

## **Anonymous Identity in Cross-Border and Cross-Sector Environment**

Libor Neumann, ANECT a.s., Czech Republic

Public eID: Cross-Border and Cross-Sector applications  
29 September 2009, Brussels, Belgium.

# Agenda

- **PKI principles**
- **PKI in Cross-Border and Cross-Sector environment**
- **ALUCID<sup>®</sup> principles**
- **ALUCID<sup>®</sup> in Cross-Border and Cross-Sector environment**
- **Conclusion**

# PKI principles

- **Basic principle**

- Human readable information about the user is included in certificate
- The information is verified by Certification authority
- Relying party trusts the verified information

- **Fundamental features**

- Sequence of actions
  1. Human readable information processing (collection, verification, signing)
  2. Use of PKI for authentication
- Data content
  - The semantic, format, verification of content of the information is not sufficiently standardised
  - Relying party relies on the data content, format and verification procedure managed by third party (Certification authority)
  - The additional human readable information is published
- Change management
  - No change management of additional human readable information exists (certificate revocation can be used)

# PKI in Peer-to-peer environment

- **One Relying party, one Certification authority**
- **Simple (one-to-one) relationship**
- **Consequences**
  - One set of additional information needed by the relying party is used
  - One verification procedure (compatible with the relying party needs) is used by the certification authority.
  - The user can understand the need of information collection and verification made by certification authority for the specific relying party
  - The user can understand the need to collect and verify personal information before use of authentication
  - Access right management can be based on the additional information placed in certificate
  - Change management of additional information made by certificate revocation should be acceptable

# PKI in Cross-Border and Cross-Sector environment

- **Hundreds of Certification authorities**
- **Thousands of Relying parties**
- **Complex relationships between Relying parties, Certification authorities and End users**
- **Consequences**
  - Every Relying party needs its own additional information (the specific “partial identity”) in certificate (specific semantic and format)
  - The verification procedure made by the Certification authority must fulfil needs of every Relying party
  - All pieces of information for every Relying party (all “partial identities”) has to be included in the certification before the first authentication is made
  - All pieces of personal information needed by all Relying parties (all “partial identities”) are placed in one place and published together readable for everybody
  - Change of any piece of the information causes revocation of the certificate and disables use of authentication for all Relying parties

# PKI in Cross-Border and Cross-Sector environment

- **Real life topology is not a tree (simple hierarchy)**
- **Additional cross-sector and cross-boundary issues**
  - Multiple trust management of the Relying party with hundreds of Certification authorities
    - citizens from different localities use different Certification authorities
  - Many semantics and formats (interoperability) used by hundreds Certification authorities
    - semantic and formats of the same piece of information are different
  - Additional language and culture differences in EU
  - Legislative framework variety in different EU countries
  - Additional jurisdiction issues – multiple sectors in one country, the sector difference in different countries
  - Publishing of joined personal information of huge number of citizens
- **Can it work?**
- **Is it the right way?**
- **Is additional human readable information really needed for authentication?**

ALUCID®

- **ALUCID® – Anonymous, Liberal, and User-Centric Electronic IDentity**

- Design from scratch
- Designed as ICT infrastructure
- Using System Design Methodology
- New way of thinking about eID
- New principles, new methods
- Internal dynamics and external stability

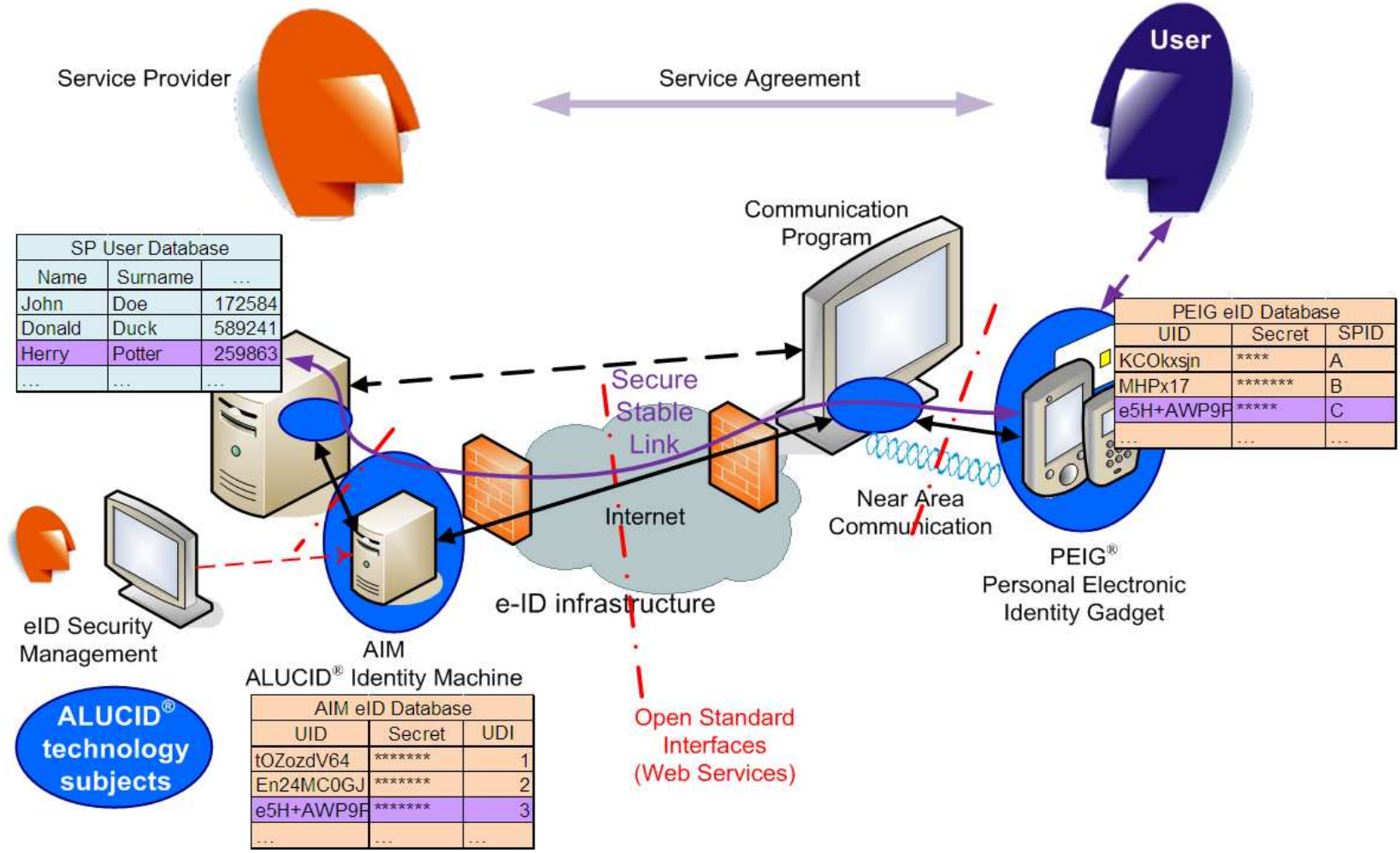
# Key Design Features I

- **Two main components**
  - PEIG® – Personal Electronic Identity Gadget – user’s automatic eID carrier
  - AIM – ALUCID Identity Machine – service provider’s eID tool
- **Extremely simple for end-users and service-provider**
  - Fully automatic eID
  - No third party
  - No personification process
  - Built-in security management support
- **Open to future innovations**
  - Enlargeable security framework
  - Flexible security parameters, multiple security protocols and algorithms
  - Open to future innovations, including new protocols and algorithms
  - Possibility to change security parameters and/or switch security protocols or algorithms in the working condition

## Key Design Features II

- **Privacy protection by design – anonymous identity**
  - No private data included in eID
  - Only random (pseudorandom) numbers changing in time
  - No identifiers and secrets shared
- **User-centric behavior**
  - Network topology
  - End-user liberty of selection (form, size, number, activation technology, etc.)
  - Multi-level security support
  - Seamless interoperability - open interface description
- **Enhanced security**
  - Built-in eID access control
  - End-user network security support (indirect communication)
  - eID security profiles managed by service provider

# ALUCID<sup>®</sup> Global Scheme



# Simplicity

- “Single sign-on” by design.
- No login names, no passwords (= no forgotten or phished passwords, etc.).
- No device personification process. No complex logistics of personal data, devices and secret information.
- No user certificates (= no recertification, no extra charges, no network names, etc.).
- No identity provider (= no communication between user and identity provider, no personal information managed by third party, etc.).
- No government-issued identity. No “numbering” of citizens, no state-issued identifiers abused, etc.
- No biometric data without access control (= no biometric data cloned from e-ID use, no remote verification of biometric data origin, etc.).

# ALUCID<sup>®</sup> in Cross-Border and Cross-Sector environment

- **Basic principle**

- No human readable information about the user is included in authentication
- The information can be managed and linked with authentication in information system
- Human readable information about the user is moved “from certificate into target information system”

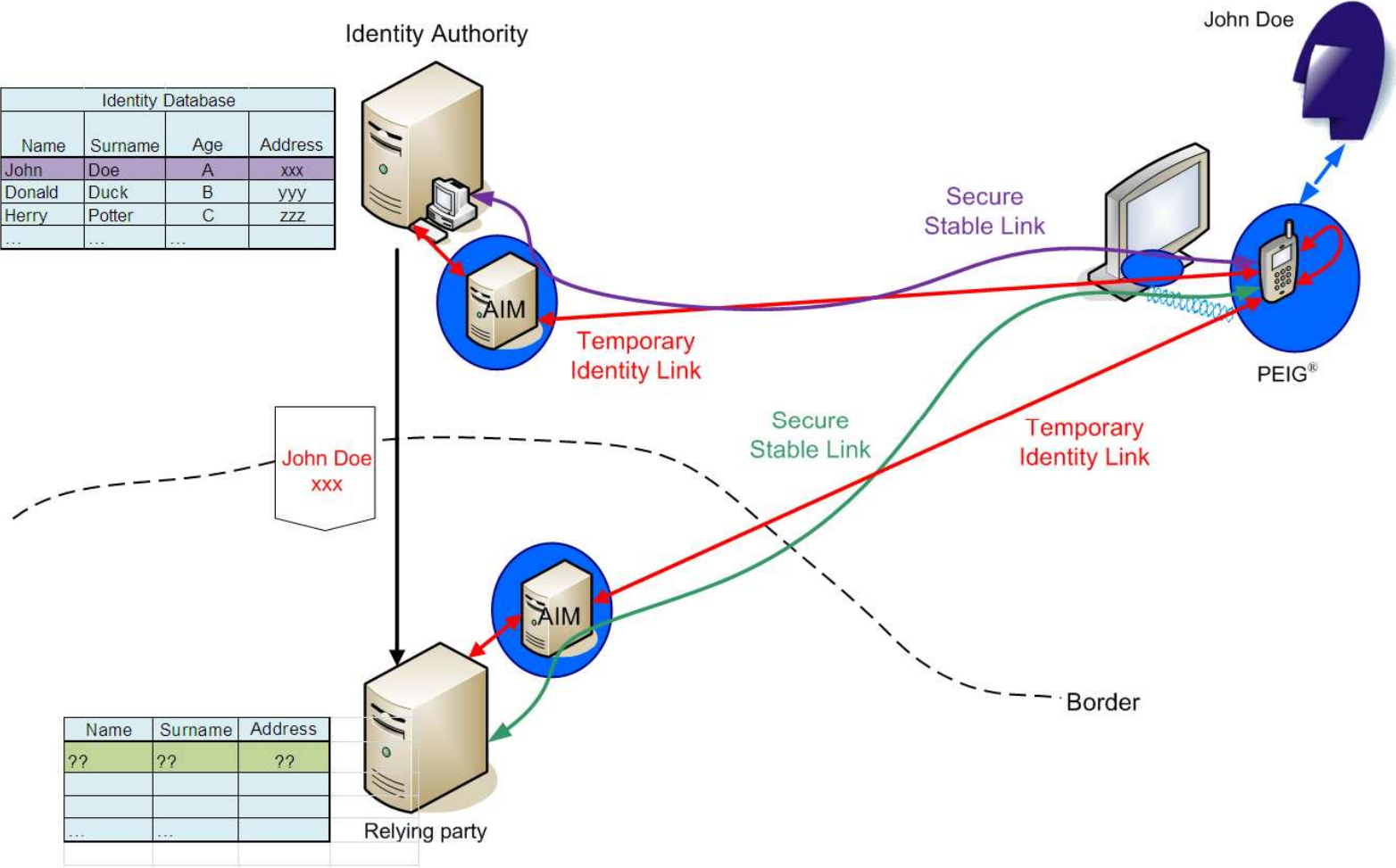
- **Fundamental features**

- Sequence of actions
  1. The authentication can be used before the human readable information processing is made.
  2. The authenticated electronic services can be used for human readable information processing
- Data content
  - No data semantic, format, verification of content of the information standardization is needed for authentication
  - Relying party need not relay on any third party
  - No additional human readable information is published by authentication technology
- Change management
  - Change management of electronic identity is supported by ALUCID technology. It is independent on human readable information change management

# ALUCID<sup>®</sup> in Cross-Border and Cross-Sector environment

- **Human readable identity data management ?**
- **Account activation and personal information verification?**
- **Sharing of identity information in Cross-Border and Cross-Sector environment ?**
  - Communication only when needed by the user
  - Minimal and specific set of personal information
  - Access management to personal information
- **Account activation and personal information verification scenarios**
  - Personal presence
  - Activation key (one-time password)
  - Signed form
  - Sharing between Relying parties
  - Identity authority
- **Scenarios in Cross-Border and Cross-Sector environment**
  - Direct peer-to-peer user communication
  - Sharing between Relying parties

# ALUCID<sup>®</sup> identity triangle



## Conclusion

- **PKI complexity and number of issues grows with size of use**
- **It is not possible to expect success of PKI in large scale Cross-Border and Cross-Sector environment**
- **Flat map & globe effect**
- **ALUCID® should be an alternative. It does not include fundamental barriers in large scale Cross-Border and Cross-Sector environment**



Thank you for your attention.

[Libor.Neumann@anect.com](mailto:Libor.Neumann@anect.com)

**ANECT**