LEGAL ISSUES OF IDENTITY MANAGEMENT IN E-GOVERNMENT

Ioannis Iglezakis,
Associate Professor,
Aristotle University, Faculty of Law

Table of contents:
I. Introduction
II. Definition of Identity Management
III. Utilization of eIDMS
IV. The problems posed with regard to electronic identification
V. New EU rules on electronic identification
VI. Data protection Issues
VII. More specific issues
VIII. Conclusion

Abstract: A key aspect of eGovernment is identity management, since the processes that are involved in the provision of public services rely profoundly on secure identification policies; it presents a challenge to create the framework for identity management that will promote digital inclusion, be efficient and privacy-friendly. In this paper, the legal issues regarding electronic identification management systems are presented and solutions to key problems are proposed, on the basis of the EU Legal Framework.

Keywords: e-Government, electronic identification, electronic identification management systems, privacy, data protection, interoperability.

I. Introduction

The development of eGovernment is one of EU’s top priorities towards the goal of exploiting the benefits of ICT across Europe. ICT enables the public sector to implement innovations in the delivery of its services to citizens, which eliminate bureaucracy and
enhance its efficiency, while reducing costs.\textsuperscript{1} To achieve these tasks, the EU has assumed an active role in promoting the very concept and specific eGovernment initiatives.\textsuperscript{2}

It should be highlighted that eGovernment and open governance are essential to modernize the organization of government and its services and open a dialogue between the state and the civil society and thus, to revitalize the democracy and lift the democratic deficit. Nevertheless, this development is hindered by the digital divide, i.e., the lack of access to digital information, which affects the Have-nots, that is, those parts of the population that make no use of ICT and/or have no access to the Internet.\textsuperscript{3}

eGovernment is defined as “the use of information and communication technologies in public administration combined with organisational change and new skills in order to improve public services and democratic processes and strengthen support to public policies”.\textsuperscript{4} This requires, however, an open and transparent public sector, a public sector not excluding anyone and a productive public sector.\textsuperscript{5}

A key aspect of eGovernment is identity management, since the processes that are involved in the provision of public services rely profoundly on secure identification policies and procedures. For that purpose, authentication mechanisms are put in place, which serve in identifying citizens in the electronic environment. The electronic identification schemes that are employed by various countries in the EU differ in many aspects, but all of them rely in great extent in the processing of a big amount of personal data, to ensure that users of electronic services are appropriately identified.

It presents a challenge, therefore, to create the framework for identity management that will promote digital inclusion, be efficient and privacy-friendly.\textsuperscript{6} At those aspects of identity management in the framework of eGovernment we will focus in this paper.

\textsuperscript{2} See the Europe 2010 Initiative: https://ec.europa.eu/digital-agenda/en/public-services
\textsuperscript{3} See, e.g., W. Wresch, Have and Have-nots in the Information Ages, 1996. For an analysis of the digital divide in Greece see I. Iglezakis, The development of E-Governance and the issue of digital inclusion in Greece with particular regard to the constitutional right of e-participation, 2008 (1) JILT, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2008_1/iglezakis/
\textsuperscript{5} Op. cit.
II. Definition of Identity management

It is important to define, at first, identity management, which is a generic term of ICT that finds application in the public and private sector. In general, identity management can be defined as the set of policies, rules, mechanisms, processes and applications that deal with identifying individuals in a system (an application, a network, or an organisation) and controlling their access to resources within that system by associating user rights and restrictions with the established identity. The objective of identity management is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials.\(^7\)

Typically, identity management encompasses the following key components:
- **Authentication**: the process of establishing the validity of a user attempting to gain access to a service. Authentication methods include: user name and password; token; biometrics; digital certificates (PKI, smart cards).
- **Access control (or authorisation)**: the process of limiting users’ access to resources and data they have specific permissions to use.
- **Accounting**: the process of keeping track of a user’s activity while accessing the service or the network resources.
- **User management**: the process of activating and de-activating users’ identities and access permissions.

For eGovernment applications to be rendered without problems, electronic Identity management systems (eIDM) are adopted that support the management of digital identities. There are three basic types of eIDMS\(^8\):
- eIDMs for account management, implementing authentication, authorization and accounting;
- eIDMs for profiling of user data by an organization, e.g. detailed log files supporting, e.g., personalized services, etc.; and
- eIDMs for user-controlled context-dependent role and pseudonym management.

However, for the purpose of our investigation, only the first type of eIDMs will be investigated.

III. Utilization of eIDMS


An eIDMS basically serves the identification and authentication of users of governmental services. As regards identification, this can be interpreted in various ways. In our view, the various stages of the identification process should be described in the following way:

a) registration process: it consists in the process of using already given attributes of an entity to establish an identity for that entity;

b) *per se* identification process: it consists in the verification of the identity of an entity

It should be noted that the different approaches can be combined in one definition of identification as the process of establishing a link between an entity and an identity for later authentication or account management or when individualizing the entity.\(^9\)

Authentication is the verification of a claim by an entity, which may also involve identification. In the framework of eGovernment it has great importance, as it is the basic requirement for accessing electronic services. In particular, a request for authentication requires that an asserting entity presents some form of evidence to prove that it is in fact who it claims to be.

The subjects of management in eIDMS are: a) members of governmental institutions and b) citizens and businesses.

It is also important to note that there are different levels of authentication, on the basis of certain factors (knowledge, possession and biometric features) and corresponding reference data.\(^10\) Examples include the following:

- User name/ password;
- Passport or ID card /biometric reference data and citizens registers;
- Administration cards and reference databases;
- eHealth cards and reference data of health insurance holders; and
- Digital Signature Cards and PKI

Moreover, another important process in eIDMS is authorization, i.e., the act of determining the permissions of an entity that requests the execution of a defined action, that is, to ‘read’, ‘modify’, ‘create’ and/or ‘delete’.\(^11\) Authorization also refers to management of roles and rights and in more particular, it focuses on rights of users, operators,

---

administrators, etc and access control to governmental property (buildings, rooms, equipment).

It goes without saying that rights and policy management play a significant role in ensuring confidentiality, i.e. in keeping the content of information and documents secret, with the exception of authorized users.

IV. The problems posed with regard to electronic identification

An important requirement for the success of eGovernment services is to build secure and effective eIDMS. More precisely, to provide electronic services it is necessary to have in place a reliable verification procedure for the electronic identity of the one requesting the performance of a service, in an environment which provides privacy protection and particularly, protection from identity theft and fraud. It is notable that the issue of identity theft in general has become a major issue due to the multitude of online sources and the availability of online information, which become the target of identity fraudsters.

This presents a challenge, since a consistent approach should be adopted to ensure interoperability across the EU, so that Member States can agree on the identity of an entity in order to enable government sectoral applications to conduct cross-border transactions with respect to that entity. EU Member States have invested significantly in e-Government and developed a diversity of eIDMS independently from each other and in an uncoordinated way. The systems adopted by various Member States employ varied technologies for hardware tokens (smart-cards, mobile phones, etc.), biometrics (fingerprint, facial, etc.) and digital signatures. From a technical point of view, there is, thus, limited compatibility between the eIDMS, currently in use.

There are also other obstacles affecting interoperability of eIDMS. Namely, there is a lack of trust of other Member States’ certification services and a prohibition, de jure or de facto, of the use of authentication or authorization from other Member States. Also, different organizational schemes are in use in different States, e.g., for example, for issuing national e-IDs and validating foreign e-IDs. And in addition, there are differences in legislation of EU Member States as regards identification, data protection and e-signatures.

14 See Stefanova et al., op. cit.
Besides security issues with regards to electronic identification, there are also privacy issues that need to be tackled. In general, eGovernment applications do not follow data protection principles by design; instead, the eIDM architecture relies in the processing of personal data in great extent. More specifically, an eIDMS relies on user identification and data exchange based on unique identifiers of the data subject. This procedure presents a risk, for the reason that personal data from one context can be linked to personal data to another context, which may have as a result interconnections of data. In turn, that would mean the creation of detailed user profiles and a risk of privacy.

In more detail, the following issues are emerging when data protection principles are taken into account at the design of an eIDMS:

- Lack of privacy, conceived as lack of control over personal data;
- Lack of transparency, as the processing of personal data is not clear in its full extent;
- Lack of auditability of the system;
- Lack of enforceability of privacy and data protection rights.

To deal with these issues, it is suggested not only to propose technical and organization measures to solve the problem of the lack of interoperability and achieve better protection of privacy for data subjects, but to study also the legal aspects of the issues related to eIDMS.

V. New EU rules on Electronic Identification

A coherent legal framework for electronic identification is created with the enactment of Regulation No 910/2014, i.e. the Electronic Identification and Trust Services (eIDAS) Regulation. The Regulation, which was adopted on 23 July 2014, replaces the eSignatures Directive (Directive 1999/93) and shall be applied from 1 July 2016, with the exception of certain provisions which will apply in different stages.

The eIDAS Regulation creates a European internal market for electronic identification and electronic trust services, including:

- electronic signatures;
- Time stamping;

---

- Electronic seal;
- Electronic delivery;
- Legal admissibility of electronic documents to ensure their authenticity and integrity;
- Website authentication.

The Regulation obliges public bodies to accept cross-border identification/authentication services that are provided under a scheme that has been properly notified to the European Commission. Thus, it ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in the EU countries where eIDs are available.

In particular, it provides for the mutual recognition of eID schemes in Article 6. Accordingly, when an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online.

This applies only if the eID meets the requirements of the Regulation, that is, when:

(a) the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9;
(b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high;
(c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online. In case, however, the assurance level is low, it is not mandatory to recognise an eID scheme.

The assurance levels of eID schemes low, substantial and high meet the criteria prescribed in Article 8. Accordingly, (a) assurance level low refers to an electronic identification means, which provides a limited degree of confidence in the claimed or asserted identity of a person; (b) assurance level substantial shall refer to an electronic identification means, which provides a substantial degree of confidence in the claimed or asserted identity of a person; (c) assurance level high shall refer to an electronic identification means, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial. The aforementioned eID schemes should be characterised with reference to
technical specifications, standards and procedures related thereto, including technical
controls, the purpose of which is to decrease the risk of misuse or alteration of the identity.
The EU Commission issued the Regulation 2015/1502 which sets out minimum technical
specifications and procedures for assurance levels.

An electronic identification is eligible for notification if it meets certain criteria, e.g., that
the eID means are issued by the notifying Member State or under a mandate from that State
or are recognized by that, it can be used to access at least one service provided by a public
service body, the eID means and the eID scheme meet the requirements of at least one of
the aforementioned assurance levels, etc.

The notification of eID schemes to the EU Commission includes the following information:
(a) a description of the electronic identification scheme, including its assurance levels and
the issuer or issuers of electronic identification means under the scheme; (b) the applicable
supervisory regime and information on the liability regime with respect to the following: (i)
the party issuing the electronic identification means; and (ii) the party operating the
authentication procedure; (c) the authority or authorities responsible for the electronic
identification scheme; (d) information on the entity or entities which manage the registration
of the unique person identification data; (e) a description of how the requirements set out in
the implementing acts are met; (f) a description of authentication; (g) arrangements for
suspension or revocation of either the notified electronic identification scheme or
authentication or the compromised parts concerned.

In case of a security breach, the notifying EU country must, without delay, suspend or
revoke the cross-border authentication, and inform other EU countries and the EU
Commission (Article 10). Failure to comply with the regulation’s obligation shall have as a
result the liability of a notifying country or the party issuing the eID or the party managing
the authentication procedure (Article 11).

To fully implement the provisions on recognition of eIDs, it is provided for that national
eID schemes notified must be interoperable. Interoperability is legally enshrined, as Article
12 of the Regulation provides for the establishment of an interoperability framework, which
meets the following criteria: (a) it aims to be technology neutral and does not discriminate
between any specific national technical solutions for electronic identification within a Member
State; (b) it follows European and international standards, where possible; (c) it facilitates
the implementation of the principle of privacy by design; and (d) it ensures that personal
data is processed in accordance with Directive 95/46/EC. Furthermore, the Regulation
defines the interoperability framework with reference to technical requirements and
procedures to be followed. More technical details are laid down in the Implementing regulation 2015/1501.

These provisions of the Regulation will facilitate secure electronic transactions and the EU-wide use of eGovernment services. However, the provisions on the mutual recognition of eIDs will entry into force in 2018.

VI. Data protection issues

The current legal framework on data protection does not include a requirement to integrate data protection rules into the design of eIDMS. The Proposal for an EU Data Protection Regulation, however, provides for the principles of data protection by design¹⁹ and by default (Article 23), which point in that direction.

Accordingly, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of the legal framework and ensure the protection of the rights of the data subject. And also, he/she should implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage.

The question is which requirements of the data protection framework should be taken into account when designing eIDMS. In our view, primarily the general principles of data protection enshrined in Article 6 of the Directive 95/46 and in Article 5 of the Data Protection Regulation should be complied with.

In particular, the following principles should be taken into account:

- Fair and Lawful Processing: personal data must be processed fairly and lawfully;
- Purpose specification and purpose limitation: personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- Data minimization: personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate

or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

- Data Preservation: personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed;

Furthermore, data processing must be in accordance with the rights of data subjects, which are established with the Directive, i.e., the right to information, the right of access to data, the right to object and the right to oppose to automated individual decisions. What is important here is to provide sufficient information to data subjects about the particulars of the data processing and the existence of their right to access to and rectification or erasure of personal data concerning them or to object to the processing of such data.

In more particular, it is crucial to ensure that users are informed about the privacy implications of using such systems. Consequently, users should be provided with clear information about the controller identity, the purposes of processing, data collected, recipients, etc. and that they should be given clear alternatives and control over the disclosure of information to participating sites.\(^{20}\) This is a prerequisite for lawful and fair processing of personal data, which derives from Articles 10 and 11 of the Data Protection Directive and the openness and individual participation principles of fair information practice.

However, this requirement could hinder the deployment of single sign-on services, as the provision of extensive information may be a burden for the user who is required to process this information and assess its relevance.\(^{21}\) A particular problem is that online notices are long and contain legal terms and industry jargon, and therefore, their value has been questioned.\(^{22}\)

An appropriate solution of this problem is to provide multi-layered information notices, in accordance with the proposal of the Article 29 Working Party.\(^{23}\) Accordingly, there could be three layers of information: i) the short notice, which must offer the core information (identity of the controller and purposes of processing) and any additional information which

---


in view of the particular circumstances of the case must be provided beforehand to ensure a
fair processing, ii) the condensed notice, which provides all relevant information required
under the Data Protection Directive and iii) the full notice, which includes all national legal
requirements and specificities. It is, therefore, sufficient for controllers to include a simplified
short notice in the user-interface, insofar as this is integrated in a multi-layered information
structure, in which more information is available.\(^{24}\)

In addition, security is a fundamental requirement in any processing of personal data and
it plays an essential role, also, in eIDMS. Therefore, the controller must take appropriate
technical and organizational measures against unauthorized or unlawful processing of
personal data and against accidental loss or destruction of, or damage to, personal data.

VII. More Specific issues

To allow the user keep control over his/her personal data is a matter under discussion.
The Article 29 Working Party notes that there are two tendencies, one considering that
citizens must keep their data under control at all stages of the administrative procedures,
and that they must have an information feedback on the data exchanges concerning any
decision taken about them. The second tendency consists in considering that administrative
simplification necessarily operates at the price of a certain loss of control of the user’s own
personal data.\(^{25}\) According to this, the requirements of faster e-government cannot be
satisfied at the same time with the requirements of traditional information of the citizens.

If one chooses the first option, it is argued that data exchange between administrations
via a network can be subjected to the consent of the persons concerned. In my view, this
will create significant hurdles in the procedure. In any case, to allow the user to have control
on his/her personal data, it is recommended (by the Irish Authority) not to feed the database
by using data already provided for a different purpose. Instead, citizens should be given the
opportunity to consent to their inclusion in the new system and to be informed about the
purposes and uses of the central database.

The application of data principles leads us to another conclusion. Namely, the
implementation of the principle of quality of data would require that excessive or irrelevant
personal data, which do not have a legitimate and relevant application, should not be asked
for or stored. In view of the multitude of personal data collected for the purpose of

\(^{24}\) See T. Olsen & T. Mahler, op. cit., p. 422.

seq.
electronic identification, this means that the collection of data should be restricted to what it is necessary.

Certain privacy issues are common to all identity management systems and should be dealt with. To start with, defining roles and responsibilities is necessary in such situations where personal data are processed in cooperation between participants in an identity management system.

In international data protection regulations responsibility falls to the controller, i.e. the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data, pursuant to the definition of Article 2 (d) of the Data Protection Directive, which is similar with the one given in Article 1 (a) of the OECD Guidelines and in Article 2 (d) of the Convention No 108 of the Council of Europe. The Directive makes the distinction between the controller and the processor, and defines the latter as ‘a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller’. The former, however, is under the obligation to comply with the requirements of data protection legislation transposing the provisions of the Directive.

Subsequently, it is crucial to determine which role the participants in identity management schemes play and whether they could be regarded as processors or controllers.26 The Article 29 Working Party suggests to consider all participating sites in an identity management scheme as controllers in respect of their own processing operations.27 In particular, this means that any service provider in a ‘circle of trust’, i.e. in identity management systems that follow the Liberty Alliance specifications, will be the controller of the personal data concerning its customers and/or employees and thus responsible for complying with data protection rules. Moreover, it is not crucial which role Liberty assigns to a participant, since one may be classified as a controller (or joint controller) depending on the role it actually performs in practice within a circle of trust.28

In case there are multiple collaborating organizations within a circle of trust, it is certainly difficult to identify the controller. But in order to do so, it has to be determined who has actual control over the data and, in particular, determines how and for what purposes the data are processed. And therefore, if the data controller’s responsibility has been delegated

27 See WP 68, op. cit., p. 9, 12.
to another organization, the delegating organization would continue to be the data controller if it actually has control over the means and purposes of the processing.\textsuperscript{29}

However, no responsibility can be placed on the designers of online authentication systems, since these are not controllers and obviously not processors. The Article 29 Working Party expressed a different approach in this issue\textsuperscript{30}, but there is no legal ground on which this could be based. On the contrary, it is the provider who implements an identity management system, regardless how it is designed, who bears the burden of complying with the law.

Furthermore, the stipulation in a contract of duties and responsibilities between controllers is seen by the Article 29 Working Party as advisable.\textsuperscript{31} This is particularly important for the allocation of responsibility, although it is not mandatory by law. In particular, the Directive only imposes an obligation to conclude a contract between the controller and the processor in Article 17 (3)\textsuperscript{32} and does not impose such an obligation to joint controllers or to collaborating single controllers. However, a contract regulating the relationships between participants in an identity management schemes is essential to ensure compliance with privacy rules, and this is also recognized by the Liberty Alliance. The formation of the contractual framework will depend on the nature and scope of the circle of trust. Thus, a relatively light framework may be enough for a small number of relatively static business partners, whereas in larger and more dynamic circles of trust it may be necessary to establish federation-wide rules and common operating procedures and processes that would minimize the problems of bi-lateral negotiations and multiple contracts with many interdependencies.\textsuperscript{33}

In relationships between controller and processor, it is clear that full responsibility lies with the controller. The processor is only bound to carry out the controller’s instructions. Pursuant to the Data Protection Directive, the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out.\textsuperscript{34} The processor must, further, ensure compliance with those measures and this means that the controller should supervise the processor. And

\textsuperscript{29} See T. Olsen & T. Mahler, op. cit., p. 420.
\textsuperscript{31} See WP 68, op. cit., where it is noted that: “...it is advisable for the different players to have clear contractual agreements between them where the obligations of each party are made explicit”.
\textsuperscript{32} “The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: 1) the processor shall act only on instructions from the controller, and 2) the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor”.
\textsuperscript{33} See Liberty Alliance Project, op. cit., p. 6.
\textsuperscript{34} Article 17 (2) of the Data Protection Directive.
finally, it is provided that the carrying out of processing by way of a processor must be
governed by a contract or legal act binding the processor to the controller, which should
stipulate that the processor shall only act on instructions from the controller and that the
processor must implement appropriate technical and organizational measures to protect
personal data.  

VIII. Conclusion

The transformation of the public administration in the 21st century is a key issue for an
efficient state and an open democratic society. In this context, it is essential to develop a
privacy-friendly and interoperable identity management, taking into account not only
technical and organizational requirements, but legal requirements as well. It should be
mentioned, however, that it is not advisable to adopt a centralized approach and create a
single authority on EU level. With the adoption of the EU Regulation 910/2014, the EU
legislator relied on mutual recognition of electronic identification, excluding thus any further
discussion on the adoption of a common infrastructure and a single identification Authority in
the EU.

35 Article 17 (3) of the Data Protection Directive.
REFERENCES

FIDIS Deliverable D2.3: ‘Models’, available online at:
http://www.fidis.net/resources/deliverables/identity-of-identity/int-d2300/

FIDIS, ‘D 2.1: Inventory of topics and cluster’, p. 27 et seq., available online at:
http://www.fidis.net


Liberty Alliance Project (2005).'Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation'.


ADDITIONAL READING


