JICLT
Journal of International Commercial Law and Technology
Vol. 8, No.2 (2013)

"Electronic Identity for Europe": Moving from Problems to Solutions

Norberto Nuno Gomes de Andrade

1. The Relevance of eID and the current "legal framework" state of the art

Electronic Identity (eID) is the backbone of modern communications and transactions in the digital world, as well as a key driver for the growth of the EU economy and the completion of the Digital Single Market. The latter, in effect, can only be accomplished when citizens from one Member State (MS) can easily and unobtrusively access services and use applications, including signing electronically, from any other Member State. In this way, the completion of a European digital single market is, to a very large extent, dependent upon an interoperable and functional eID mutual recognition system across Europe.

Despite the implementation of different identity management systems (IMS), the numerous political declarations and initiatives in this area, the development of various research projects and eID technologies, the discussion on the necessary legal means through which to create an interoperable pan-European eID has not yet taken place. In addition, the processing and management of electronic identities is regulated – at the EU level - through principles, rules and concepts "borrowed" from different EU legal instruments (Data protection, eSignatures and Services Directives being the most relevant ones). As such, one of the main challenges[1] posed to European electronic Identity is of a legal nature. In this regard, it is important to note that the technology necessary to enable an interoperable eID across Europe already exists and is being implemented,[2] while legal interoperability is largely missing. It is the lack of legal harmonization and compliance in combination with the technical interoperable solution chosen that constitutes the most salient inhibiting factor preventing the cross border deployment of services based on electronic identity. A structured debate is thus necessary to promote consensus on viable legal solutions.

In this context, the Institute for Prospective Technological Studies (IPTS),[3] within the framework of the 2011 LSPI Conference organized a workshop – entitled "Electronic Identity for Europe" – devoted to the legal framework that is necessary to set in place in order to accompany and enforce the already existing technological answers.

2. The Work and the Strategy developed by the EC in the field of eID

The EU, since the mid-nineties, has been developing a significant number of initiatives (roadmaps, agendas, action plans, research projects, etc) in the field of eID. The overall objective guiding such initiatives has been the construction of a European cross-border eIDM framework, based on interoperability4 and mutual recognition of national eID resources and management systems. In 2006, the EC established the so-called eID Roadmap[5] a list of measurable objectives and milestones for the

[1] See, for example, http://ec.europa.eu/information_society/policy/esignature/docs/pub_cons/consultation_summary.pdf

[2] eID Interoperability for PEGS: Update of Country Profiles Framework contract ENTR/05/58-SECURITY, SC N°13 Analysis & assessment report, October 2009

[3] http://ipts.jrc.ec.europa.eu/

[4] See the European Interoperability Strategy (EIS) and the European Interoperability Framework (EIF) for European Public Services, published as annex 1 and 2, respectively, to the Communication "Towards interoperability for European public services" (COM(2010) 744).

[5] A Roadmap for a pan-European eIDM Framework by 2010, see *http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf*

construction of such framework. It later reconfigured the objectives with the launch of the Digital Agenda,[6] presenting two important key actions in the field of eID:

- the proposal for a Council and Parliament Decision on mutual recognition on e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States;
- the proposal for a revision of the eSignature Directive[7] with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems.

In terms of implementation, the EC has been pursuing the construction of an interoperable European eIDM reality through a research-focussed, gradual, step-by-step approach, addressing first specific sectors before expanding to all sectors. The paradigmatic example of this gradual approach is the Stork Project,[8] which is implementing a number of specific cross-border pilot applications and services (supporting eID tokens from multiple projects). In each of the planned pilots, participating countries agree to mutually recognise each other's means of identification and authentication (which can, afterwards, serve as a model for other types of applications and services).

In terms of strategy, the construction of a European eIDM framework has been based, until now and to a very large extent, on the interoperability of eSignatures in the context of the provision of public services. The emphasis has thus been on eSignatures, identities created through formal validation processes (formal identities) and public sector applications.

3. Adopting a broader perspective: the idea of a dedicated European eID Legal Framework

The workshop on Electronic Identity for Europe was built upon the work developed previously by the IPTS in this area[9] and aimed to raise consensus on the adoption of a broader perspective in framing the debate on the regulation of eID in Europe. In arguing that eSignatures, formal identities and public sector applications constitute only a part of a larger identity ecosystem for which there is no current regulatory framework, the workshop proposed the idea of a specific and dedicated European legal framework for eID as the central theme for discussion. The workshop thus focussed on a broader picture, looking at how a full-scale European legal framework could regulate a cross-border, mutual recognition system of e-identification and e-authentication in the EU. Before summarizing the papers presented by the legal experts participating at the workshop, it is worth listing the main challenges and questions that the idea of a specific and comprehensive legal framework for eID in Europe poses.

4. eID Legal Framework: Challenges and Questions

The construction of a European dedicated eID legal framework assumes complex contours that need to be addressed. The objective of the workshop was to delve into such complexity and propose solutions. In addition to the important technical, semantic and organizational steps that have been taken vis-à-vis the construction of an interoperable eIDM infrastructure within the EU, the workshop suggested new ways and means to legally frame and regulate such cross-border infrastructure and network of identity resources. Among the many unresolved challenges and questions involved in the development of a specific legal framework for eID, the workshop pointed out the following ones:

---

[6] European Commission, "Communication from the Commission - a Digital Agenda for Europe," (Brussels: European Commission 2010).

[7] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[8] www.eid-stork.eu

[9] Wainer Lusoli, Ioannis Maghiros, and Margherita Bacigalupo, "eID Policy in a Turbulent Environment: Is There a Need for a New Regulatory Framework? ," *Identity in the Information Society* 1, no. 2 (2009).; Norberto Nuno Gomes de Andrade, "Towards a European eID Regulatory Framework. Challenges in Constructing a Legal Framework for the Protection and Management of Electronic Identities," in *European Data Protection : In Good Health ?*, ed. Serge Gutwirth, et al. (Springer, 2012 - forthcoming).

- *Techno-legal integration:* How should national identity management systems, along with their architecturally different infrastructures, be articulated within the umbrella of an appropriate and specific European eID legal framework? How should such a legal framework enable the 'legal interoperability' of authentication processes involving different Member States (with identities issued by one MS being authenticated to access services in another MS)? How should an eID legal framework regulate the information flows of identity-related data across Europe in a privacy-controlled manner?
- *Liability of actors*: What kind of legal framework should be put in place in order to clarify the assignment of responsibilities and liabilities to the various relevant actors involved in the processing of identity resources: end-users, identity providers, relying parties, service providers?
- *User-centricity:* How can the principle of user-centricity, and the need to provide the end-users with greater control over their own identity, be reconciled with the need to enable swift and simple identification/authentication processes across the EU (as automated exchanges of identity information can be more efficient and user-friendly, avoiding the imposition of unnecessary burdens on the end-user)?
- *Anonymity and Pseudonimity*: How can anonymity and pseudonimity be provided and conciliated with the need for *identifiability* (for the compliance with contractual obligations, law enforcement purposes, etc)? How could an eID legal framework encompass eIDM systems that allow for a spectrum of different identification and de-identification possibilities, ranging from full and unique assertion of identity to the creation of pseudonyms and the option for anonymization? What are ex-ante implications on the existing legal framework?

- Based upon the idea of a specific legal framework for eID, the workshop counted with the presence of six legal and policy experts in the area of electronic identity, providing a platform for discussion that involved the following themes and issues: (a) the important role of Human Rights in the regulation and protection of digital identity involvement (Prof. Paul De Hert); b) the shortcomings of the current eSignatures directive and the need to move towards a comprehensive legal framework for eID (Dr. Hans Graux); c) a concrete proposal for a future EU ID model (Prof. Patrick Van Eecke); d) legal issues raised by social networks as providers of digital identity (Prof. Omer Tene); e) identity assurance schemes, the role of consent and users' control over personal data (Prof. Edgar Whitley); f) governance models and structures implementing eID frameworks in Europe (Dr. Tobias Mahler).

In the following each of the experts' contribution to the workshop are briefly described.

Prof. Paul De Hert (Vrije Universiteit Brussel)
eID: A Human Rights perspective

Prof. De Hert pursued a Fundamental Rights perspective to his study of electronic identity. Based upon recent developments in the field of human rights (treaties and case law), the speaker developed the idea of a right to digital identity, discussing its shortcomings as well as its advantages and feasibility. Prof. De Hert offered two technological-oriented scenarios regarding possible future developments in the field of eID, presenting interesting and stimulating theoretical perspectives on the important role that law (in particular human rights law) could play in the protection and management of electronic identities.

Dr. Hans Graux (time.lex)
Rethinking the e-signatures Directive: Moving towards a comprehensive legal framework for eID

Dr. Hans Graux's presentation explored the possible avenues for the creation of a legal framework for e-Authentication, discussing – in this context - the revision of the European eSignatures Directive (eSig directive). The latter, as argued by the expert, does not provide a material legal framework for electronic identification and authentication services, covering only one possible application of certification services in detail: electronic signatures. The directive, in this respect, fails to comprehensively address other services using, or ancillary to, electronic signatures, such as electronic identification, time-stamping services, long-term archiving services, electronic registered mail, or signature validation services. The current review of the eSig directive was depicted as an opportunity to remedy this issue. Based on such idea, Dr. Hans Graux proposed to broaden the current legal framework to ensure that certification services

(thus including electronic identification) are more comprehensively covered and to avoid further barriers in the internal market. In this context, the expert discussed an ambitious vision for a future legal framework for IAS services in Europe, putting forward – in specific details – the idea of an "e-Authentication Directive," within which electronic identification would be considered an e-authentication service.

Prof. Patrick Van Eecke (DLA Piper)
EU future electronic identification, authentication and signature policy

Prof. Van Eecke proposed a new model for an EU future electronic Identification, Authentication and Signature policy (IAS), naming it "EU ID." One of the most interesting aspects of the proposed model is the fact that it follows the same principles of the .eu Top Level Domain (TLD). As such, the model presents a number of advantages. Firstly, it is based upon a regulation and not a directive (avoiding thus all the hurdles and delays involved in the implementation of the latter by the various MS). Secondly, the presented scheme consists of a more flexible and agile governance model, within which the standard setting and the international alignment would be carried out by an agency. Thirdly, and from a policy perspective, the EU ID framework would be configured according to the principles of scalability, voluntariness and subsidiarity. The model, in this respect, would not only have the potential to trigger an IAS market at the EU level, but it would also be able to co-habit with other eID policy frameworks (such as in the area of eGovernment), as well as with other general IAS frameworks (eSignature, eArchiving, etc). From a user perspective, the system would allow users to choose their identity providers (CSP), independently from service providers (relying party) in order to receive their service. Users, in this way, would not communicate their personal details directly with the relying party, as identity providers would act as a trusted third party that authenticates and stores user's information. In conclusion, the system would operate as a "user-centric" identity management system, endowing users with greater control over their personal information.

Prof. Omer Tene (College of Management School of Law, Rishon Le Zion)
Me, Myself and I: Aggregated and Disaggregated Identities on Social Networking Services

Prof. Tene, in his presentation, explored some of the legal issues arising from the transformation of SNS operators to providers of digital identity. In particular, Prof. Tene identified and developed the following legal issues: neutrality, deletion, portability and disaggregation vs. aggregation of online identities.

The speaker addressed, firstly, the wide degree of control that SNS enjoy over complete vectors of our identity and how these operators are able to influence what content users consume on the web and how they are portrayed online. Prof. Tene addressed this issue as (lack) of neutrality problem, drawing the attention to the little information we have regarding the logic and the considerations underlining SNS's decision-making process. Another important theme was the deletion of one's digital identity and its legal implications. In this context, the speaker addressed the question of the deletion of user accounts by SNS operators (namely the pseudonymous ones), as well as the attribution of a so-called "right to be forgotten" to users with respect to content stored on a SNS. Such right, in fact, has emerged as one of the central tenets of the European data protection framework revision. Another important issue raised by Prof. Tene concerned data portability, and in particular portable online identity. The latter enhances transactional efficiencies, but it also creates privacy and security concerns. While data portability reduces the risk of "lock in" and concentration of power, it nevertheless challenges the protection of third parties' personal data under shifting privacy policies. As a last topic of analysis, the expert emphasized the need to allow users to maintain disaggregated identities and obtain authorizations on an anonymous or pseudonymous basis. In this respect, SNS operators should ensure, on the one hand, the portability of credentials (which contribute to the development of an aggregated identity); while, on the other, they should also provide users with the means to disaggregate their different identities, namely their pseudonymous ones. Such recommendation entails a significant change in SNS policies, as they currently outlaw both use of pseudonymous and active disaggregation of identities.

Prof. Edgar Whitley (London School of Economics and Political Science)
Enabling customer–centric identity assurance: A role for dynamic–consent?

Prof. Whitley depicted the marked shift that has been taking place in the UK in recent years from government–centric identity management schemes to citizen– or customer–centric identity assurance schemes. As explained by the speaker, identity assurance aims to allow customers to have effective control over their personal data by minimising the amount of (identity-related) data to be disclosed to third parties and allowing customers to choose which additional data needs to be shared with them.

In this context, the expert explored the role that consent can play in such a scheme. Consent was described as a core principle of most data protection regulation but one which is legally problematic as it is not always required for the processing of data. Moreover, Prof. Whitley added that there is growing evidence that consent is an ineffective mechanism for online transactions as it is rarely truly informed and freely given. Drawing on the work of the EnCoRe project (www.encore-project.info) the speaker argued that many of these limitations can be addressed by considering a technologically leveraged notion of consent, which has been named as "dynamic–consent." Dynamic–consent recognises that the initially given consent might not be completely informed or freely given, while EnCoRe–enabled "dynamic–consent" supports the revocation of consent using secure and tested advanced cryptographic techniques operating within a regulatory and compliance regime. This approach, as pointed out by Prof. Whitley, can enhance customer control over their personal data in the context of identity assurance and hence their confidence in participating in such a scheme.

Dr. Tobias Mahler (Norwegian Research Center for Computers and Law)
Governance Models for Interoperable eID

Dr. Tobias Mahler focussed his presentation on the various governance models and structures implementing eID frameworks in Europe. This spans from primarily state-driven eIDs to different degrees of public-private collaborations, in which both private and public entities collaborate together in the provision and use of eIDs. Rather only than depicting the variety of implementations and governance models in Europe as a challenge (and arguably a barrier) for interoperability, the speaker affirmed that such variety could also be viewed as an illustration of some of the breadth of available options and solutions for the future governance of eID in Europe and beyond. In such context, Dr. Mahler briefly examined some of the existing European eID frameworks including solutions for interoperability challenges, with a particular focus on the Nordic countries.
Further to the existing eId models, the speaker argued that inspiration for the governance of eID in Europe could also be found in existing models used in the context of other electronic identifiers (such as domain names and email addresses, IP addresses, RFID tags, and telephone numbers). These provide evidence for a wide variation of governance models, including some with broad multi-stakeholder participation. Moreover, and as a working hypothesis, Dr. Mahler argued that some of these models may even be used to structure the provision of eID in Europe. Along these lines, a multi-stakeholder governance approach could facilitate competition and contribute to innovation, as evidenced in other sectors. Furthermore, such a governance model could even include intermediaries with a core focus on interoperability, who might be able to address and manage some of the existing inconsistencies between different eID implementations in Europe, thereby allowing sufficient flexibility to facilitate interoperability with other non-European eIDs in the future.

5. Conclusion

By drawing together such a panel of knowledgeable and prestigious legal and policy experts, the workshop succeeded in presenting and debating the idea of a specific and dedicated European eID legal framework, addressing the various legal aspects involved in the construction of such regulatory framework. The presentations delivered at the workshop were particularly original and bold. In effect, all of the presentations went beyond the mere identification of problematic areas and challenges in the field of eID, delivering instead original and concrete solutions to the identified challenges. While conscious of the difficulties and complexities surrounding the implementation of a dedicated eID legal scheme in Europe, the workshop participants agreed on the pressing need to revise the current regulatory framework, contributing to such purpose with a set of innovative and ambitious legal proposals, which

definitively draws us closer to realising the vision of an effective and interoperable electronic identity for Europe.

As a follow-up to the interesting work presented in this venue, this special issue encompasses four important contributions to the eID debate in Europe, authored by the workshop participants.

References

Andrade, Norberto Nuno Gomes de. "Towards a European eID Regulatory Framework. Challenges in Constructing a Legal Framework for the Protection and Management of Electronic Identities." In *European Data Protection : In Good Health ?*, edited by Serge Gutwirth, Paul De Hert, Ronald Leenes and Yves Poullet: Springer, 2012 - forthcoming.

European Commission. "Communication from the Commission - a Digital Agenda for Europe." Brussels: European Commission 2010.

Lusoli, Wainer, Ioannis Maghiros, and Margherita Bacigalupo. "eID Policy in a Turbulent Environment: Is There a Need for a New Regulatory Framework? ." *Identity in the Information Society* 1, no. 2 (2009).

.* * * * *

Cite as: Andrade, Norberto Nuno Gomez de. “Electronic Identity for Europe” Moving from Problems to Solutions. *Journal of International Commercial Law and Technology*, Vol.8 No.2 (April,, 2013)