Privacy Issues in Cross-Border Identity Management Systems: Pan-European Case

Svetlana Sapelova[1,*] and Borka Jerman-Blažič[2]

[1] Jozef Stefan International Postgraduate School, Ljubljana Slovenia
svetka@e5.ijs.si
[2] Laboratory for Open Systems and Networks, Jozef Stefan Institute, Ljubljana Slovenia
borka@e5.ijs.si

Abstract. The paper presents a Pan-European Identity Management System that was developed through the concerted efforts of several European research initiatives, and identifies gaps in the privacy protection mechanisms, which occur because privacy is considered strictly from the EU Data Protection regulation perspective. Privacy protection problems are identified, and measures to eliminate them are outlined on the basis of an extended notion of privacy, which includes aspects of unlinkability, transparency, anonymity and pseudonymity.

Keywords: Identity Management System, pan-European environment, regulation of privacy in the European Union, electronic identification, eID, pan-European eServices.

1 Introduction

The function of a Pan-European IdMs is to enable cross-border recognition of electronic credentials (eID) between the Member States (MS) of the European Union (EU) and to provide an interoperability bridge authorities located in different MS. In this way, foreign eServices (electronic Services) could identify citizens using identity attributes stored directly on the eID (i.e. Electronic Identity Card, Digital Certificate, or other type of credentials, which keep identity attributes) or delivered by Identity Providers (IdP) and Attribute Providers (AP) from another Member State.

Driven by multiple directives and roadmaps numerous research projects have addressed this problem. Embarrassed by its complexity, in particular by the sophisticated and often controversial data protection laws in force in different MS, they focused on the development of architecture that would be consistent with all these laws, and thereby would enable legal transfer of citizens' identity data between MS. This approach considers the protection of privacy in terms of conformity with the Data Protection rules. However, this leaves a gap with respect to the ubiquitous comprehension of privacy. One of the most recent European research initiatives – the

* Corresponding author.

M. Hansen et al. (Eds.): Privacy and Identity 2014, IFIP AICT 421, pp. 214–223, 2014.

STORK European Project [22] has developed a system in order to demonstrate the feasibility of cross-border eID recognition. In this paper we review the system and argue it suffers from multiple privacy protection gaps.

The paper is organized as follows: objectives of the Pan-European IdMs and related EU initiatives are presented in Chapter 2, Data Protection laws and the extended notion of privacy we use to analyze the system are reviewed in Chapter 3, architecture of the Pan-European IdMs is presented in Chapter 4, and the privacy analysis of the system is in Chapter 5.

2 Towards a Pan-European IdMs

The need to build a Pan-European IdMs has been emphasized by the European Commission (EC) with an objective to facilitate interaction between EU MS. Numerous initiatives [9], [3], [5], [14], [19], [20] driven by EC directives and roadmaps [1], [3], [7] have contributed to research and development in this field. The original proposal focused on the promotion of the cross-border eID recognition for eGovernmental (eGov) services. That would allow citizens to use foreign eGov services with electronic credentials issued either by their home countries or any other EU Member States. For instance, a citizen from Spain would be able to pay electricity bills via Italian eGov service, that would recognize a Spanish eID. Services enabled for cross-border communication would send identity attribute requests to citizens' native countries via the Pan-European IdMs system. The system will contact appropriate IdPs and send back highly reliable identity information from governmental and non-governmental registers. Currently no operable solution exists. The only prototype has been built by the STORK research initiatives (Secure Identity Across Borders Linked) [19] based on studies conducted by IDABC (stands for Interoperable Delivery of European eGov Services to Public Administrations, Businesses and Citizens) [5], a program launched in 2004 to promote the building of the cross-border IdMs for eGov services. STORK, launched by the EC in 2010, embraces not only governmental but also other spheres of life (eUniversity portals, eLearning platforms, eBank, and other services). The system developed within the project scope has been tested by several pilots. STORK is now in its second phase named STORK2.0 [20] that pursue the goals to extend the number of services participating in the cross-border collaboration, increase the number of identity attributes recognized across borders, and involve private service providers to collaboration.

The following use case illustrates a functional scenario of the STORK Pan-European IdMs:

> *A student from Italy wants to apply for Erasmus exchange at a Spanish university (eUni). In order to get identified by the service as an eligible participant, the student should provide the name of his home university, year of study, and a proof of a student status. This data is managed by the IdMs of his home university in Italy (homeUni). To collect the data eUni redirects the student to his homeUni IdMs via STORK IdMs, where he is identified with his*

home credentials, collects necessary identity attributes from the homeUni database and sends them back to the eUni via STORK IdMs. Because Italian and Spanish IdM systems have enabled interoperability and established mutual trust in advance, Spanish eUni grants access based on the attributes received from the homeUni.

3 Privacy Regulations in the Pan-European Environment

3.1 Privacy Perspective

EU data protection rules are delivered in the form of directives manifesting the legal notion of privacy [11], which must be respected by all Member States. The main EU directive on Data Protection is Directive 95/46/EC, the Data Protection Directive (DPD) [8], which regulates the transfer of Personal Identifiable Information (PII) [16] within and beyond the EU. National data protection laws in all EU Member States were harmonized with the DPD [8]. Because the STORK system serves for the transfer of personal identity data, it becomes a subject to the DPD rules. The Data Protection principles laid down by the DPD:

1. Personal data is only processed once the citizen gives unambiguous consent.
2. The purpose of data transfer must be explicitly specified.
3. The amount of data released to the service should be minimal.
4. The transfer of National Identification Number (NIN) is a matter of special concern. It must be processed according to the national legislation.
5. Respect the right of an individual to access his/her personal data.
6. Ensure the appropriate technical and organizational measures to protect data from unauthorized access, disclosure and loss.
7. There should be at least one supervising authority monitoring the personal data handling within the MS.

Every MS interprets and applies instructions laid down by the DPD in its own way. Complying with all local data protection laws is particularly challenging due to their heterogeneity and incompatibility. Some of the most challenging issues are: controversial regulations about the transfer of NINs (some countries allow the cross-border transfer of NINs, while others do not [15]), different amount of NINs used for the identification of citizens (single or multiple, sector-specific [15]), different obligations for the personal data processing (e.g., Austrian Data Processing Register must be notified of each data transfer and application, while Denmark does not require any notification [15]), and different regulations about data sharing between public administrations (some countries explicitly allow data sharing, if it complies with a specific law, while other countries have special authorities authorized to issue the data sharing permissions [15]).

3.2 Extending the Notion of Privacy

Although the adherence to all data protection regulations ensures the legitimate handling of data by an information system, it is not sufficient to cover all implications of privacy [10]. That is, with respect to eID Identity Management, protection and management of electronic identity are not addressed by legal regulations, thereby leaving room for interpretation [4]. Unlinkability, transparency, anonymity and pseudonymity were assumed to be of great importance for privacy protection in Identity Management [4], [24]. They manifest user control over personal data by adding user-centricity aspect to the system design. The paper uses this extended notion of privacy to analyze the privacy protection implications within the Pan-European IdMs.

We also refer to the recent Data Protection Regulation Proposal [25] that will soon replace the current DPD. We recap new elements introduced by the Proposal and recognize their impact on the identified privacy issues.

4 Architecture of the Pan-European Identity Management System

The biggest challenge in the use-case implementation is to comply with all data protection principles mentioned in the previous section. It was assumed that the following functional requirements derived from the principles were the most relevant ones for the system in question:

1. Built-in citizens' consent is the core of every transfer process.
2. Manage adherence to the data minimization principles.
3. Clearly inform the user about the purpose of the data transfer and the name of the data receiver.
4. Perform the data transfer only if the transfer complies with the legal regulations in the MS owning the data.
5. Implement appropriate security measures to protect the transferred data against unauthorized disclosure, access, or eavesdropping.

Figure 1 illustrates the architecture of the Pan-European IdMs for eGov delivered by IDABC and approved by the European Commission [13]. It is based on proxy services (PEPS), which function as gateways between the national eID IdMs, mediating the flow of data between MS. Such approach adapts to the heterogeneity of local data protection laws by hiding details of data handling behind the national gateways. Each MS is free to decide what identity attributes can be released and what eID IdMs technology to deploy. Because the Pan-European IdMs is placed on the proxy position between MS, not all data protection principles are applicable. Table 1 shows the relation between the data protection principles and the two types of data handling (cross-border transfer and data collection from the local source before the cross-border transfer) with respect to the described architecture.

So far, the PEPS-based architecture of the Pan-European IdMs is the state-of-the-art in the field and STORK project use it to design the system.

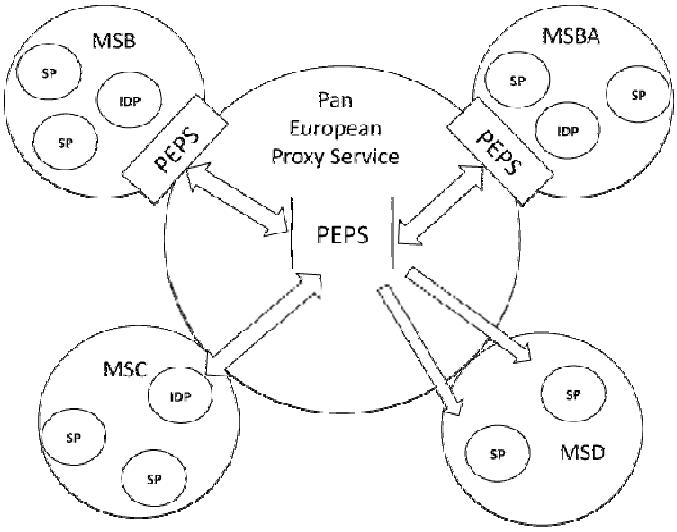

Fig. 1. Architecture of the Pan-European IdMs proposed by IDABC (Source: [13])

5 Privacy Issues in Cross-Border IdMs

This analyses privacy and identifies privacy breaches in the STORK Pan-European IdMs. It is impossible to perform an ubiquitous analysis of such a complex system based only on the scope of pilots; thus, we also review privacy with respect to the possible scenarios likely to occur once the system is pushed to its logical extreme.

5.1 The Loss of Control over Identity Data

The lack of control over the personal identity data in the eID IdMs has been identified as an issue long time ago [4], [21]. Some of the reasons were identified during the system review:

- The data handling mechanisms used by the system lack transparency
- In the light of emerging technologies the EU regulations get obsolete

The cross-border eID recognition catalyzes ubiquitous adoption of the eID identification and thereby creates a threat to privacy. The Pan-European IdMs amplifies problems of eID IdMs at the national level and propagates them to the cross-border context. Missing transparency masks data handling mechanisms and causes unawareness in legal regulations that apply to the system. Although the Pan-European IdMs obtains consent before it transfers identity data, it does not inform users about the legal aspects of the process, nor obliges the SPs to provide such

information. It is necessary to inform users about the legal regulations in the MS that receives their identity data; having accepted these regulations, users should give their explicit consent.

Table 1. Relations between data protection principles and data handling types

	Cross-border data transfer	**Data collection within MS**
Unambiguous consent	PEPS obtains consent from users	Local IdMs infrastructure obtains consent
Purpose of data transfer	PEPS informs about the purpose of the data transfer	User is informed by the local IdMs infrastructure
Data minimization	X	Responsibility of the local eID IdMs
Process NINs according to the national laws	X	Responsibility of the local eID IdMs
Right of an individual to access his/her personal data	X (PEPS does not store any identity data)	Every MS implements it at the local level
Data protection	Protect data transferred between PEPSes	Protect data handled by the national eID IdMs
Supervising authority	X (no authority in cross-border contexts)	Every MS implements it at a local level

Further research is necessary to develop appropriate technical means to implement this procedure in the most convenient way. The issue has been recognized by the EC and addressed by the new Data Protection Regulation Proposal [25]. In particular, Articles 12, 13 and 14 of the Proposal emphasize the responsibility of data controllers in providing comprehensive information about the purpose of data transfer, the names of data recipients and the period the recipient will store the data etc. By the decision of the STORK project Consortium, the roles of data controllers are assigned not only to the IdPs, but also to the SPs that receive identity data; in this way, the requirements laid down in the above-mentioned articles will be duly fulfilled by all parties, significantly increasing transparency of the cross-border identification procedure, and thereby easing the burden on the Pan-European infrastructure.

Another dimension of the problem emerges when identity data are put at the disposal of third parties; e.g., the cloud technologies. In the light of a growing interest for cloud storages, we can expect an increasing number of providers will use clouds

to deploy their services and data storages. This poses a great risk potential for the privacy breaches [22]. For instance, third parties could monitor data stored on clouds [23], while the legal regulations that apply to the clouds and data handling mechanisms used by them are not clear. Another potential privacy threat is the lack of awareness of security measures employed by the cloud providers. The new Regulation does not explicitly address cloud computing, but refers to issues relevant to the technology such as data breach notification (Article 31), increased enforcement regime against controllers and processors (Article 79), assurance of proper security measures by data controllers and data processors (Article 30) etc. However, a lot of existing difficulties and problems with regards to cloud computing will still remain [26]; clearly, they will have to be carefully considered by all the involved parties when pushing the pan-European IdMs to the extreme.

5.2 Linkability by Default

The same NIN is used for identification purposes via the STORK Pan-European IdMs, leaving the possibility to link users' identities across different contexts. Furthermore, there is no data minimization compliance control in place. In order to tackle this issue, the STORK Consortium proposed the encryption of NINs before their cross-border transfer, and devised a NIN transformation scheme [18], however, the employment of the scheme is left to the discretion of every MS. Currently, every MS that legally allows cross-border transfer of simple NINs enables identity linkage by different parties. Multiple surveys identified this problem in the context of eID, and emphasized the necessity to adopt the "eID unlinkability" rule "as a must" [4][12], obliging eID IdMs to derive specific identification numbers for every context or service. This would reduce the risk of linkability through NINs, however, members states would have to invest significant efforts into the reorganization of their local eID IdMs. Clearly, the solution still has a long way to go.

Nevertheless, simple NIN proliferation prevention alone will not eliminate the problem of linkability. Identity linkage will still be feasible by comparing the sets of other identity attributes (sometimes referred to as the quasi-identifying attributes). For example, when a student provides a combination of his/her "fist name/last name/date of birth" to an eLearning service and sends the same data through an online application for Erasmus exchange, it is possible to claim with a certain degree of probability that the two sets of attributes belong to the same person. Adherence to the data minimization principle can help reduce the risk [10]. Raising user awareness regarding the linkability issues should encourage them to share only the minimum necessary information. It could be implemented as a feature of the pan-European IdMs that tracks the amount of identity data released by an individual user, alerting him/her about the risk of identity linkage before the transfer of data is launched.

With respect to the issue the new Data Protection Regulation Proposal brought several regulations that have a direct impact on the mitigating the risk of linkability. Thus, Article 23 of the Proposal sets obligations of the controller derived from "privacy by design" principles [2] that address different aspects of protecting Personally Identifiable Information (PII) such as follow the principles of data

minimization, purpose binding, end-to-end security etc. Article 20 concerns the data subject's right not to be subject to a measure based on profiling. Profiling would be allowed only with a consent of users, when provided by law or when needed to pursue a contract. It must not lead to discrimination and should not be based on automated processing.

5.3 Anonymity and Pseudonymity

Because the STORK objective is to enable services to obtain highly trustworthy identity attributes from different MS, such problem statement left the consideration about the anonymous and pseudonymous participation out of the project's scope. However, with regards to the current efforts in providing means for a large number of heterogeneous services to use the STORK system [20] we can expect multiple STORK-enabled services will not require real data to identify users. The case a foreign service, which allow anonymous or pseudonymous participation, receives real identity data must be eliminated. Clearly, the step towards anonymous and pseudonymous participation must be taken by the MS. They have to enable these features in their local eID IdMs. Such approach would facilitate the adoption of anonymity and pseudonymity at the pan-European level. However, considering the current gap in the EU data protection regulations [4], the fastest way towards a solution is by means of the pan-European eID infrastructure that employ the anonymisation and pseudonymisation as additional PEPS functionalities.

6 Conclusion

However, STORK has demonstrated that interoperability by means of a pan-European IdMs is technically feasible, the system suffers from significant privacy protection gaps. Although the view of privacy as an implication of the Data Protection regulations is a prerequisite for a legitimate cross-border identity data transfer, it leaves a lot of privacy-related aspects out of scope. In our analysis, we identified privacy protection problems of the pan-European IdMs, using the extended notion of privacy that embraces transparency, linkability, anonymity and pseudonymity. We argued that the level of privacy protection provided by the pan-European IdMs depends not only on privacy protection mechanisms employed by the system itself, but also on the mechanisms provided by the local eID IdMS. The lack of such mechanisms is caused by insufficient EU Data Protection regulations, and inadequate attention to the problem from the MS. Clearly, the problem must be addressed from legal and technical perspectives. MS should join efforts to enhance technical means for privacy protection of their local eID IdMs and subsequently of the entire pan-European IdMs, while refining implication of privacy from the legal perspective. The recently proposed new Data protection Regulation is a first step with regards to the problem; it addresses important aspects of privacy like security, transparency, unlinkability and user centricity of local eID IdMs that consequently impact entire cross-border infrastructure. However, we' seen a lot of existing problems are out of

the scope of the Regulation. This lays on an additional burden to researchers and requires them to undertake specific measures at the following stages of design and development of pan-European IdMs.

References

1. A Roadmap for a Pan-European eIDM Framework by 2010 (2010), http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf
2. Cavoukian, A.: A Foundation Framework for a Privacy by Design – Privacy Impact Assessment (2011), http://privacybydesign.ca/content/uploads/2011/11/PbD-PIA-Foundational-Framework.pdf
3. Commission of the European Communities: i2010 eGovernment Action Plan, Brussels (2006), http://europa.eu/legislation_summaries/information_society/strategies/l24226j_en.htm
4. de Andrade, N.N.G.: Towards a European eID Regulatory Framework, Challenges in Constructing a Legal Framework for the Protection and Management of Electronic Identities. In: Gutwirth, S., et al. (eds.) European Data Protection: In Good Health? (2002)
5. Document on IDABC - Interoperability Activities, http://ec.europa.eu/idabc/en/document/5319/5883.html
6. European Commission, How does the data protection reform strengthen citizens' rights? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf
7. European Union (EU), Directive 2006/123/EC of the European Parliament and of the council on services in the internal market. Official Journal of European Communities of 23 November 1995, No L. 376, 36 (1995)
8. European Union (EU), Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data. Official Journal of the European Communities of 23 November 1995, No L. 281, 31 (1995)
9. FIDIS, Future of Identity in the Information Society, http://www.fidis.net/
10. Hansen, M.: Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals. In: Camenisch, J., Crispo, B., Fischer-Hübner, S., Leenes, R., Russello, G. (eds.) Privacy and Identity 2011. IFIP AICT, vol. 375, pp. 14–31. Springer, Heidelberg (2012)
11. Jori, A.: Data Protection Law – An Introduction. Privacy and privacy protection (2007), http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Privacy
12. Lusoli, W., Maghiros, I., Bacigalupo, M.: eID policy in a turbulent environment: is there a need for a new regulatory framework? European Commission Joint Research Centre (2009)
13. Majava, J., Graux, H.: Common specifications for eID interoperability in the eGovernment context, eID Interoperability for PEGS. Technical Report, IDABC eGovernment eServices (2007)
14. Modinis-IDM, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi
15. Otjacques, B., Hitzelberger, P., Feltz, F.: Identity Management and Data Sharing in the European Union. In: 39th Hawaii International Conference on System Sciences (2006)

16. Personal Identifiable Information, http://en.wikipedia.org/wiki/Personally_identifiable_information
17. Stefanova, K., Kabakchieva, D., Nikolov, R.: Design Principles of Identity Management Architecture Development for Cross-Border eGovernment Services. Electronic Journal of e-Government 8(2), 189–202 (2010)
18. Stern, M.: D5.8.3d Security Principles and Best Practices. STORK Deliverable (2011)
19. STORK, Secure identity across borders linked, https://www.eid-stork.eu/
20. STORK2 – Secure identity across borders linked 2.0, https://www.eid-stork2.eu/
21. Strauß, S.: The Limits of Control – (Governmental) Identity Management from a Privacy Perspective. In: Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R., Zhang, G. (eds.) Privacy and Identity Management for Life. IFIP AICT, vol. 352, pp. 206–218. Springer, Heidelberg (2011)
22. Svantesson, D., Clarke, R.: Privacy and consumer risks in cloud computing. Computer Law & Security Review, 391–397 (2010)
23. Whittaker, Z.: Yes, U.S. authorities can spy on EU cloud data. Here's how, http://www.zdnet.com/yes-u-s-authorities-can-spy-on-eu-cloud-data-heres-how-7000010653/
24. Zwingelberg, H., Hansen, M.: Privacy Protection Goals and Their Implications for eID Systems. In: Camenisch, J., Crispo, B., Fischer-Hübner, S., Leenes, R., Russello, G. (eds.) Privacy and Identity 2011. IFIP AICT, vol. 375, pp. 245–260. Springer, Heidelberg (2012)
25. European Commission, Proposal for a Regulation of the European Parlament and of the Council, on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels (2012)
26. Marchini, R.: Cloud Computing Under The European Commission, Proposed Regulation To Revise The EU Data Protection Framework. In: World Data Protection Report, vol. 12, Bloomberg BNA (2012)