Koulolias, V.; Kountzeris, A.; Leitold, H.; Zwattendorfer, B.; Crespo, A.; Stern, M., "STORK e-privacy and security"
5th International Conference on Network and System Security (NSS), 2011, pp.234-238
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6060006&isnumber=6059944

STORK e-Privacy and Security

V. Koulolias, A. Kountzeris
Gov2U
Athens, Greece
info@gov2u.org

H.Leitold, B. Zwattendorfer
EGIZ, eGovernment Innovation Center
Graz, Austria
Herbert.Leitold@egiz.gv.at,
Bernd.Zwattendorfer@egiz.gv.at

A. Crespo
Atos Origin, Atos Research & Innovation
Madrid, Spain
alberto.crespo@atosorigin.com

M.Stern
Approach Belgium
Louvain-la-Neuve, Belgium
marc.stern@approach.be

Abstract— **The paper focuses on the legal, data security and privacy issues of the STORK (Secure idenTity acrOss boRders linKed) infrastructure and aims (a) to summarize the main findings and (b) to identify key points that the STORK consortium and stakeholders need to resolve in order to make the STORK security and privacy framework more robust, with the ambition to contribute to more strategic and far-reaching road-mapping and decision making in Europe in the field of electronic identification and authentication. Our findings are based on the roundtable discussion with experts and other stakeholders on the privacy and security legal challenges associated to cross-border use of national authentication solutions within STORK pilot projects.**

Keywords; STORK, Privacy; Authentication, Data Security; EU Cross-border Electronic Identification, eID

I. Introduction

Privacy and data security challenges are associated primarily to the privacy of the citizen, via the unwanted disclosure of personal information and its subsequent misuse, as happens with online identity fraud. Insofar as privacy and security issues threaten fundamental citizen rights, STORK addresses them in the context of cross-border eServices it enables. Privacy risks can affect the various eID (electronic Identity) schemes' degree of usage and decrease their popularity, making enforcement of any obligations more difficult. Good management of such risks relates to both the identification of potential impacts resulting from an exposure of information assets to loss, theft or destruction, as well as the definition of protection mechanisms that will deliver a reasonable assurance that information is effectively protected and that the residual risk can effectively be accepted by individuals and/or organizations.

Addressing privacy and data security issues in the light of these risks is of the utmost importance in order to create the necessary trust in the users of STORK-enabled cross-border eServices in the context of a future single European electronic identification and authentication area.

This paper addresses the mentioned privacy and security challenges by identifying STORK goals in relation to them (Section II) and by explaining STORK's comprehensive approach to privacy, security and data protection (Section III). In Section IV the main findings on key relevant aspects are presented together with STORK choices for each of them (exchange of national identifiers, user centricity and consent, data minimisation and storage, information security in IDM (Identity Management) systems, certification and legal liability/accountability). Finally, section V addresses the key question of implementation of a trust framework model listing possibilities that require further exploration in the near future.

II. Goals and Challenges for STORK

A major goal of STORK is to create trust and consensus on data protection and other privacy and security issues (such as security level compatibility) between European States in order to win acceptance and recognition for STORK's specific electronic IDM solutions amongst the eID community in Europe and beyond. The security of STORK IDM systems and respective communications requires the development and implementation of consistent policies to ensure confidentiality and integrity of identity data stored and exchanged by participants across private and public systems and networks, as well as across sectors.

Additional to privacy, legal liability and security, the key challenge is to successfully deal with regulatory complexity and turn regulatory obligations into an enabler rather than a barrier to eID interoperability across European borders. Considering that STORK is a flagship for European e-Government and by proving that pilot services delivered across borders can make a significant difference to citizens, businesses and administrations, STORK has the potential to create substantial demand for key enablers such as electronic identification and interoperability; for instance, by providing common pan-European privacy and security mechanisms to foster the necessary trust between all parties involved. The above issues pose a set of legal and security challenges, which also arise from the analysis of the legal provisions pertaining to authentication in the various Member States of the European Union (EU) [1] and the proposed Security Environment [2].

III. STORK PRIVACY AND SECURITY APPROACH

STORK's privacy, data protection and security approach is based on a strong architecture; on the definition and application in practice of a set of common (valid at pan-European scope) security QAA levels (Quality Authentication and Assurance levels) and the adoption of SAML 2.0 (Security Assertion Markup Language) protocol for identity information exchange. Moreover, STORK employs a user centric approach for addressing privacy issues with respect to user control of personal data.

A. Architecture

STORK acts as a key enabling agent for cross-border electronic identity processes. STORK architecture encompasses two existing models and enables their mutual interoperability. Each model has its own advantages and limitations; for STORK neither one can be considered superior to the other. It is worth noting that STORK architecture builds on and extends previous work on the field of eID interoperability such as IDABC's (Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens) European Interoperability Framework (EIF) and acknowledges and incorporates pre-existing national eID infrastructures and schemes. STORK architecture can be federated by means of national gateways or implemented in a fully distributed way, integrating the various identity tokens and assuming direct communication between the citizen and the service provider with no intermediaries as shown in Fig. 1.

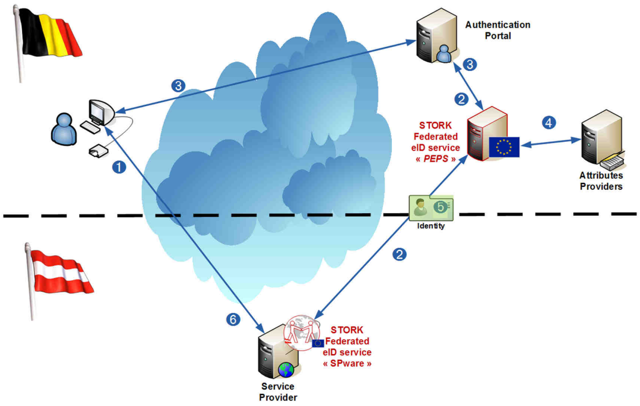

Authentication Portal
3
3
2
STORK Federated eID service « PEPS »
4
Attributes Providers
1
5
Identity
2
6
STORK Federated eID service « SPware »
Service Provider

Figure 1. STORK federated architecture

B. QAA model

Existing electronic authentication and identification mechanisms across Member States (MS) are often heterogeneous and each application makes its own design decisions leading to a large variety of mechanisms effectively implemented without coordination i.e. pin code, passwords, PKI (Public Key Infrastructure), smartcard, etc. Such a situation results in high implementation costs, recurring charge to maintain and operate the authentication processes and difficulties to interconnect systems.

STORK has defined a common model and recommendations for assurance level mapping, to determine the Assurance Level provided by each Member State administration (service) in a cross-border context (STORK QAA) necessary to increase trust and achieve interoperability. Four quality assurance levels (no, low, high, or substantial assurance) have been defined, as shown in Fig. 3. In defining the four QAA assurance levels, based on a descriptive approach of underlying registration and authentication phase processes, STORK took into account several organizational and technical factors; therefore, a set of requirements has been defined for an authentication process to fit a specific level (mapping). The QAA model assesses the overall assurance level of each MS to an authentication scheme (including registration or enrolment and provisioning or authentication). This model aims to guarantee the correct mapping of MS eID authentication levels onto a common QAA.

Standardised quality measures and correct mapping of the different QAA levels is expected to improve the confidence of the service providers and the citizens. It allows using a unified approach and semantics to communicate among member states with respect to authentication processes, the direct comparison of the quality of such processes and offers the same opportunities to equally QAA rated authentication processes.

Therefore, it is necessary that all MS implement the necessary mapping of the national eID solutions onto the common STORK QAA model defined for interoperability. In the STORK project, the correct interpretation of the QAA levels by service providers in the participating MS is assured by close links between real pilots and providers.

C. Protocol for identity information exchange

The SAML v2.0 federated identity protocol for identity information exchange has been chosen considering its widespread use in several MS, implemented and extended with proprietary metadata by STORK, as shown in Fig. 2.

The protocol representation shows that all actions are carried through the citizen's browser. This integrates smoothly with the "user centric approach" employed by STORK (see next section). All messages exchanged (both requests and responses) are digitally signed and also carry QAA Level information.

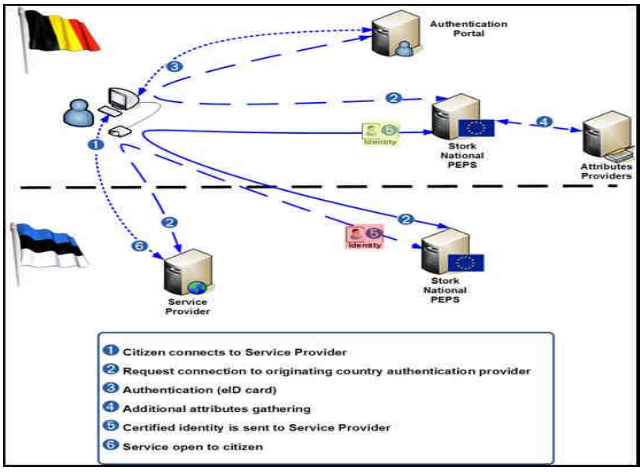

Authentication Portal
3
2
1
5
Identity
Stork National PEPS
4
Attributes Providers
2
6
Service Provider
5
Identity
2
Stork National PEPS
1 Citizen connects to Service Provider
2 Request connection to originating country authentication provider
3 Authentication (eID card)
4 Additional attributes gathering
5 Certified identity is sent to Service Provider
6 Service open to citizen

Figure 2. Federated Identity (SAML 2.0) protocol

D. User centric approach

STORK employs a user centric approach for addressing privacy issues with respect to user control of personal data. This approach lets users choose what personal data to disclose under various conditions and which credentials to present in response to authentication or attribute requests; instead of relying on the vendor-to-vendor systems integration and trust contracts of federation, service providers or relying parties authenticate a claimant by relying on the identity services of an identity provider of the claimant's choice.

In order to enforce a user centric approach, STORK asks unambiguous consent of the user, as meant in Article 7(a) of the Data Protection Directive (1995/46/EC) [4]. This requirement:

- Does not present a problem when the data is disclosed by the claimants themselves.
- It is also not a problem when data can be obtained from a certificate presented by the claimant (for instance, taken from a certificate on a smart card used by the claimant). The attributes that are relevant to the STORK service (e.g. the name) are well standardised.
- May present a problem in some cases because certain MS do not allow the use of national certificates & other identifiers across borders.

IV. Key Findings and Decisions

The Data Protection Directive (1995/46/EC) has a direct bearing on the STORK project because most of the data exchanged in citizen-government interactions are to be considered personal data. This means that personal data (including attributes of the claimant) may only be processed if the requirements of Article 7 of the Directive are met.

A. Use and exchange of national identification numbers and other identifiers

The use of national identification numbers by a number of member states (such as Estonia, Germany and the Netherlands) presents a challenge. Article 8(7) provides that MS determine conditions for use for national identification numbers and other identifiers. In most countries, the use of these numbers is restricted and regulated by law. This in effect means that they cannot be processed in cross border e-Government interactions, which include storage. To make things more complicated, the use of such persistent (unique) identifiers is not allowed in certain MS such as Germany.

Therefore, as (national) ID numbers may generally not be used across MS borders, there are two major legal implications [3]:

- The legal status of digital certificates used for authentication purposes - if you cannot certify the attributes it is very difficult to identify who is the claimant.
- The use of identifiers across Member States – there is no common legal framework across the EU.

For certificates used in the context of STORK's pilot applications (that may include national ID numbers), the solution proposed by STORK is the use of opaque (i.e. unstructured with no semantic meaning to its value) and transient identifiers with the following characteristics.

- Opaque and transient identifiers
  - √ E.g. one-way encrypted value
- Session-based
- Service-context based or country-specific identifiers: Each Service Provider (SP) has its own unique identifier (e.g. university, or a private company). Then user will keep a specific identifier for each service and does not have to share an identifier from one service with the other. This is obtained by using national number derivation, without any storage of these "mappings".
  - √ Different per country, sector, institution, application
  - √ Original number only recoverable by Government

Processing and rules that potentially derive from national identifiers need to consider the territorial principle of the data protection directive – the applicable law is determined by the national law where the data controller is established.

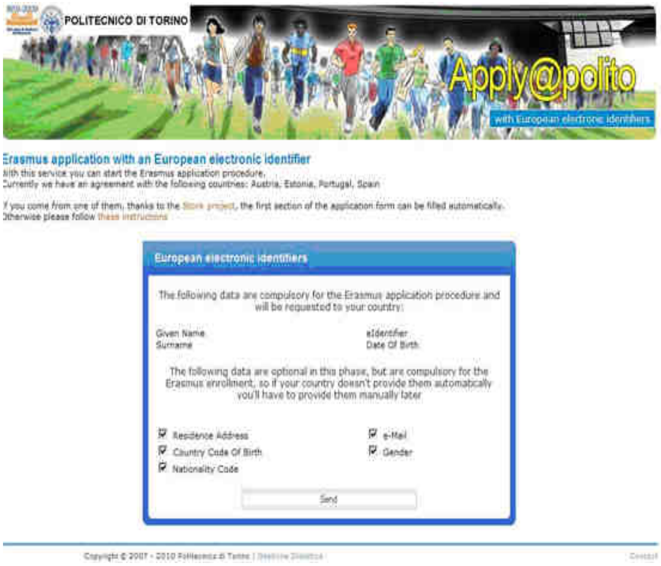
B. User centric identity management and user consent implementation

STORK is entirely user centric and aims to provide all the tools that are required to fulfill every MS's respective needs. The proposed user centric solution relies on user consent (as the only 'general enough' basis valid across MS on data processing legitimacy) and ensures that individuals have total control over how their personal data is obtained and used. The proposed user-centric solution offers the following features:

- Privacy declaration is available at the user interface level.
- The user will always have to give consent for the process to go through – in some few cases they may have to actually sign but that depends on the requirements of each Member State.
- Confirmation is performed in the PEPS (Pan European Proxy Service) and it is provided before leaving the country.

An example of STORK interface for such citizen consent as shown in Fig. 3.

However, for eID data there is currently no clear legal framework about personal data interchange between MS. By relying on user consent rather than on a solid legal basis, STORK has chosen one option offered by the Data Protection Directive (Article 7) that provides a sufficient condition for legitimacy. Eventually, a Europe-wide clear legal framework is necessary for defining the user consent process.



Erasmus application with an European electronic identifier
With this service you can start the Erasmus application procedure.
Currently we have an agreement with the following countries: Austria, Estonia, Portugal, Spain

If you come from one of them, thanks to the Stork project, the first section of the application form can be filled automatically.
Otherwise please follow these instructions

European electronic identifiers

The following data are compulsory for the Erasmus application procedure and will be requested to your country:

Given Name	eIdentifier
Surname	Date Of Birth

The following data are optional in this phase, but are compulsory for the Erasmus enrollment, so if your country doesn't provide them automatically you'll have to provide them manually later

☑ Residence Address	☑ e-Mail
☑ Country Code Of Birth	☑ Gender
☑ Nationality Code	

Send

Copyright © 2007 - 2010 Politecnico di Torino | Gestione Didattica

Contact

Figure 3. Example of STORK consent form

As a result of the above legal considerations, the final decision on how to implement user consent is not reached yet. STORK should still consider whether the proposed user consent approach is grounded on legal processes:

- Via website: The data is provided by the user into an online form on the service provider's website. The data is validated by the service provider at the appropriate data controller in another MS based on the user's consent. In a practical workflow, the SP contacts the attribute provider authority in order to access the claimant's ID attributes that are needed for an authentication/ registration process. In this case, there has to be a legal relationship between these entities, and the best place to obtain the user's consent for the attribute transfer might be at the attribute provider authority (or the responsible government actor). This authority will immediately provide the identity attributes after having obtained the consent. Attributes may only be obtained for very specific reasons communicated to the user as per data protection's principles of data minimisation and proportionality. Processing of personal data should additionally be limited to a specific timescale (i.e. until the purpose for which personal data were requested is fulfilled or ceases to exist).

- Direct user interaction: A system of user control which is quite different in that the information is always provided by the owner of that information. In a practical workflow, it will be information sent by the users' computer (the data will be stored on the users' computer, signed by the user and sent to the SP), so in effect it is always the user sending eID data and attributes to the SP. This is very important because otherwise we face the problem of one server sending information to another (depending on the specific MS and/or cross-border interaction this might be unavoidable but otherwise legal). In the direct user interaction model there is no direct connection between one server and another; one public admin server cannot send attributes to another directly, even if the user gives consent. The process always has to go through the user.

In December 2010, STORK and Art. 29 e-Government Subgroup explored in detail aspects like the PEPS model, the approach to user consent and control, applicable law (i.e. territorial principle), traceability aspects (hashed logs, retention periods), security (self-assessments, accreditation/certification), identifiers, requirements for special categories/sensitive data (beyond STORK), etc. STORK sought advice from Article 29 on whether the intermediary role of the PEPS component should be considered to fall under data controller or data processor categories (or a combination of both).

C. *Data disclosure and storage*

When the deployment of the STORK architecture is fully distributed, no data is transmitted to other parties than the SP.

There is no storage of personal data in PEPS either; the PEPS do not store any attributes. The PEPS is a stateless server, once the transaction is completed, the data is deleted from memory. Some technical security logs may be held, but no citizens' attributes whatsoever are stored in the servers or in those logs.

Minimal data disclosure is supported:

- Only needed data should requested; there is no need to ask all attributes.

- The citizen is always in charge of the step to explicitly accept to send the attributes asked by a service provider.

- A SP has the possibility to ask optional attributes. In this case, the user has the choice to send them or not.

- Some "derived" attributes are available as a data protection and minimisation mechanism. An example is the possibility to request a check of the age ("Is the citizen older than 18?"). In this case, only "yes/no" is sent, not the exact age.

D. *Information security*

Data security requires the development and implementation of consistent policies to ensure confidentiality and integrity of identity data stored and exchanged by participants across private and public systems and networks. Furthermore, compliance of systems applying such policies to national and European regulation should be enforced and assessed. The following are some of the discussion issues inherent to ensuring effective security:

- Major challenges relate to the need to minimise the impact of the disruption or corruption of an IDM system on any other services that may be dependent upon it. Consistent security policies that can be applied across all components of the services will need to be developed and implemented.

- In the case of sensitive personal data, security concerns are especially relevant. Auditing controls may be useful, including automated enforcement of user roles and rules. Developing processes and procedures to address the possibility of a data breach will also require attention.

- Another important consideration will be to ensure that the security of IDM systems is rigorously maintained in all public and private components. Audit controls can help to ensure that the security measures in place are operating as intended. Likewise, regular appraisals can help ensure that the security of the IDM system is appropriate and fit for the purpose.

A thorough security assessment was explicitly conducted by each participating MS according to agreed rules and implementation of STORK´s security levels were re-examined from a technical viewpoint to answer several questions; e.g. is SAML sufficient to secure citizen's data for transfer? Is the model proposed sufficient to address everyone's needs?

E. Certification legal liability and accountability issues

Certification accountability and legal liability issues arise from invalid certificates and inaccuracy of the information contained in a certificate (smart card based or soft certificate or provided by the user) for QAA3/4 eIDs. Some member states use Qualified Certificates (QC) for their eID's, while others don't. This may lead to difficult liability issues because the liability for damage caused to any entity or legal or natural person who reasonably relies on that certificate as regards the accuracy and completeness of all the information in the certificate, in the case of QC's rests on the Certification Authority that issued the certificate, whereas this is more complicated for non qualified certification-service providers; these are likely to have provisions (waiving) regarding their liability in their terms of service. Because there are potentially many certification service providers this may lead to a complicated mesh of different liability regimes.

Liability for damages caused to a legal entity or citizen by invalid or inaccurate qualified certificates is dealt with in Article 6 of the e-Signature Directive [5]. In principle the CA (Certification Authority) issuing qualified certificates is liable for damages arising out of inaccuracy of the information contained in the certificate at the time of issuance. The various member states may have particular arrangements to address specific damages. These provisions should in principle make cross-border verification of certificates possible. In the case where non-qualified certificates are used or available, liability issues in pan-European e-Government services are much more complex and need further analysis.

In the context of the STORK pilots there isn't yet a clearly defined liability and responsibility framework and this issue can also be linked to the clarifications on the roles as data processor or controller (or both) of STORK PEPS by Article 29 Working Party.

V. How to Implement the Trust Model

The major challenge is the definition of a trust framework which provides confidence in the identity management processes and the physical security of the systems. This framework will have to look at:

- Trust considerations: A model to guarantee the correct mapping of eIDs onto a common QAA, considering business requirements. In particular, it remains to be decided on a political level whether the mapping of national security levels to QAA levels shall be performed by a European Authority or whether this should be left to the individual Member States. The model can be further revised to cater for aspects like eIDs issued by the private sector, usage (and limitations to usage) of eIDs across sectors or specifically provisioned services, further elaboration of token robustness and evaluation of QAA required for different services, etc.

- Legal considerations linked to a cross-border service: these include SLAs (Service Level Agreement), review of legal acts like the Data Protection Directive, as well as liability, responsibility and accountability issues. While it seems that the current legal framework may not be sufficient to deal with the new challenges and with issues related to cross-border authentication (MS national legal rules show different approaches regarding security, data protection and privacy), key actions envisaged in the e-Government Action Plan 2011-2015 and the Digital Agenda 2020 will play a relevant role in the short and medium terms.

The key question is "how to implement the trust model". It is proposed that several possibilities should be explored that have been under discussion in STORK:

✓ Bilateral and multilateral agreements among MS covering any issue related to liability/ responsibility/ accountability.

✓ Common Memorandum of Understanding (MoU) for all MS.

✓ Accreditation of the systems by a supranational supervisory/ accreditation authority. Common European legislation regulating all the issues.

References

[1] R. Leenes, B. Priem, C. van de Wiel, and K. Owczynik, "D2.2 – Report on Legal Interoperability" STORK Deliverable, February 2009.

[2] D. Berbecaru et al., "D5.7.1 Functional Design for PEPS MW models and interoperability" STORK Deliverable, February 2009.

[3] B. Hulsebosch, G. Lenzini, and H. Eertink, "D2.3 - Quality authenticator scheme", STORK Deliverable, March 2009.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data**,** Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

[5] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L 013 , 19/01/2000 P. 0012 – 0020.