Use of ePassport for Identity Management in Network-Based Citizen-Life Processes

Pravir Chawdhry and Ioannis Vakalis

Institute for the Protection and Security of the Citizen
Joint Research Centre, 21027 Ispra (VA) Italy
{Pravir.Chawdhry,Ioannis.Vakalis}@jrc.ec.europa.eu

Abstract. Digital identity management (IdM) for citizen-life processes requires trusted relationship among the service providers and users. Current IdM systems tend to lack the trust component in particular for online transactions. We propose the use of ePassport as a globally interoperable trust token to bridge the gap between offline and online environments. The paper analyses trust attributes of the ePassport and recognizes the extensions required to its deployment in an online IdM for high-value transactions. An architecture is proposed for a network-based IdM system to support three categories of life processes: eGovernment services, high value private services, and eCommerce. The solution is compatible with privacy-enhancing technologies while at the same time creating trusted digital identities and offering users convenience.

Keywords: identity management, online services, trusted identity, privacy.

1 Introduction

Citizens engage in a variety of life processes, managed by public and private sectors, where there is need to provide a proof of identity to participate in the process. In some cases the proof of identity is required only once, in other cases it may be asked repeatedly. Examples of such processes are: banking, social security, international travel, staying in hotels, high-value purchases, car rental, use of credit card, joining private clubs, admission to a school or university, seeking employment, health services, etc.

There are numerous types of identity documents: national identity card, passports, social security card, health insurance card, employer's card, banker's card, driving license, etc. Most of the identity documents, with the exception of the national identity card, are function-specific and context-dependent, even though in practice they may be accepted in other contexts.

The kind of identity-related information offered by identity documents also varies: ranging from facial identity linked to the name of a person, it may also include signatures, date of birth, address, citizenship, medical information, and other personal and biographic data. With the advent of smart cards in the past decade, the ambition of storing a variety of information has suddenly taken a leap. The idea of a multi-function identity card has been mooted but reservations remain due to the privacy risks involved.

M. Bezzi et al. (Eds.): Privacy and Identity, IFIP AICT 320, pp. 122–133, 2010.

Passports are official identity documents intended to facilitate international travel of citizens. However, due to their official status and universality passports are also used and accepted as identity documents with photo-Id in various citizen-based processes other than travel. This is particularly true in the countries where national identity cards are not mandatory, such as Ireland and the United Kingdom.

Electronic passports (or, ePassports) were introduced in the EU in August 2006 as a means of strong authentication for border control. The ePassports store certain biometric data of the bearer on a chip embedded within the passport booklet. In the EU, the biometric data stored on the chip is digital image of the face and from mid-2009, it will also include the fingerprint.

Only authorized readers at EU border control points can access the fingerprint image stored on the chip whereas the facial image and biographical data may be read by any ePassport reader available commercially. With the diffusion of ePassports and related technology, it is quite feasible that in the near future various citizen-service outlets will be equipped with the devices to read and store the biographical data and facial biometric.

In face-to-face interaction, the printed biographic data page of the ePassport can still be used as a photo-Id like the traditional passport. However, to provide a function for network-based identity, it needs to be augmented so that a whole range of trust-based services may be offered in a convenient and uniform manner. This will avoid the need to create a separate electronic identity, detached from the physical realm.

The idea of using governmental tokens as the basis for identity services has been investigated in some countries, with the recent introduction of eIDs. Questions have been raised if eIDs are more appropriate tokens for eCommerce in comparison to ePassport with privacy issues already pointed out.

This paper investigates key issues of trust in a network-based identity infrastructure based on ePassports. The paper is organized as follows. Section 2 presents a brief overview of trust mechanisms in the ePassport infrastructure. In Section 3 we examine key approaches to network-based IdM and identify key requirements for a network-based IdM system. In Section 4 we propose an IdM architecture for deploying ePassports in network-based citizen-life processes characterized by varying degree of risk. We conclude with a discussion of key challenges in Section 5.

2 Trust Mechanisms in the ePassport Infrastructure

There are two types of definition of trust one is social/legislative and the other type is quantitative/mathematical. So the definitions for trust of the first type refer to qualities [11] that the trusted party should possess:

- predictability of the trusted party,
- completion of transactions even in the absence of full knowledge,
- immediate payback of any type is not a strict requirement,
- exposed vulnerabilities are not exploited,
- reputation

Table 1. Trust relationships and constraints in ePassport infrastructure

Infrastructure Perspective	Roles & Constraints		
	Passport Holder	**Issuing State**	**Border Control Post**
IdM role	principal	identity provider	service provider
Trust relationship boot up.	Provides pre-requisites (e.g. feeder documents on his identity) to the issuing authorities.	Establishes the pre-requisites to the trust relationship with the principal.	Establishes the pre-requisites to the trust relationship with the issuing authorities.
Legacy function.	Presents the passport as a traditional booklet to authenticate himself. Doesn't know how the scanned MRZ data is used, shared and retained.	Provides identity through a photo and biographic data on a printed page.	Uses the visual inspection means to check the authenticity of the passport and match the printed photo with the live subject.
BAC minimum scope.	In addition to the printed biographical data, also provides primary biometrics[1] (live facial image) to authenticate himself. Agrees tacitly to allow access his biometric data for the purpose of border control.	Provides facial biometric on a contactless smartcard chip, embedded in the passport booklet. Permits passive authentication to anyone with a suitable ePassport reader. Through ICAO membership, implicitly authorizes other ICAO members right to read their chips.	Uses the MRZ data on the printed page to enable access to the facial biometric on chip. May use visual means or image recognition to do the match between the facial biometric and the subject.
BAC max scope.	No additional action required.	Separately provides a digital certificate to authorized service providers for active authentication of chip data. These digital certificates are not highly protected.	Global scope – Needs certificate of the issuing country to authenticate the validity of data on the ePassport chip.
EAC.	Also provides his secondary biometrics (fingerprints) to authenticate himself. Agrees tacitly to allow access his biometric data for the purpose of border control.	Provides certificates in a hierarchy of identity providers and service providers. Explicit authorization provided only to other EU countries.	Terminal authentication needed: Requires terminals with explicit authority from identity providers via secret cryptographic keys to enable reading of the secondary biometrics.
Organizational model.	National passports / travel documents are recognized internationally as trusted credentials for identity.	National passport issuers as identity providers; implicit authorization to all ICAO states for BAC level trust; explicit authorization to the other EU States for EAC level trust.	No specific steps are required to operate at BAC level; at EAC level, the protection of private cryptographic keys is a major responsibility. Mutual recognition of passports as trusted identity.

[1] According to the EU passport specification [9] ace is the primary biometric, fingerprint and iris are secondary.

In the quantitative models of trust, a special category of logic representing belief is used as a base [12] and the trust levels are expressed in terms (e.g. high, medium, low) or in number scales (e.g. 1-5).

The European ePassport infrastructure is specific to border control applications and is designed for wide-scale interoperability. It consists of two trust levels. Level 1 trust is built in a mechanism known as Basic Access Control (BAC) designed to offer global interoperability and specified by ICAO. Level 2 trust is built at an enhanced level, known as Extended Access Control (EAC) and is based on additional specification for EU-wide interoperability. Trust in the context of border control can be defined between three parties: (a) principal – the entity holding the passport as an identity token; (b) identity provider – the passport issuing State; (c) the service provider – a border control post in the same or another State. Table 1 shows trust relationships and constraints between the three parties.

As Table 1 shows, the ePassport infrastructure is based on federated trust. It has been developed on top of the legacy passport infrastructure. It grants right to access basic identity information to all ICAO members through the BAC mechanism.

There is no explicit provision of privacy policy of the (border control) service providers nor is there option for privacy preferences by the holder. The basic as well as advanced functions of the ePassport (EAC and eVisa) assume implicit consent of the holder in all usages by service providers (i.e. the border control). For advanced functions, however, only a targeted subset of federation members are authorized to access privileged information (i.e. the secondary biometrics).

However, ePassport infrastructure is designed for identity verification in face-to-face mode. Feasibility of its deployment in the networked environment will be examined in Section 4.

3 Network-Based Identity Management

3.1 Current Approaches

Currently there are two main approaches to network-based identity management: centralized and distributed. In the centralized approach, a single entity acts as the identity provider (IdP) in the context of several service providers (SPs). The centralized IdP may offer an option to use pseudonyms as well as creating several service groups which require similar set of personal data. An example of centralized IdP is *Microsoft Passport*. In the decentralized approach several IdPs may form a federation mutually to recognize each other's user sets as well as services. Examples of federated systems are Liberty Alliance and OpenID. Whereas both of these approaches have put considerable emphasis on privacy protection and user convenience, neither of them is particularly strong in mandating trust mechanisms either on the part of the service providers or the end users. Instead they tend to rely on mechanisms such as reputation. Moreover, OpenID lacks the trust model and Liberty Alliance lacks an end-to-end implementation.

Practical implementations of IdM by several commercial vendors are geared towards large enterprises who would have various data services and a large number of

users spread around several locations and/or departments with different roles and privileges. This latter is generally termed as a Centralized Authentication Service (CAS). Although this last category is interesting in its own right due to its practical commercial relevance, it is not so much relevant for multi-organizational services directed to citizen-life processes, spanning eGov services, banking, healthcare, e-shopping, education, edutainment and social networks.

The proposed scenario assumes that both the IdPs and the SPs organizations are trustworthy and they follow the legislation regarding the personal data protection and they have clear privacy policies.

For citizen-oriented services, in recent years there have been national initiatives to issue government-certified electronic identity (eID) e.g. in the form of X.509 certificates. Both card-based and file-based schemes have been proposed, however there is a lack of consensus on technical standards thus the interoperability remains a challenge [5][7]. Furthermore, in case of X.509 certificates, the certification authority needs the proof of identity at the time of issuance and since the certificates are possession based tokens, a loss of the storage medium would lead to the risk of impersonation or identity theft.

3.2 Main Requirements of eID

Whereas in face-to-face identity verification scenario human decision is often combined with the technical mechanisms to deliver an acceptable degree of trust in the claimed identity, network-based identity verification needs to rely on technical means only. We identify the following requirements of digital identity management in relation to citizen-life processes for network-based interaction:

(a) Trust
    a. Trusted credentials of the service providers
    b. Trust credentials of the identity provider
    c. Trusted credentials of the consumers (end users)

(b) Privacy and data protection
    a. Data protection as required by law
        - By the IdP
        - By the SP
    b. Common Criteria[10]
        - Anonymity
        - Pseudonymity
    c. Data Avoidance[10]
        - Unlinkability
        - Unobservability

(c) Security
    a. Communication security – confidentiality, integrity, availability, non-repudiation
    b. IdM infrastructure security
    c. Protection against identity fraud (protection of identity)

i. Authenticity of breeder documents (proof of identity at the time of enrolment)
ii. Binding between the user with trust credential at the time of authentication

(d) Interoperability
   a. Between diverse identity providers
   b. Between identity providers and service providers
   c. Between the IdM system and the user environment (context)

(e) Usability
   a. Ease of use
   b. Accessibility
   c. Efficiency
   d. Adaptable to widest range of users, use cases, life processes

From a brief inspection of the above list, it becomes quite obvious that an IdM solution would have to make design trade-offs between the diverse requirements based on the priorities, cost, state of the art technology and scalability of alternative options for the underlying IdM architecture. Alternative solutions can still be evaluated in terms of the above requirements.

3.3 Risk-Based Authentication

In relation to security and trust, a key issue is the binding mechanism between the claimed identity and the claimant in a scheme. The strength of binding during authentication should be appropriate enough to mitigate the risks involved in the transaction as well as the limitations or possible circumventions of different types of identity tokens (biometrics, digital certificates, password, etc). The scheme can be based on *possession*, *knowledge* or *personal traits* of the subject. NIST has proposed four levels of authentication[13] which we extend as shown in Table 2. In many applications, multi-factor authentication may also be a practical option leading to a combination among password, biometric, hardware token and digital certificate.

Table 2. Risk-based Authentication Options

Authentication Level	**Risk assessment by Service Provider**	**Registration Policy of the Identity Provider**	**Means of User Authentication**	**Examples**	**Primary Concern**
0	No risk – no damages	No proof of identity required; self-certification; unlimited period of enrolment	None or Userid / password; password strength not enforced	Chat rooms, email services; shopbot search; blog hosts	Privacy; Usability
1	Low – small damages	Weak proof of identity: by referral of a trusted token or trusted identifier; implicit identity verification through an online payment gateway; unlimited fixed period of enrolment	Userid / password password strength may be enforced; repeated authentication attempts blocked	Online shopping; low-value social networks	Data protection; usability; security

Table 2. (*Continued*)

Authentication Level	Risk assessment by Service Provider	Registration Policy of the Identity Provider	Means of User Authentication	Examples	Primary Concern
2	Medium – significant damages	Remote enrolment accepted; online validation of identity; offline validation Periodic re-validation of identity and privileges	Identity tokens (software or hardware); biometrics	Online tax filing and other eGov services; high-value social networks	Trust; Security; data protection; usability
3	High – considerable damages	Personal presence and/or verification of claimed identity through multiple sources; security vetting; periodic re-validation of identity and privileges	Biometrics; hardware or software tokens; secure access; cards with hard crypto	Banking; eHealth services; access to sensitive data	Trust; security
4	Very high – unacceptable level of damages	Personal presence of the applicant is required; verification of breeder documents; security vetting; limited time enrolment; periodic re-validation of identity, privileges and security vetting	Cards with hard crypto; multi-factor authentication; access to service only within supervised premises with physical access control; two-person authentication	National security; commercial secrets; services for high-value persons	Trust; security

4 Proposed Architecture

4.1 Federation of Trusted Identities

As outlined in Section 3, the main requirements of a user-based IdM system are trust, privacy, security, interoperability and usability.

We adopt the federated model where ePassport as the primary identity token to ensure trust and convenience whereas a SAML-2 based federation technology ensures security and interoperability [14].

A separation of the identity providers from the service providers will in itself enhance privacy protection. User demand for privacy protection and the multi-vendor based competing solutions would further encourage adoption of the most powerful privacy-enhancing technologies by the identity providers and service providers.

Figure 1 shows the proposed model where users are enroled with a trusted identity provider of their choice, based on trusted credentials. When using trusted networked services, the relevant identity provider verifies the user's identity and furnishes the user information required for service provision.

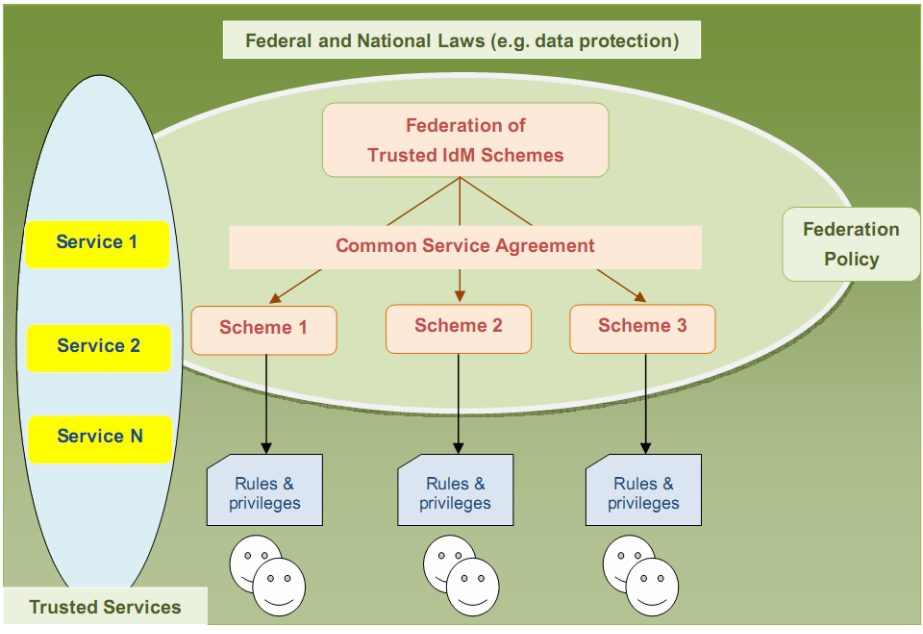

Fig. 1. Federation of Trusted Identities based on common trust policy

4.2 Services for Trusted Identities

A trusted identity management architecture based on ePassport is proposed in Figure 2. The diagram represents the use of the three main risk categories of services utilizing e-passport based identity verification.

(a) **Public / eGov services:** For the government online services the IdP can use passport as a base document for identity enrolment. When providing entitled services in a trusted kiosk-based environment, the ePassport can be used for real-time biometric authentication. In this case, the user is in control of his passport and the eGov service provider is in control of the trusted kiosk incorporating passport reader and biometric scanner (e.g. digital camera). Use of fingerprint is not foreseen for services unrelated to border control. Accessibility to the national passport database may not be needed if the kiosk can do the chip authentication.

(b) **High-value private services:** Trusted organizations (banks, hospitals) offering high-value services often use own identity management, thus acting both as identity provider and service provider. However, this type of IdM can be simplified by deriving core identity from the ePassport and supplementing it with relevant demography data for health services and/or financial services. Registration would require the physical presence of the user. The identity provider will be responsible for releasing only the relevant data depending on the service requested. Facial biometric verification with ePassport as a reference token may be done for security or convenience, depending on the service. The Service provider will be in control of the ePassport reader terminal which in some cases may include a

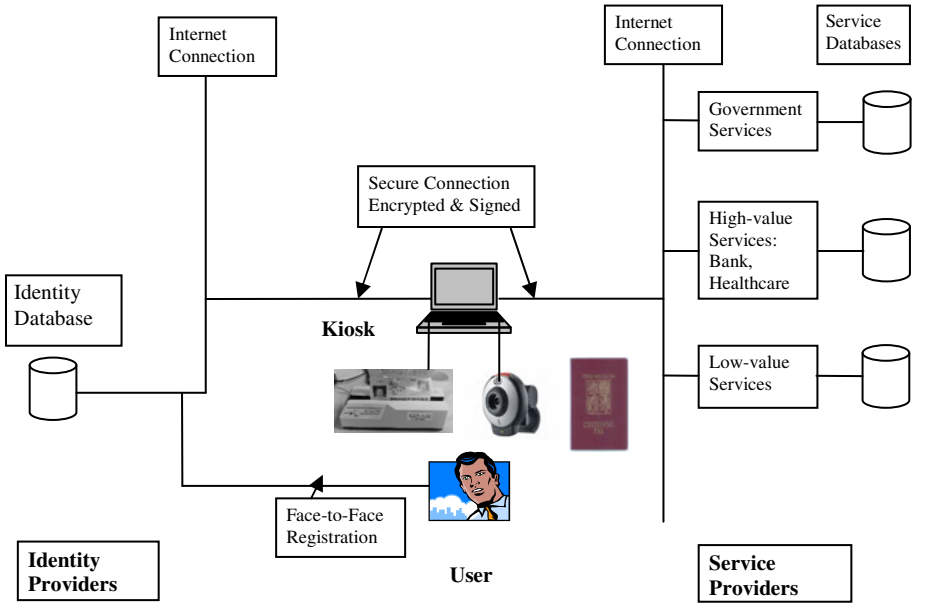

Fig. 2. Trusted identity management based on ePassport

webcam for face recognition. This will avoid the need for creating private biometric databases for authentication by private sector.

(c) **Low-value private services**: A multitude of private service providers (e-shops, social networks) do not need to verify the precise and full identity of the user, rather only a partial identity yet still more than just the self-declared pseudonyms to have sufficient trust in the user. The trust level of the service provider is also a very important requirement. They may find it adequate for service provision to have, for instance, a pseudonym with a genuine age and password verified by an IdP who could ensure the pseudonymity and trust in the user at the same time. No biometric verification would be needed for such services even though the enrolment with the IdP was based on ePassport and biometrics.

With the three categories of use scenario above, it is technically feasible for a single IdP to serve all three types of service providers if the end-user so prefers whereas it is also feasible for a user to have more than one IdP. The IdPs will need to demonstrate their capability for privacy-enhancing features such as anonymization and unlinkability to satisfy user demands and compete openly based on value-added benefits for trust, privacy, and risk minimization for the end users as well as the service providers.

4.3 The Scheme - Two Remote Identification Schemes Binding to e-Passport Information

A major question that arises in such a scheme is how to bind the passport to the holder in a remote environment. There are two emerging categories of technical implementations that we can distinguish in the literature for this type of services:

(a) **Direct model.** Based on a trusted device concept, which can provide real-time identity verification directly using ePassport. This is particularly relevant for the eGov services based on multi-service kiosks. Figure 3 shows the communication between the user and the IdP in this scenario.

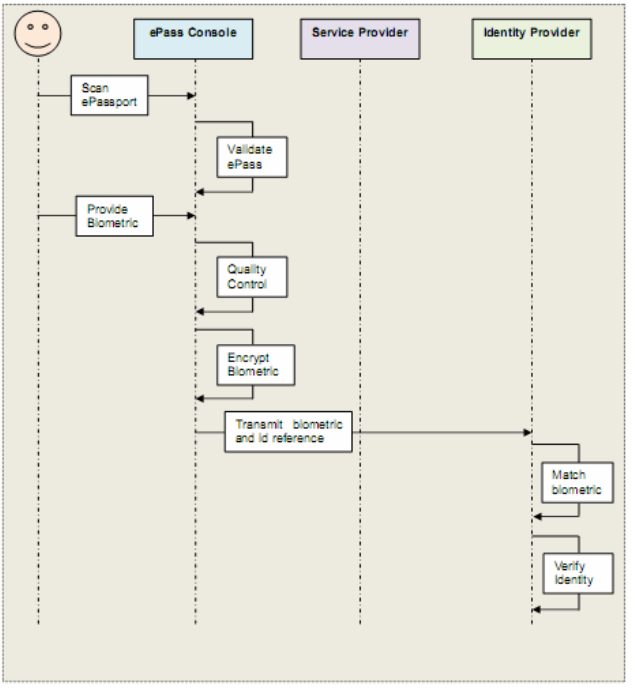

Fig. 3. ePassport-based remote identity verification by the IdP

(b) **Indirect Model.** The Identity Provider (IdP) supplies an e-security token (smart-card, certificate etc.). The IdP operates under regulations (national or international). The token is provided after an enrolment phase based on the information that exists on the ePassport and may include additional information, the IdP may consider as generally required by the high-value service providers.

The indirect model requires an enrolment phase where the client is providing his passport information to the IdP and in return he receives a customer card (smart-card) to which the e-passport information is tied to. Every time the client requests a service from a service provider (also referring as Relying Party) he uses his e-security token. In the smart card there is no passport information is stored only an identification number which is read during a transaction with a local smart card reader. For multi-factor authentication, the user could also use a password in conjunction with the smart card to identify himself.

On the other hand the direct model does not use an additional e-security token. Only the passport data is used for verification by face biometric. A futuristic implementation of the direct model may obviate the need for the use of an IdP where user

becomes his own IdP through the use of a certified personal trusted device which are sealed tamper-resistant mobile devices. These devices can be thought of as extended mobile devices (PDA, mobile phones) employed with a passport reader (even with biometric reader). However, they are not yet in the consumer market arena.

There are two main risks regarding the above methods in common with any authentication scheme based on possession and knowledge. This applies to both the direct and the indirect methods.

1. An impostor could try to use the services in the name of the holder using the passport information.
2. the holder could try to repudiate a genuine transaction claiming that an impostor used his online identity.

Advancement in the security of real-time remote biometric verification could minimize these risks. From the privacy requirements, the federated approach already admits unlinkability, pseudonyms and even anonymity if the service provider admits this property.

5 Discussion

An ensemble of citizen-life services in online world would require a trusted identity management infrastructure where identity of the end users can be trusted by the service providers while at the same time the citizen could reasonably expect to have respect of privacy, along with support for partial identities and in some cases anonymity. These requirements need to be satisfied simultaneously in a balanced manner.

The electronic passport offers a globally interoperable trusted identity infrastructure for face-to-face border control applications. We have examined its feasibility to be used in the online world to provide trusted identity as an extension. This will require introduction of certain new features in a federated identity management system to bridge the gap between online and offline identities.

There are several challenges that remain in the realm of research and technical advances continue to be made. It seems evident that the binding between the end user and the network-based enrolment and authentication processes is the key challenge for electronic identity management. The extent to which biometrics can be used for trusted remote authentication is fast becoming a reality and banking services are already running trials of such systems around the world. As more experience is gathered in managing risks in such scenarios, routine deployment will follow.

Another issue is about who should be in control of the authentication devices (ePassport reader, smart card readers etc)? Ideally, in a two-party transaction, both parties should be able to exert an equitable degree of control to maintain the required amount of trust in the transactional relationship. The kiosk environment is state of the art in offering self-services to citizens while ensuring trust as well as secure transaction.

The schemes proposed in this paper are amenable to the adoption of privacy-enhancing technologies by the identity providers as well as service providers. The framework allows the citizens to exert a value-based preference on the market offerings in terms of convenience, security, privacy and trust thereby promoting innovation in identity management for online environment.

References

1. Hansen, M., Krasemann, H., Krause, C., Rost, M.: Identity management systems, IMS: identification and comparison study (2003)
2. Hansen, M., Pfitzmann, A., Steinbrecher, S.: Identity management throughout one's whole life. Information Security Technical Report 13(2), 83–94 (2008)
3. ICAO, MRTD specifications Technical document 9303, Machine Readable Travel Document (2006), http://www2.icao.int/en/mrtd/Pages/default.aspx
4. Ostdjk, M.: Using the ePassport for online authentication, Telematica Institute, Report TI/RS/2009/002 (2009), http://www.telin.nl
5. Bruegger, B.P., Huehnlein, D., Schwenk, J.: TLS federation – a secure and relying party-friendly approach for federated identity management. In: BIOSIG 2008, pp. 93–106 (2008)
6. Bottoni, A., Dini, G.: Improving authentication of remote card transactions with mobile personal trusted devices. Computer Communications 30, 1697–1712 (2007)
7. Bruegger, B.P.: eID interoperability scenario, http://www.vrk.fi/vrk/fineid/files.nsf/files/71D771700F919761C22573EC00293FAC/file/10-scenarios-8.pdf
8. Arora, S.: National eID card schemes – a European overview. Information Security Technical Report 13(2), 46–53 (2008)
9. EU passport specification Working document (EN) (28/06/2006)
10. Anonymity Terminology, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.18.pdf
11. Abdul-Rahman, A., Hailes, S.: Supporting trust in virtual communities. In: Proceedings of the 33rd Hawaii International Conference on System Sciences, vol. 6, p. 6007 (2000)
12. Josang, A.: Prospectives for Modelling Trust in Information Security. In: Mu, Y., Pieprzyk, J.P., Varadharajan, V. (eds.) ACISP 1997. LNCS, vol. 1270, pp. 114–125. Springer, Heidelberg (1997)
13. NIST Electronic Authentication Guideline, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
14. Ragouzis, N., et al.: Security Assertion Markup Language (SAML) V2.0 Technical Overview. OASIS Committee Draft (March 2008), Document ID sstc-saml-tech-overview-2.0-cd-02, http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf