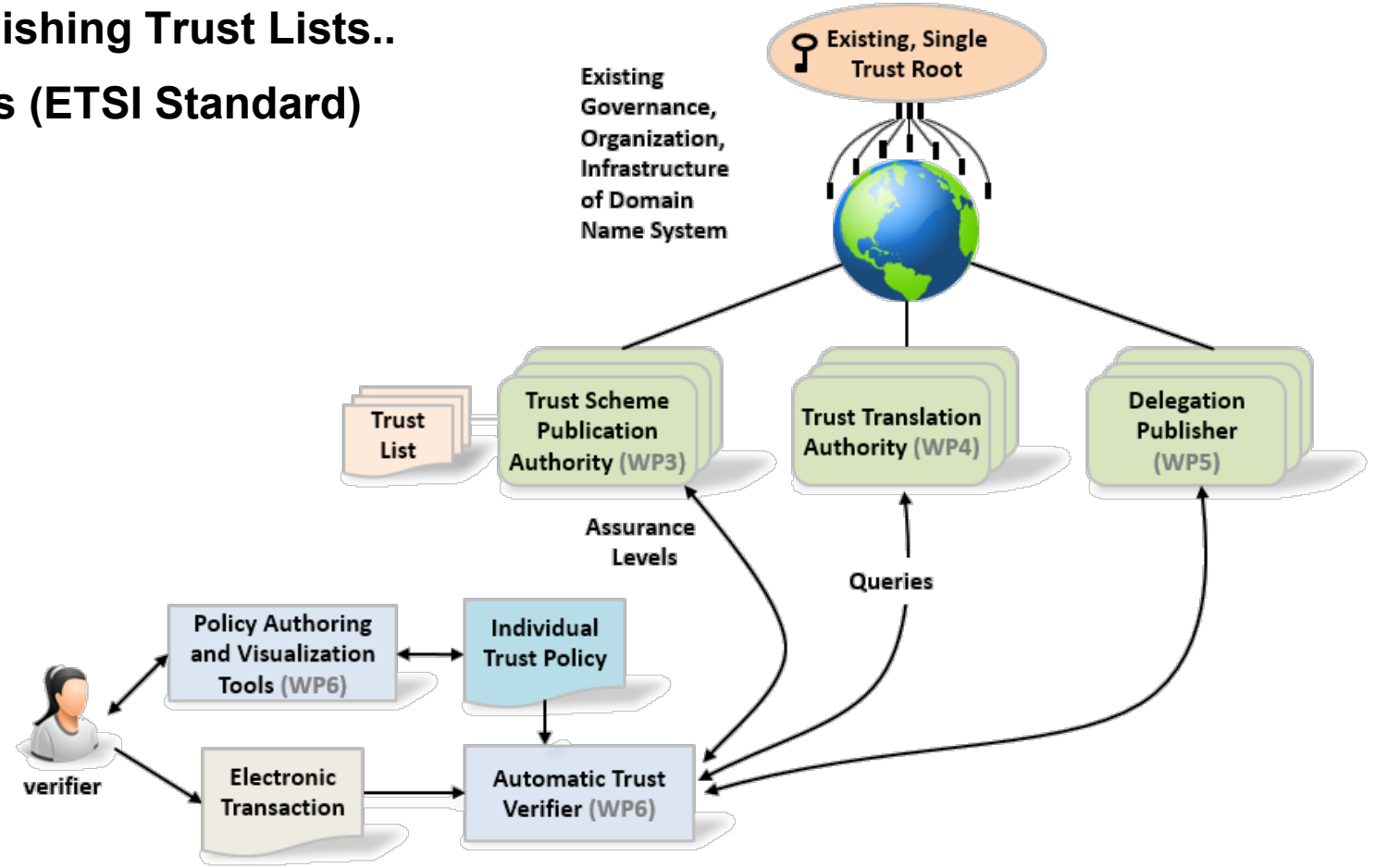
- What is LIGHT*est* ?
- What does LIGHT*est* do?
- LIGHT*est* pilot overview in eProcurement
- How LIGHT*est* can be used for Trust Establishment in PEPPOL

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

What is LIGHT*est*?

Infrastructure for Publication and Querying of Trust Schemes

- Create a global Standard Way for publishing Trust Lists..
  - Using Trust Service Status Lists (ETSI Standard)
- ..on a global Trust Infrastructure
  - DNS using DNSSEC



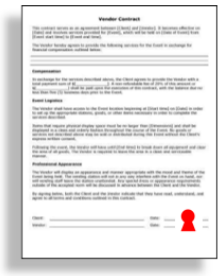
LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

What does LIGHT^{est} do? Trust Policy and Automatic Trust Decisions

- Make it automatic for Verifiers to **query Trust Lists**
- Combine multiple queries to **validate**
  - an **Electronic Transaction**
  - against an easy to author **Trust Policy**

Our Policies

Transaction



Is it trustworthy? YES/NO

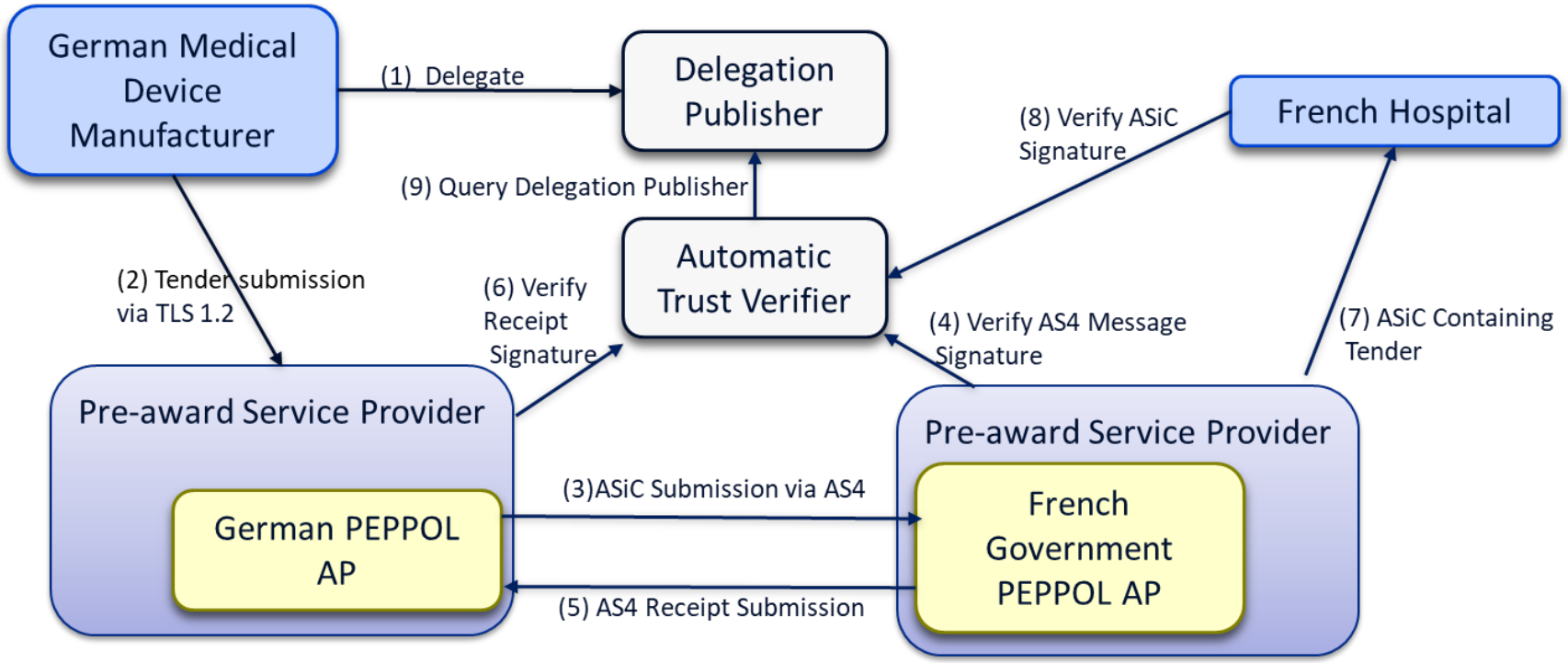
LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

LIGHT*est* pilot overview in eProcurement

- Trust Establishment between pre-award Service Providers (SPs)
  - Investigating the use of LIGHT*est* infrastructure in a HealthCare Procurement Scenario
  - Trust Establishment and Delegation between Service Providers
- Trust Establishment on eDelivery Access Points (APs)
  - Investigating the change of PKI on a closed Trust Environment

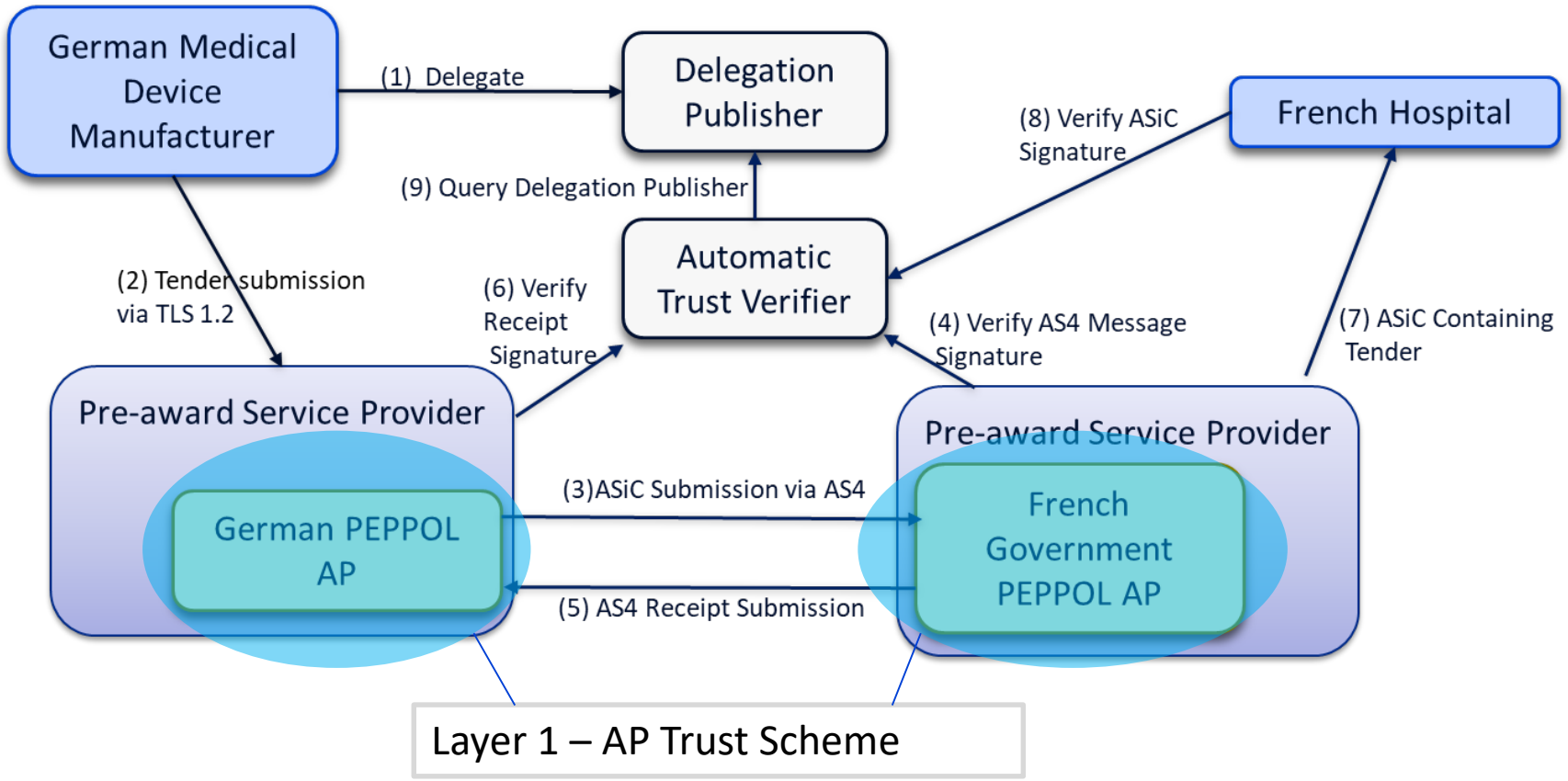
LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Pre-award Service Provider Use Case
Multi-layered Trust Establishment



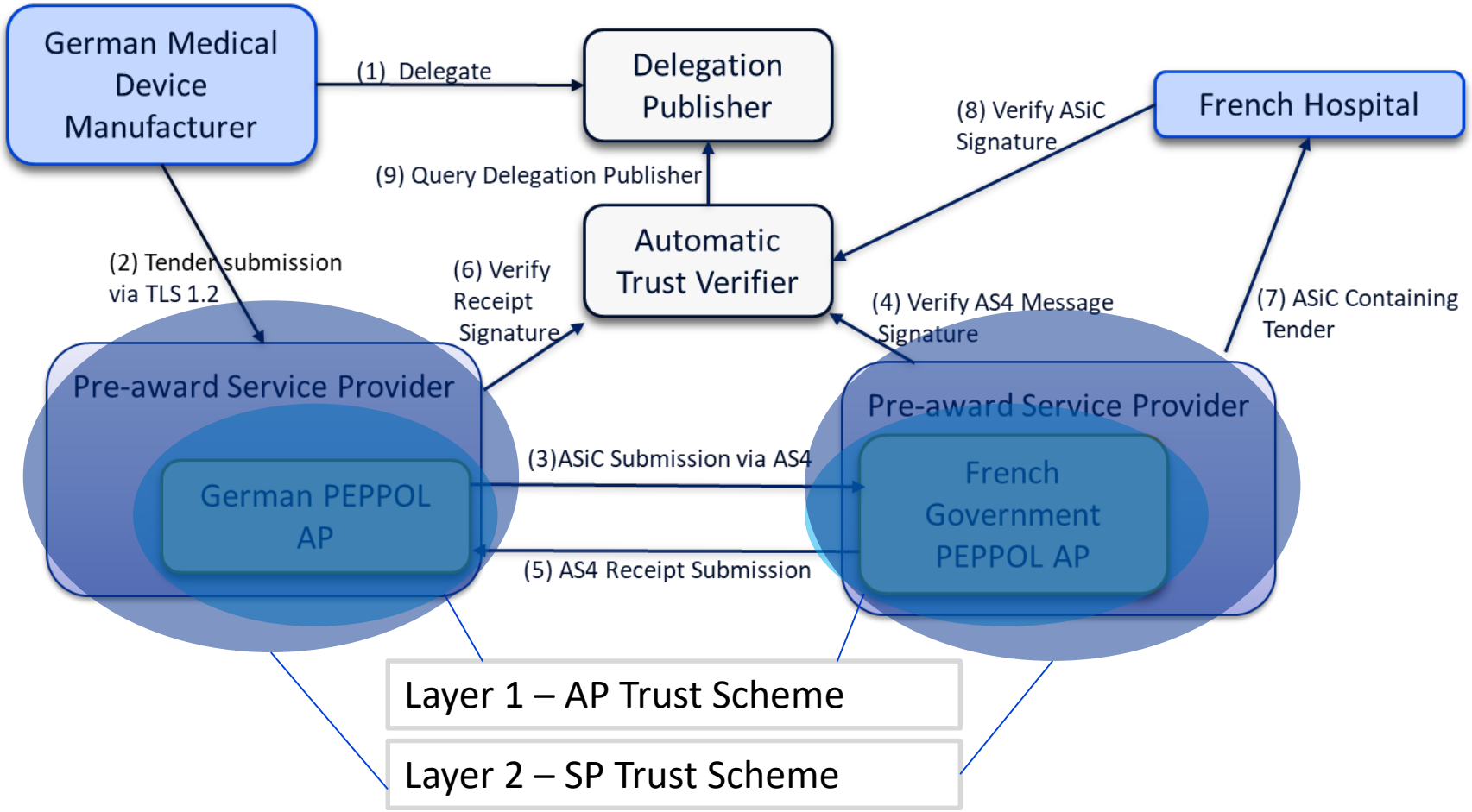
LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Pre-award Service Provider Use Case
Multi-layered Trust Establishment



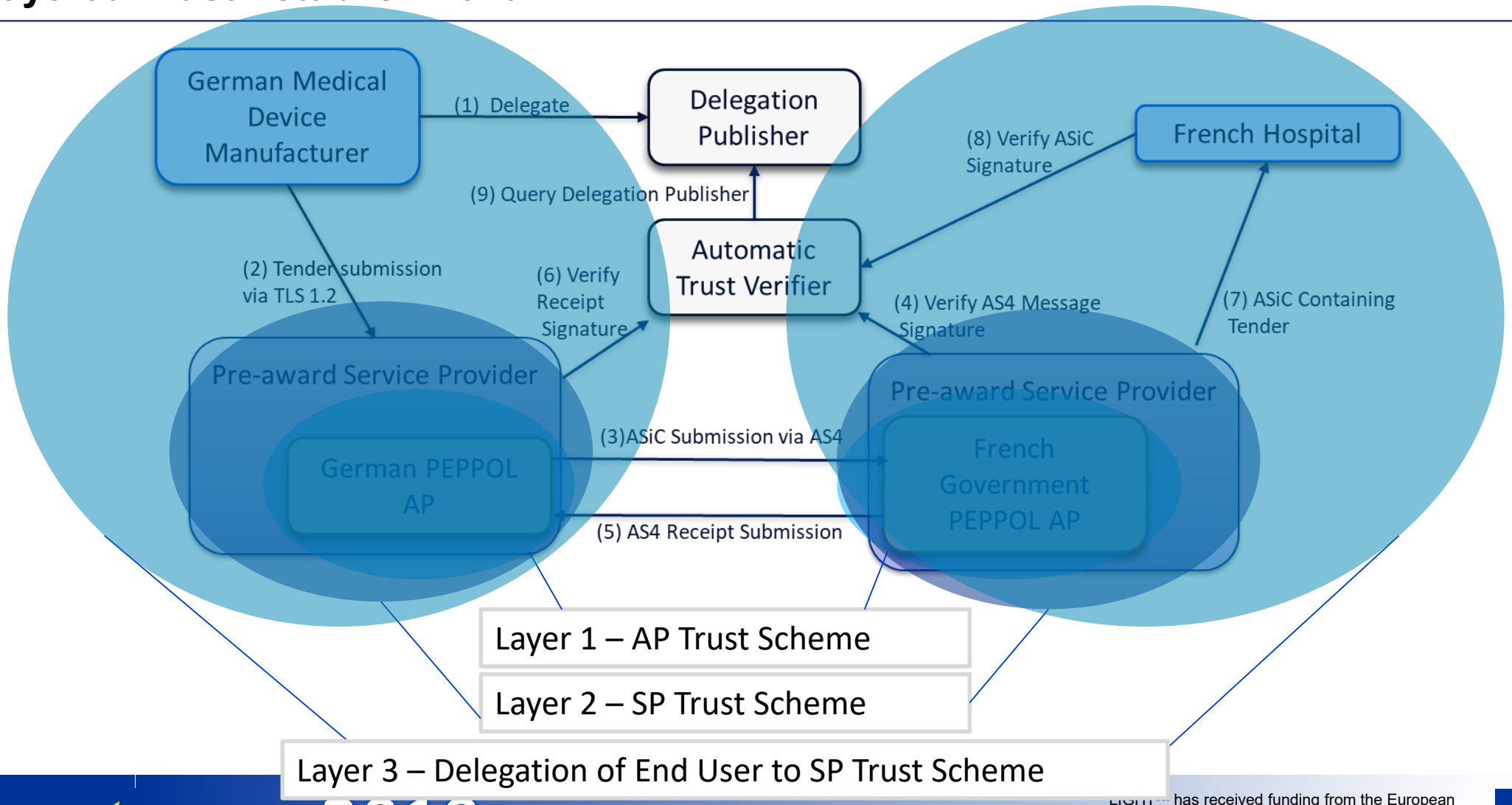
LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Pre-award Service Provider Use Case
Multi-layered Trust Establishment



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

Pre-award Service Provider Use Case
Multi-layered Trust Establishment



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

Trust Scheme Publication Examples
Publication to DNS

- LIGHT*est* uses DNS(SEC) for the publication of the Trust Schemes
- Access Point Trust Scheme:
  - DNS Record: _accesspoint_._trust_.peppol.eu
  - Points to: https://trust.peppol.eu/accesspoint
  - Contains a Trust List with the AP CA (Issuer) or the AP certificates themselves
- Pre-award Access Point Trust Scheme:
  - DNS Record: _accesspoint-preaward_.trust_.peppol.eu
  - Points to: https://trust.peppol.eu/accesspoint-preaward
- Service Provider Trust Scheme:
  - DNS Record: _serviceprovider-preaward_.trust_.peppol.eu
  - Points to: https://trust.peppol.eu/serviceprovider-preaward

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

Trust Scheme Publication Examples
Verifying (1)

- Using LIGHT*est* tools like Automatic Trust Verifier (ATV):
  - When an AP receives a Message from another AP
  - Validates the certificate against a policy stating that the certificate should be a pre-award PEPPOL Access Point (Trust Claim)
  - Using DNS, the ATV:
    - Resolves the Trust Scheme from the Claim
    - Fetches the Trust List and validates it
    - Checks that the certificate used for signing the message is verified against the Trust Scheme (e.g. Issuer is in the Trust List)

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

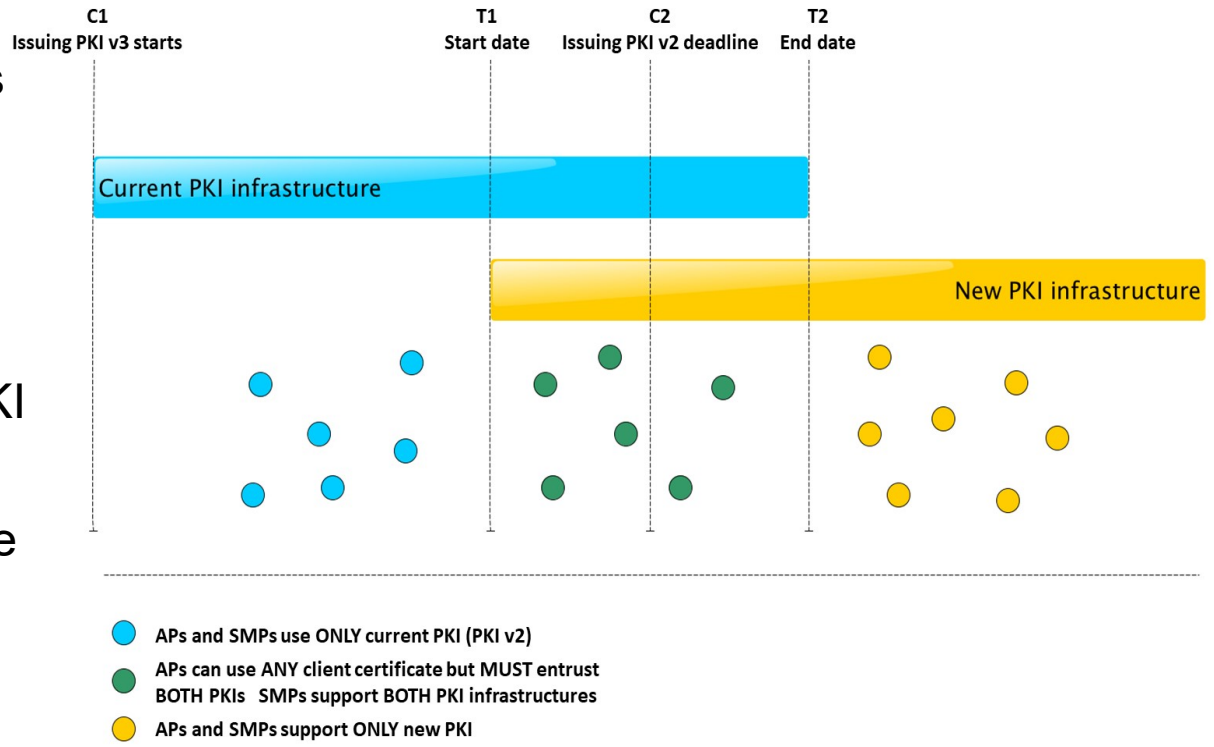
Trust Scheme Publication Examples
Verifying (2)

- Any updates on the Trust Schemes do not affect the configuration of the ATV and the AP
  - New CAs are added as trusted or new AP certificates are added as trusted (or removed as non-trusted)
- Granularity of the Trust Scheme can be arbitrary
  - Trust scheme on AP able to send orders
  - Trust scheme on an SP able to send specific BISes

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

Trust Establishment on eDelivery APs
PKI Migration using LIGHT*est*

- APs use LIGHT*est* Infrastructure for Trust Establishment
  - Before T1:
    - A Trust Scheme containing the old PKI CAs
  - After T1 and Before T2:
    - A Trust Scheme containing both PKI CAs
  - After T2:
    - A Trust Scheme containing only the new PKI CAs
- OpenPEPPOL APs **automatically** get **updated** on the **updated trust schemes** using **LIGHT*est*** and the **ATV**



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

Thank You

Questions?

www.lightest-community.org
info@lightest-community.org
@LIGHTest_trust
www.linkedin.com/groups/12017516

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