ITU Kaleidoscope 2014
Living in a converged world - impossible without standards?

Global Convergence in Digital Identity and Attribute Management: EMERGING NEEDS FOR STANDARDIZATION

D. Merella
Fondazione Inuit University of Rome Tor Vergata
daniela.merella@uniroma2.it

Saint Petersburg,
Russian Federation

PAPER PRESENTATION

Global Convergence in Digital Identity and Attribute Management: EMERGING NEEDS FOR STANDARDIZATION

M. Talamo[1,2], M.L. Barchiesi[2], D. Merella[3], C.H. Schunck[3]

1 Nestor Lab University of Rome Tor Vergata
2 University of Rome Tor Vergata
3 Fondazione Inuit University of Rome Tor Vergata

talamo@nestor.uniroma2.it, barchiesi@nestor.uniroma2.it, merella@uniroma2.it, schunck@nestor.uniroma2.it

INTRODUCTION

- In a converging world, where traditional borders have been overcome through the digital environment, it is necessary to develop:
  - systems to replace with digital means the recognition “vis-a-vis” for entities and people;
  - Innovative devises and systems to ensure security and reliability of data.

EXISTING STANDARDS I

Organiz.	Standard/ Recommendation[S]/[R]	Concepts
ITU-T	Framework for Discovery of Identity Management Information [R X.1255]	Concept of a persistent identifier for digital entities; for the discovery of formal method of linking attributes to digital entities.
ITU-T ISO/IEC	Information Technology- Open systems Interconnection The Directory: Public Key and attribute certificate frameworks	Framework for public-key certificates and attribute certificates with a strong focus on privilege management infrastructures. An attribute certificate binds attribute values with identification information about its holder.
ISO/IEC	Information Technology - Security techniques - A framework for identity management" [S 24760]	Part 1 defines the framework for the definition of terms for identity. Parts 2-3 are under study and are related to the model of life cycle of information concerning the identity.

EXISTING STANDARDS II

Organiz.	Standard/ Recommendation[S]/[R]	Concepts
ISO/IEC	Information technology -- Security techniques - Entity authentication assurance framework [S 29115]	Provides a framework for managing entity authentication assurance in a given context examining also the level of assurance.
	Information technology - Security techniques - A framework for access management [S 29146]	Is a under development standard. Contains references about the joining of different identities considering the different attributes.
	Information technology -- Security techniques -- Privacy framework [S 29100]	This standard provides a framework for processing and protecting Personally Identifiable Information (PII). It addresses organizational, technical and procedural aspects.

MISSING STANDARDS I

- Current standardization is mostly related to "access management and level of assurance" areas;
- In the following we will follow a broader, bottom-up approach to point out important gaps in international standardization with regard to identity management and in particular attribute management and their use.

MISSING STANDARDS II

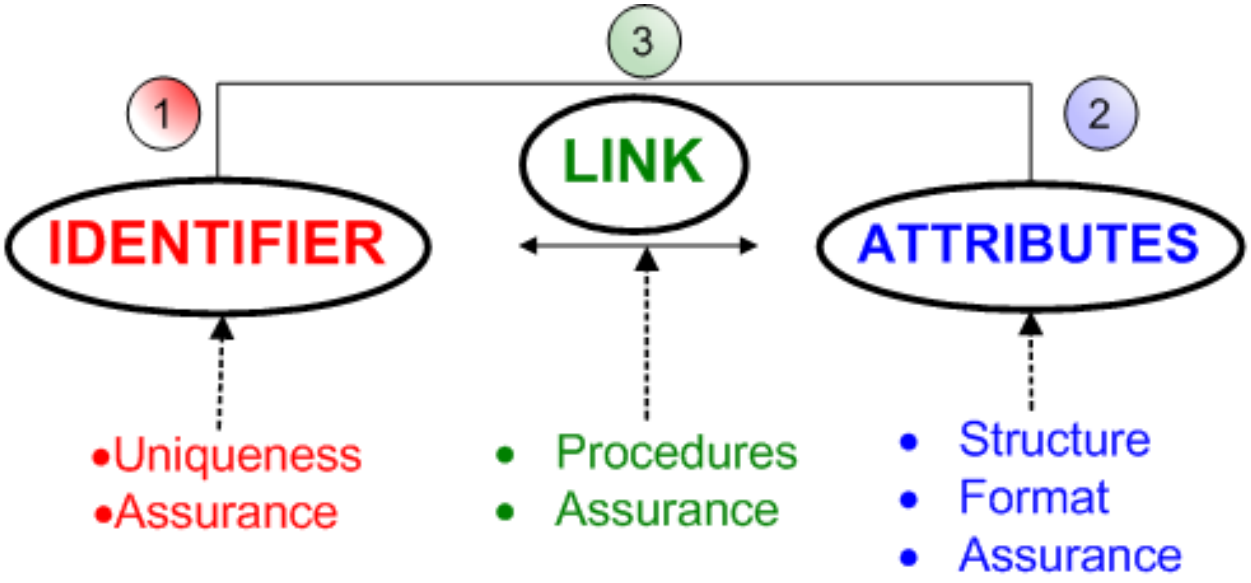
One important standard is still missing regarding "Attribute Management": data building or can contribute to build one or more digital identity/ies:

- name, gender, and date of birth
- attributes can be related to a person's health information (e.g. blood group, allergies, vaccinations),
- school and university degrees (Bachelor, Master, Ph.D),
- professional life, financial data (credit scores, status of bank accounts), hobbies, etc…

OPEN CHALLENGES

further standardization in this specific area of attributes can be very useful:

- architecture and management of the elements building a digital identity;
- the link between them
- reliability and assurance



IDENTIFIER

- The identifier consists of a unique code that uniquely identifies the person and which can be associated with different attributes.
- Unique Identifiers are the basis for efficient and secure Identity Management but It is important to note that can be more than one identifier.
  - Some standardized procedures and techniques (providing standardized levels of assurance) should be in place through which an entity can demonstrate that a unique identifier has been issued to it, ideally without revealing any of the associated attributes (if any).

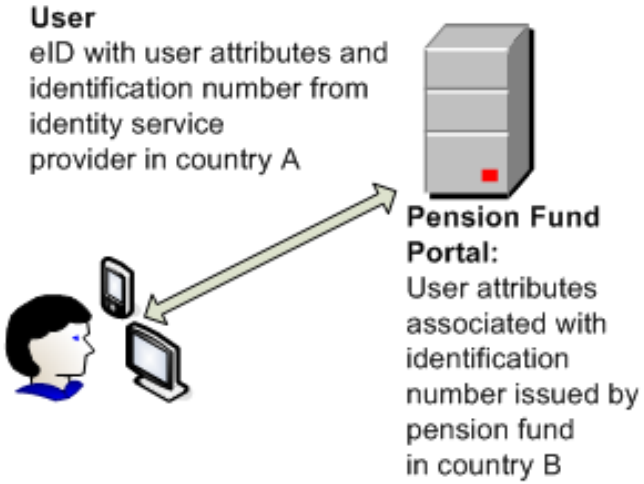
ATTRIBUTE MANAGEMENT

- A standardized approach is needed for the exchange of metadata related to attributes. Further standardized procedures are required for verifying the compatibility between the information that is provided by the attribute provider and the information which is expected by the receiver (relying party) on the basis of the metadata.
- The structure that may underlie a set of attributes as well as the format of the attributes must be communicated clearly before an attribute is exchanged or an attribute based assertion is made.

LINK

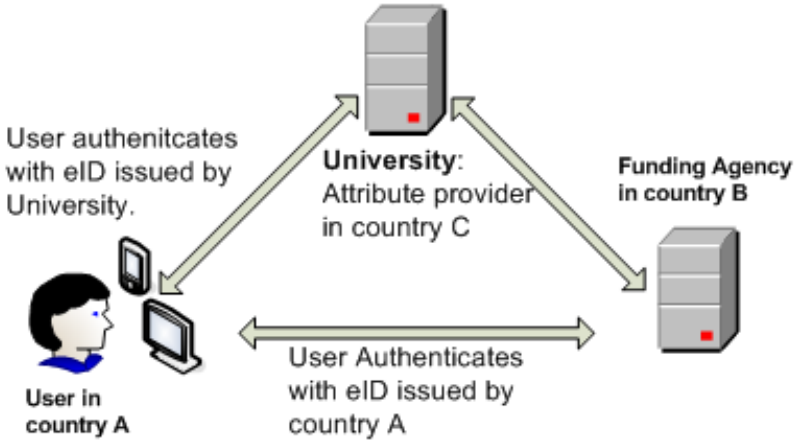
- Today users have a large amount of eIDs issued to them by various entities including governments, financial institutions, social networks, online merchants and many other online service providers.
- The process of linking attributes to eIDs and vice versa as well as eIDs to eIDs will become of increasingly importance.

LINK EXAMPLES



Example 1

Standardized procedures and techniques to match the attributes provided by the user's eID with the attributes in the records of the online service provider are missing



Example 2

Standardized procedures to asses the assurance of the link between
a)the user who authenticated with the eID from country A
b) the user to whom the University degree attribute is provided to are currently missing.

CONCLUSIONS
I

- For several thousand years societies have learned to establish cooperation and trust in non-digital environments. A key requirement for creating trust is the ability to recognize counterparts.
- Digital identity management plays a key role in enabling recognition and the creation of circles of trust. In this paper we have highlighted several areas within digital identity management where standardization is urgently needed to achieve further international convergence.

CONCLUSIONS II

- We have argued that attribute management is of central importance to make continued progress in these areas.
- A standardized environment for the exchange of certified attributes is highly desirable for online service providers seeking certified information for those data items that are central for their business model as well as for users who would like to protect their privacy and obtain pseudonymous access to digital services.

REFERENCES

[1] SSEDIC, "SSEDIC recommendations & roadmap," SSEDIC Deliverable 6.3; available at http://www.eidssedic.eu/deliverables.html, 2012.

[2] Veseli F., Paillier P., Schallabock J., and Krontiris I., "D8.4 architecture for standardization v1" ; available at http://www.ec.europa.eu ABC4Trust, 2012.

[3] European Commission, "Regulation on electronic identification and trust services for electronic transactions in the internal market", available at http://eurlex.europa.eu, 2012.

[4] "Framework for discovery of identity management information," Recommendation ITU-T X.1255, 2013.

[5] Robert Axelrod, "The evolution of cooperation," New York: Basic Books, 1984.

[6] SSEDIC, "SSEDIC deliverable report: Business and regulatory 5.1," SSEDIC Deliverable 5.1; available at http://www.eid-ssedic.eu/deliverables.html, 2012.

[7] Talamo M. and Schunck C.H., "Re-thinking the evaluation of eid credentials to simplify interoperability" in *European Journal of ePractice, vol. 14, pp. 51–62,*2012.

THANK YOU