eFOCUS KONFERENCIE & SEMINÁRE

SUTN Slovenský ústav technickej normalizácie

Attribute-based Credentials and Partial Identities for a more Privacy Friendly Internet

Ochrana dát a súkromia v cloudových službách (Normy & technológie pre riadenie a IT prevádzku)

Bratislava

Bratislava, *2013-02-21*

Kai Rannenberg (Kai.Rannenberg@m-chair.net)
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt, Germany
www.m-chair.net

A research project funded by the European Commission's 7th Framework Programme

SEVENTH FRAMEWORK PROGRAMME

Agenda

- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - ABC4Trust in Perspective
- Mobile Platforms & Privacy-ABCs
- Conclusions & Outlook

Agenda

- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - ABC4Trust in Perspective
- Mobile Platforms & Privacy-ABCs
- Conclusions & Outlook

Identity Management (IdM)
An early approach

- „Fear not, for I have redeemed you;
  I have called you by name: you are mine.”
  [Isaiah 43:1]

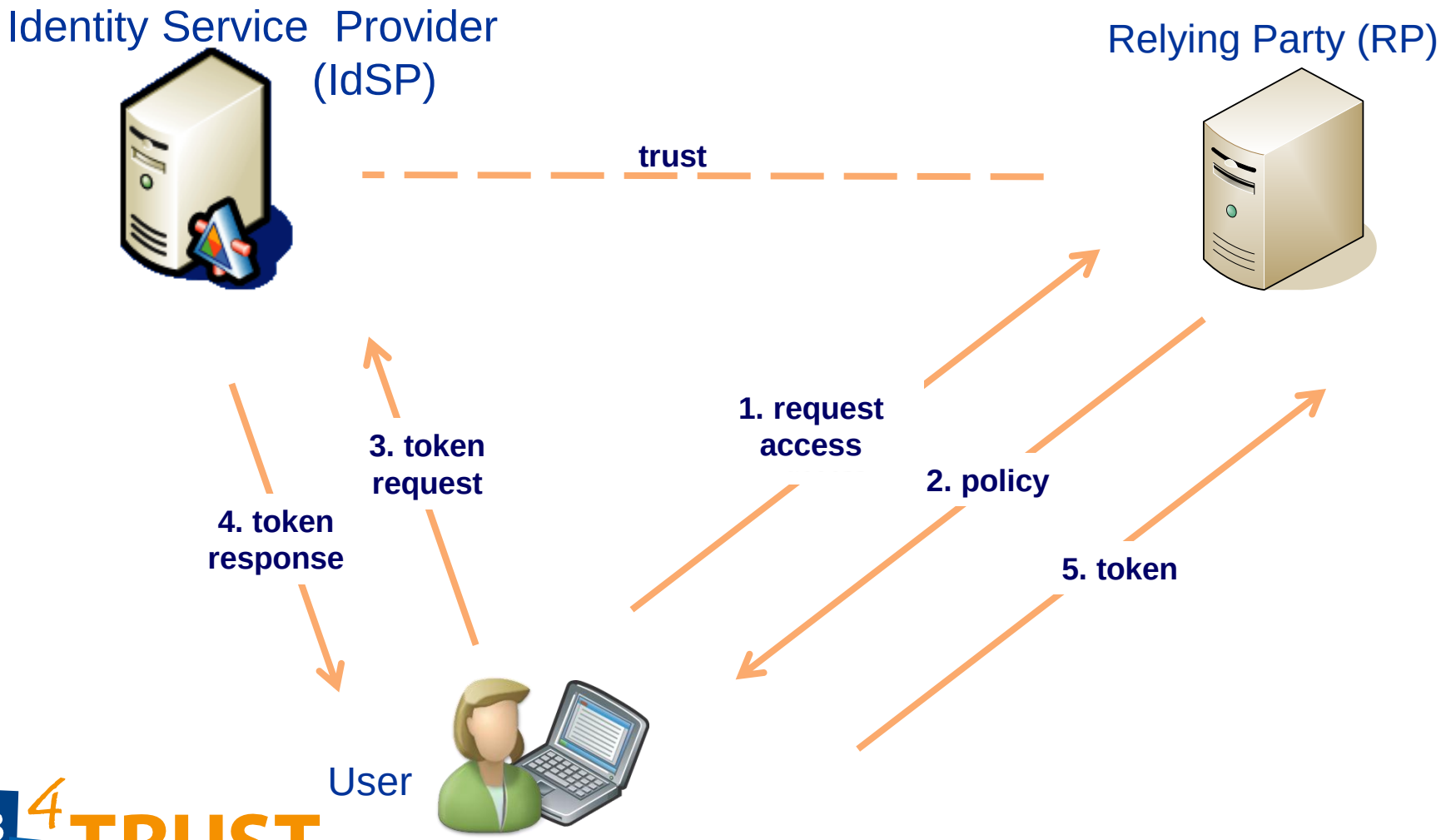
- „Neboj sa, ja som ťa vykúpil,
  povolal som ťa tvojím menom, si môj.”
  [Izaiáš 43:1]

- „Μη φοβου· διοτι εγω σε ελυτρωσα,
  σε εκαλεσα με το ονομα σου· εμου εισαι“
  [Ησαιαν 43:1]

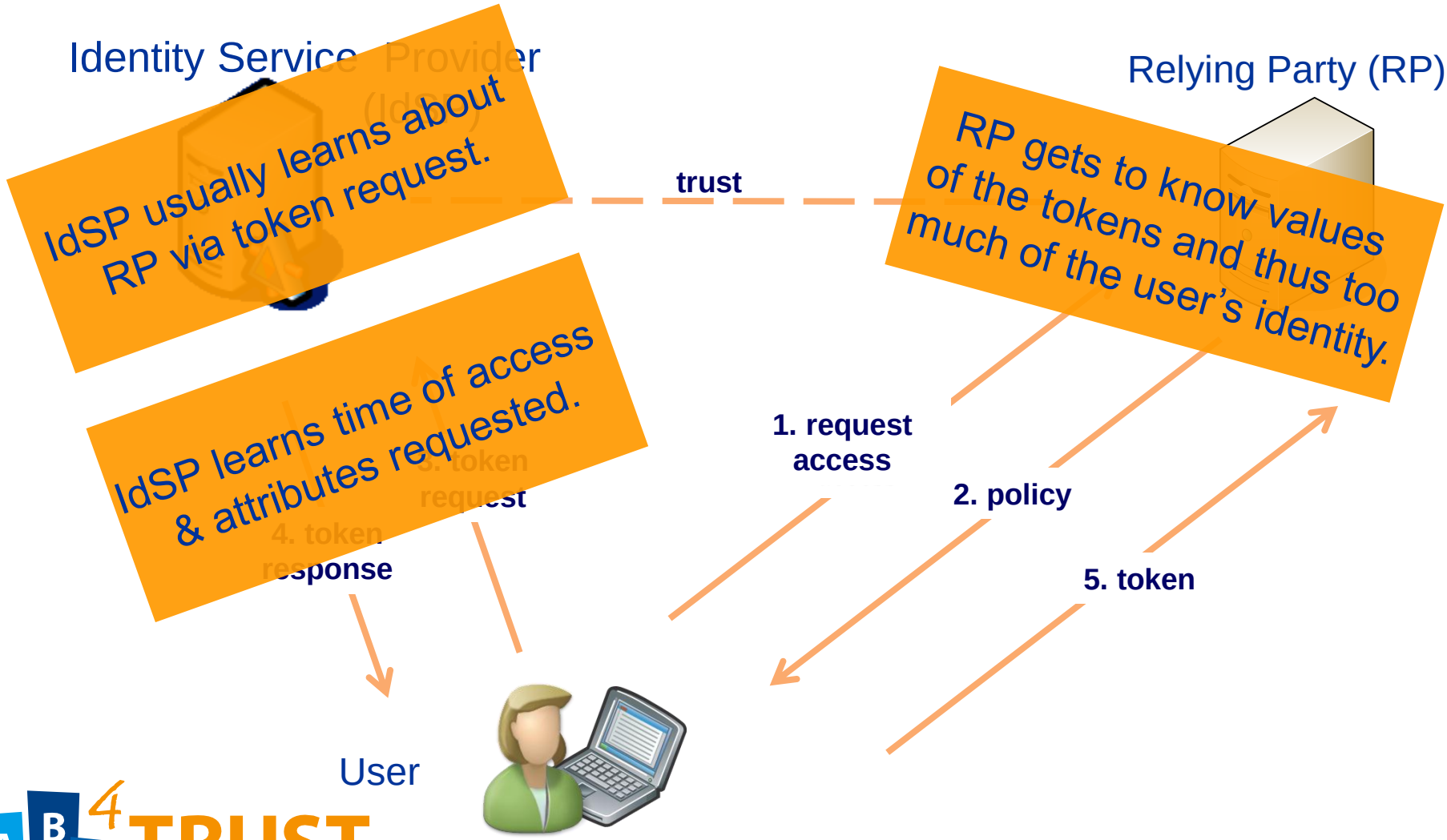
- „No temas, porque yo te he redimido,
  te he llamado por tu nombre; mío eres tú.“
  [Isaías 43 [1]]

- „Fürchte dich nicht, denn ich habe dich erlöst;
  ich habe dich bei deinem Namen gerufen; du bist mein!“
  [Jesaja 43,1]

Typical federated architecture for Identity Management (IdM)



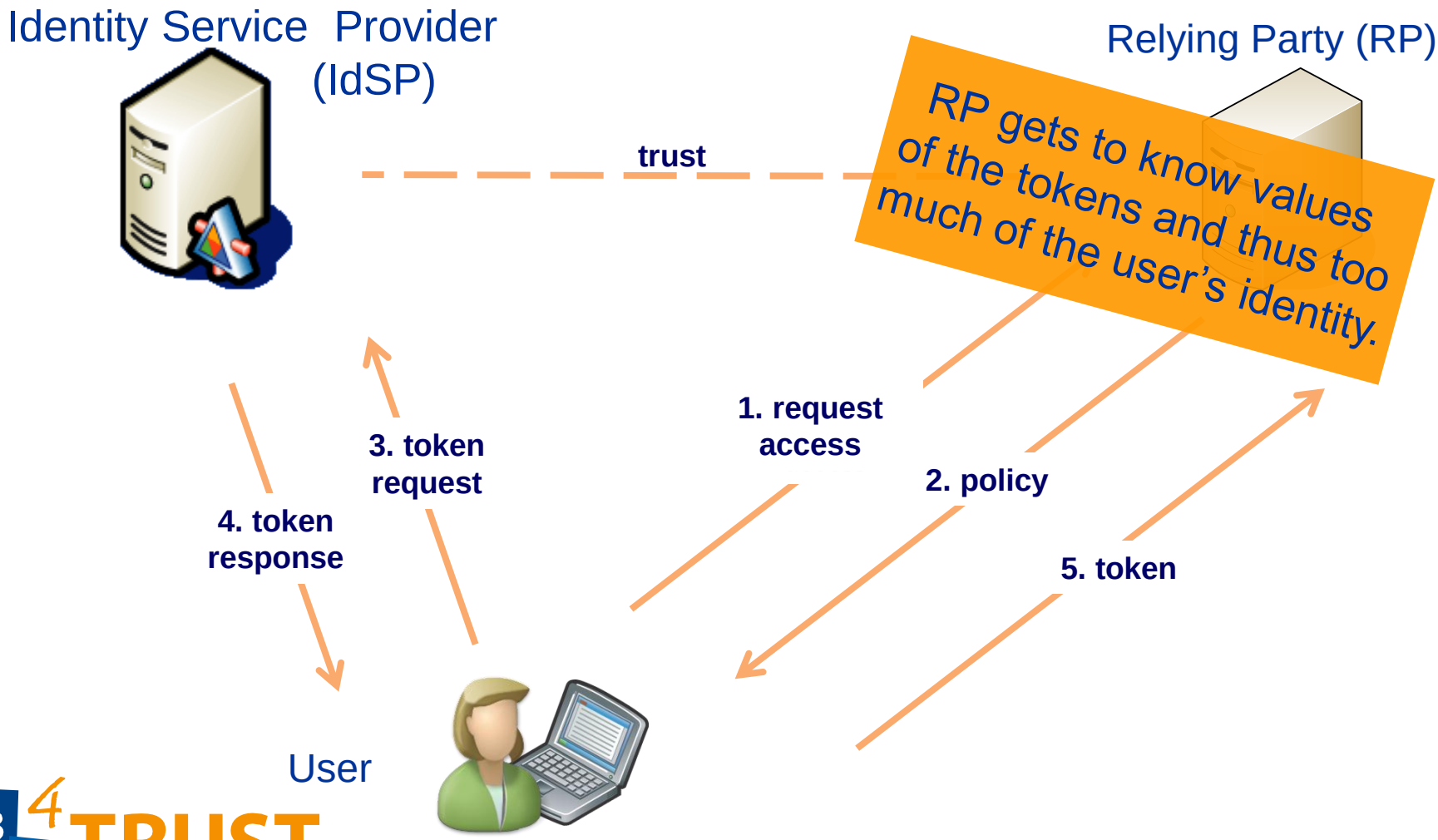
Privacy (and security) issues of typical federated IdM architectures



Agenda

- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - ABC4Trust in Perspective
- Mobile Platforms & Privacy-ABCs
- Conclusions & Outlook

Identity Management and Overidentification



Identity Management (IdM)
2 sides of a medal with enormous economic potential

- **Organisations** aim to sort out
  - User Accounts in different IT systems
  - Authentication
  - Rights management
  - Access control
- **Unified identities** help to
  - ease administration
  - manage customer relations
- **Identity management systems**
  - ease single-sign-on by unified accounts
  - solve the problems of multiple passwords

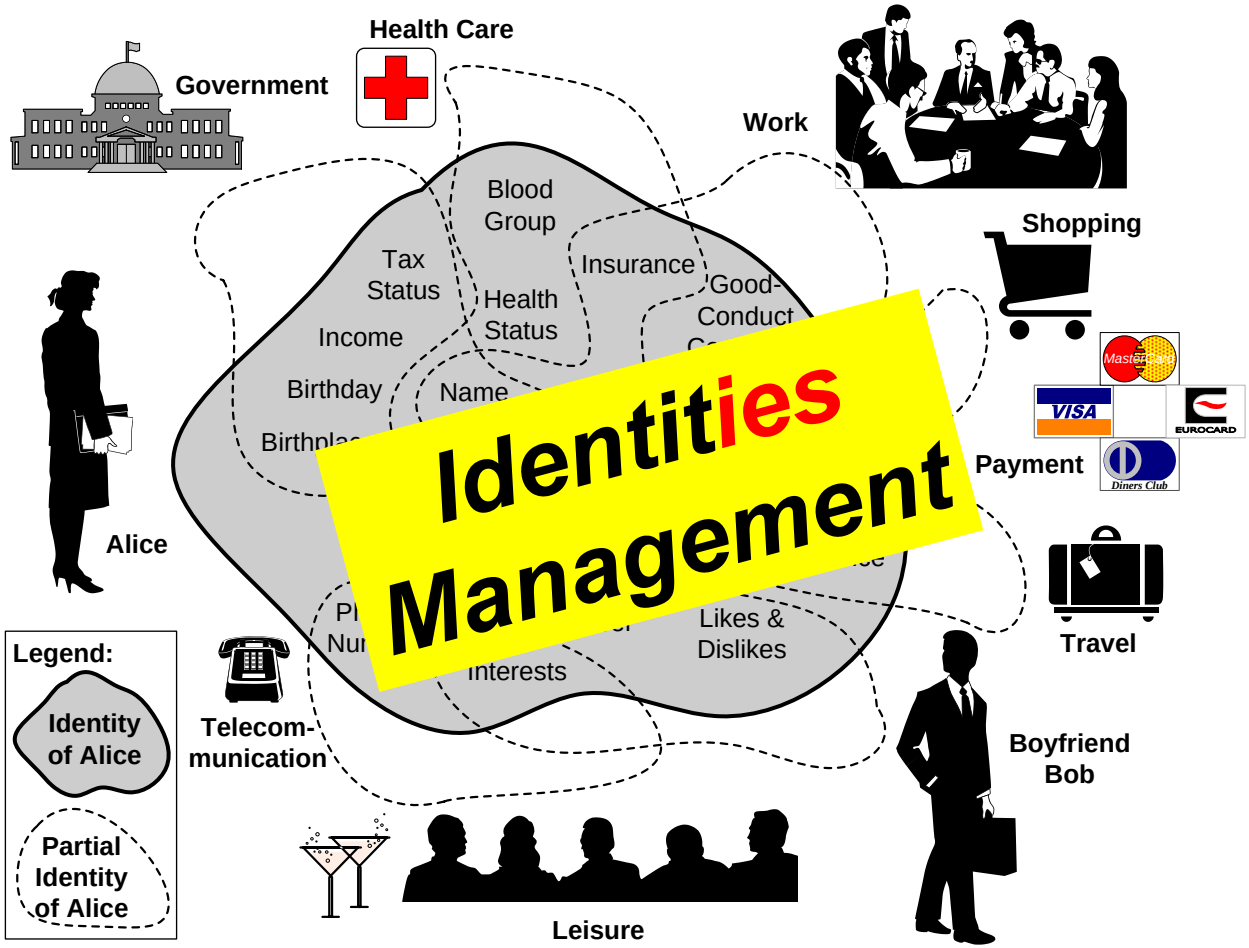
- **People** live their life
  - in different roles (professional, private, volunteer)
  - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, 2ndLife names, …)
- **Differentiated identities** help to
  - protect
    - privacy, especially anonymity
    - personal security/safety
  - enable reputation building at the same time
- **Identity management systems**
  - support users using role based identities
  - help to present the “right” identity in the right context

Identity Management (IdM)
2 sides of a medal with enormous economic potential

- **People** live their life
  - in different roles (professional, private, volunteer)
  - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, 2ndLife names, …)
- **Differentiated identities** help to
  - protect
    - privacy, especially anonymity
    - personal security/safety
  - enable reputation building at the same time
- **Identity management systems**
  - support users using role based identities
  - help to present the “right” identity in the right context

- **Organisations** aim to sort out
  - User Accounts in different IT systems
  - Authentication
  - Rights management
  - Access control
- **Unified identities** help to
  - ease administration
  - manage customer relations
- **Identity management systems**
  - ease single-sign-on by unified accounts
  - solve the problems of multiple passwords

Partial Identities needed

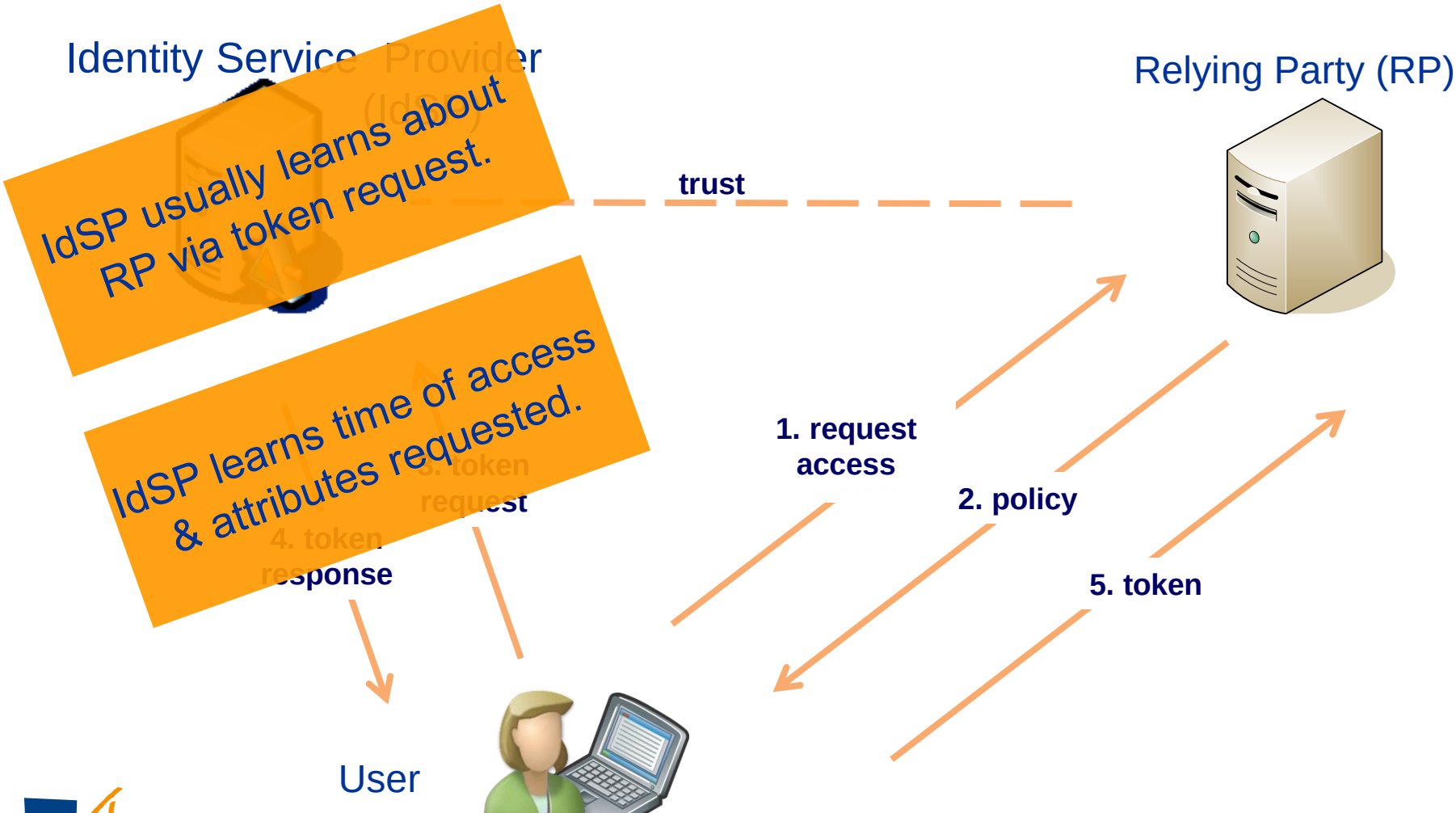


Based on [Clauß, Köhntopp 2001]

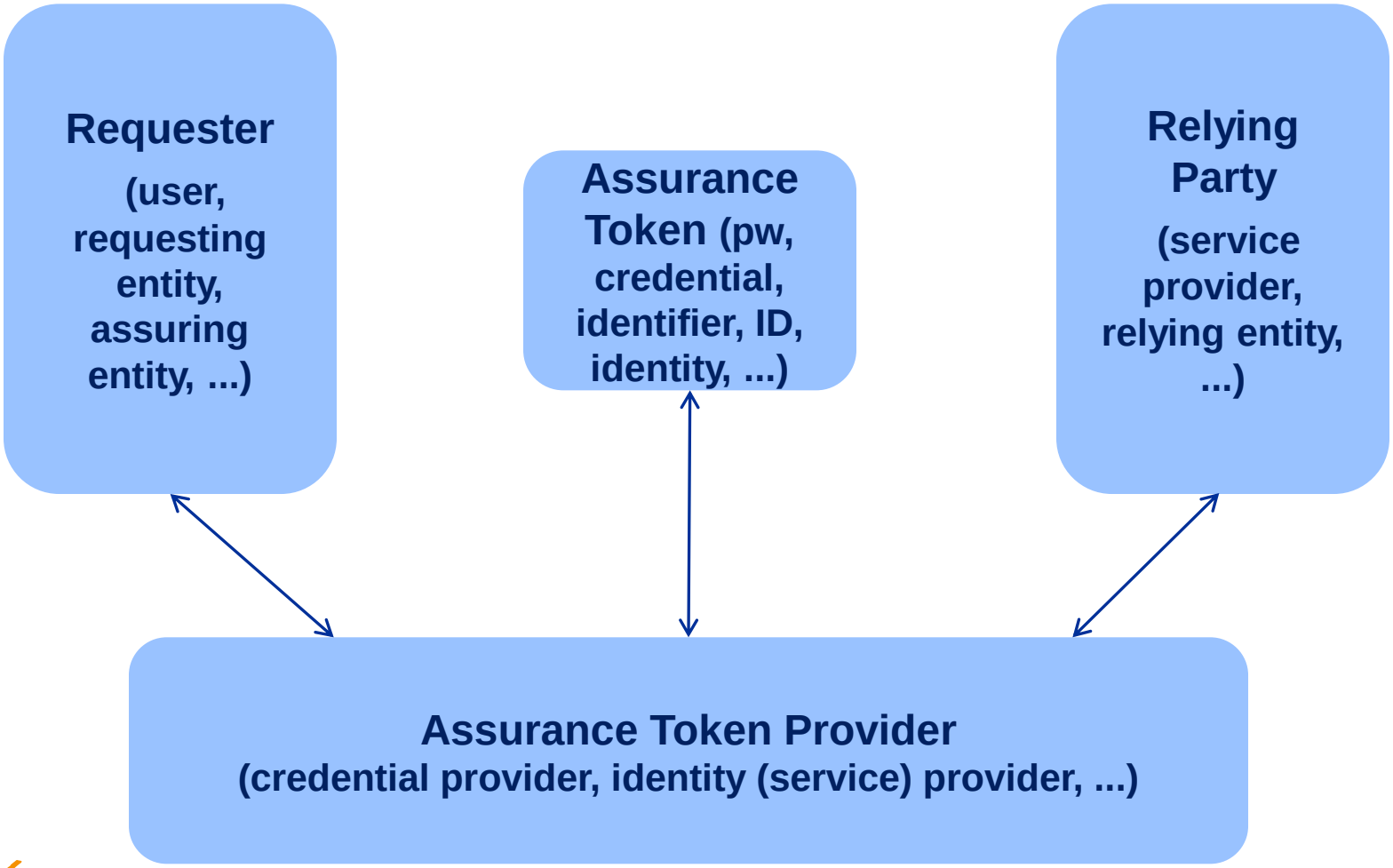
Agenda

- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - ABC4Trust in Perspective
- Mobile Platforms & Privacy-ABCs
- Conclusions & Outlook

The “Calling Home” Problem

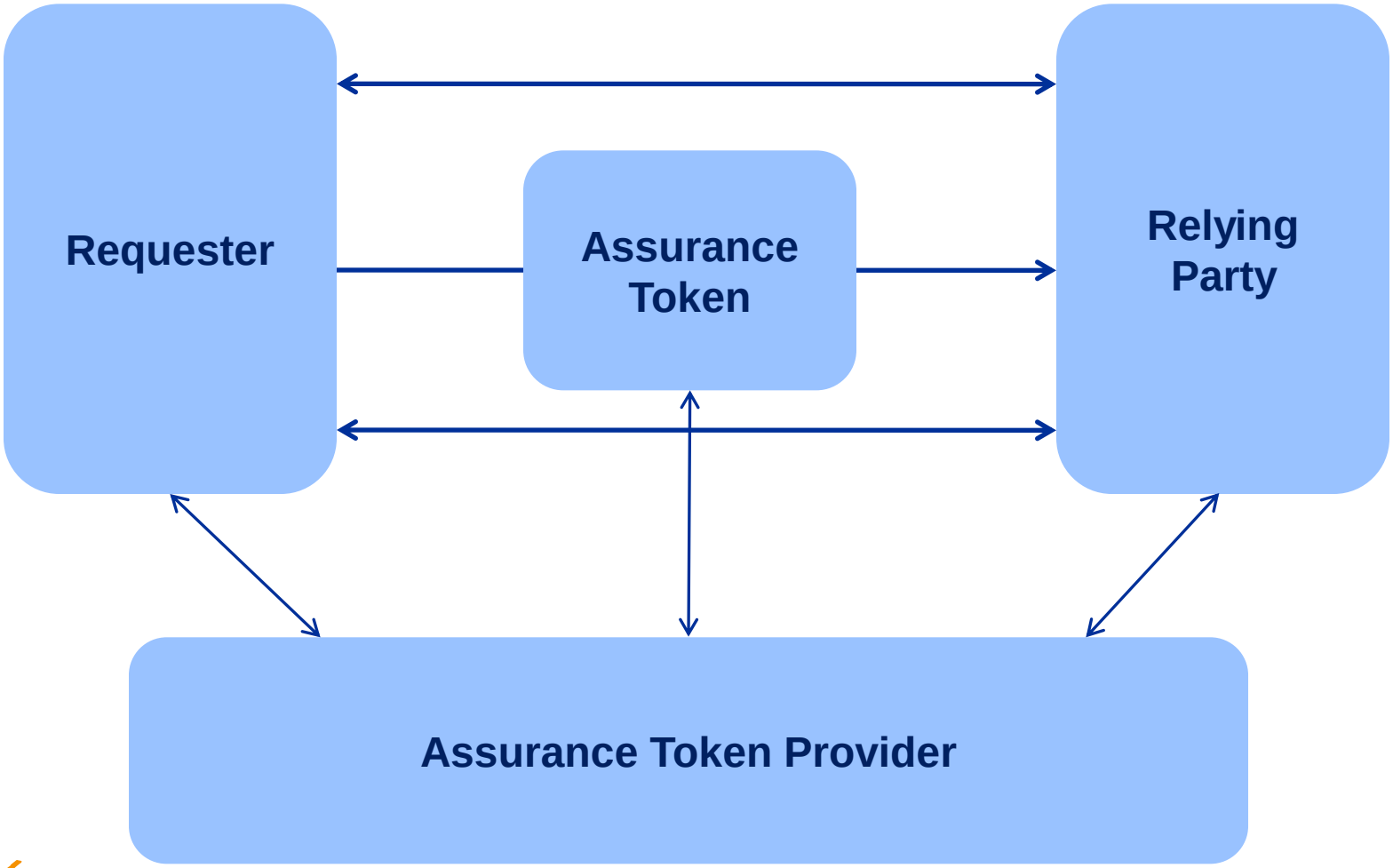


Identity Assurance
4 Entities and multiple names

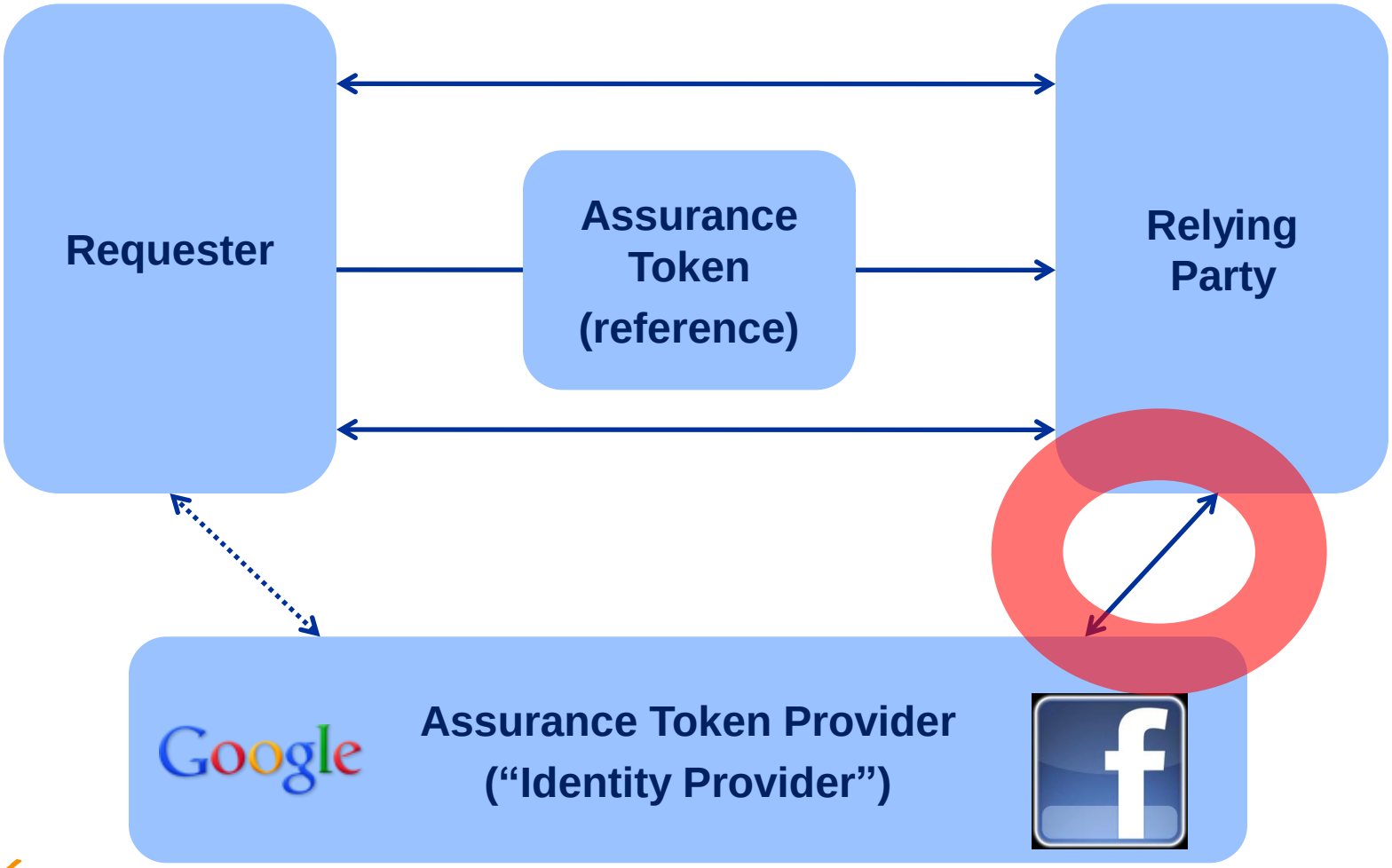


ABC4TRUST

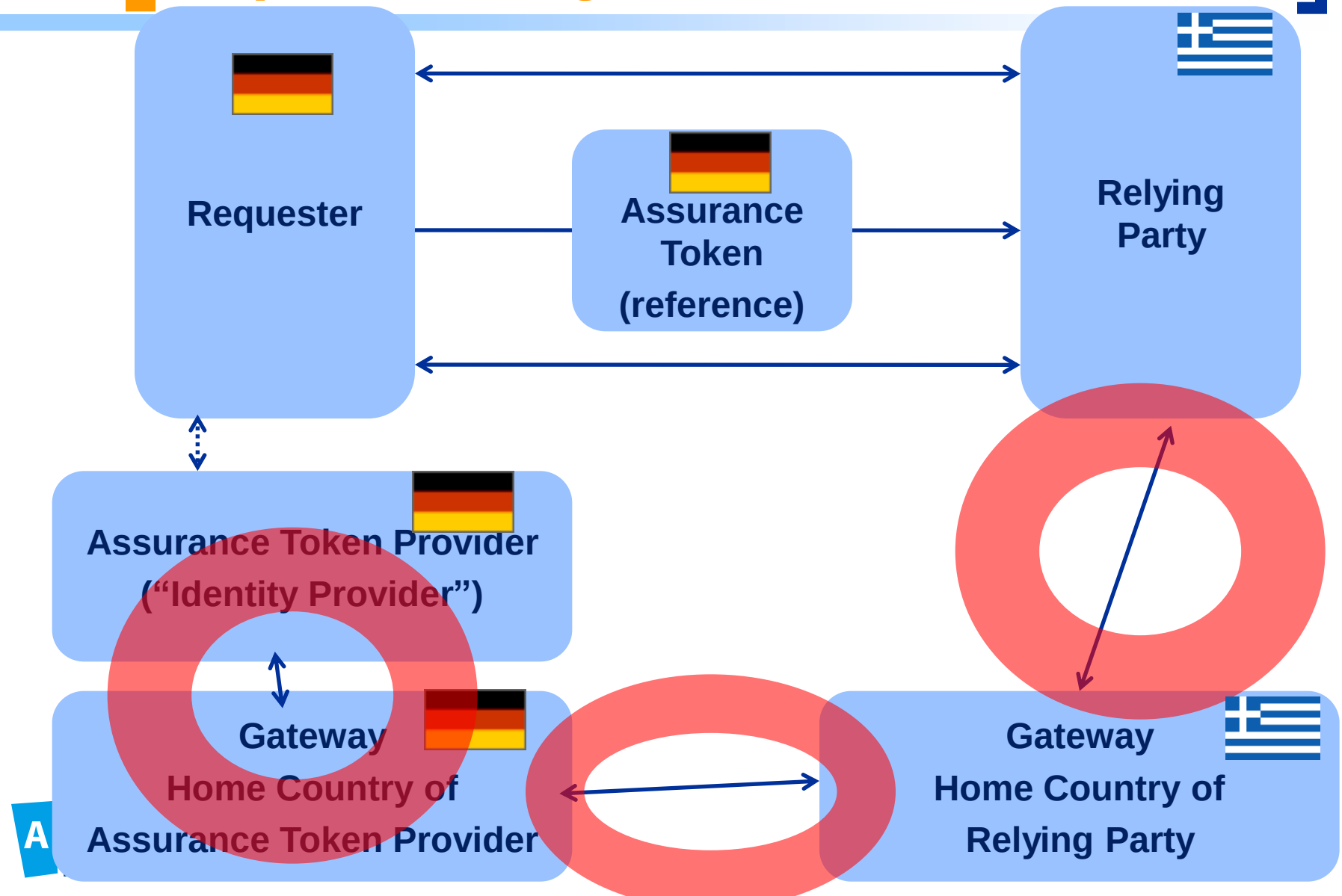
The 4 Entities and their relations



The “Identity Provider” Model “Calling Home”



STORK European eID PEPS
Triple “Calling Home”



Agenda

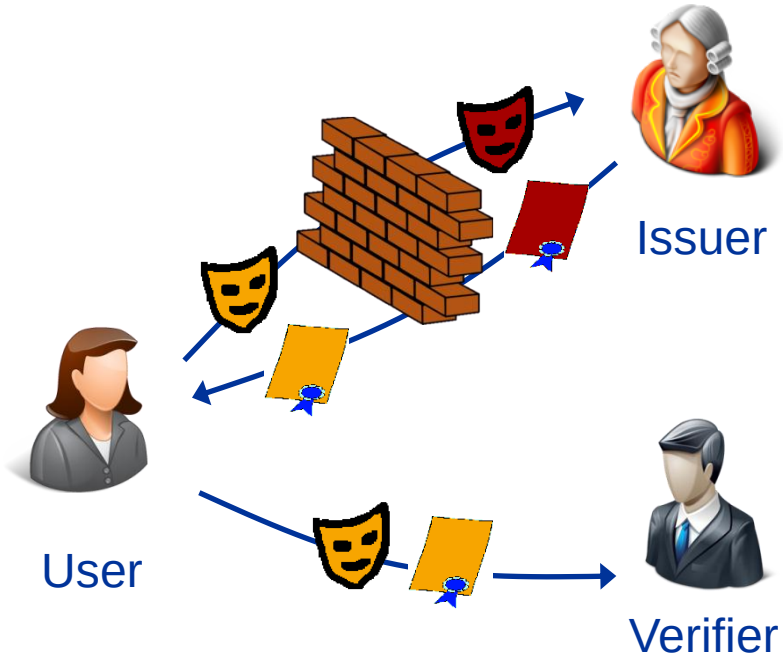
- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - ABC4Trust in Perspective
- Mobile Platforms & Privacy-ABCs
- Conclusions & Outlook

Attribute Based Credentials (privacy-ABCs)

- Certifying **relevant attributes**
- Token issuance and presentation **unlinkable**
  - Rather “coins” (that cannot be distinguished) than “bank notes” (that have a serial number)
- Users can disclose (minimal) **subsets** of the encoded **claims**
  - To respond to unanticipated requests of RPs
  - Without invalidating the token integrity
  - E.g. Certificate for birth date -> Claim for being over 21
- Two major **approaches** and **technologies**
  - U-Prove (Credentica -> Microsoft)
  - Idemix (IBM)

Two approaches for privacy-ABCs

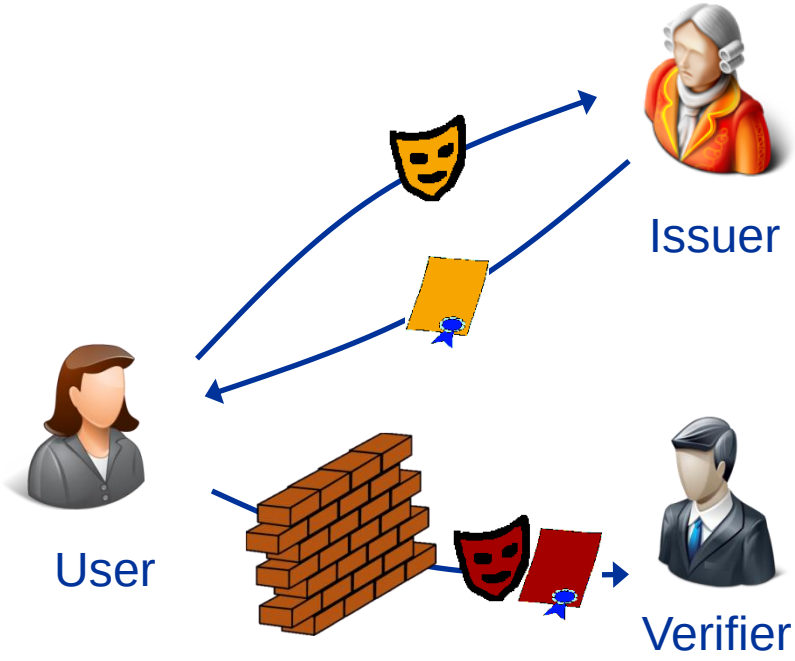
Blind Signatures



U-Prove

Brands, Paquin et al.
Discrete Logs, RSA,..

Zero-Knowledge Proofs



Idemix (Identity Mixer)

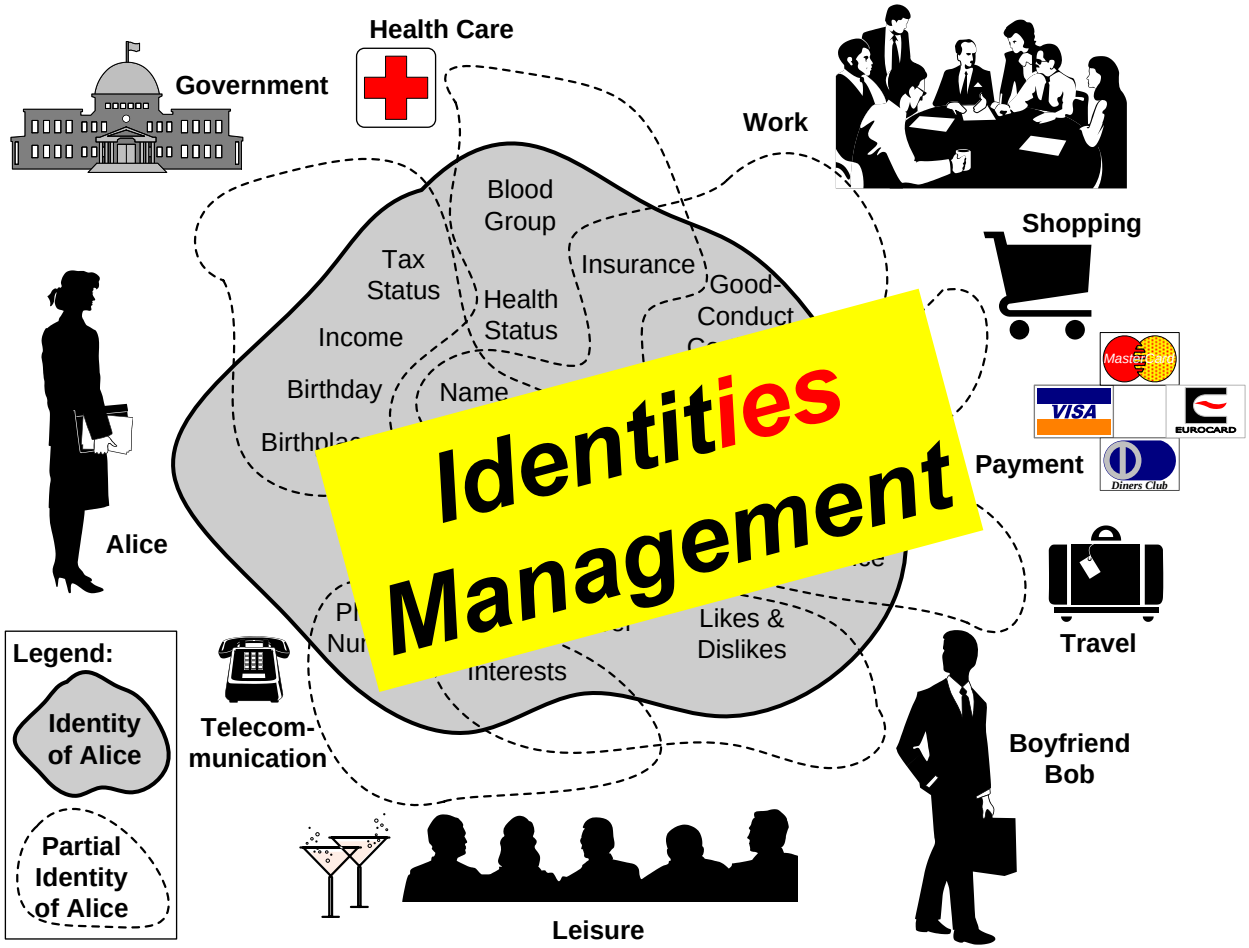
Damgard, Camenisch & Lysyanskaya
Strong RSA, pairings (LMRS, q-SDH)

ABC4TRUST

Identity Definition in ISO/IEC IS 24760-1:2011 to reduce the risk of overidentification

- **Identity** (partial identity):
  - Set of **attributes** related to an **entity**
  - From “A Framework for Identity Management” (ISO/IEC 24760)
    - Part 1: Terminology and concepts (IS:2011)
    - Part 2: Reference framework and requirements (WD)
    - Part 3: Practice (WD)

Partial Identities



Based on [Clauß, Köhntopp 2001]

Agenda

- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - ABC4Trust in Perspective
- Mobile Platforms & Privacy-ABCs
- Conclusions & Outlook

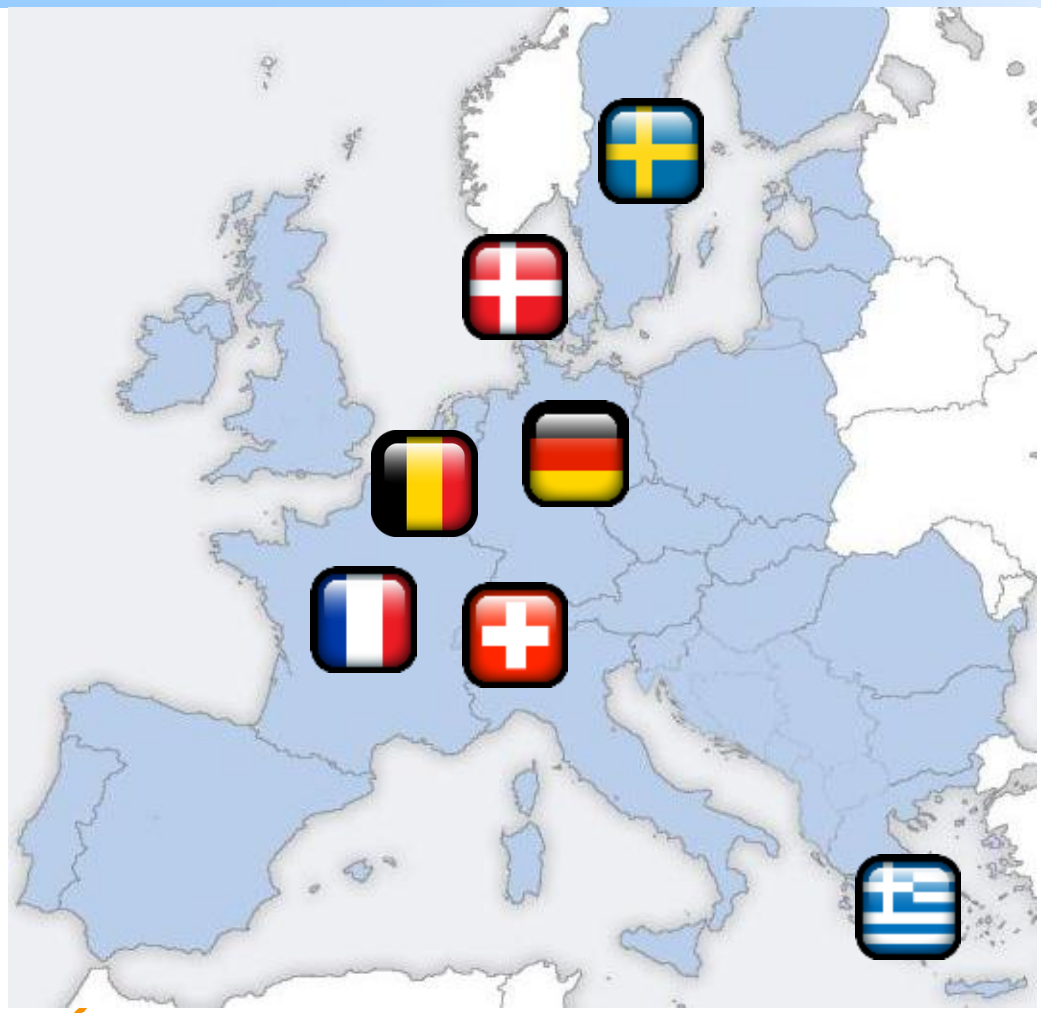
ABC4Trust Objectives

- A common, unified architecture for ABC systems to enable
  - Comparing their respective features
  - Combining them on common platforms
  - “Lock-In” free usage of ABC systems
- Open reference implementations of selected ABC systems
- Deployments in actual production enabling
  - Minimal disclosure
  - Provision of anonymous feedback to a community to one is accredited as a member
- Relevant Standards
  - e.g. in ISO/IEC JTC 1/SC 27/WG 5 “Identity Management and Privacy Technologies”

SEVENTH FRAMEWORK PROGRAMME

ABC4TRUST

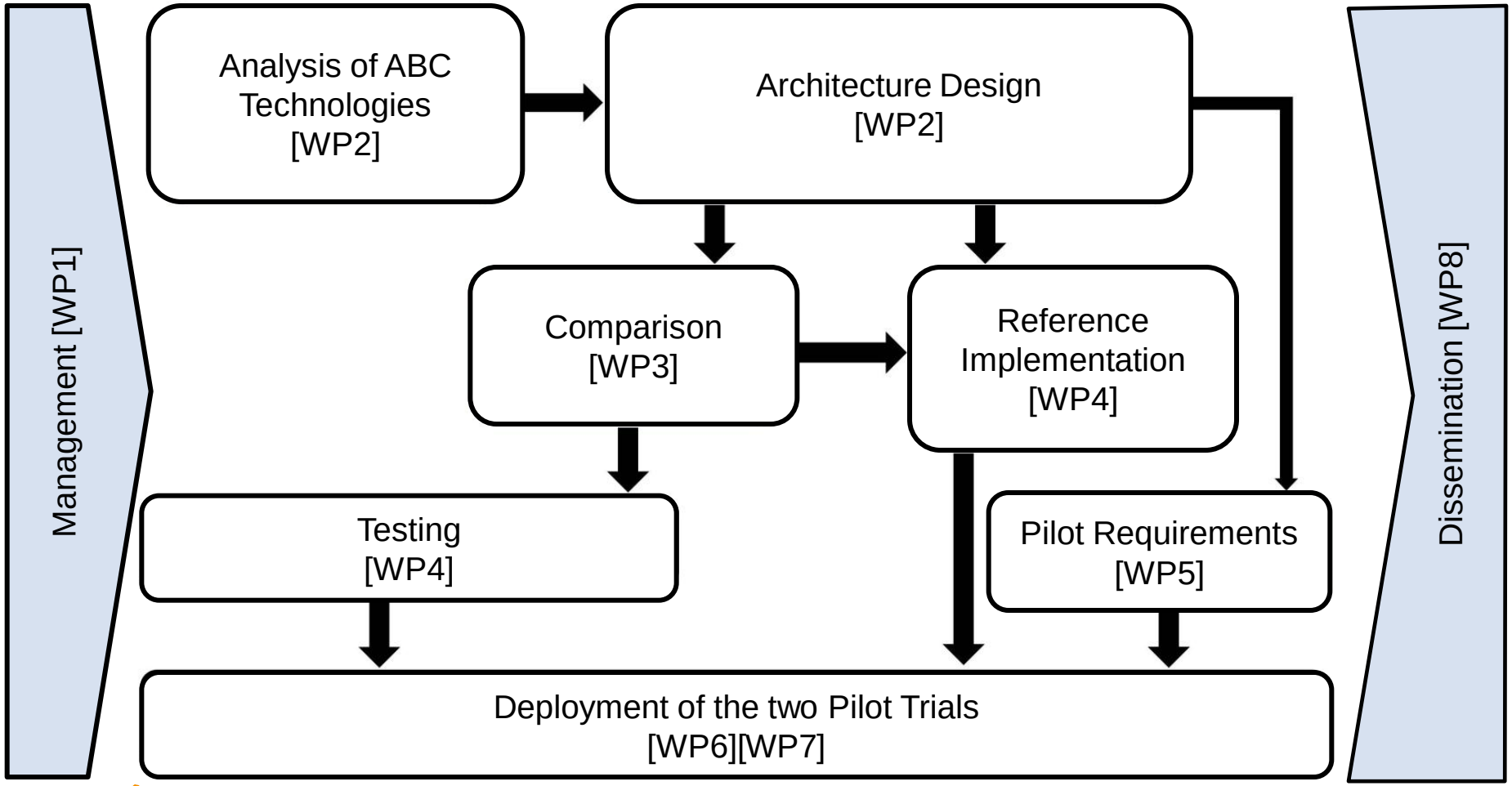
ABC4Trust Partners



- Johann Wolfgang Goethe-Universität Frankfurt, DE
- Alexandra Institute AS, DK
- Research Academic Computer Technology Institute, GR
- IBM Research - Zurich, CH
- Miracle A/S, DK
- NSN Management International GmbH, DE
- Technische Universität Darmstadt, DE
- Unabhängiges Landeszentrum für Datenschutz, DE
- Eurodocs AB, SE
- CryptoExperts SAS, FR
- Microsoft NV, BE
- Söderhamn Kommun, SE

ABC4TRUST

Project Workflow



ABC4TRUST

Agenda

- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - ABC4Trust in Perspective
- Mobile Platforms & Privacy-ABCs
- Conclusions & Outlook

ABC4Trust Pilot Trial: Community Interaction

Norrtullskolan School
Söderhamn, Sweden

- School internal social network for communication among pupils, teachers, and personnel
- Provide trusted authentication while protecting anonymity
- Usability: make privacy technology understandable for non-technical users (e.g. pupils)

ABC4TRUST

ABC4Trust Pilot Trial: Course Rating

Computer Technology Institute

Patras, Greece

- Course ratings conducted anonymously without lecturers knowing participants' identities
- Conduct polls based on attendance
- Issue multiple credentials (student cards, class attendance)
- Verify with anonymous proofs towards "untrusted" infrastructure

ABC4TRUST

Agenda

- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - ABC4Trust in Perspective
- Mobile Platforms & Privacy-ABCs
- Conclusions & Outlook

The ABC4Trust Architecture Objectives

- Abstraction of concepts of privacy-ABCs & unification of features
- A common unified architecture
  - That is independent of the specific technologies
  - Federation of privacy-ABC Systems based on different technologies
  - Interoperability between different privacy-ABC technologies
- Avoid technology lock-in
- Raise trust in privacy-ABC technologies
- Users will be able to
  - obtain credentials for many privacy-ABC technologies and
  - use them on the same hardware and software platforms
  - without having to consider which privacy-ABC technology has been used.
- Service providers and Identity Service Providers will be able to
  - adopt whatever privacy-ABC technology best suits their needs.

ABC4TRUST

The ABC4Trust Architecture

- Entities and Interactions
- High-level features and concepts of privacy-ABCs
- System architecture and components for handling privacy-ABCs
- Component APIs
- XML specification of all data formats

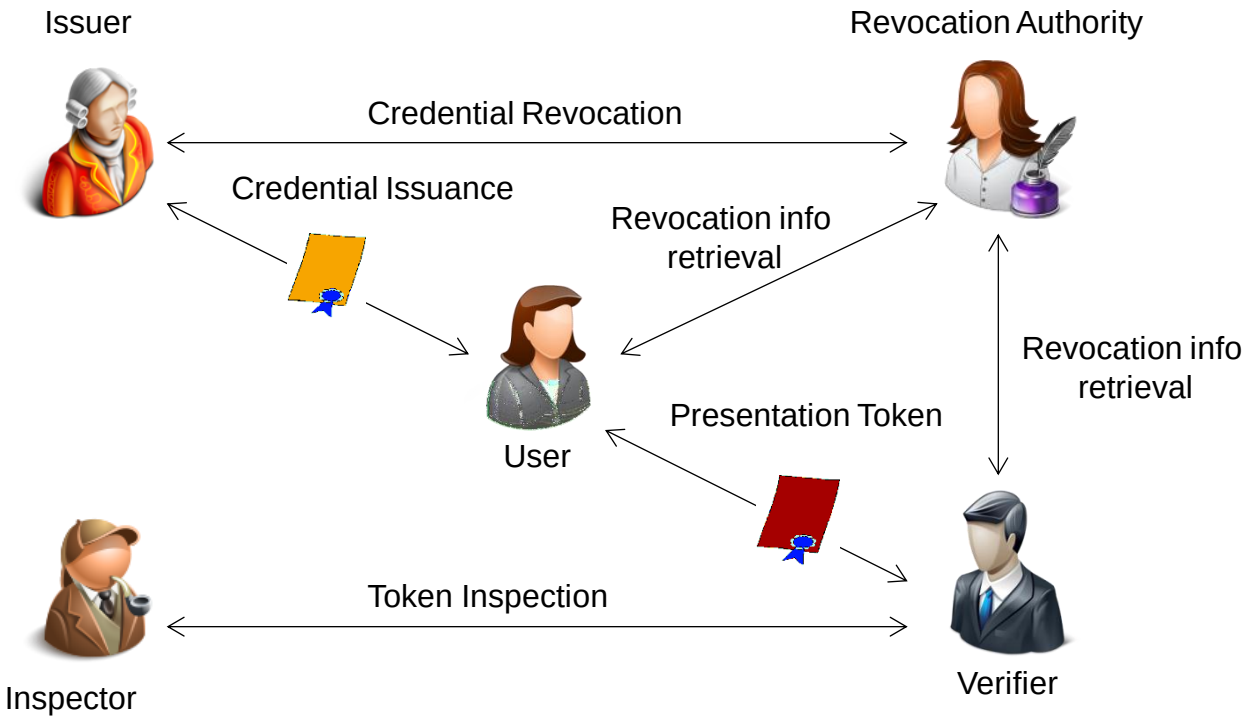
The ABC4Trust Architecture Elements

- **Entities and Interactions**
- **High-level features and concepts of privacy-ABCs**
- **System architecture and components for handling privacy-ABCs**
- Component APIs
- XML specification of all data formats

The ABC4Trust Architecture Elements

- **Entities and Interactions**
- High-level features and concepts of privacy-ABCs
- System architecture and components for handling privacy-ABCs
- Component APIs
- XML specification of all data formats

Entities and Interactions



The ABC4Trust Architecture

- Entities and Interactions
- **High-level features and concepts of privacy-ABCs**
- System architecture and components for handling privacy-ABCs
- Component APIs
- XML specification of all data formats

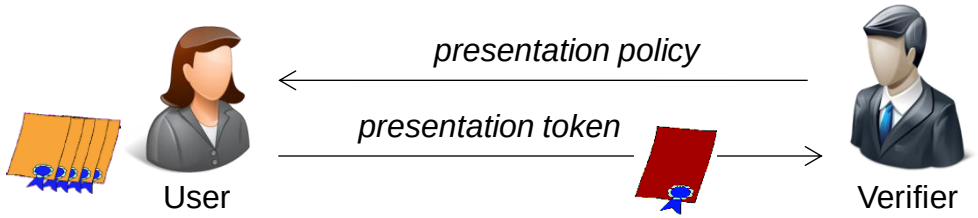
Features and concepts

- Credentials
  - List of attributes, encoding, etc.
- Presentation policies, presentation tokens
- User binding and device binding
- Issuance policies
- Pseudonyms
  - Verifiable, certified, scope-exclusive
- Inspection + revocation

Features and concepts

- Credentials
  - List of attributes, encoding, etc.
- **Presentation policies, presentation tokens**
- User binding and device binding
- Issuance policies
- Pseudonyms
  - Verifiable, certified, scope-exclusive
- Inspection + revocation

Presentation



- Presentation policy
  - Which (combination of) credentials from which issuer
  - Which attributes or attribute predicates to reveal
- Presentation token
  - *Description*: mechanism-agnostic revealed information
  - *Evidence*: mechanism-specific crypto blobs
  - Untraceable and unlinkable by default, traceable and linkable when so desired

ABC4TRUST

Presentation policy

```
<?xml version="1.0" encoding="UTF-8"?>

<PresentationPolicyAlternatives xmlns="http://abc4trust.eu/wp2/abcschemav1.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc"
    xsi:schemaLocation="http://abc4trust.eu/wp2/abcschemav1.0 schema.xsd"
    Version="1.0">
<PresentationPolicy PolicyUID="policy1" EnforceSameUserBinding="true" EnforceSameDeviceBinding="false">

    <Message>
        <Nonce>aDk3UEMzOTNjOTl1cmZHQ210U0c=</Nonce>
    </Message>
    <Pseudonym Alias="nym" Scope="http://sweden.gov/poll0105" Exclusive="true"/>
    <Credential Alias="id">
        <CredentialSpecAlternatives>
            <CredentialSpecUID>urn:sweden:id</CredentialSpecUID>
        </CredentialSpecAlternatives>
        <IssuerAlternatives>
            <IssuerParametersUID>urn:sweden:id:issuer</IssuerParametersUID>
        </IssuerAlternatives>
        <DisclosedAttribute AttributeType="urn:sweden:id:city"/>
    </Credential>
    <AttributePredicate Function="urn:oasis:names:tc:xacml:1.0:function:date-less-than">
        <Attribute CredentialAlias="id" AttributeType="urn:sweden:id:bdate"/>
        <ConstantValue>1994-01-20</ConstantValue>
    </AttributePredicate>

</PresentationPolicy>
</PresentationPolicyAlternatives>
```

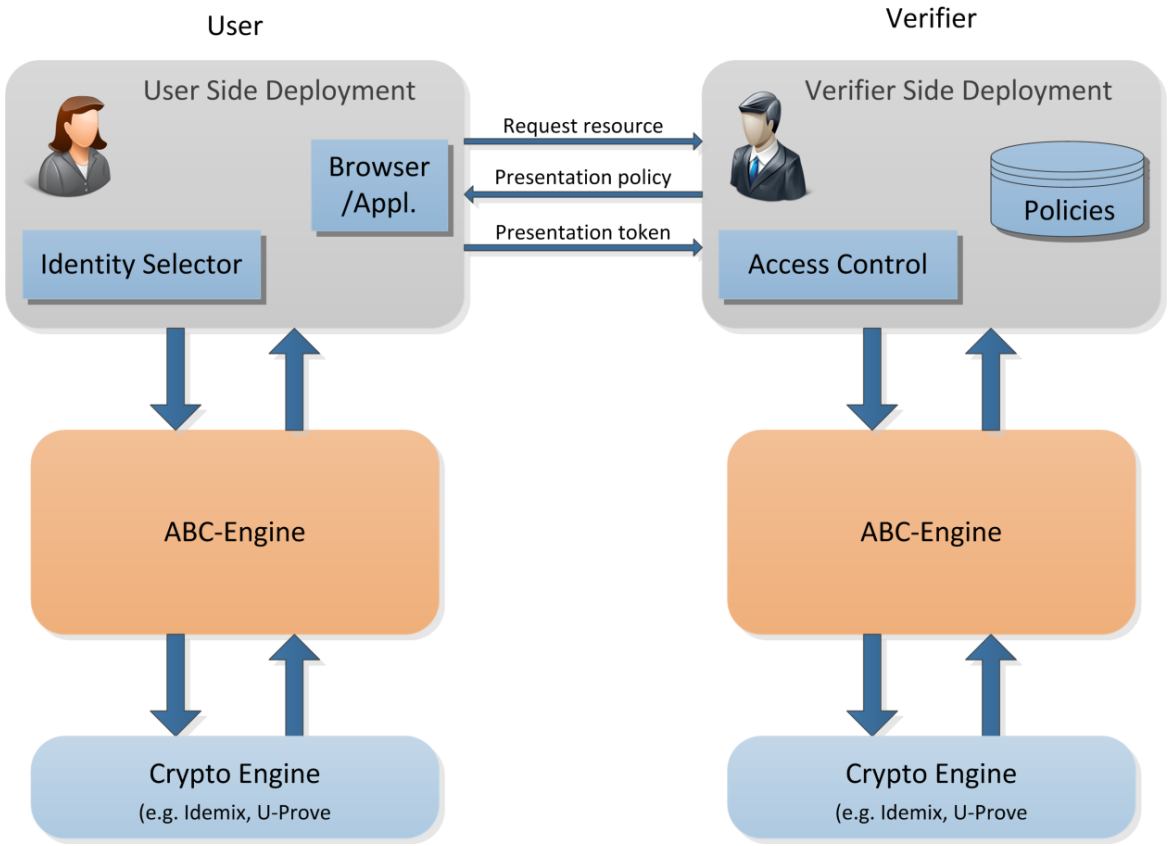
Presentation token

```
<?xml version="1.0" encoding="UTF-8"?>

<PresentationToken xmlns="http://abc4trust.eu/wp2/abcschemav1.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc"
    xsi:schemaLocation="http://abc4trust.eu/wp2/abcschemav1.0 schema.xsd"
    Version="1.0">

    <PresentationTokenDescription PolicyUID="policy1" EnforceSameUserBinding="true"
EnforceSameDeviceBinding="false">
        <Message>
            <Nonce>aDk3UEMzOTNjOTl1cmZHQ210U0c=</Nonce>
        </Message>
        <Pseudonym Alias="nym" Scope="http://sweden.gov/poll0105" Exclusive="true">
            <PseudonymValue>MER2VXpyR0VaOW51YXdVNHRISHI=</PseudonymValue>
        </Pseudonym>
        <Credential Alias="id">
            <CredentialSpecUID>urn:sweden:id</CredentialSpecUID>
            <IssuerParametersUID>urn:sweden:id:issuer</IssuerParametersUID>
            <DisclosedAttribute AttributeType="urn:sweden:id:city">
                <AttributeValue>Söderhamn</AttributeValue>
            </DisclosedAttribute>
        </Credential>
        <AttributePredicate Function="urn:oasis:names:tc:xacml:1.0:function:date-less-than">
            <Attribute CredentialAlias="id" AttributeType="urn:sweden:id:bdate"/>
            <ConstantValue>1994-01-20</ConstantValue>
        </AttributePredicate>
    </PresentationTokenDescription>

    <CryptoEvidence> ... </CryptoEvidence>

</PresentationToken>
```

The ABC4Trust Architecture Elements

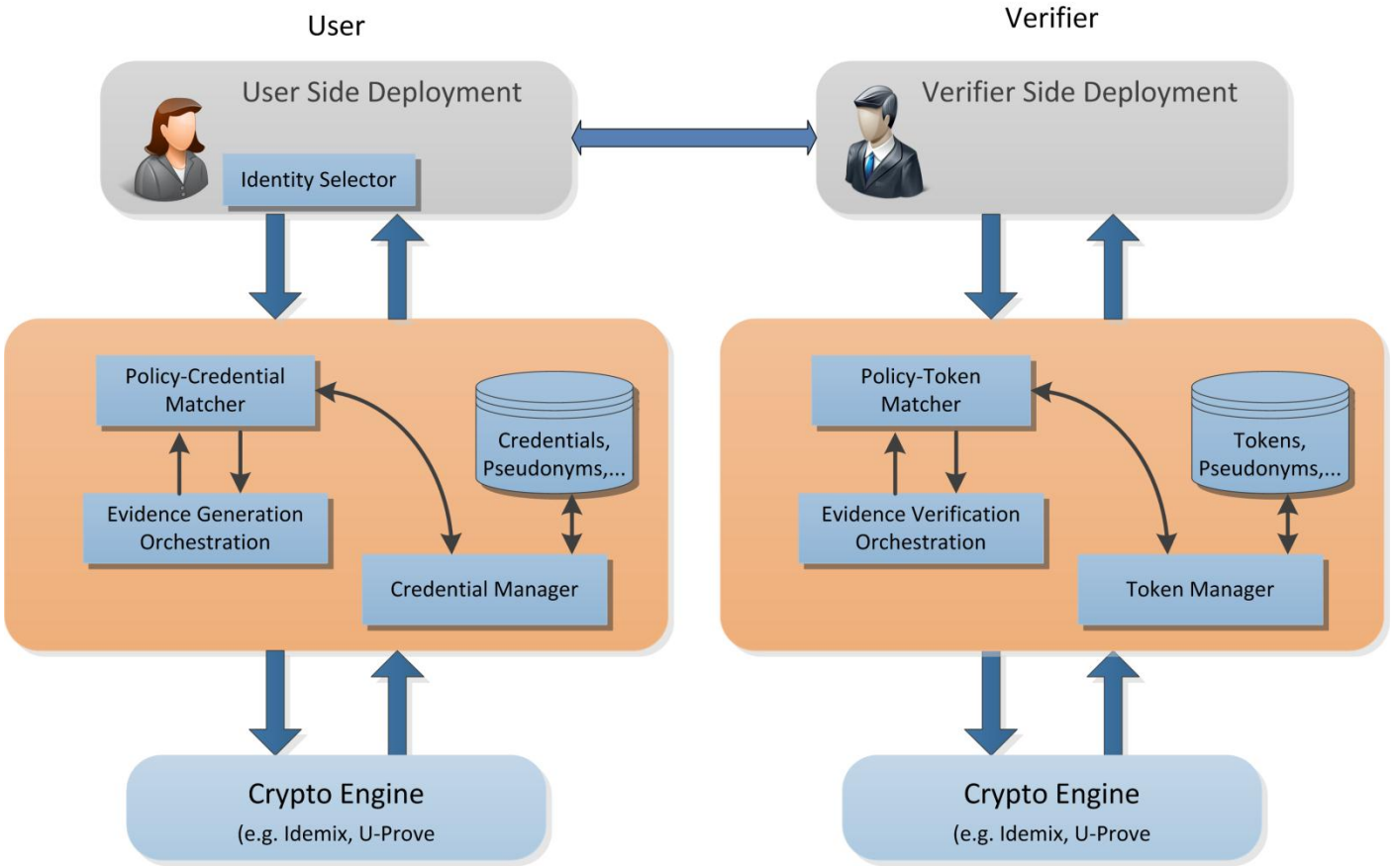
- Entities and Interactions
- High-level features and concepts of privacy-ABCs
- **System architecture and components for handling privacy-ABCs**
- Component APIs
- XML specification of all data formats

ABC4Trust architecture components - high-level view



- All mechanism-agnostic components of Privacy-ABC systems included

ABC-Engine Components



ABC4TRUST

Legal considerations for the ABC4Trust architecture

To limit processing to necessary data is supported by Privacy-ABCs:

- **Selective disclosure** of attribute-values out of a certificate and
- **Inspection** allowing conditional disclosure of data once this is really necessary.

ABC4TRUST

Agenda

- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - ABC4Trust in Perspective
- Mobile Platforms & Privacy-ABCs
- Conclusions & Outlook

General Challenges & Potential Identity Management

- Considering
  - the views of the respective stakeholders (Multilateral Security)
  - separations of domains that had been natural “before”
- Enabling users to manage their identities and IDs
- Frameworks and reference architectures
  - Along the value chain (with appropriate incentives)
  - For business processes and applications
  - For new communities and networks
- Globally standardized (e.g. in ISO/IEC JTC 1/SC 27/WG 5 “Identity Management and Privacy Technologies”)

Agenda

- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - ABC4Trust in Perspective
- Mobile Platforms & Privacy-ABCs
- Conclusions & Outlook

Principles for designing Assurance Tokens

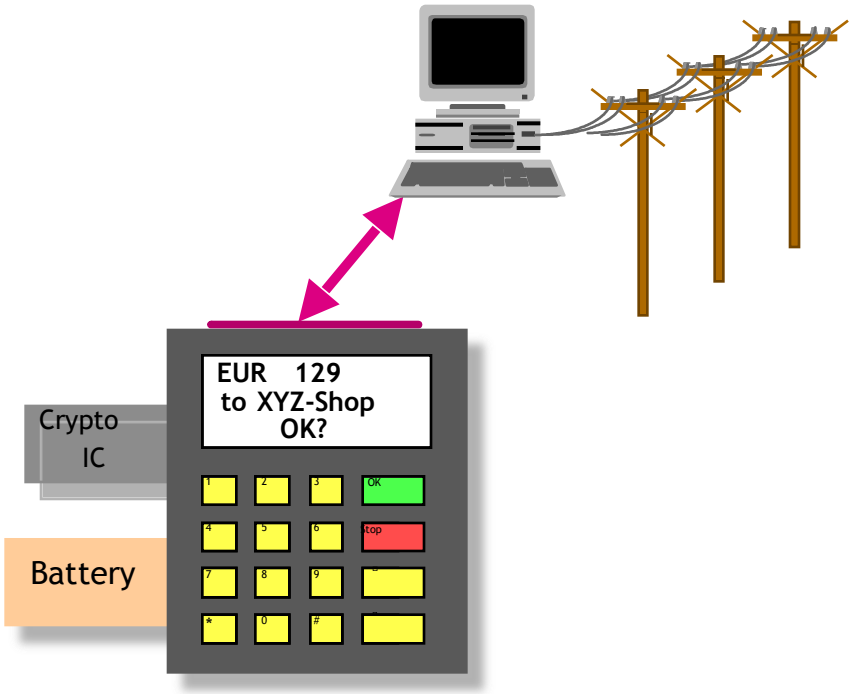
- Enabling the assurance token holder to influence
  - character and degree of identification and
  - amount of identification information
- Enabling communication
  - between assurance token holder and assurance token
- Enabling the assurance token to protect itself:
  - Ability to verify the controller by e.g. extra channel
  - A portfolio of communication mechanisms for redundancy
  - Sufficient access control towards relevant data (which platform?)
  - Enough processing power for complex operations

Smartphones vs. Smartcards as Assurance Tokens

- Better Usability
  - Credential selection
  - Security advisor
- More processing power
- More Communication Channels
  - Can be used for authentication/check of context (e.g. reader, time, certificates)
- Secure Storage?
- Trusted Environment?
  - Trusted User Interface
  - Trusted Platform ?

ABC4TRUST

Secure Equipment (20th century): Avoiding Threats from Trojan Horses

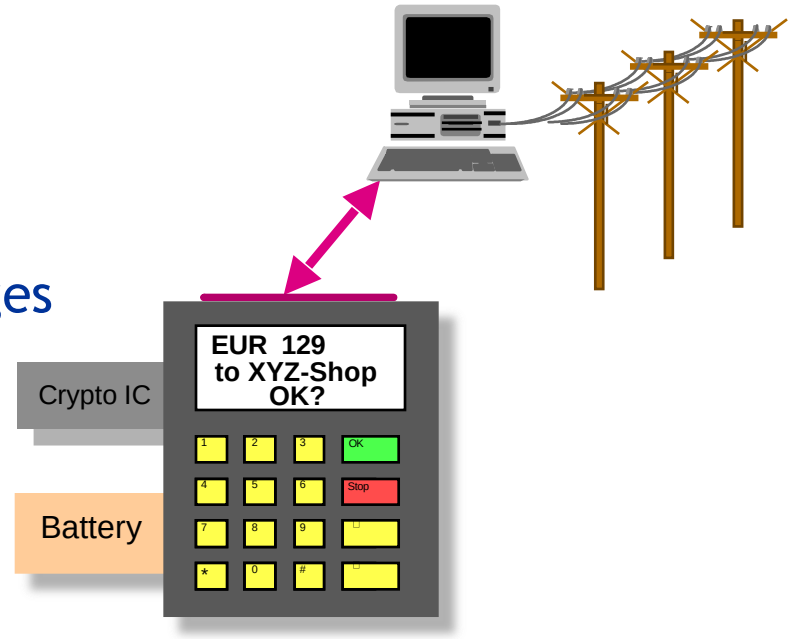


Wallet with private key and signature function

Personal Terminals (early 21st century)

A popular vision: Personal Security Assistants

- Storing personal data
  - Addresses, calendars
  - Money, keys
  - Preferences, …
- Performs sensitive processes
  - Decoding of confidential messages
  - Signature creation
  - Contract confirmation
- Assists negotiations
  - Documents which are accepted by other parties
  - Methods of payment
  - Reachability



ABC4TRUST

Challenges for Personal Terminals

- Usability
  - Portability
  - Good visibility of important information (“new network“)
  - Adequate representation of the functionality
- Protection from
  - Unauthorized access to stored data
  - Manipulation of the functionality (e.g. “Trojan Horses”)
  - Denial-of-Service attacks
- Trust (of non-experts)
  - Does the equipment what it shall do?
  - How (much) can I trust it?

Personal Security Assistants Platforms?

- Personal digital assistants
- Watches
- Mobile phones
- Smartphones
- Tablets
- …

Agenda

- Some Privacy Problems in Identity Management and Assurance
  - Identity Management and Overidentification
  - Identity Assurance and the “Calling Home” Problem
- Attribute Based Credentials
- The ABC4Trust Project
  - The Trials
  - The Architecture
  - ABC4Trust in Perspective
- Mobile Platforms & Privacy-ABCs
- Conclusions & Outlook

Conclusions & Outlook

- ICT and related services are coming ever closer to people.
- A more privacy friendly Internet requires:
  - Partial Identities and Identifiers
  - Minimum Disclosure
  - Attribute Based Credentials
  - Strong Sovereign Assurance Tokens (smart cards, mobile devices?)

- Kai.Rannenberg@m-chair.net

- www.m-chair.net

- www.abc4trust.net
- www.fidis.net
- www.primelife.eu
- www.prime-project.eu
- www.picos-project.eu

- Back-Up

SEVENTH FRAMEWORK PROGRAMME

Identity Theft (?)