Leveraging the e-passport PKI to achieve interoperable security for e-government cross border services

Dimitrios Lekkas and Dimitrios Zissis

Department of Product and Systems Design Engineering
University of the Aegean, Syros, Greece
{Dlek, Dzissis}@aegean.gr

Abstract.: Electronic governments across Europe, but also globally, are moving towards increasing participation in democracy by offering services that improve collaboration and effective participation. These initiatives, target at achieving cross border interoperability and scalability, while leveraging existing resources and knowledge, and in doing so overcoming economic, social and environmental challenges. A critical factor to the success of these initiatives, is achieving these goals securely. As an increasing amount of security sensitive processes and data are being digitalized, current electronic government authentication measures are becoming inadequate to meet with the scaling demands. Public Key Infrastructure is identified as the essential architecture upon which security and trust are built, in order to provide authentication, identity verification, encryption and non-repudiation in electronic transactions. Cross border availability of e-government services requires such a security infrastructure to provide a horizontal level of service across all implicated entities. This paper identifies the unique characteristics of a necessary interoperable security infrastructure and towards this goal explores the restrictions of current authentication approaches. Following this, the ability of the electronic passport PKI solution to extend and meet the demands of an interoperable cross border e-id solution is explored, as the requirements of such an authentication mechanism correlate to the characteristics of the deployed e-passport infrastructure. Finally, this paper proposes leveraging the e-passport infrastructure, to build a secure cross border authentication mechanism.
Keywords: Public Key Infrastructure (PKI), e-passport, e-ID, identification, authentication, e-government, e-voting

1 Introduction

Countries and states globally, realizing the benefits that Information and Communication Technologies can offer, by increasing the effectiveness, efficiency [1], interactiveness [2], decentralization, transparency [3], and accountability of delivered services [4][5] have proceeded in implementing electronic governments. These implementations have been guided by a number of initiatives and policies which set the target goals and required development frameworks. Today the field has reached a stage of relative maturity, due to the intense scrutiny that has occurred over recent years, and a change of focus is taking place. Current initiatives are moving away from offering solutions in an asymmetrical method and are building towards electronic governments with strong synergy between them, while achieving high citizen participation, promoting knowledge sharing and achieving economies of scale.

Towards this goal, the Lisbon Treaty, which entered into force on 1 December 2009, introduces a whole new dimension of participatory democracy alongside that of representative democracy on which the European Union is founded [6]. The Lisbon Treaty, enables one million citizens who are nationals of a significant number of Member States to call directly on the European Commission to bring forward an initiative of interest to them in an area of EU competence"[6]. This provision initiates the exploration of electronic participation channels with the capacity to hold the expression of citizen's opinion in a pan European context. It provides an opportunity to bring the Union closer to its citizens

and to foster greater cross-border debate about EU policy issues, by bringing citizens from a range of countries together in supporting one specific issue.

The guiding principles for the implementation of the citizen initiative in the Lisbon Treaty are as follows; [6],

- The conditions should ensure that citizen initiatives are representative of a Union interest, whilst ensuring that the instruments remain easy to use.
- The procedures should be simple and user-friendly, whilst preventing fraud or abuse of the system and they should not impose unnecessary administrative burdens on Member States.

Given the importance of these new provisions of the Treaty for citizens, civil society and stakeholders across the EU, and considering the complexity of some of the issues to be addressed, the Commission launched a broad public consultation with the adoption of a "GreenPaper" on 11 November 2009. Respondents broadly supported the idea of having a common set of procedural requirements for the collection and verification of statements of support, so as to ensure a uniform process across the EU and to avoid organizers having to comply with different rules in each Member State. The possibility of online "signing" was called for unanimously, since it would greatly facilitate the collection of signatures [7]. However, in order to ensure that statements of support collected online are as genuine as those collected in paper format, and that the Member States can check them in similar fashion, the proposal requires that online collection systems should have adequate security features in place, and that the Member States should certify the conformity of such systems with those security requirements, without prejudice to the responsibility of the organizers for the protection of personal data [7].

Although the vision of using digital certificates for the verification and authentication of e-government services deployed across Europe, appears to be commonsense, the inherent perplexities and complexities of the task at hand, are soon evident. Digitally signing a document is a process we have become accustomed to, as it provides for the electronic representation of the traditional signing process. Digital signatures are used to preserve the basic security characteristics of digital documents, such as integrity and authenticity, while acting as the principal verification method of the signer's intended meaning, as expressed in the respective document. The creation of a digital signature cannot be denied as an action (non-repudiation), since it can be algorithmically proven, using cryptographic techniques. But the process of evaluating a digital signatures authenticity relies upon a horizontal support infrastructure that guarantees the uniqueness and originality of the signature, while correlating it to a specific individual (the signer). Cross-border digital signing requires an infrastructure that can provide this service uniformly across borders and services, that at present is not in existence. The vision expressed in the EU Ministerial Declaration of Manchester that "by 2010 all European citizens, businesses and administrations shall benefit from secure means of electronic identification (eID) that maximize user convenience while respecting data protection regulations" today seems to be a utopia. At present, the e-government services themselves are rarely, or not easily, available across borders. Europe currently needs better administrative cooperation to develop and deploy cross-border public online services, including practical e-Identification and e-Authentication solutions [8].

It is vital, that all present and future plans and implementations for electronic democracy build upon the principles identified in these initiatives, which include

- Targeting enhancing participation in electronic democracy [7]
- Providing better services delivered over fewer resources, by optimizing the use of available resources and instruments [9]
- Targeting overcoming existing economic, social and environmental challenges [9]
- Promoting cross border interoperability of services [8]
- Promoting cross border collaboration and scalability [8]
- Encouraging the exchange of best practices between Member States[8]
- Are designed as part of a horizontal security service, so as to ensure uniform conditions of access to e-government services across member states [7]

These principles suggest a design framework for architects, implementers, researchers and stakeholders with recommendations that can assist in decisions regarding deployment choices but also assist in understanding the ambiguities, complexities and requirements of planning, designing and deploying such Information Systems.

2 Electronic Identification and Authentication

At the core of information system security is access control. Access to protected information must be restricted to people who are authorized to access the information. Electronic authentication is the process of establishing confidence in a users identity, electronically presented to an information system [10]. During this process an entity provides an authentication authority with a number or set of attributes that allows for the unique identification of the entity. Authentication mechanisms use any of three types of attributes to confirm a user's identity, something a user knows; something a user has; something a user is. Two or more forms can be combined to achieve a more solid (strong) authentication, referred to as multi-factor authentication.

Today the most common way to authenticate such transactions is by means of passwords, but more secure solutions protecting privacy are increasingly needed [8]. High risk threshold applications, such as electronic government services, services dealing with highly sensitive information, require strong multifactor authentication to ensure protection of data and communications. This need is addressed by electronic IDentification (e-ID) systems. The purpose of eID systems is to provide the means to reliably identify and authenticate citizens remotely over the Internet while provide citizens with signature creation facilities [11]. An e-ID infrastructure is understood as an Authentication Framework that enables individuals to access various e-services offered by government and non-governmental entities, using a single dedicated identity profile and making use of multi-factor authentication techniques. In terms of STORK project "Electronic Identity" is defined as “a collection of identity attributes in an electronic form” [12]. These attributes are combined with smart card technology, digital signatures and a user’s “knowledge” of a pin number to generate multifactor authentication.

The development of e-ID infrastructures varies considerably across Europe. From 2000 onwards, a number of countries have implemented e-ID card projects, with Italy and Finland being the early adopters (2000 and 2003, respectively), Austria and Belgium followed in 2004, the Netherlands and Sweden in 2005, Portugal in 2007, Germany and Poland are currently starting their e-ID card rollout, while a large number of countries are planning deployment[13].

3 Certificates and Public Key Infrastructures

Public Key cryptography realizes the concept of digital signatures; it provides a practical, elegant mechanism for symmetric key agreement; and in combination with smart card technology currently enables the strongest available authentication of involved entities and secure communications. A Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. A PKI infrastructure is comprised of several working units, which can be easily correlated to the required services an e-Id infrastructure is required to provide. PKI deployments include a Certification Authority. This authority, within a PKI, is delegated with the responsibility of binding a specific unique cryptographic key pair to a given identity. The CAs role is to certify the key pair/identity binding, by digitally signing a data structure that contains some representation of the identity and a corresponding public key. This data structure is called a digital certificate. Often PKI deployments include a Registration Authority, which is tasked with confirming the identity of an individual as part of the initialization process, distributing shared secrets to end users, and performing certain key/certificate life-cycle management functions. The concept of National PKI is conceived by a large number of governments, as the de facto infrastructure onto which policies, technology and security can be built upon, in order to provide authentication, identity verification, encryption and non-repudiation in electronic services [13].

It is safe to say that across Europe, all countries are not only at different stages of maturity with regards to deployment of e-id infrastructures and respective PKI's, but also lack a common set of implementation mechanisms [14]. While at a national level the schemes might operate as initially designed, attempting to use e-ID cards to address cross-border function's, has proved to be nearly impossible as these systems are highly interoperable; at a smart card communication level, data access protocols, data definition, algorithms and at a PKI level[11][14].

Identifying the problem, a series of European Union initiatives and frameworks have been issued. Notable examples include the Secure Identity Across Borders Linked (STORK) for Electronic Identities (e-ID), the eID Interoperability for PEGS project, the Pan European Public Procurement Office (PEPPOL) for public procurement and the European Patient Smart Open Services (epSOS) for e-health services [15]. and the European Citizen Card framework. While these initiatives can be considered as steps into the correct direction, unfortunately they are mostly lacking to capture some vital requirements, such as enabling in-card el-gamal signature to achieve scalability such as e-voting etc [16].

Additionally, achieving interoperability of e-ids at a PKI trust level is crucial as the electronic services for identification, authentication and signature creation purposes are based on public key procedures. The validation of these processes requires a level of trust above the end user. This trust requires cross border cooperation, between the Certification Authorities of National PKI's. This certainly requires a common understanding of all identity management issues (legal, technical, organizational). End user certificates, which are stored on the card and link user specific data (unique identifiers, etc.), with the corresponding public keys, are signed with the PKI's root certificate (or an intermediate certificate, which in turn is signed by the root certificate)(Figure 1). If this cross border cooperation is not achieved, it is not possible to effectively validate a citizen's signature, or authentication request successfully [11]. Differences exist either at a policy or functional level, placing serious limitations on cross border availability of these services. Unfortunately in current implementations the notion of trust is not clearly identified and either the researchers do not address it or it is considered as de facto granted.

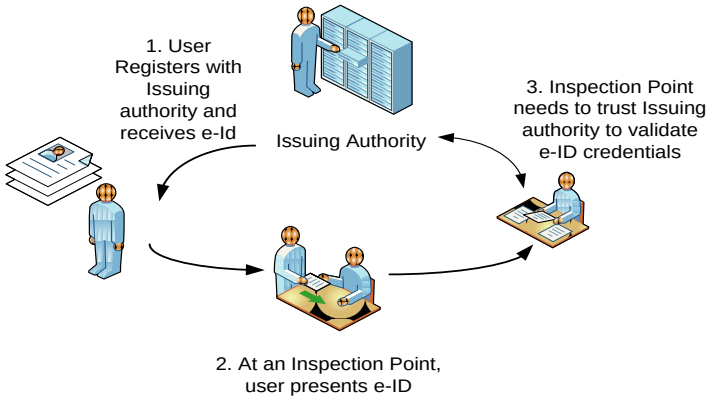

Figure 1 Cross border interoperability requires the validation of e-id credentials at a level higher than the end user

The deployment of a large Public Key Infrastructure, that shall effectively and proficiently escalate into a pan-European Electronic Identification Infrastructure, covering all needs of security for e-Government, is a highly complex task. Such an infrastructure is itself required to be highly-interoperable, scalable and efficient.

Overall, an authentication mechanism, achieving cross border interoperability is required to fulfill a number of requirements,

- Technology compatibility
    - Common Data formats-Semantics
    - Communication Protocol Compatibility
    - Algorithm usage compatibility
    - Card compatibility-Reader Compatibility
- Policy Compatibility
    - Registration procedures and requirements(identity proofing etc)
    - Operational Requirements
- Security Schema Compatibility
    - Common understanding of security risk assessment analysis
    - Common definition of risk assessment criteria, typically combined with a consideration of potential damage in case of incidents; these should be the basis for determining security requirements, i.e. Authentication Assurance Levels;
- Legal Compatibility
    - Privacy & Data Protection legal framework
    - Legal Data Signature Validity
- PKI Compatibility
    - Trust relationships must be established between issuing authorities
    - Deployment architecture compatibility
- Directories must be complex free and achieve high compatibly
- Infrastructure must be able to achieve high scalability to respond to dynamics of user population

4 Leveraging e-Passport Infrastructure

While the research community has been involved in time consuming recursive debates on how to implement a globally acceptable and trusted Public Key Infrastructure, it seems that the e-passports PKI currently deployed in several countries provides a potentially friendly environment for achieving the necessary global trust. Electronic passports, or e-passports, are being issued and inspected across the globe in accordance with International Civil Aviation Organization (ICAO) standards for Machine Readable Travel Documents (MRTD). Every e-Passport has an embedded electronic chip that contains the holder's personal information and photo found in the passport. To achieve interoperability a common understanding between participants on data structures and communications was required. This was achieved in MRTD, as all MRTDs follow a standardized layout to facilitate reading of data on a global basis by both eye readable and machine readable means. In order to increase confidence in the MRTD scheme, the ePassport chip is digitally signed to prevent unauthorized alteration and ensure authenticity. In order to verify a digital signature, border and other authorities need to access the ePassport's public key. As electronic passports are designed to be of maximum use in facilitating international travel, successfully validating these documents at inspection points is critical. That is why it is crucial to share the public keys as widely as possible [17].The aim of this process is to link the passports validity and authenticity back to the issuing authority.

To achieve this, a web of trust is set up between implicated parties. The inspecting entity accepts the e-passport as valid, because it trusts the authenticity of the signing respective authority. Basically, a chain of electronic certificates and signatures is created with one end securely anchored in the authority of the issuing state and the other end securely stored in the respective chip [18]. The validity of these documents is checked by comparing the validity of the implicated certificates, usually at the top of the chain, with the certificate of the country's issuing authority. This validation, requires that the inspection entity has access to the certificate of the respective country, to validate against it, otherwise this process is broken. The ability for any implicated entity, to validate the authenticity of a signature of a third parties certification authority, is critical.

The most important advantage currently offered by the e-passport infrastructure is the established worldwide trust; the e-passport PKI offers a global multilateral framework to verify the entire chain of certificates issued by each country. This is achieved either with country cross certification, or by using the ICAO Public Key Directory (PKD). Technically, a trust relationship is established when a Country

decides to trust the root certificate (the certificate of the CSCA) of another Country. This de-facto trust infrastructure overcomes the basic drawback of the most commercial or closed-groups PKIs. It is critical that e-id infrastructure's leverage this global trust framework, as it provides the required platform for global interoperability at a PKI level. In addition, leveraging the e-passport infrastructure achieves economies of scale and knowledge, according to the requirements set by recent initiatives, (as identified in previous section). A strategic decision for the current implementation of e-passports, is the lack of citizen certificates, in order to facilitate a fast-track implementation and to avoid the complexity of managing client certificates and keys. The X.509 digital certificates, which are issued for the ICAO PKI implementation, are currently restricted only to the authorities issuing the passports (i.e. the hierarchy of Country Signing CA and the subordinate Document Signing CA). Although the e-passport does not contain an X.509.v3 certificate and it is not designed for everyday Internet transactions, it exhibits all-but-one of the characteristics of a typical PKI-enabled smart card, containing a private key and the relevant digital certificate.

The e-passport member states PKIs, follow the standard proposed by ICAO and are deployed in a hierarchical architecture. A hierarchical architecture has been proven under real-world conditions to scale smoothly from hundreds to millions of users [19]; thus achieving the demanded scalability requirement. Trust operates in a hierarchical manner, starting at the country's highest certification authority. At the top of the hierarchy is the Country Signing Certificate Authority, which is responsible for issuing certificates for the subordinate Document Signer Certificate Authority and for cross certification with other national CSCA. The Document Signing CA signs the passport's data, including a public key (Active Authentication key) stored in each passport. Leveraging existing software, procedures and policies, we propose deploying a subordinate CA, the Identification Signing Certification Authority (ISCA), which can be deployed with minimal complexity and cost, and shall be delegated with the authority of issuing end user X509 certificates. This ISCA is deployed as a subordinate CA to CSCA inheriting cross country trust relationships. This enables certificates issued by the ISCA, to be automatically trusted by any other state or country that has been cross certified or has joined the ICAO PKD.

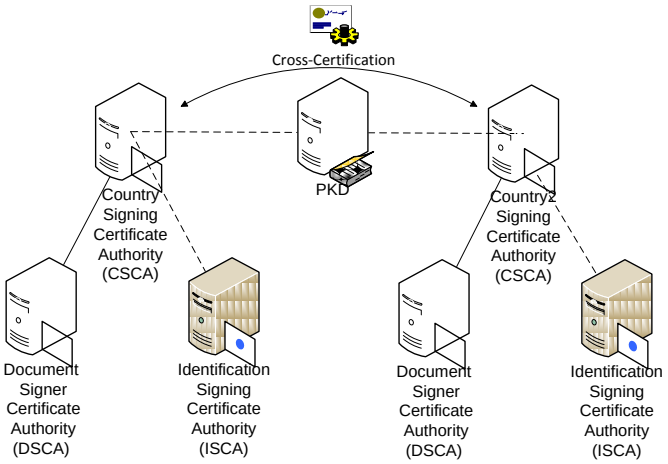

Figure 2 The proposed infrastructure creates a subordinate Identification Signing Certification Authority that shall be delegated with the authority of issuing X509 certificates.

The proposed ISCA can leverage the deployment of the e-passport infrastructure and be responsible for the creation of personal citizen certificates, as hard or soft tokens. Hard tokens offer greatest security, but a number of low security services may require soft tokens to increase process efficiency.

- Personal Certificate- Hard: on smartcard, personal phone
- Personal Certificate- Soft: email, compact disc

- E-Government Services certificate: application certificate

Extending the e-passport infrastructure can address a plethora of previously identified requirements, while adding value to the overall security of e-government. The deployment of the e-passport infrastructure enabled the development of policies and procedures that guarantee strict citizen identification and registration required for a secure e-id infrastructure. These procedures include designing processes such as secure registration, deployments, contingency and recovery planning, and many more. These procedures easily correlate to the required procedures for safe issuance of secure e-ids as they share a common security profile. Leveraging the e-passport infrastructure provides a plethora of additional benefits. Since the ID cards are accepted as travel documents within Schengen States, their profile is required to be in conformity with many ICAO specifications, common to the e-passport [20].

The global e-passports implementation seems to be an attractive PKI establishment, since:

- The passport as a digital identity is issued by governmental authorities, under very strict and reliable identification and issuance procedures for the citizens; due to the standardization of most of this process, member states are interoperable at policy procedures.
- The e-passports and electronic identity documents have common security profiles.
- The technology used throughout the world is compatible and, thus, interoperable. Due to the standardization of the PKI infrastructure it is highly interoperable and scalable, as common deployment models have been adopted across member states.
- High security procedures and operational models were defined during the deployment of e-passports, including the creation of high security facilities for the issuance of e-passports and for the protection of related data. The e-passport requirements are identical to the requirements of an e-id infrastructure at this level.
- A worldwide Web-of-Trust is established through a reliable and secure exchange of countries self-signed certificates.
- The member states legal framework has been addressed to be compatible with the e-passports; thus providing compatibility for e-id cards (registration requirements, policy, digital signatures , etc)
- The e-passport member states PKIs, follow the standards proposed by ICAO and are deployed in a hierarchical architecture. A hierarchical architecture has been proven under real-world conditions to scale smoothly from hundreds to millions of users [19]

Many enterprises currently operate independent directories based on closed propriety protocols. As the number of applications and utilities relying on these directories are increasing, current practices are becoming inefficient. In numerous occasions, electronic communications between unknown entities are staggered due to the lack of authenticity. There is a trust deficit in electronically presented credentials. Relying on information provided by a trusted directory would increase trust in all communication between member entities. The homogenous availability of a trusted directory, easily accessible and highly available overcomes this requirement, enabling stronger and safer e-commerce as it guarantees the validity of credentials of implicated parties. But also on a citizen's side, interaction with web services can be verifiable, as directories contain lists of information of natural but also legal entities. Validating an e-services certificate would thus increase the integrity of communications.

5 Conclusion

Currently, initiatives globally, and specifically in Europe, are targeting at increasing the interoperability and scalability of their services as they are aiming at providing cross border service delivery to their citizens. There is a growing need that stronger authentication mechanisms are implemented and in this direction e-id solutions based on PKI and smartcard technology are explored. A crucial element of e-ID infrastructures is achieving interoperability and scalability at PKI level. An e-ID infrastructure is as strong and as effective as the authentication services ability to correlate an entity's provided credentials with an entity's valid credentials. The validation of these processes

requires a level of trust above the end user. Current PKI deployments lack the ability to address cross border cooperation, as differences exist either at a policy or functional level, arising serious limitations on cross border availability of these services.

In this paper we explore the e-passport PKI deployment, as it provides a potentially friendly environment upon which the necessary global trust is built. The e-passport infrastructure provides a successfully deployed architecture in many countries and states, which exhibits a plethora of required characteristics, that efficiently correlate to the requirements of an e-id infrastructure. At present, the e-passport infrastructure has established a worldwide trust net, offering a global multilateral framework to verify the entire chain of certificates issued by each country. We propose leveraging the existing infrastructure and processes by deploying the Identification Signing Certification Authority as a subordinate to the CSCA, inheriting the global web of trust relationships. The ISCA is delegated with the responsibility of issuing member states natural or legal entities certificates, either in hard or soft format, leveraging the existing infrastructures abilities and knowledge. The e-passport PKI infrastructure can be extended, with minimum complexity and cost to meet the additional demands of an interoperable e-id infrastructure. The proposed architecture provides a common interoperable security platform, while achieving economies of scale and knowledge.

6 References

1. Heeks, R. (2001a). Building e-governance for development: A framework for national and donor action. The University of Manchester, Institute for Development, policy and management information, systems, technology and government: Working papers series Retrieved December 15, 2010 from. http://www.man.ac.uk/idpm/ idpm_dp.htm#ig.
2. DiCaterino, A., & Pardo, T. A. (1996). The World Wide Web as a universal interface to government services. E-Government Act of 2002. Retrieved May 10, 2003, from, http://www.ctg.albany.edu/resources/abstract/itt96-2.html
3. La Porte, T. M., De Jong, M., & Demchak, C. C. (1999). Public organizations on theWorld WideWeb: Empirical correlates of administrative openness. Retrieved December 1 2010, from. http://www.cyprg.arizona.edu/publications/correlat.rtf.
4. Ghere, R. K., & Young, B. A. (1998). The cyber-management environment: Where technology and ingenuity meet public purpose and accountability. Public Administration and Management: An Interactive Journal, 3(1) Retrieved December 1, 2010 from:. http://www.pamij.com/gypaper.html.
5. McGregor, 2001 E.B. McGregor Jr., Web page accountability: The case of public schools, Paper presented at the National Public Management Research Conference, Bloomington, IN (2001).McClure, C. R., & Bertot, J. C. (2000). The Chief Information Officer (CIO): Assessing its impact. Government Information Quarterly, 17(1), 7−12.
6. SEC(2010) 370. (2010). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the citizens' initiative. Brussels.
7. COM(2010) 119. (2010). Outcome of the public consultation on the Green Paper on a European Citizens' Initiative. Brussels.
8. MEMO/10/681. (2010). Digital Agenda: eGovernment Action Plan - what would it do for me? Brussels.
9. EU Ministerial Declaration on e-Government. (2009). Malmö, Sweden.
10. NIST SP 800-63. (2006). Electronic Authentication Guideline. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.
11. Zefferer, T. (AT-TUG). (2010). STORK Work Item 3.3.5 Smartcard eID Comparison. Retrieved from https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1384.
12. Gutierrez, A., & Piñuela, A. (2009). STORK Glossary and Acronyms.
13. Patsos, D., Ciechanowicz, C., & Piper, F. (2010). The status of National PKIs – A European overview. Information Security Technical Report, 15(1), 13-20. doi: 10.1016/j.istr.2010.10.007.

14. Arora, S. (2008). National e-ID card schemes: A European overview. Information Security Technical Report, 13(2), 46-53. doi: 10.1016/j.istr.2008.08.002.

15. IDABC. (2009). Study eID Interoperability for PEGS, Analysis & assessment report.

16. Meister, G., Huhnlein, D., Eichholz, J., & Araujo, R. (2008). eVoting with the European Citizen Card. BIOSIG 2008, 67-78. Retrieved from http://www.ecsec.de/pub/ECC-voting.pdf.

17. ICAO. (2009). Overview- The ICAO Public Key Directory.

18. Hartmann, M., Körting, S., & Käthler, O. (2009). A Primer on the ICAO Public Key Directory. Retrieved from http://www.securitydocumentworld.com/client_files/hjp_pkd_promotion-paper_v1_5_20090520.pdf.

19. HHS-IRM-2000-0011, HHS IRM Policy for Public Key Infrastructure (PKI); Certification Authority (CA), January 8, 2001.

20. Eurosmart. (2008). Position Paper European Citizen Card: One Pillar of Interoperable eID Success. Retrieved from https://www.eid-stork.eu/dmdocuments/public/ecc-position-paper-final.pdf.