EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology

eIDAS Task Force and Health & Well-being Unit

Brussels, 24/10/2012

eHEALTH NETWORK 7TH NOVEMBER 2012

Subject: Point 3 of the agenda: eIdentification (eID) for eHealth

For information: information paper suggested by the Secretariat

Electronic Identification and authentication in the Health sector

Information paper

Introduction

The purpose of this document is to clarify the dividing line **between electronic identification and authentication and the right to electronically access health data and/or a health service**. To this end, it recalls the key elements of the Proposal for a Regulation on "electronic identification and trust services for electronic transactions in the internal market"[1] (hereinafter referred to as: "proposed Regulation"), which are relevant to e-health, and identifies the aspects that need to be addressed under the mandate of the eHealth Network under Directive 2011/24/EU.

While the electronic identification and authentication prove who you are, granting access to certain health services or data requires a further step to verify that you are entitled to the service at all. The proposed Regulation sets rules only for the first phase, i.e. for electronic identification and authentication. Any requirements regarding managing access rights to health data or services, the storing and processing of health data, fall clearly outside of the scope of the proposed Regulation.

1. The proposed Regulation

Overview

Chapter II on "Electronic identification" of the proposed Regulation sets out minimal common rules to ensure that **electronic identification and authentication means, enabling access to public services** at national level, **are mutually recognised and accepted throughout the EU**. These provisions respect the sovereignty of Member States on matters related to identity, in particular whether or not to provide their citizens with electronic identification means. However, electronic identification and authentication services being a key element for reliable and seamless cross border electronic interactions, the proposed Regulation provides **that citizens and entities** who have been provided with electronic identification means to access public services at national level shall be able to use such means to access at least similar services in any other EU Member State where electronic identification means are accepted.

While Member States are free to decide whether to notify or not their eligible electronic identification schemes, **they are obliged to accept other Member States' schemes**, once they have been notified and published. This obligation is applicable if **the electronic identification is required by law or administrative practice** either in the context of public services or in the context of a private service.

Cross-sector approach on electronic identification and authentication

[1] COM(2012)238 of 4.6.2012

The proposed Regulation enables the **cross-border and cross-sector** use of electronic identification and authentication for persons and entities. In case multiple and eligible identification schemes exist at national level, Member States would be free to decide whether to notify one or more such schemes. However, they must accept all notified electronic identification means **for all services (and sectors)** where they require electronic identification.

The implication for the eHealth sector: even if a Member State chooses a sectoral approach for eHealth electronic identification (based for instance on a specific eID means), it will have to accept, but only for the identification and authentication step, as said above, the notified "cross-sectoral" electronic identification means of other Member States.

To ensure citizens access to eHealth services at European level, the option of a federated approach was agreed by the representatives of the Member States in the eHealth Network in its Conclusion Paper on stating that this federated approach would "respect and interconnect national infrastructures already operating in Member States, which will enable mutual recognition of electronic identities".

The Commission stresses the importance of taking into account sector-specific requirements, and emphasizes that a secure and reliable cross-sector approach to electronic identification has the advantages of economy of scale, citizens' convenience, greater simplification of administrative procedures and, last but not least, avoid fraud. Therefore:

The Commission believes that a cross sector approach to secure and reliable electronic identification should be the way to be followed, including by those Member States that have not decided yet on an electronic identification strategy for eHealth.

Security and integrity of electronic identification and authentication

Each Member State is fully responsible for **ensuring the security, confidentiality and integrity of the technical systems** implementing electronic identification schemes at national level. Consequently, the proposed Regulation does not specify any **technical or procedural requirement** to harmonise the security, confidentiality and integrity of such technical systems at national level. In addition, it shall be emphasized that the mutual acceptance and use of electronic identification means will be based on the authentication process used by the issuing country.

Article 8 establishes the legal setting for all Member States to jointly cooperate to ensure technical interoperability and security of electronic identification means. Via the coordination mechanism, if appropriate, Member States may share, discuss and agree on common minimum requirements and practices (with particular attention to be EU and international standards) to ensure interoperability and enhance security.

2. Measures under the eHealth Network mandate on electronic identification and authentication

Overview

Art.14 of Directive 2011/24/EU, creating the eHealth Network foresees the development of common measures on electronic identification and authentication for eHealth.

The eHealth Network's Conclusion paper on "eID EU governance for eHealth Services" (hereinafter referred to as: "Conclusion Paper") agrees that a first step towards electronic identification interoperability is to ensure mutual recognition and acceptance by the Member States of electronic identification and authentication to enable interoperability for continuity of care and improving patient safety.

Bridge building between key EU legislation

The Conclusion Paper is fully in line with Art. 8 (1) of the proposed Regulation on electronic identification foreseeing that: "Member States shall cooperate in order to ensure the interoperability of electronic identification means falling under a notified scheme and to enhance their security". This is coherent with the lessons learned by the Large Scale Project STORK on cross-border electronic identification and reflections on the future digital service infrastructure on electronic identification in the context of the proposed Connecting Europe Facility.

Using these potential synergies is obvious:

The Commission recommends that the common measures on electronic identification and authentication for eHealth to be defined under Directive 2011/24/EU would be developed to build synergies with the proposed Regulation and contribute concrete elements for its future implementation, in particular with regard to the first layer of identification of natural and legal persons.

Security of electronic identification and access to services or data in the health sector

Health data are very sensitive data. Several Member States require a higher level of security for eHealth services. Currently the level of security varies widely among the Member States, which is a concern for a few of them. As mentioned above, under the proposed Regulation the European Commission will be empowered to adopt delegated acts concerning "*the facilitation of cross border interoperability of electronic identification means by setting of minimum technical requirements*". This might naturally result in establishing different levels of security in order to meet the specific requirements of sensitive services and data like the health ones.

Taking the above into account, the eHealth Network could discuss what level of security is required in the health sector to support the possible mapping of eHealth services into various security levels.

Authentication of roles

Authentication of the roles of a patient and a doctor is the second layer required for the safety and security of eHealth services. The proposed Regulation does not regulate roles, but it would fall under the scope of the common measures on identification and authentication for eHealth of Directive 2011/24/EU.

Therefore, building upon the work already done by epSOS, it is important to clarify whether all Member States have electronic systems for authentication of roles in place or at least plan to do so and to access their need to have common specifications for roles (see mapping).

Identification on the spot and access to health data and services

Electronic identification of citizens inside as well as outside their country of residence is a key instrument to ensure cross border use of eHealth services in due acknowledgement that privacy and data security are of utmost importance. However, we must emphasize the difference between *online* and *on-the-spot* electronic identification. When a citizen (or an entity) identifies itself electronically online, it uses its own hardware (card reader, mobile phone etc.) and the relying party receives electronic data, therefore there is no need to harmonise the electronic identification means (tokens). Contrary to this, on-site electronic identification foresees such kind of a harmonisation, and all places (hospitals, doctor's chambers, pharmacies etc.) shall be equipped with dedicated hardware or interface. The proposed Regulation governs only online electronic identification.

As it has been announced in the introduction, any specific security requirements regarding access rights to data or services and data transfer goes beyond the scope of the proposed Regulation.

Any harmonisation work regarding electronic identification means used in the eHealth sector (practically the eHealth cards), security requirements regarding access rights and health data transfer shall be done through the common measures on electronic identification and authentication for eHealth under Directive 2011/24/EU.

Lessons learnt from epSOS

During its three years of activities, the epSOS project has cumulated useful experiences which could facilitate discussions on security aiming to achieve secured transferability of eHealth data across the Member States.

The Commission suggests discussing the experiences of epSOS with regard trust between the participating countries, terms of encryption, architecture, use of standards, security, the problems and constraints arisen. Based on this discussion, the relevant issues shall be considered in the scope of the common measures under Directive 0211/24/EU.