Trust Services for Electronic Transactions

ROUMEN TRIFONOV
Faculty of Computer Systems and Control
Technical University of Sofia
8 st. Kliment Ohridski bul., 1000 Sofia
BULGARIA
r_trifonov@tu-sofia.bg

Abstract: - The trust services for electronic transactions in the integral market are related with the last year adopted Regulation (EU) No 910/2014 on electronic identification. In accordance with its performance requirements currently in the country a draft law on electronic identity is the process of discussion. These circumstances make it necessary to conduct a serious analysis of international standards in the field of electronic identification and solving a number of issues related to their application.

Key-Words: - Electronic services, electronic transactions, electronic identification, international standards, identity authentication, identity management

1 Introduction - the New European Regulation and its Relations to the Standardization

On July 23th, 2014, the European Parliament and the Council of Ministers adopted the Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the integral market and repealing Directive 1999/93/EC [1]. With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation:

- lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;
- lays down rules for trust services, in particular for electronic transactions; and
- establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

The identity management systems are complex applications oriented to facilitate the management of personal information, credentials, identifiers, and the presentation of this information to other parties by means of powerful web features [2].

The Regulation defines assurance levels, which should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. The assurance level depends on the degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented. Various technical definitions and descriptions of assurance levels exist as the result of Union-funded Large-Scale Pilots, standardisation and international activities.

The regulation addresses the issue of standardization in general, paying attention to their compliance, without focusing on many standards. An example is the following passage: "In adopting delegated acts or implementing acts, the Commission should take due account of the standards and technical specifications developed within the European and international organizations and standards bodies, in particular the European Committee for Standardization (CEN), the European Institute for Telecommunications Standards (ETSI), the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU), with a view to ensuring high levels of security and interoperability of electronic identification and trust services. "

The document mentions specifically only two international standards: ISO 29115 “Entity

authentication assurance framework" and ISO 15408 "Evaluation criteria for IT security" (popular under the name "Common Criteria"). The second one is not directly related to electronic identification.

In accordance with the requirements of the Regulation currently in the country a draft law on electronic identity is the process of discussion. These circumstances make it necessary to conduct a serious analysis of international standards in the field of electronic identification and solving a number of issues related to their application.

2 The Main Direction of the Standardization and the Main Players

Especially in the European Union's privacy legislation technical standards are given significant role, e.g. when the law requires technical mechanisms to be put in place to protect the privacy of users. The specific mechanisms are usually not spelled out in the law itself, as the regulation aims to be "technology neutral". Effectively, such regulation would allow for a strong harmonization of technical measures in specific domains under the control of the Commission.

Over the past few years have seen increased interest of international standardization bodies to problems of electronic identification. As a result of this intense activity has been adopted many standards that in general beam can be systematized in the following areas:

- Identity Management;
- Identity Authentication;
- Identity Federation.

This standardization work has been realized not only in official intergovernmental standardization organizations (ISO, ITU), but also in a number of technical consortia. It is worth noting that often ISO acts as an integrator of the work of different standards bodies around the world and enjoys a high level of recognition especially with national governments and international institutions.

The application of standards in the field of IT is closely linked to the concept of IT Governance. „IT Governance is a subset discipline of Corporate Governance focused on information technology (IT) systems and their performance and risk management." [3]

There are three kinds of standards [4]: reference, minimum quality and compatibility standards. Compatibility standards are particularly important in telecommunications and networking as they ensure that component adheres to set of standards that ensure that it can be installed into a larger system.

2.1 Standards Related to the Identity Management

The main standards in this area, adopted in recent years, can be marked as follows, broken down by standardization organizations:

2.1.1 Standards of the International Standardization Organization (ISO):

- ISO/IEC 24760 A framework for identity management ;
- ISO/IEC 29144:2014 The use of biometric technology in commercial Identity management applications and processes;
- ISO/IEC 29003 Identity proofing;

2.1.2 Standards (Recommendations) of the International Telecommunication Union (ITU):

- X.1250 Baseline capabilities for enhanced global identity management and interoperability;
- X.1251 A framework for user ISO/IEC 24760 control of digital identity;
- X.1252 Baseline identity management terms and definitions;
- X.1253 Security guidelines for identity management systems;
- X.1255 Framework for discovery of identity management information;

2.1.3 Standard of the American National Standardization Institute (ANSI):

- ANSI/NASPO-IDPV-2014 Requirements and Implementation Guidelines for Assertion, Resolution, Evidence, and Verification of Personal Identity.

The basal ITU recommendation X.1252 [5] determined graphically the Identity Management as follows (Fig. 1).

The basal ISO standard ISO/IEC 24760 [6] "specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations or information technology components, which operate on behalf of individuals or organizations. Furthermore, it specifies fundamental concepts and operational structures of identity management."

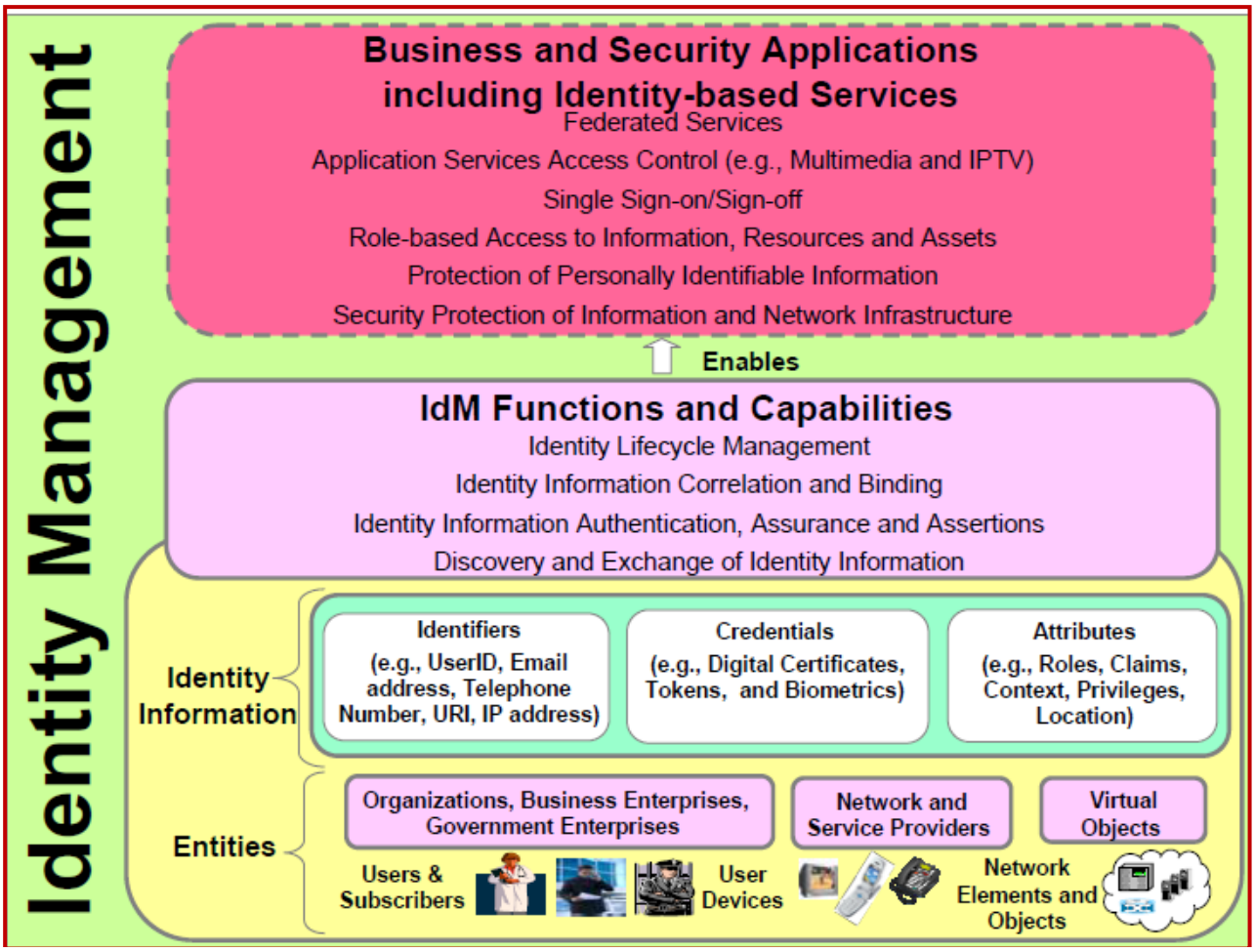

Fig. 1. Graphical determination of Identity Management

2.2. Standards Related to the Identity Authentication

The main standards in this area, adopted in recent years, can be marked as follows, broken down by standardization organizations (some of the basic standards of ISO coincide with similar recommendations of ITU):

2.2.1 Standards of the International Standardization Organization (ISO):

- ISO/IEC 29115 (ITU-T X.1254) Entity authentication assurance framework;
- ISO/IEC 24761:2013 Authentication context for biometrics;
- ISO/IEC 17922 (ITU-T X.1085) Tele-biometric authentication framework using biometric hardware security module;
- ISO/IEC 29146 A framework for access management;
- ISO/IEC 29191:2012 Requirements for partially anonymous, partially unlinkable authentication;
- ISO/IEC 20009:2013 Anonymous Entity Authentication;
- ISO/IEC 20008:2013 Anonymous Digital Signatures;
- ISO/IEC 29100 Privacy Framework;
- ISO/IEC 29101 Privacy Architecture Framework;
- ISO/IEC 29190 Privacy Capability Assessment Model;
- ISO/IEC 24475 Biometric Information Protection;
- ISO/IEC 27018 Code of Practice for Data Protection Control for Public Cloud Computing Services;

2.2.2 Standards (Special Publications) of the National Institute for Standardization and Technology (NIST):

- SP 800-63-2 Electronic Authentication Guideline;
- SP 800-118 Guide to Enterprise Password Management;

- SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII);
- FIPS 201-2 Personal Identity Verification of Federal Employees and Contractors.

The author would like to pay particular attention to the NIST special publication SP 800-63-2 [7], whose specificity is largely coincides with the objectives of e-Governance in Bulgaria. This SP contains the guiding technical principles for federal authorities using electronic authentication. It covers the "online" authentication of users (employees, contractors and individuals) interacting with administrative information systems through open networks. The SP also defines the technical requirements for each of the four levels of protection in the field of proof of identity, the registration, the technical media, the management processes, the protocols for authentication and the related claims. The main part of these processes is illustrated in the Fig. 2.

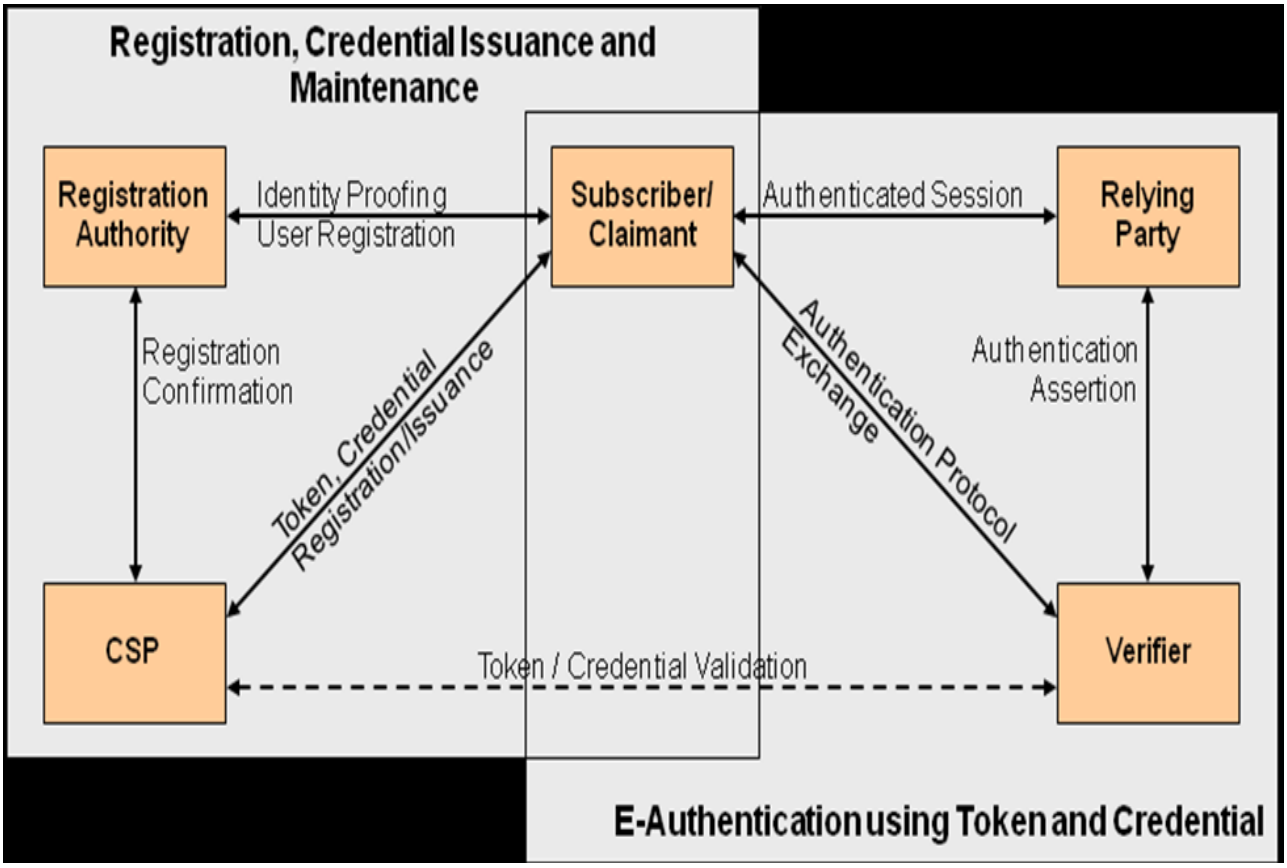

Fig. 2. Main processes of proof of identity

Also, we consider appropriate to focus on the Standard ISO / IEC 29115 (ITU X.1154) “Entity authentication assurance framework” [8]. Many electronic transactions within or between ICT systems have security requirements which depend upon an understood or specified level of confidence in the identities of the entities involved. Such requirements may include the protection of assets and resources against unauthorized access, for which an access control mechanism might be used, and/or the enforcement of accountability by the maintenance of audit logs of relevant events, as well as for accounting and charging purposes.

Using four specified Levels of Assurance (LoAs), this International Standard provides guidance concerning control technologies, processes, and management activities, as well as assurance criteria that should be used to mitigate authentication threats in order to implement the four LoAs. It also provides guidance for the mapping of other authentication assurance schemes to the specified four levels, as well as guidance for exchanging the results of an authentication transaction. Finally, this International Standard provides informative guidance concerning the

protection of personally identifiable information associated with the authentication process.

This Standard is intended to be used principally by credential service providers and by others having an interest in their services (e.g., relying parties, assessors and auditors of those services). This Entity Authentication Assurance Framework specifies the minimum technical, management, and process requirements for four LoAs to ensure equivalence among credentials issued by various credential service providers.

Furthermore, each LoA describes the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity that uses a particular identity is in fact the entity to which that identity was assigned. For the purposes of this International Standard, LoA is a function of the processes, management activities, and technical controls that have been implemented for each of the phases based on the criteria set.

Selection of the appropriate LoA should be based on a risk assessment of the transactions or services for which the entities will be authenticated. By mapping impact levels to LoAs, parties to an authentication transaction can determine what LoA they require and can procure services and place reliance on assured identities accordingly.

2.3 Standards Related to the Identity Federation

The main standards in this area, adopted in recent years, can be marked as follows, broken down by standardization organizations:

a) Standards of the Organization for the Advancement of Structured Information Standards (OASIS):

- Security Assertion Markup Language 2.0 (SAML 2.0);
- Identity Metasystem Interoperability Version 1.0;
- WebServices-Trust Version 1.3

b) Standard (Recommendation) of the International Telecommunication Union (ITU): X.1154 - General framework of combined authentication on multiple identity service provider environments

c) Standard (Specification) of OpenID Foundation: OpenID Connect 1.0;

d) Standard (Specification) of Fast IDentity Online Alliance: FIDO v1.0.

Recently, many application services, especially financial services, require more reliable or combined authentication methods such as multifactor authentication due to the increase in identity theft. For example, one-time password authentication and other new authentication methods are used instead of traditional password-based authentication.

The combinations of authentication methods provide multiple identity service providers the ability to enhance the assurance of authentication. Recommendation ITU-T X.1154 [9] provides the general framework of combined authentication in multiple environments for a service provider.

In this Recommendation, three types of combined authentication methods are considered: multifactor authentication, multi-method authentication and multiple authentications.

The framework in this Recommendation describes models, basic operations and security requirements for each model component and each message between the model components to maintain an overall level of authentication assurance in situations of a combination of multiple providers. In addition, the framework also describes models, basic operations and security requirements to support the authentication service that manages a combination of multiple identity service providers.

3 Problems that must be Solved in National Legislation

The analysis of the draft law on electronic identification, which was presented for public discussion, in terms of the aforementioned standards shows the presence of a number of "white spots".

Among the identified problems, which should receive unambiguous answer, can be specified the following ones:

- the above mentioned and cited in the Regulation Standard ISO / IEC 29115 (ITU X.1154) identifies four levels of authentication assurance (Levels of Authentication - LoA) of the object and describes requirements and guidelines for each of the levels. The choice of the appropriate level should be carried out on the base of the risk assessment for transaction and for respective service. Bringing the levels of exposure to the levels of LoA, the parties of the transaction can determine their necessary LoA. Therefore, it is advisable to legitimize a range of methods for e-ID intended for various applications, in order to meet different LoA;
- moreover, the legislation must answer the question: will it be used in e-Governance applications the principle of so called “Federated Identity Management (FIdM)” and its particular

applications, such as so called “Single Sign-On (SSO)”.

4 Conclusion

The purpose of this paper is to contribute to the public discussion on the draft of the Electronic Identification Act, which must be adopted in compliance with the relevant EU regulation. It is necessary to take actions aimed targeted to the understanding and the compliance with international standards in this area.

5 Acknowledgments

This research is conducted and funded in relation to the execution of a scientific-research project № H07/56 “Increasing the level of network and information security using intelligent methods” under the contract № D 07/4 with National Science Fund in Bulgaria.

References:

[1] Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the integral market and repealing *Directive 1999/93/EC*

[2] R. Mendoza – Gonzales, S. Jimenes – Gonzales Guidelines to Design Usable Security Feedback for Identity Management Applications *WSEAS - Mathematical Methods and Systems in Science and Engineering*

[3] M. Velikanu, I. Surugiu, D. Litan, O. Raduta, A.-M. Mocanu Information Technology Standards – A Viable Solution to Reach the Performance *WSEAS - Recent Researches in Neural Networks, Fuzzy Systems, Evolutionary Computing and Automation*

[4] Seppo Sirkemaa IT infrastructure: standards and flexibility *Proceedings 444-117 of WSEAS*

[5] ITU Recommendation X.1252 Baseline identity management terms and definitions

[6] ISO/IEC 24760 A framework for identity management

[7] NIST Special Publication 800-63-2 Electronic Authentication Guideline August 2013

[8] ISO / IEC 29115 (ITU X.1154) Entity authentication assurance framework

[9] X.1154 General framework of combined authentication on multiple identity service provider environments