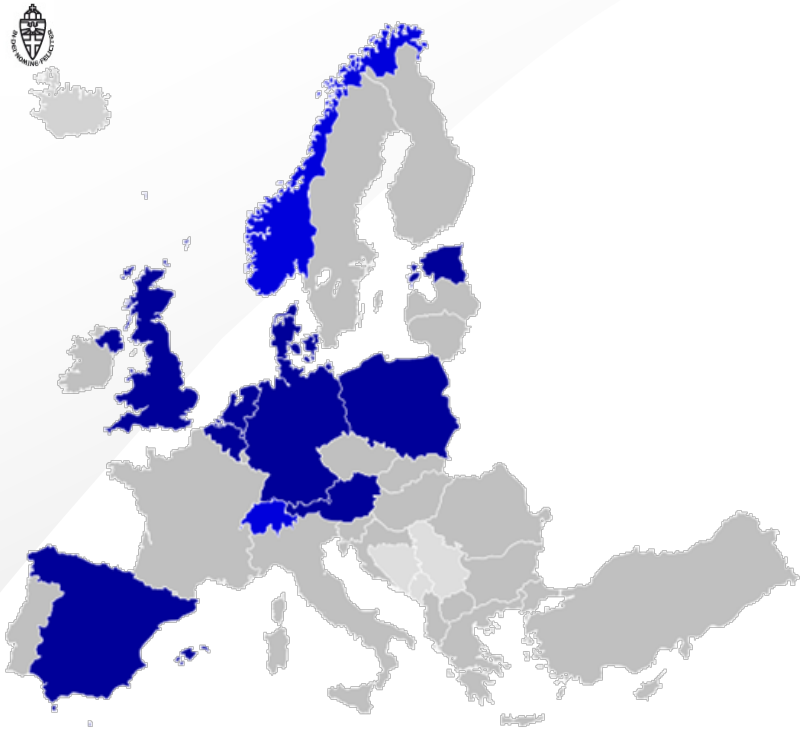
The Globally Scalable FutureID Trust Infrastructure



WORLD e-ID AND CYBERSECURITY

Identity and Protection Services for Government, Mobility and Enterprise

September 15-17, 2015 – Marseille, France

Bud P. Bruegger, Fraunhofer IAO

FutureID is partly funded by EU FP7 under GA n°318424

Agenda

- Context: The FutureID Identity Management Infrastructure
- Requirements for Trust Infrastructures
- Current Way of using Trust Lists and their Limitations
- The FutureID Approach
- Conclusions and Outlook

FutureID is partly funded by EU FP7 under GA n°318424

FutureID Objectives

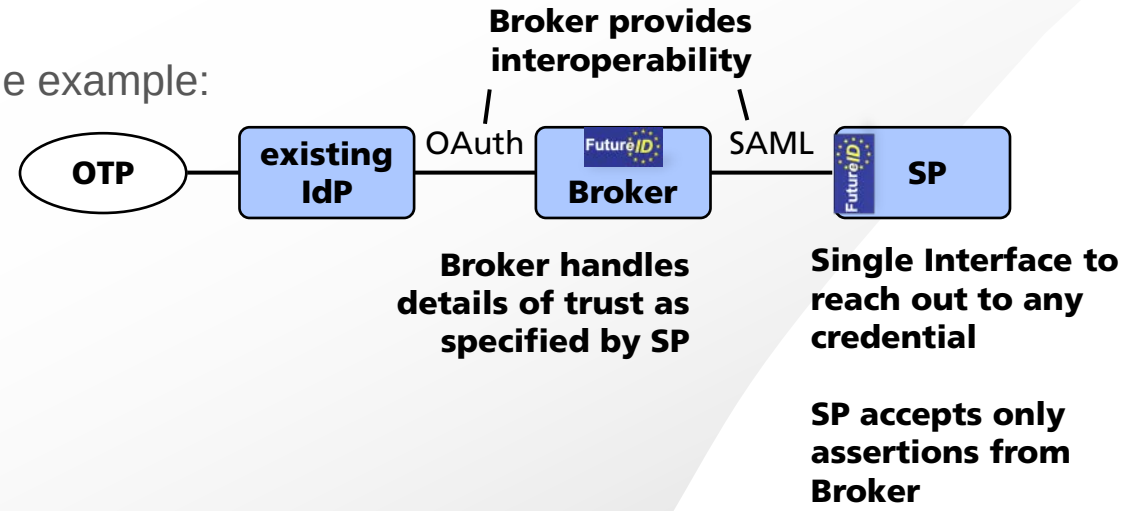
Identity Management Infrastructure for Europe

- **Arbitrary ID credentials**:
  - **gov. eIDs**: directly, through existing IdPs, through STORK
  - **priv. sector eIDs**: existing user base (e.g., bank OTPs), mobile, …
- **Extensible Open System**:
  - New Credentials, IdPs, Brokers (intermediaries), Federation Dialects
- **Decentralized Identity Management Ecosystem** (DIME):
  - Free Marketplace for Identity and Intermediation Services
  - No central control / component / registries
  - Open number of participants

FutureID is partly funded by EU FP7 under GA n°318424

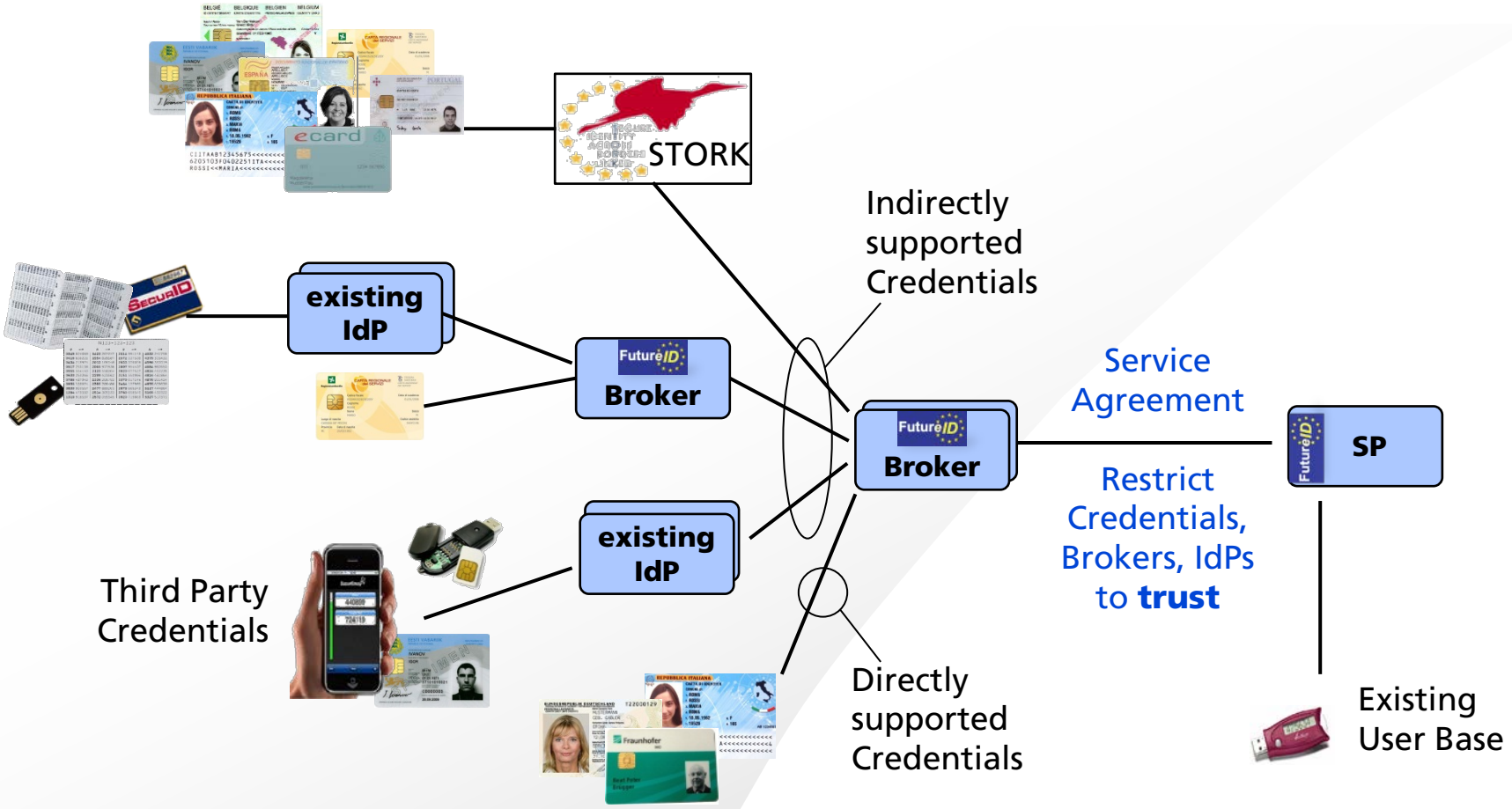
Interoperability through Intermediation: The FutureID Broker

- **Interoperability through Intermediation:**
  - FutureID **Broker** (similar to Hub, PEPS, ..)
  - Encapsulates a complex world behind a single interface
- Can optionally use of existing **IdP**s and **Infrastructures** (STORK)
- Simple example:



FutureID is partly funded by EU FP7 under GA n°318424

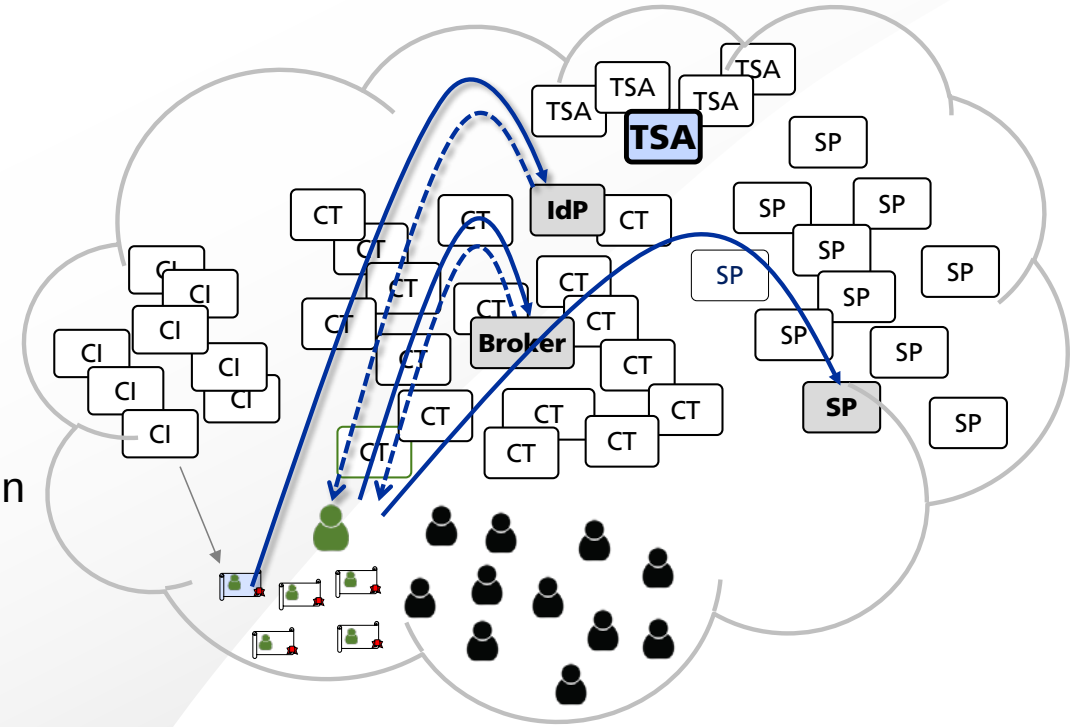
Service Providers Maximize their Market Outreach with FutureID



FutureID is partly funded by EU FP7 under GA n°318424

FutureID Stakeholder / Component:
Trust Scheme Authorities

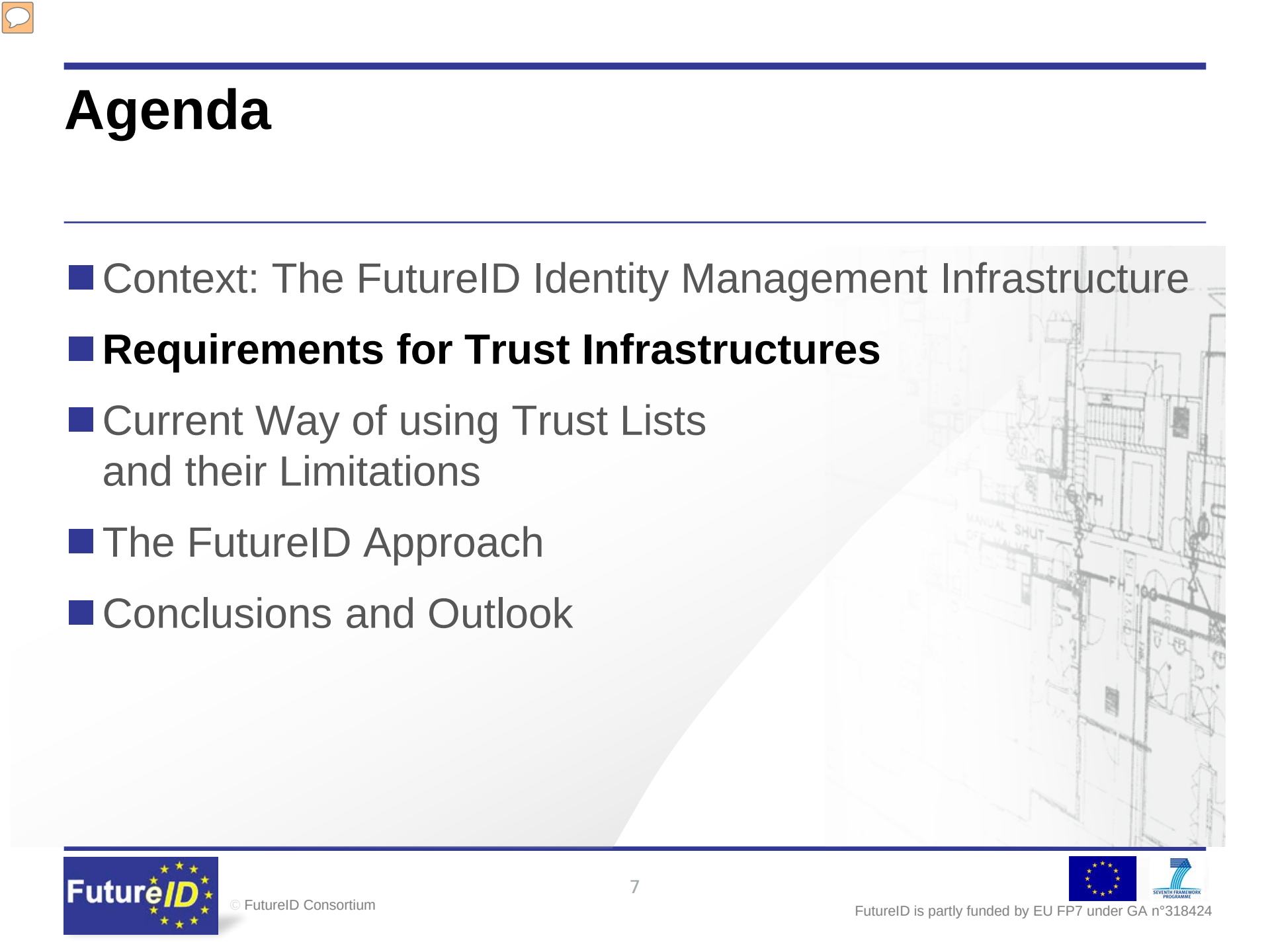
- **Which Certificates are Trusted?**
  - Signature Certs
  - Signed Assertions
  - X.509 Certs
  - …
- **Trust Scheme Authorities (TSA):**
  - Regulation and Supervision
  - Issue **Trust Lists**
- **All other Stakeholders:**
  - Make trust decisions based on Trust Lists



FutureID is partly funded by EU FP7 under GA n°318424

Agenda

- Context: The FutureID Identity Management Infrastructure
- **Requirements for Trust Infrastructures**
- Current Way of using Trust Lists and their Limitations
- The FutureID Approach
- Conclusions and Outlook



FutureID is partly funded by EU FP7 under GA n°318424

Many Types of Trust Lists

- Authentication: Trusted IdPs and Brokers (assertions):
  - Corporate internal, in Finance, for Official Gov. Identities
  - **Different verifiers have different trust perceptions**
  - Different Levels of Assurance (LoA)
- Electronic Signature (FutureID client):
  - Qualified (legally valid)
  - Non-qualified specific to application, business sector, corporation, .. at different LoAs
- Transaction Specific:
  - Registration in Business Register, Sector-Specific Register
  - Minimal Reputation or Credit Rating
  - Black Lists

FutureID is partly funded by EU FP7 under GA n°318424

Requirements for a Trust Infrastructure

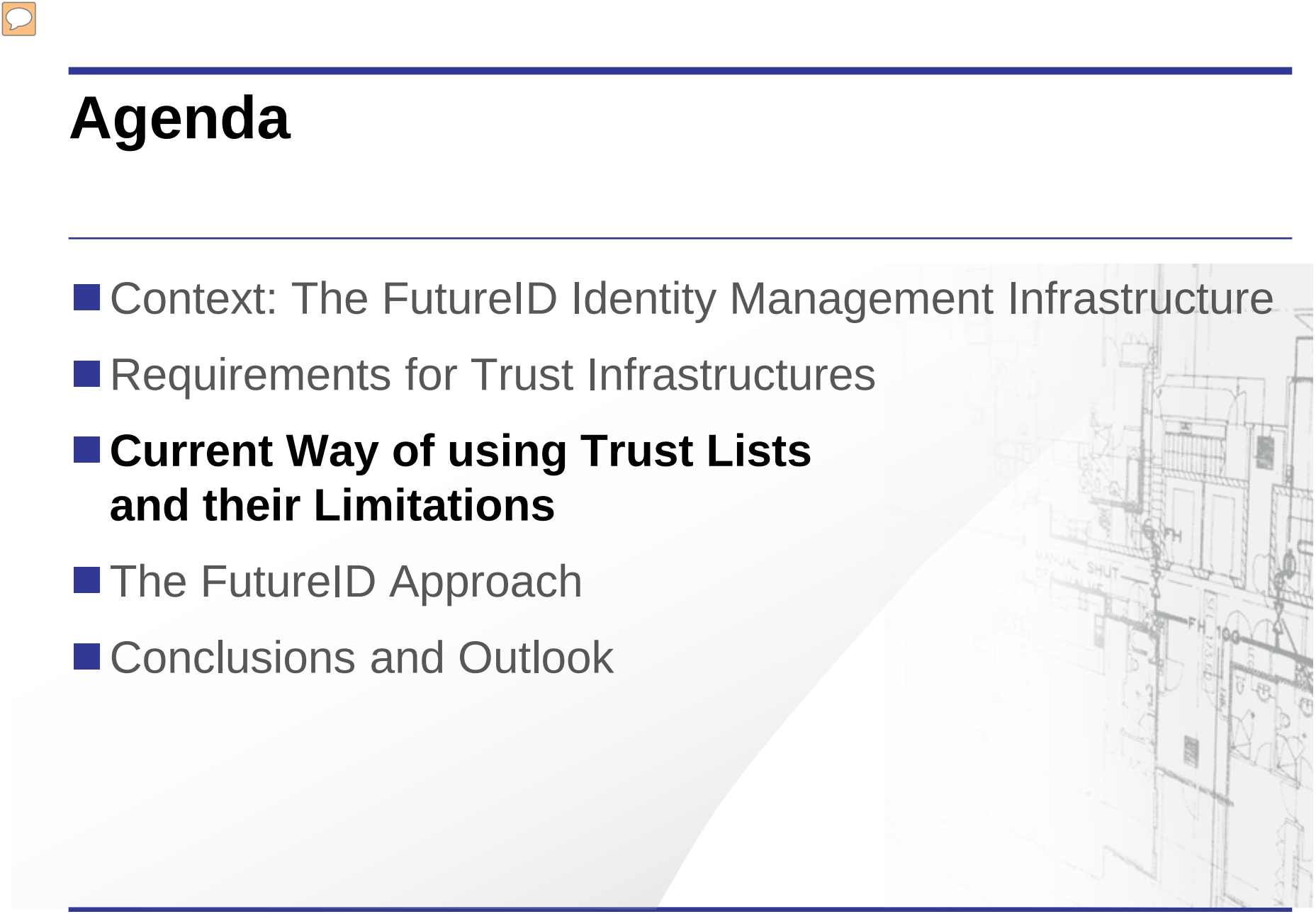
- **Open Number of Trust Lists / Trust Scheme Authorities** (TSA)
  - A Trust Scheme can consist of several Trust Lists
    - Example: EU delegates to MSs in Scheme of qualified Signature
  - Inherently **global** (multinationals, trade, …)

- **Verifier determines which TSAs to use**
  - Individual perceptions of trust
  - Select trusted TSAs in **personal Trust Policy**
  - **Combine Trust Lists** (qualified + corporate – blacklist)

FutureID is partly funded by EU FP7 under GA n°318424

Agenda

- Context: The FutureID Identity Management Infrastructure
- Requirements for Trust Infrastructures
- **Current Way of using Trust Lists and their Limitations**
- The FutureID Approach
- Conclusions and Outlook

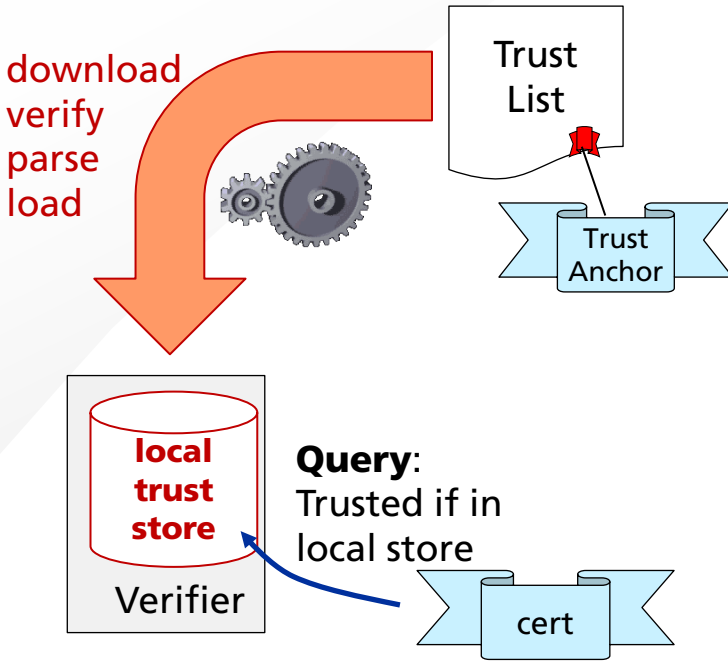


FutureID is partly funded by EU FP7 under GA n°318424

Existing Solution:
Direct Use of Trust Lists

Verifier's responsibilities:

- Securely Provision (for each List):
  - Trust Anchor (=cert)
  - Download Location
- At every Update of Trust List:
  - Download new version
  - Verify signature
  - Parse List
  - Populate local Trust Store
- Query local Trust Store



FutureID is partly funded by EU FP7 under GA n°318424

Existing Solution:
Direct Use of Trust Lists: Limitations

- **Prohibitively Complex for Verifier**
  - Multiple Trust Lists
  - Different update cycles
  - Provisioning of Trust Anchors very Security Sensitive!
  - Even Trust Anchors expire and have to be renewed

Analogy: Certificate Revocation Lists (**CRL**s):

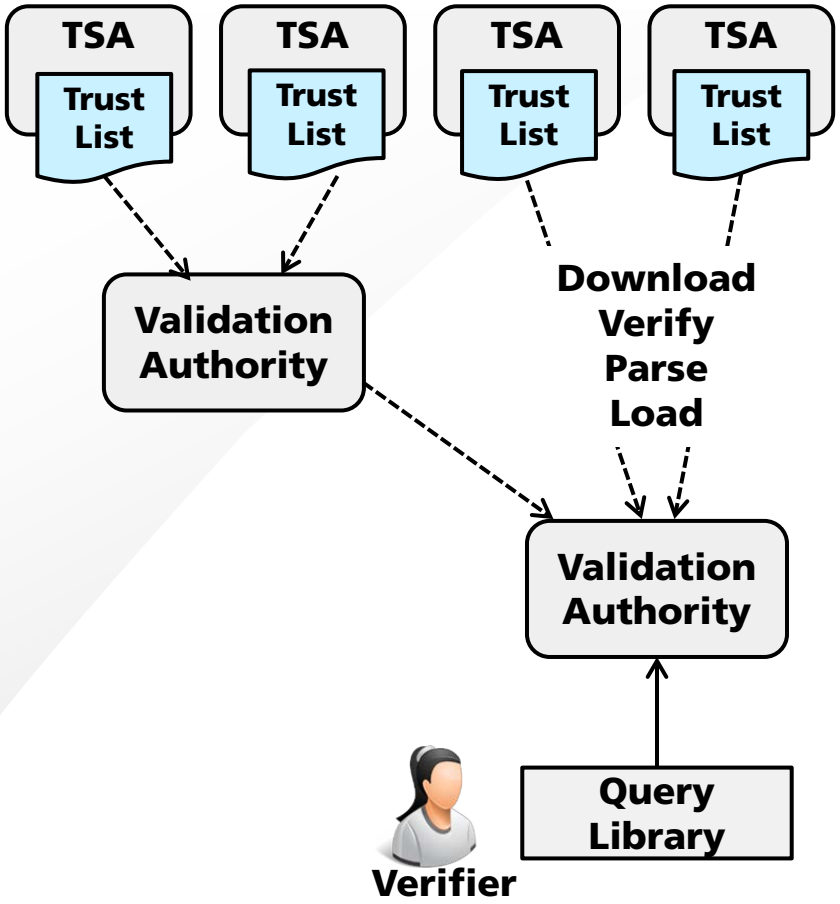
- Hardly any application uses CRLs directly
- Revocation checking has become practical only with OCSP:
  - Query of remote Trust Store of CLR-Issuer

FutureID is partly funded by EU FP7 under GA n°318424

Existing Solution:
Validation Authorities

- **Validation Authorities** (VAs) directly or indirectly **take the burden** of managing Trust Lists

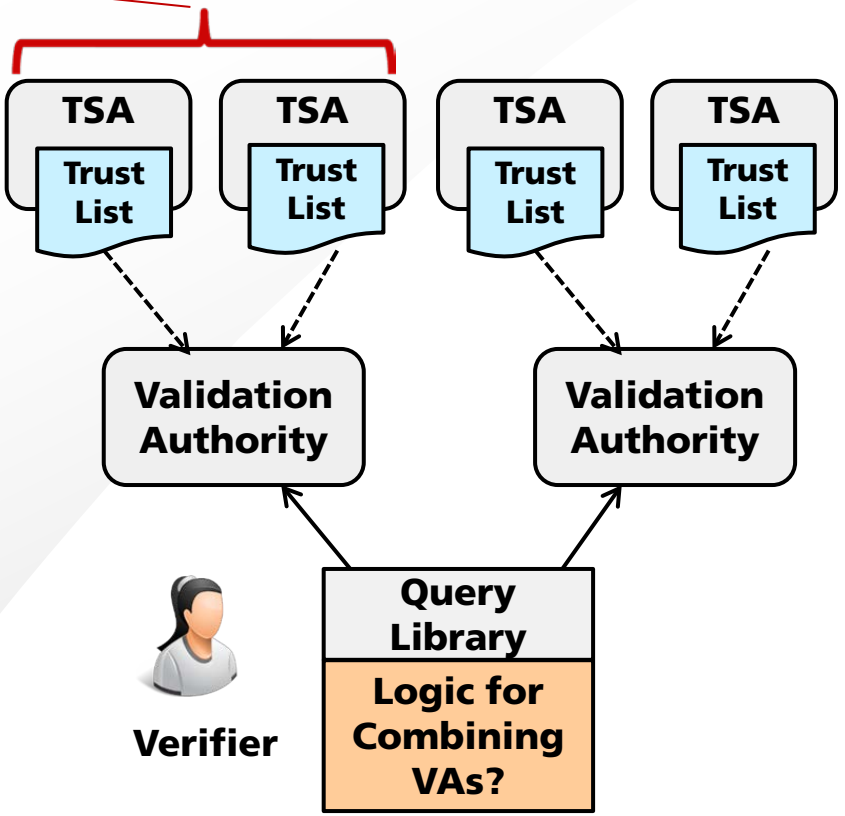
- **Verifiers** can **query** the trust status of **individual certificates**



FutureID is partly funded by EU FP7 under GA n°318424

Existing Solution: Validation Authorities: Limitations (1)

- **VAs render *Combinations of Trust Lists* Queriable** (not individual TLs)
  - Verifiers can only query if they share the same perception of trust
  - All or nothing
- **All Trust Lists need to be covered by a VA.**
- **Logic for combining queries to multiple VAs not readily available.**



FutureID is partly funded by EU FP7 under GA n°318424

Existing Solution:
Validation Authorities: Limitations (2)

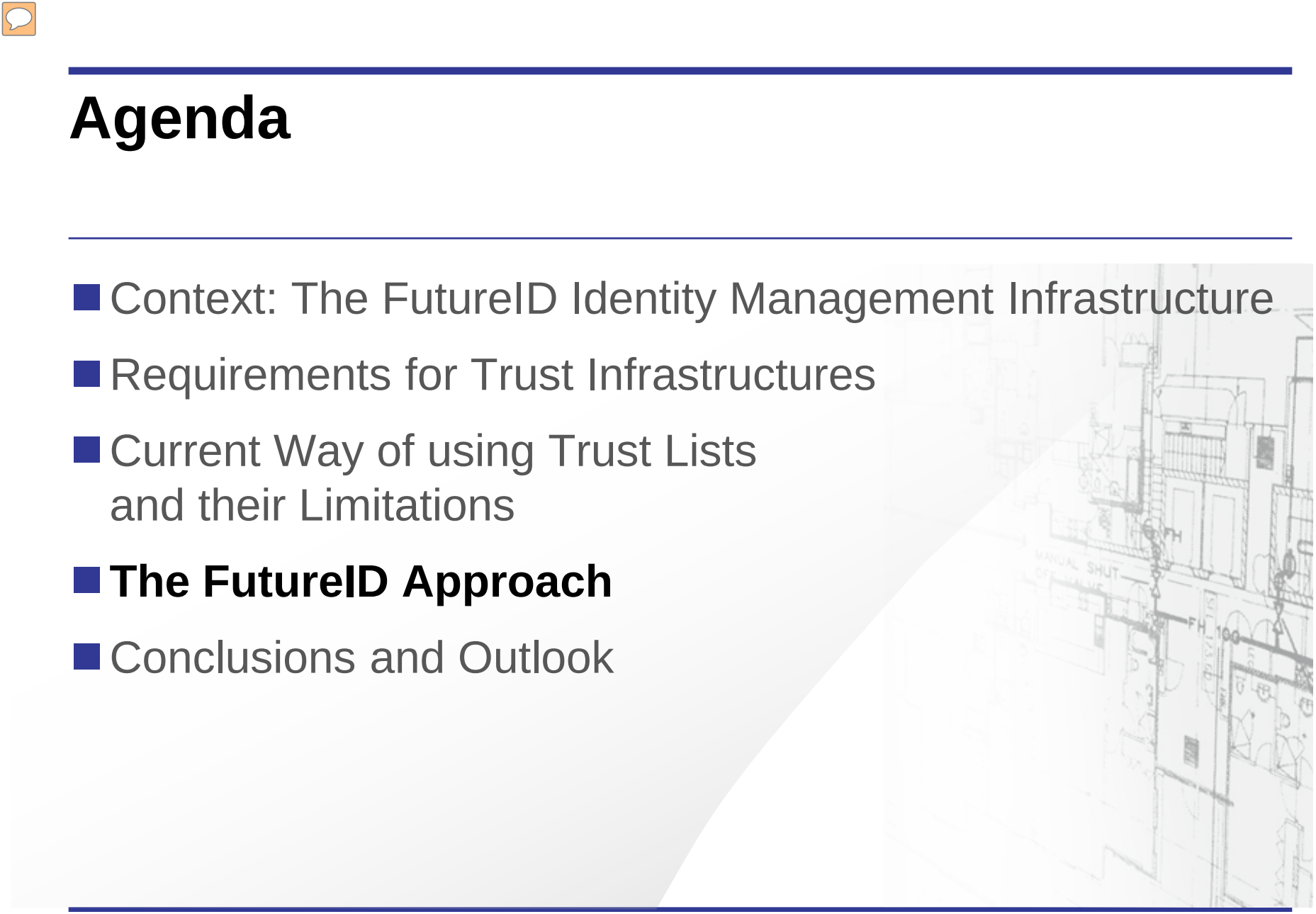
- **Validation Authorities are additional Stakeholders**
  - Who pays?
  - Liability?

- **Potential Confidentiality / Privacy Issues with certain Query Protocols**
  - Example: OASIS DSS
  - Queries require sending signed document to VA
    - Disclosure of potentially sensitive data to (central?) VA

FutureID is partly funded by EU FP7 under GA n°318424

Agenda

- Context: The FutureID Identity Management Infrastructure
- Requirements for Trust Infrastructures
- Current Way of using Trust Lists and their Limitations
- **The FutureID Approach**
- Conclusions and Outlook



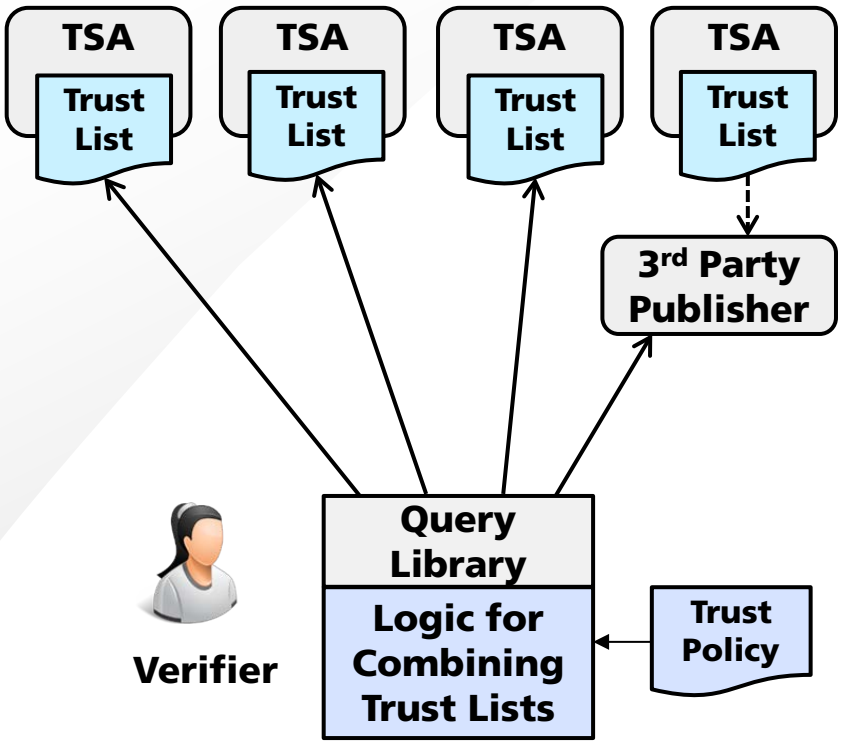
FutureID is partly funded by EU FP7 under GA n°318424

The FutureID Approach

- **Query Trust Lists directly at their Authentic Source (TSAs)**
- **Exception: 3rd Party Publisher if TSA is unwilling**
- **Logic to Combine Trust Lists based on Verifier's Trust Policy**
- **Query based on Digest of Certificates (not whole documents)**

Benefits:

- Easy for Verifiers
- Most flexible: diverse perceptions of trust
- No additional Stakeholders
- Newtwork efficient and private



FutureID is partly funded by EU FP7 under GA n°318424

Challenges of Implementation

Challenge	Consequences
Easy **Verification** of Query Reponses, Easy **Provisioning of Trust Anchors**	**Single Trust Root** instead of many Trust Anchors
Easy References to **Trust Lists** in Trust Policies	**Unique Names** for Trust Lists
Easy **Locating of** Trust List **Servers**	**Name-based Location of Service**
Support for **Subsidiarity** in Trust Schemes	Hierarchical Trust Schemes with **transparent delegation**
Mature Solution	**Protocols**, **SW**-components, Base **Infrastructure**, **Security** Review,..
Scales **Globally**	Global **Governance** of trust root Global **Organization** of Registries Global Base **Infrastructure** Global **Consensus**

FutureID is partly funded by EU FP7 under GA n°318424

Challenges of Implementation

Challenge	Consequences
Easy **Verification** of Query Reponses, Easy **Provisioning** of Trust Anchors	**Single Trust Root** instead of many Trust Anchors
Scales **Globally**	**Global Governance** of trust root **Global Organization** of Registries **Global Base Infrastructure** **Global Consensus**

Is this **Excessively Ambitious?**

How can it be achieved with **Limited Resources?**

FutureID is partly funded by EU FP7 under GA n°318424

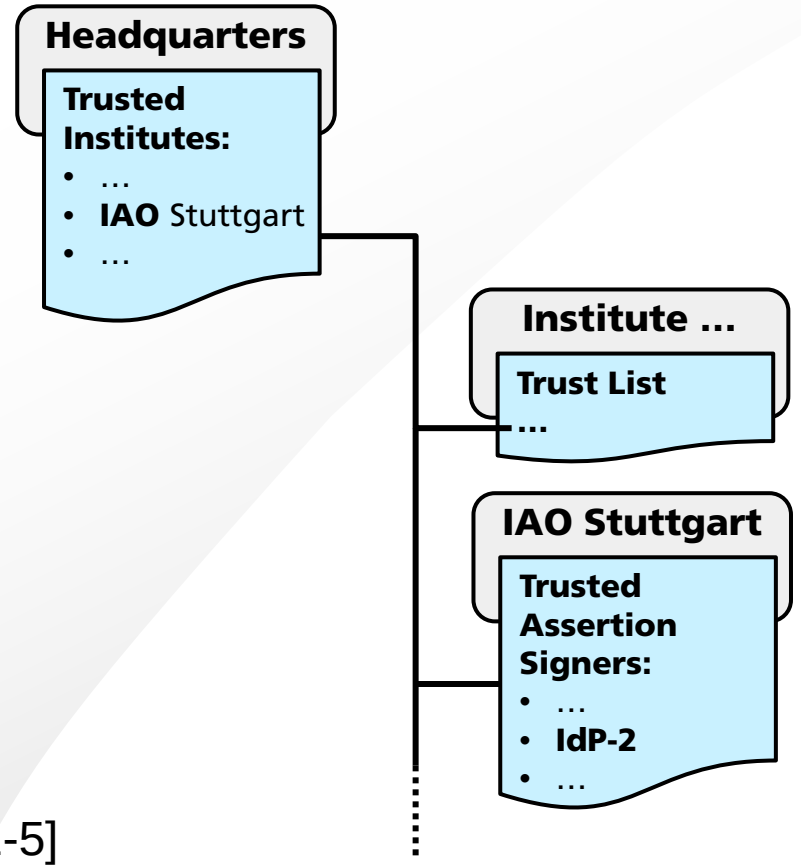
Impossible !
Unless it Already Exists:

Feature	Existing Internet Domain Name System
Single Trust Root	**Globally Accepted Single Trust Root** **Chain of Trust** down to Domain data *(DNSSEC)*
Unique Names for Trust Lists	Trust Lists == Domains **Existing DNS-Registries** can be used
Name-based querying of Trust Lists	Trust List Content == Domain data DNS server is located as part of **DNS query**
Subsidiarity through **transparent delegation**	DNS provided standard **mechanism to delegate Sub-domains** to other parties
Mature Solution	DNS **protocols**, **software** is readily available, highly mature, globally accepted, widely reviewed.
Scales **Globally**	**Governance**, **Organization**, Base **Infrastructure** (root and TLD servers) exist

FutureID is partly funded by EU FP7 under GA n°318424

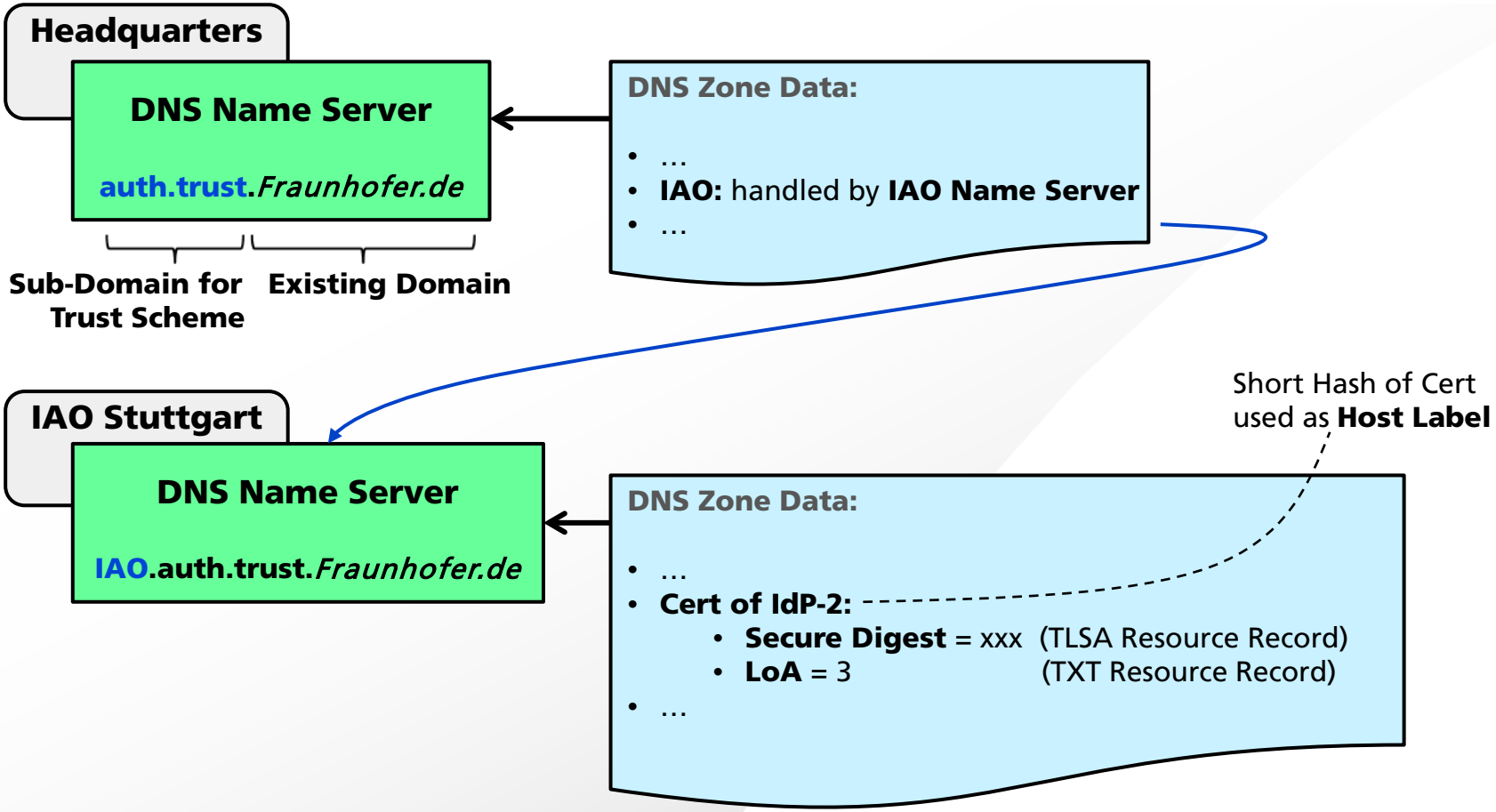
Simple Scenario:
Fictitious Fraunhofer Federation

- Fraunhofer Society:
  - More than 67 Institutes
  - Offices World-Wide
- Trust Scheme for Identity Providers
- Headquarters: **List of Lists**
- Subsidiarity Principle:
  each Institute a **Trust List**
- Each IdP has its Level of Assurance [1-5]



FutureID is partly funded by EU FP7 under GA n°318424

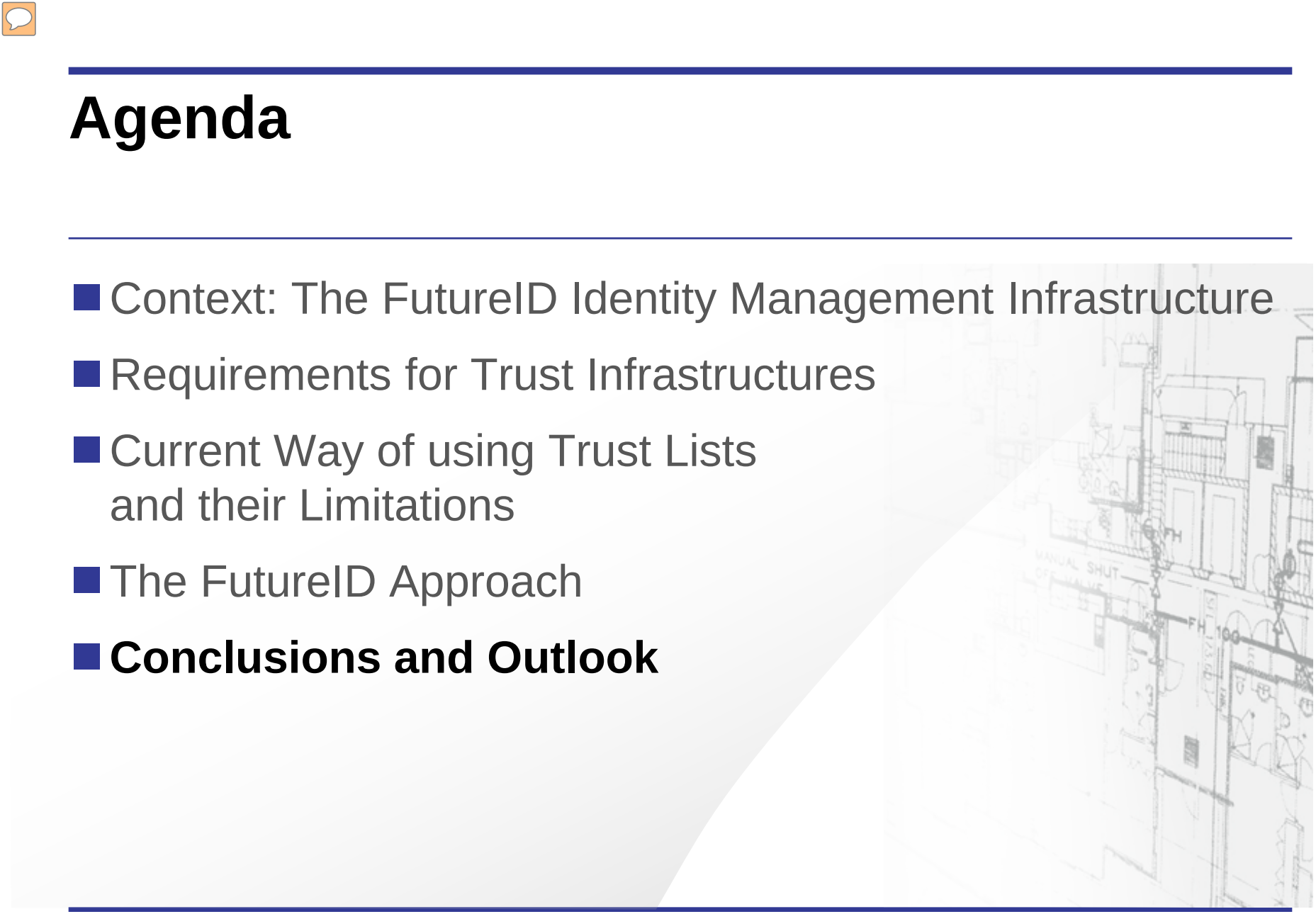
Simple Scenario:
Fictitious Fraunhofer Federation



FutureID is partly funded by EU FP7 under GA n°318424

Agenda

- Context: The FutureID Identity Management Infrastructure
- Requirements for Trust Infrastructures
- Current Way of using Trust Lists and their Limitations
- The FutureID Approach
- **Conclusions and Outlook**



FutureID is partly funded by EU FP7 under GA n°318424

Conclusions / Outlook

- FutureID IDM for Europe is very flexible and open
- Presented: a matching Trust Infrastructure
- Status: Proof of Concept Implementation (sufficient for small applications)

- Outlook: H2020 proposal to bring it to market:
- What LIGHT*est* adds:
  - More **elaborate Trust Policies** for Verifiers
  - **Mandates/Delegation**
  - **Translation** across Trust Schemes (mapping Levels of Assurance)
  - Trust evaluation of **Complete Electronic Transactions**
  - **Global organizational approach**

FutureID is partly funded by EU FP7 under GA n°318424

Contact

Bud P. Bruegger

bud.bruegger@iao.fraunhofer.de

http://FutureID.eu

FutureID is partly funded by EU FP7 under GA n°318424