# ALUCID®

**Petr Hummel, Libor Neumann**

Petr.Hummel@anect.com, Libor.Neumann@anect.com

ANECT a.s.
Prague, Czech Republic

## Abstract

The ALUCID® (Automatic Liberal and User Centric Electronic Identity) is a new complex authentication technology built on a principle of infrastructure of electronic identities. Basically, it is a new authentication framework providing and ensuring unified and secure authentication services between the users, their client's applications and server's application/services.

The ALUCID® authentication system is based on following ideas:

- User centric – only one piece of small device should be enough for proving user identity to all systems compatible within the ALUCID®
- Automatic as much as possible
- A True eID pseudonymity of all electronic identities – only identity provider and trusted applications can recognize the real physical identity of a user
- New organization procedures in eID management
- A trust sharing between independent systems compatible with ALUCID® framework (building trusts between independent IT systems on the fly without a necessity of changes in eID cores or IT infrastructure.)
- An integrated control and management of the eID infrastructures
- A build-in independence on pre-selected specific cryptographic methods
- General support for future extensions

**Keywords:** secure authentication, electronic identity, personal data protection, identity management, access and right management.

## 1 Introduction

Privacy protection is probably the greatest weakness of all current electronic identity (eID) solutions. The private information related to millions of citizens – and with a very long validity time (years or more) – is spreading over the internet with very limited or no access control. This is a side effect of the technology used and/or the way of implementation.

Cross-Border and Cross-Sector communication in commercial sector as well as in e-Government is the known complicated area of identity management. The need of strong authentication, privacy protection as well as complex relationships among a large number of government or commercial subjects and many citizens create a very complex environment. Privacy protection is becoming a very serious issue today, especially in large environments.

In the 2006 we started an analysis of current existing technologies concerning the electronic identity, authentication, privacy protection, feasibility and simplicity of usage as well as implementation. The analysis indicated that no current technology and no way of implementation used in enterprise systems (composed from many independent organizations/subject) is a feasible task.

Current technologies supporting strong authentication, which are applied in Cross-Border and Cross-Sector environment raise many significant issues, particularly in identity management: overcomplicated organization, insufficient security (including privacy protection issues), interoperability issues, etc.

### 1.1 A definition of needs

A work on the new concept of electronic identity has begun in 2006. On the basis of existing issues we formulated an analysis of current needs related to electronic identity [1] as follows:

1. User-centric solution.
2. Technology-neutral solution.
3. Support of scalable levels of security, including high security standard to respect technological limits of systems.
4. Protection against known and future attacks in the network environment.
5. Privacy protection – a separation of personal data off the electronic identity
6. Support for the functions and levels of security needed for e-government.

## 2 Main Concept

The basic principle of the designed solution is the transfer of all specific knowledge-demanding activities into the infrastructure. Experience from systematic design of other infrastructures has been used, and especially experience from the Internet itself. Well-known, high-quality eID technologies and algorithms have been integrated and modified for the distributed seamless use by millions or even billions of mutually communicating systems.

- The infrastructure topology has been simplified. No intermediate subject, such as a certification authority or identity provider, is enforced. A personification of the eID device is not required. The identical eID devices can be produced without including any user-specific information. The eID devices are interchangeable with regard to their production and sale. The eID device creates an identity automatically by its own use in real life.
- No global identity, no global naming, and no naming authority are used. Unique identifiers are valid only between the user and service provider. The uniqueness of identifiers is solved automatically by the eID means themselves, by the eID infrastructure. The only worldwide coordinated identifiers are those of the service provider. They are based on identifiers that are well-known and widely used on the internet, i.e. URI (DNS).
- No personal information is used in the eID infrastructure. Only pseudorandom numbers with temporary validity are carried over the public networks. No discoverable relation exists between the user's eID devices and the information carried over the network during the authentication stage.
- The solution is not based on a single eID technology. Rather, it supports several authentication technologies simultaneously and is open for future enhancements.

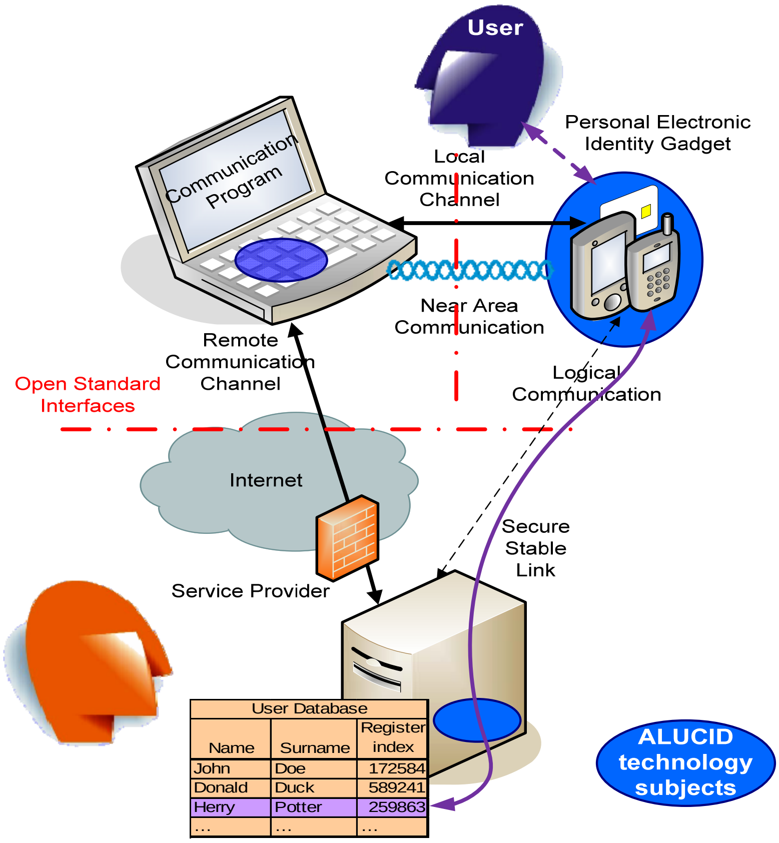
- There is no global electronic ID for any person. Each identity domain (like separated organization, departments) is using their own separated electronic identities for their users. This feature offers better handling of local security needs and better independence on the security breach in a different identity domain.
- Full mesh topology is supported by design.

## 2.1 Key elements of the ALUCID® framework:

### 2.1.1 User-centric identity

The ALUCID® solution is based on the idea of a **PEIG®** (a Personal Electronic Identity Gadget). This is a piece of hardware, with software, personally used by the citizen for all tasks related with eID. The PEIG® automatically does all tasks related with eID for the user. The user only needs to have a PEIG® and to activate or deactivate it. In this way, the user requirements are minimized, as no specific knowledge or specific skills are needed, and there is no need to memorize many changing secrets (e.g. PIN codes), etc. A PEIG® can take various forms. It can be built into a mobile phone, a smart card, a USB device, a specific key ring, an electronic watch, or other object.

Another important part of the ALUCID® system is **AIM** – ALUCID® Identity Machine – relaying party's eID tool intended as a network service with a managed security in a form of appliance or a cloud service. AIM provides and ensures all authentication requests between client's and target applications/services. AIM is responsible for managing electronic identities in a scope of defined identity domain as well as for secure maintaining of proper clear evidence between electronic identities and appropriate description of physical identities.



User Database

| Name | Surname | Register index |
|---|---|---|
| John | Doe | 172584 |
| Donald | Duck | 589241 |
| Herry | Potter | 259863 |
| … | … | … |

Figure 1: Main concept of the ALUCID®

A permanent secure link is created during the entire lifecycle of electronic identity. It is the mutual ability of a proofing the proper validity of remote identity. Proofing is ensured by usage of cryptographic methods.

## 2.2 A layer design

A great lesson how to survive and live with one system in the world is the Internet. Why is the Internet so successful technology that connect so many different devices and applications around the world? One key element of that success story is a use of a proper abstraction. A proper layer separation together with exact but still simple definitions of interfaces and operations between each layer allows an easy modification and replacement of each internal part in the ALUCID® layer without a necessity of change in other layers. This enables an easy upgrade or change of any component including the cipher selection. Just recall how difficult was a change of the hash function SHA-1 to SHA-256 in some operating systems and applications. The following picture [Figure 2: Layer design abstraction] shows the abstract levels of the ALUCID® authenti-cation network.

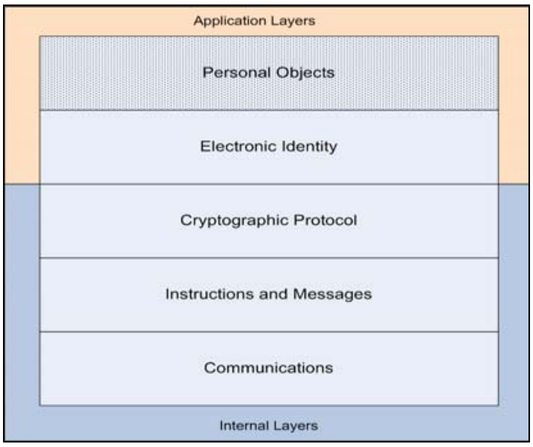


Figure 2: Layer design abstraction.

### 2.2.1 Layer "Personal Objects"

This layer is responsible for description of physical identities as well as additional information related to infrastructure of electronic identities. Personal objects maintained by each identity provider are independent and strictly separated, but they can be exchanged in a controlled manner – for example the information about physical identity can be transferred only when the user himself permits the exchange via his/her PEIG®.

### 2.2.2 Layer "Electronic Identity"

This layer is the core of the framework. It provides fully automatic management of the electronic identity lifecycle. This layer handles all parts of the electronic identity lifecycle in a form of "eID operation". It defines following operations:

- Identity Init – eID creation under the conditions of selected security parameters (security levels, parameters like validity time etc.)
- Identity Use – eID usage ("classic authentication" activity when someone is trying to authenticate)
- Identity Change – eID change – all internal identifiers as well as secrets are being changed
- Identity Renew like Identity Change but at least one security parameter is expired (like validity time)
- Identity Link – creation of relationship between two electronic identities of the same person if the person needs to share his/her identity proofing/personal data between two identity providers. A new temporary common link is created in conformity of centrally defined security parameters like defined validity time, the maximum number of usage etc.
- Identity End – electronic identity termination.

Electronic identity layer defines three main security spaces:

1. Local Security Space is the point where a user "manually" activates the PEIG®. The user can use any known technique for PEIG® activation – like password, biometric or combination of them.
2. Cyberspace – a public part – is the space in the cybernetic world between PEIG® and identity/service provider – a typical public Internet. Only electronic identities are used in that space without any personal data.

3. Cyberspace – a private part – is the space between the identity provider and server applications / services. This is the area under the control of provider and personal data can be transferred in a secure manner there.

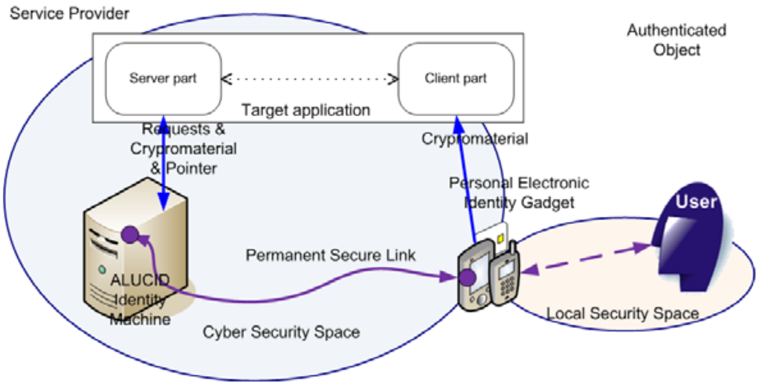


Figure 3: Electronic identity layer.

The main point of that mental space separation is the fact that each space contains a different security threats and consequently different risk mitigation techniques.

### 2.2.3 Cryptography protocol layer

This is the one of the most important parts of the ALUCID® idea itself. The real world offers copious technologies with different limits of computational power. Therefore the new concept of electronic identity should reflect these various needs in a global perspective and incorporate flexibility into authentication framework. On the one end of the scale there are technologies like RFID, which have just limited capabilities of cryptographic techniques due to limited power. On the second end of the scale there are really powerful devices with a great computational potential. The internal cryptographic layer encompasses two main philosophical components:

- A Security Levels
- An Universal Cryptographic Protocol

**The Security Level is** a way or method of verifying the secret possession between the AIM and PEIG®. The ALUCID® offers three main security levels incorporated into ALUCID®.

- LZ – Level Zero (No secret) – No secret verification, only public information is verified. This method is intended especially for technologies with limited computational capabilities like RFID technologies.
- LB – Level Basic (shared secret) – It this case the verification of secret possession is accomplished by the use of shared secret (i.e. usage of symmetric cryptography).
- LAC – Level Asymmetric Cryptography (private and public keys) – The verification of secret possession is performed by the use of asymmetric cryptography.

The second component of the cryptographic layer is the UCP – universal cryptographic protocol, which is the new instrument for an easy built-in support of assembling various ciphers used for secret protection. The point of the UCP is that cipher method can be easily altered without a need of the protocol structure change for the same security level. It is just on a decision of the security officer, which cipher should be used for internal secrets or private keys protection.

The combination of the security level design and universal cryptographic protocol allows usage of multiple cryptographic protocols in the same authentication framework. Of course – the word “universal” does not mean any cipher in the world, but UCP can handle large amount of common known symmetric and asymmetric ciphers.

### 2.2.4 Instruction and Message Layer

The instruction and message layer is responsible for exchanging all messages between all components. A proper abstraction of messages and instructions in a form of requests and responses provide reliable information exchanges. Form of web services is used for unified and simple way of communication.

### 2.2.5 Communication Layer

The last layer is responsible for physical transfer of data handled by the layer “Instruction and Messages Layer”. This communication layer uses standard transfer protocol between remote sides like http (TCP/IP) or a local communication like Bluetooth, NFC and others …

## 3 Conclusion

ALUCID® is a new concept, a new solution. It is the outcome of a systematic design of a new eID infrastructure initiated by difficulties and aspects of electronic identities, privacy protection and inadequate high effort on the field of integration of authentication systems especially in enterprise deployment crossing the border of a single organization. It aspires to address all existing requirements for an absolute majority of participants in the real environment of today’s public networks, and especially the Internet.

A decision to abandon other todays known concepts of electronic identity and to build a new system from scratch brought valuable experiences how to break through limits of current concepts caused by inflexibility, insufficient privacy protection and exhaustive overhead of management and operation task relating to entire eID lifecycle.

## 4 References

[ 1 ] NEUMANN, L. “An Analysis of E-identity Organizational and Technological Solutions within a Single European Information Space”, e-Challenges e-2007, The Hague, Netherlands, 2007, pp. 1326–1333.

[ 2 ] Neumann, L., Sekanina, P. “Distributed Authentication and Authorization in e-Government”. Conference Proceedings, 5th European Conference on E-Government, University of Antwerp, Belgium, 2005, pp. 597–606.

[ 3 ] Neumann, L. “Strategic Options for Pan-European E-Government Interoperability”, e-Challenges e-2006, Barcelona, Spain, 2006, pp. 333–340.

[ 4 ] Neumann, L. “Anonymous, Liberal and User-Centric Electronic Identity Supports Citizen Privacy Protection in e-Government”. Conference Proceedings, 8th European Conference on e-Government, Ecole Polytechnique, Lausanne, Switzerland 10-11 July 2008.