Versatile Privacy Preserving Electronic Identity Framework

B. A. Malalasena, S. Nimalaprakasan, S. Ramanan, K. Shayanthan, C. Gamage and M. S. D. Fernando

Abstract— **For eGovernment and eBusiness to function to their full potential, people need a secure, convenient and effective way of identifying themselves. Electronic Identity systems draw the fundamental basics for the implementation of full range of eGovernment services, for both citizens and businesses. Privacy and security issues play a vital role in user acceptance of any electronic identity system, which decides the success of the system.**

Index Terms— **Computer Security, Electronic Identity, Identification of Persons, Policy based Authentication, Privacy**

I. Introduction

ELECTRONIC Identity (eID) is the electronic replacement for conventional ID cards. An eID can play the same role as that of a conventional national identity card (NIC) which is used to establish the identity of a person by another person (that is, the verifier) but do so in which the verifier is a computer-based system. Electronic identities will be the basic tools for authentication and identification in future when people participate in eGovernance, eCommerce, eLearning and eSociety initiatives.

eID systems draw the fundamental basics for the implementation of full range of eGovernment services, for both citizens and businesses. As more government, personal and commercial transactions are conducted electronically – especially where documents exist only in digital form – parties need to be sure of a person's or an organization's identity. Registered letters are still required in many official exchanges between people and organizations. With alternatives such as e-mail, there is no way to verify when an attached document, such as a tender application, was really written. Thus an eID system is essential to speeding up online business, and to promote more online based services and businesses.

The operation of an eID system is in a socio-technical environment where the acceptance of eID becomes the main challenge, due to objection to the change in the conventional way of identity systems. There are many concerns related to electronic transaction and digital security which could influence the acceptance of an eID system. While the eID can serve as a mechanism for authentication in the conventional offline setting without significant drawbacks but with many benefits, its use in an online setting creates new issues with respect to user privacy and information security. Privacy becomes an important aspect of the eID system as many users are concerned about how their private data would be handled by the system and if any of those personal will be disclosed to any third parties.

A. *Advantages of Electronic identity systems*

A reliable system of eID means citizens, businesses and government departments can identify them and certify their transactions accurately, quickly and simply. Widespread confidence in eID will enable the day-to-day transactions between public agencies and people and businesses to move online. That move will lead to gains in efficiency in public services, and corresponding gains in time and money for citizens and businesses through simplifying their dealings with government agencies.

eID systems are more reliable than a paper based ID as they provides more data security with privacy features. The use of cryptographic techniques and digital signatures in eID, make them harder or even impossible to be forged. A citizen with an eID would have the ability to use it for various services, thus it would be versatile in terms of applications and usability. The ability to authenticate and identify a ID holder in the real world services and online services is a unique aspect of the eID systems. An eID would enable it's holders to authenticate themselves securely when using an online service, while protecting their privacy. In the same way it could be used to identify them in the real world situations.

Convenience to both the users and the authorities is another advantage that an ID system would have. Especially the time and effort that needs to be spent for issuing and updating the IDs could be reduced by a large amount with eIDs. Also the data that are saved in the eID could be easily updated by the authorities, thus it would make up to date information. Also authorities would have the control over eIDs as all services would be connected to a centralized system with multiple access levels for different services.

Manuscript received March 31, 2009.

B. A. Malalasena, S. Nimalaprakasan, S. Ramanan, K. Shayanthan, C. Gamage and M. S. D. Fernando are with the Department of Computer Science and Engineering, University of Moratuwa, Sri Lanka (e-mail: {anuradha, nimal, ramanan, shayanth}@project-eid.org, {chandag,shantha}@uom.lk).

B. Disadvantages of Electronic Identities

The eID system as a whole has few drawbacks when it comes to the wide usability. As a national level eID would be issued national wide, it should provide equal opportunity to any citizen in obtaining a service. But when going outwards from city centers, the access to Internet becomes more unreliable and expensive. This could make the people in those areas not getting the full benefit from the eID system. Technical knowledge level of the citizens also plays a major role as some level of competency would be needed to get the full benefits of the system.

II. RELATED WORK

A. Existing electronic identity systems

FINEID: FINEID used a smart-card based identification card, based on Public Key Infrastructure and it is one of the very successful implementation of a national level electronic identity card for Finland citizens [11]. There are various levels of information about electronic identity is contained on web site by the Population Register Center (PRC). This site contains information about card readers, card reader software and creating an on-line service utilizing certificates of FINEID.

The citizens will be given citizen certificates, and service providers are allowed to build services which utilize the citizen certificates. The PRC offer technical information about the Citizen Certificate and other PRC certificate products, as well as instructions for builders of on-line services. It also provides technical descriptions of certificates' information content, revocation lists and certificate directory specifications. The site also contains, for instance, certificate policies, FINEID specifications and other standards, and information about legislation. In addition, the FINEID website contains information about the software and card readers required for using the card, and about international development.

Estonian eID: SK (Certification Center) is Estonia's primary and currently the only certification authority (CA), providing certificates for authentication and digital signing to Estonian eID Cards [12]. The core function of SK is to ensure the reliability and integrity of the electronic infrastructure behind the Estonian eID Card project. It also functions as a competence center for ID card and spread the knowledge necessary for creating electronic applications to the card.

Estonian eID cards were started issuing in January 2002, and in five years period they have issued more than one million eID cards. SK as a service provider played a crucial role in the first e-voting using the eIDs in Estonia local elections in year 2005 as well as in Estonia parliamentary elections in year 2007 [13].

SK and its partners have developed a secure, reliable, easy to use digital signature architecture named DigiDoc, based on European standards. People can use Estonian ID cards and DigiDoc to give digital signatures in any form of communications and acting in any role. The system is used by most of the public sector, e.g. by the Estonian courts, central government, local municipalities as well as the businesses, banks being the leaders.

Australian eID: Australian Government decided to go on in principle with a new access card for health and welfare services in April 2006. Although it was called an access card, actually it was realized as a national identity card system. Anyway this access card project was subsequently abandoned by the new Government elected in December 2007 due to the public offense [7]. There was a similar project initiated earlier with the name "Australia Card", which was also rejected by the public.

The proposed Access Card was a smart card based eID, with a unique personal identification number, linked to a centralized database containing an unprecedented amount of personal identification, and other, information about almost every adult Australian and Australian resident. The people argued that the so-called Access Card system is even more dangerous to individuals' security and privacy than was the Australia Card due, in part, to the planned use of a multi-purpose smart card electronically linked to a centralized national identity database. They were also concerned about their privacy, security, and also the risk of identity theft and identity fraud.

B. Issues and weaknesses in existing systems

Success of any identity system depends on the acceptance by its users. Privacy issues play a vital role in user acceptance of any electronic identity system. Traditionally access control is enforced based on policies that who can or cannot access some data. However in an eID system, data may be accessed in different contexts and users are required to disclose a rich set of personal information about themselves, such as identity attributes and other dynamic properties such as their location attributes. Here privacy becomes vital as studies have revealed that some users prefer to abort a transaction rather than disclosing what they consider private information, and others expect a degree of control over its secondary use, to protect their privacy. Protecting user identities by providing anonymity, Pseudonymity, Unlinkability, and Unobservability of users is needed to address privacy issues and these need to be enforced at communication level, system level, or application level. This introduces the need for defining authorization policies and models and the development of new paradigms for access control and in particular authorization specification and enforcement for an eID system.

III. PROPOSED eID FRAMEWORK

The proposed framework for an electronic identity system has many distinct features which are lacking in several existing identity solutions. This framework allows the holder to use the eID to authenticate himself/herself to consume online services, through which permits online transactions. This system would handle the privacy issues of the holder and provide anonymity and unlinkability requirements appropriately when and where it is required. Proposed eID framework handled all the online services as policy negotiated, thus each user is aware of the appropriate policy of the consumed service. This results in data sharing with user consent, which enable the users to preserve their privacy. In addition, this procedure does not allow the service providers or relying parties to gather any data which never have to be revealed for that purpose.

The eID can be used as an identification token for citizens to prove their identity, when consuming online based services. The eID framework provides means for secure authentication for online transaction with full user consent. This eID framework also supports offline authentication, where the holder will be able to prove his/her identity in settings such as checkpoints, or reception desks. Further the eID is designed to be a forge free to the extent under present information security recommendations. The main focus of this framework is to promote the usage of eCommerce and enhance eGovernance. This eID system will facilitate the wide spread of eCommerce application by imposing acceptable level of identification and trust on the system.

Service Oriented Architecture (SOA) is used for the service side implementation if this identity solution. SOA is an approach to loosely coupled, protocol independent, standards-based distributed computing where software resources available on the network are considered as Services. The eID authentication application is published as a web service, that can be used for authentication purposes of other service providers or relying parties. Users can also prove their identities offline when prompted by law enforcement authorities such as police. The data in the eID card will be verified by the application and will be checked with Person of Interest (PoI) list.

The data collection policy developed for this eID framework ensures the privacy concerns of users are addressed. It ensures that any personal information will not be revealed without the permission of law authorities. The policy is implemented in such a way so that you can stay anonymous until you don’t commit any forbidden action.

A. *eID Framework*

The overall eID framework mainly relies on four fundamental components of this solution. eID System is a main component that consists of the eID Authentication Server and the Master database for the eID system. eID Authentication service provides the objective function of the eID framework. Relying parties should use the eID authentication service adhering to the eID system policies. eID users are individuals/citizens who are registered with eID system and obtained an eID card. These three components function on online mode of operation of the eID framework. eID framework also defines the offline mode of operation in which supports verifying a person’s identity in an offline setting. The eID framework also includes supportive application that enable the registration, issuing and updating of eID Cards.

B. *eID Card*

This eID Framework relies on eID Card and supportive applications in establishing an electronic identity solution. Thus the eID Card can be considered as the heart of this project. All other applications and modules depend on the eID card and use it. There are two aspects of an eID card; first what is going to be stored in the card in digital format and second how it is going to be accessed and used. The main goal is to answer both these questions with one solution that could fulfill these basic requirements. In this projects these two parts are handled separately as eID Info Card, which is used to store the holders details in a digital format and eID Card which is the physical design of the card. Though the manufacturing of the real eID Card was out of the scope of this project, two alternative eID Cards have been proposed, that use two different technologies of Smart Cards and Write-once Memories.

C. *eID Info Card*

eID Info Card is a simple XML file document. This XML document contains Personal Identifiable Information (PII) and images of the citizen, which would’ve been signed by an issuing authority. The following types of PII also know as Claim Types are digitally stored in the eID Info Card. These clam types are in accordance with RFC 2256 [14].

Apart from these textual personal details, the photo image of the holder is also digitally saved inside this eID Info Card as a MIME object. This image is stored in the eID Info Card as Base64 encoded. This will be used to verify the ownership of the eID Card in certain offline applications.

eID Info Card will also has a eID Card Number, which will act as an identifier for the eID Card. For this two alternatives are available to be chosen among. The first one is having an eID identifier which will not imply any information about the user. The sole purpose of having this identifier is to identify the eID card. This will give the advantage of privacy protection. This will be a random string of 11 digits followed by a check-sum character.

The next number format the eID system supports is an improved version of the current Sri Lankan NIC number. This will also be a string of 11 digits followed by a check-sum character. But in these 11 digits, certain personal details of the eID holder, such as date of birth and sex are encoded, which could be extracted for verification purposes. This has the disadvantage in privacy, but this is mostly preferred in the Sri Lankan context. The following shows how this new proposed number format is formulated.

CYYDDDSXXXXZ
18531711439P (Sample Number)
C - Century (18-- 0 19-- 1 20-- 2)
YY - Year of Birth
DDD - Day of the year
S - Sex
XXXX - Random Serial Number
Z - Check-sum Character

In this numbering format, the first digit 'C' represents the century of birth, starting from nineteenth century. The next two digits 'YY' represents the year of birth and the next three digits 'DDD' gives day number of the year of the date of birth. Next we have 'S' which is used to specify the sex of the ID holder. One important aspect we have included is transgender also as a separate category. Also this field has one more use when it is set to '0' and used the same eID and eID number as an organizational ID, which is out of the scope of this project. The next four digits 'XXXX' are random serial number that is used as to handle multiple persons with same sex and date of birth. The selection of 4 digits is made considering the Sri Lankan birth rate statistics which indicate daily births of any particular gender is less than 9999 [15].

Another significant feature both proposed number formats have is a check-sum character. This check-sum character is a one-character alphabet, located at the end of each eID Number, representing the "two's complement" of the first 11 digits. In other words, each digit value is XOR'ed. One of the important aspects of this check-sum is simple validation of the number. In real world this will be very useful as this could easily detect simple typo errors.

eID Info Card are digitally signed and they are enveloped in the form of XML Signatures. XML Signature (also called XMLDsig, XML-DSig, XML-Sig) is a W3C recommendation that defines an XML syntax for digital signatures [16]. Functionally, it has much in common with PKCS#7 but is more extensible and geared towards signing XML documents, thus it has been chosen for the use with eID Info Card which is also a XML document. XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.

D. WOM-eID

WOM-eID is an eID Card that is build on a write-once memory device. In one arrangement, the memory device comprises write-once memory adapted to store data files, re-writable memory that contains a file access table, and a device controller that is configured to control operation of the storage device. In use, digital data written to WOM cards will be effectively locked as soon as it is recorded; there is no physical way to alter or delete individual recorded files.

The WOM-eID Card will be of the same size of a phone card in low height of less than 3mm, which comprises of a connector part, and a set of metal terminals. The connector part has a height compatible with the height of an inner space in a standard USB interface slot socket so as to be inserted into the standard USB interface slot socket. The set of metal terminals is arranged on the connector part and composed of a plurality of metal sheets and each metal sheet has an end disposed in the connector part and another end extending outward the connector part. The first end of the respective metal sheet in the set of metal terminals contacts with internal electronic signal of the standard USB interface slot socket and the second end of the respective metal sheet is soldered to a printed circuit board. Thus the WOM-eID cards can be directly connected into any device with a standard USB interface.

E. SC-eID

The SC-eID is a Smart Card based eID card, which runs in Java Card operating system. The selection for this Java Card was made considering the privacy and security issues of the holder [17]. The eID info card is stored in the Smart Card and it is loaded with customized applets for accessing and processing the data contained in the card. This Smart Card is protected with a PIN which controls the access to the card. Using standard credit card like Smart Cards require a Smart Card reader for operation and the use of USB Smart Tokens instead of Smart Cards will eliminate the need for a card reader, which can be directly plugged in to any USB ports and used.

F. On-line Identification

The eID can also be used for identification and authentication in online applications apart from the offline world. In e-governance services authenticating a citizen to access an online service is crucial and eID provides means to do this effectively. The card will have electronic signature of the holder and that are signed by the issuing authority. This data would be read from the card directly by the authenticating service and authentication would be done. This authenticating service could be used by approved authorities and and other service providers. Citizens may use the card to gain access to e-government services, sign online contracts and access other web based services and applications.

G. Off-line Identification

The traditional IDs provide identification with physical presence of the card owner. The authentication is performed by checking the visual appearance of the holder and the picture on the card. An eID will also have similar printed card with holder's picture and other basic details on it. This could be used as the same way as the existing ID cards. The migration from paper-based to eIDs enables extended functionalities in authentication. Personal data stored in the eID can be read much more efficiently when a citizen uses it to identify in person. The eID enables authorities to verify a person's identity by connecting to the central authenticating server or by reading information from the digital data stored in the eID.

One important feature provided in the offline mode operation is the verification against a Persons of Interest (PoI) database. This will enable law enforcement agencies to check for wanted persons at locations such as check points. Updating of these PoI database would be independent of the eID framework, thus providing more control to the law enforcement agencies of the country.

IV. How it solves the problems?

A. Confidentiality

Confidentiality in eIDs is to keep information secret from entities those are not authorized to have access to it. Keeping information in the card in digital form secret and the transactions secure from entities that do not have any need on it, is an effective measure to prevent illegitimate use of the data. Confidentiality is particularly relevant when sensitive data that would be saved in the eID (such as ethnicity, personal details or health related information) is concerned [1]. The confidentiality of the information should be protected, so that unauthorized third parties are not capable of eavesdropping on the communication between the eID holder and the services that the eID is used by the citizen. There are many available cryptographic algorithms that provide confidentiality, and eID would use public-key encryption schemes to achieve this. One of the main problems of storing encryption/decryption keys in the eID card is that the card may get lost, making it impossible to decrypt data. In order to solve this problem, some back-up or key escrow mechanism needs to be implemented [2].

B. Integrity

Integrity in eIDs is the quality which ensures the data in eID could not be subjected to any sort of manipulation such as insertion, deletion, substitution etc. Cryptographic methods such as message authentication codes (MACs) and digital signatures would be used for achieving data integrity [3]. The integrity of the data contained in the eID card is protected by a digital signature generated by the card issuing authority. Anybody who has access to the card can read out the information it contains: public key certificates, personal data of the card owner, etc., if they posses relevant access level. However, only the card issuer can modify the contents of the card.

C. Authentication

Authentication serves to demonstrate the integrity and origin of what is being pretended. The security and reliability of authentication mechanisms may vary dependent on the desired authentication level. During the authentication process, one makes often use of credentials. Authentication is often achieved by proving something you know (e.g., PIN or password), something you have (eID) and/or something you are (biometrics) [4]. In the case of the eID, authentication in the current version is performed by “something you have” (i.e., the physical eID card) and “something you know” (the PIN to the card).

D. Non-repudiation of origin

Non-repudiation is the concept of ensuring that an action cannot later be denied by one of the entities involved. With regard to digital security, non-repudiation means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively [5]. Non-repudiation of origin and delivery are very important for assuring legal effectiveness to actions done in a digital context (e.g., signing a contract). As the user may obtain official statements with legal value, it should not be possible for the server to deny having produced the document. Therefore, the server may have to produce some signature on the information in order to ensure non repudiation properties. The current version of the eID provides non-repudiation by using digital (qualified) signatures.

E. Access control and Authorization

Access control is restricting access to resources to privileged entities. Access control works at a number of levels: There are access control mechanisms that work at application level and for the user they are expressed as a very reach and complex security policy [6]. Usually, authorization is used in the context of authentication. Permission is granted or denied based on the result of data or entity authentication, and on the allowed activities, as defined within the system. Once an entity is authenticated, it may be authorized to perform different types of access, each of which is referred as a role.

F. Trust Requirements

A system or party is trusted when an expectation rests on it to behave in a determined way or achieve a determined result, and where the relying system or party acts on this assumption. More generally, trust is a quality of a relationship between two or more entities, in which an entity assumes that another entity in the relationship will behave in a fashion agreed beforehand, and in which the first entity is willing to act on this assumption.

Whether or not to trust depends on a natural person’s decision. It is possible, but not necessary, that several entities trust each other mutually in a certain context. Trust decisions of legal persons depend on the decisions made by the legal person’s responsible natural persons. Trust may be limited to one or more specific functions, and may depend on the fulfillment of one or more requirements.

G. Enforcement and Accountability

The use of policies is a very important aspect in enforcement and accountability. A person can only be held accountable if there is some way to specify what he/she is allowed to do within a system. Therefore the policies have to be defined. Each policy should clearly define which actions are prohibited and what are the consequences of misuses. Policies should also include the rules to state what is allowed by law, where applicable [8].

Next to discuss which actions are allowed, it should also be possible to define the functionality of the services. That way a service provider has to deliver the promised functionality. If he fails to do this, he can be held accountable. There can be different levels of policies defined for to be used in the system. It can be classified as follows; International policies, governmental policies and internal system policy. The International policies are defined by international organizations according to the international norms. The governmental organizations define the governmental policies and every particular system can have its own internal system policy. Some policies can be defined in the very low level of this hierarchy and some can be used in the high level according to their properties.

It is not possible to hold users or service providers accountable by only using some policies. From a legal point of view accountability has no meaning unless the party in question can be forced to assume liability for his actions. The aim of enforcement is thus to ensure that accountability is translated into liability where appropriate. The following properties are required to ensure the enforcement possible.

Persons should be able to act anonymously in the system. However when they abuse the system somehow, they should be identifiable. To ensure the privacy of the users, only trusted third parties can identify people. Policies should describe the conditions under which a user may be identified. To ensure anonymous operations, different actions of a user should not be linkable. But in some cases, it may be useful to link some of the actions. This way, it can be possible to find out information about how the abuse was performed.

In case a controversy arises, the parties involved will need reliable evidence in order to enforce their rights. Every protocol must be engineered securely to ensure that every party can gather enough evidence. Only the necessary evidence should be kept to limit the amount of disk space required. Policies must clearly state how long evidence must be saved. When some party cannot deliver certain evidence his chances to win a dispute are very small.

H. *Anonymity and Unlinkability*

To enable anonymity of a subject, there always has to be an appropriate set of subjects with potentially the same attributes. Anonymity is thus defined as the state of being not identifiable within a set of subjects, the anonymity set. The anonymity set is the set of all possible subjects. With respect to acting entities, the anonymity set consists of the subjects who might cause an action. With respect to addressees, the anonymity set consists of the subjects who might be addressed. Both anonymity sets may be disjoint, be the same, or they may overlap. The anonymity sets may vary over time. Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together. This requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system [9].

The use of identity data by default in electronic transactions enables serious risks for the privacy of eID holders. In most cases, identity data is not necessary to carry on secure transactions, where all parties are ensured that their requirements are met. The identity data is stored along with transactions that may reveal sensitive personal information. The data gathered by databases in different domains contain common identifiers (such as the national ID number), the possibilities of aggregating huge amounts of data on all users of the eID card grow dramatically. The possession of such extensive information on large amounts of people would enable very sophisticated profiles that could be used for criminal purposes such as identity theft, or for unfair commercial practices, such as price discrimination [10]. In scenarios where human rights and legal guarantees are not respected, this information could also be abused for undermining civil liberties or exercising discrimination on minorities. These risks can be greatly reduced by implementing security mechanisms that rely on anonymous or pseudonymous authentication, Unlinkability on the archival data and access control technologies.

Although it should be possible to identify persons who abuse the system, it should not be possible to systematically monitor normal users. The system must maintain the anonymity as much as possible, while maintaining the possibility to hold users accountable for their actions.

When agreeing on privacy policies, every party commits himself to act according to this policy. Service providers can only perform actions on data if this is allowed by the policy. Especially when providing identifiable information, users should be ensured transactions are performed the way they should. This way it is possible to have more trust in an application. Furthermore, when an organization has put much effort in techniques to handle information correctly, it is more difficult to be held accountable in case of mistakes.

There are two ways to ensure the correctness of transactions. A service can go through a procedure to get accredited. When actions of an accredited service are not performed correctly the accreditation organization can be held accountable. A more technical solution is the use of policy enforcement mechanisms.

V. Possible enhancements in future

A. *Improve in language support.*

Multi language support is one of the main future expected requirements which would be more desirable in a multi ethnic county like Sri Lanka. It could be done using transliteration methods. This makes the services very much usable for all citizens of the country in their own languages. For example the central database could hold the data in one specific language, but a service user who prefers his own language can enjoy the service features without any language bars.

Improve the Browser extension portable to more OS platforms and more browsers.

Currently eID system has Browser extension only for the Firefox browser. It will be a bottleneck when it comes to action. So it should me very flexible for the eID users and not to restrict them in only one browser. In future this bottle neck should overcome through the improvement in the Browser extension.

B. *Hand held device for offline operation.*

eID system provides the online mode of operation and as well as the offline mode of operation. For the offline mode of operation eID system needs stand alone hand hold device which can easily handle in the road side check points. That device should be a small hand hold device which will need to design only for the POI application. And also it should be stand alone device which small power packs. That device should be very user friendly because it is intended to develop to use by the non technical peoples who don't have much knowledge about the running system on that device.

C. *Handle the Biometric data inside the card.*

Another improvement for this could be to store some biometric data such as a fingerprint, so that the offline authentication will be independent from individual's evaluation, in other terms this procedure can be automated.

VI. Example Applications

A. *eBanking*

eBanking is the service where a customer connects to his bank via the Internet to perform any of the virtual banking operations. Any person who has bank account that supports eBanking he can perform normal banking tasks, pay utility service bills and do transactions without being physically present at the bank. In physical banking transaction the identity of the user is proved using any identification document such as a passport or a identity card. But when it comes to virtual banking, a mechanism is needed to prove the identity of the user. In the current scenario user name, password based systems are used, but that can be vulnerable to many forms of malpractices.

eID can be used here as a medium to prove the identity of the user to the banking system and to authenticate to use its services. Tje user can access bank's web site using his web browser. When the baning sites needs authentication, he can select the option "Authenticate with eID", and this will be handled by the eID Browser plug-in that will be installed in the users' browser. Then the browser plug-in uses the eID card that is plugged into the use computer and the eID Web Service to authenticate the user, and he can continue using this banking services.

This is something that is not possible with normal paper-based identity cards, as they have no provision to prove users identity in online. Also the eIDs are more secure and forge free, thus banks can have a trust on the eID cards for authenticating. Users also will have trust on the system as this will be a national level system that is managed by the government. Also the privacy and security aspects of the eID system will attract more users to use eID Cards in this nature of applications.

B. *eHealth*

A hospital that is providing eHealth services could require the patients to be validated as citizens of Sri Lanka at the registration system. People are allowed to register themselves in the hospital for the health check up. For this the a valid person should be a citizen of Sri Lanka and should be above the age 21. In some cases a person who is willing to do a HIV check-up through the eHealth system, but would prefer not to disclose his personal information such as name, age and place to the system, considering his personal privacy. Therefore the eHealth system needs a authenticating mechanism which could ensure the persons authenticity and age limits, while those details are not disclosed to the eHealth system.

In this scenario the eID Authentication service could be used by the eHealth system. eID Authentication system will only validate the requirements that are requested by the eID Health system through their usage policy which comes with the consent of the user. Then the person can prove his identity to the eID system and the eID Authentication will respond to the eHealth system with the person's authentication status. Therefore anonymity and privacy of the user is ensured by the system.

VII. Conclusion

Many of the existing identity solutions are lacking in some of the important aspects related to privacy and security of user data. Our solution takes care about the privacy issues of the holder and provide anonymity and unlinkability requirements appropriately. Further we have designed our system to address many of these issues using policy based authentication mechanism. We provide forgery-free identity solution to the extent under present information security recommendations, using asymmetric keying systems.

Our project also has few unique elements that are not found in any known identity that are implemented. The common idea about electronic ID is that they can be used in the online transactions, but many people do not see the usefulness of eID is offline environments too. Thus we have addressed this issue by making our eID usable both in online and offline for authentication and identification of a user. Especially in the offline identification mechanism we have introduced the persons of interest database based verification, which has a potential use in places where we might want to restrict access to certain individuals. Our project supports two physical types of eID cards, the standard Smart Card based SC-eID cards and our own write-once memory based WOM-eID cards. Smart Cards are widely used for the purpose of eID cards, but our own solution of WOM-eIDs is another unique feature of this project.

This eID system will facilitate the widespread adoption of eCommerce applications by imposing an acceptable level of identification and trust on the system. Also, the eID framework could provide a strong basis for implementing wide variety of eGovenment initiatives.

References

[1] UK Data Archive, "Defining Personal, Confidential And Sensitive Personal Data", February 2009 . [Online]. Available: http://www.data-archive.ac.uk/sharing/define.asp, [Accessed: March 4, 2009]

[2] A. Rundgren, "Page 1Attested Key-Pair Generation with ”Key Escrow”. V0.2. A. Rundgren 20091/2Attested Key-Pair Generation with “Key Escrow”", 2009. [Online]. Available: http://webpki.org/papers/keygen2/keygen2-key-escrow.pdf, [Accessed: March 10, 2009]

[3] Wikipedia, "Message authentication code", 2009. [Online]. Available: , [Accessed: March 4, 2009]

[4] Professor Fred B. Schneider, "Something You Know, Have, or Are", 2008. [Online]. Available: http://www.cs.cornell.edu/Courses/cs513/2005fa/NNLauthPeople.html, [Accessed: December 8, 2008]

[5] Wikipedia, "Non-repudiation", 2008. [Online]. Available: http://en.wikipedia.org/wiki/Non-repudiation, [Accessed: December 8, 2008]

[6] Motta, G.H.M.B.; Furuie, S.S., "A contextual role-based access control authorization model for electronic patient record", September 2003, pp 202-203

[7] Joel Hruska, "Australia's controversial national ID program hits the dumpster", December 2007. [Online]. Available: http://arstechnica.com/tech-policy/news/2007/12/australias-controversial-national-id-program-hits-the-dumpster.ars, [Accessed: December 9, 2008]

[8] Marco Casassa Mont, "Privacy Management - Focusing on the Real Issues: Enforcement and Accountability", November 2003. [Online]. Available: http://www.hpl.hp.com/personal/Marco_Casassa_Mont/Projects/IdentityManagement/LibertyAlliance2003-mcm-v2.ppt, [Accessed: December 8, 2008]

[9] Andreas Pfitzmann, Marit Hansen, TU Dresden, ULD Kiel, Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, Feb 2008

[10] Jo Mellemans, Account Manager, eID Success or failure?, March 2008

[11] FINEID.FI , "Technical information about electronic identity", 2008. [Online]. Available: http://www.fineid.fi/en, [Accessed: December 8, 2008]

[12] Estonian ID, "ID-Card - a contemporary personal identification document", 2008. [Online]. Available: http://www.id.ee/?lang=en, [Accessed: December 9, 2008]

[13] AS Sertifitseerimiskeskus, The Estonian ID Card andDigital Signature Concept, 2007

[14] M. Wahl, "A Summary of the X.500(96) User Schema for use with LDAPv3", December 1997. [Online]. Available: http://www.ietf.org/rfc/rfc2256.txt, [Accessed: January 12, 2009]

[15] UNICEF, "Sri Lanka - Statistics", 2008. [Online]. Available: http://www.unicef.org/infobycountry/sri_lanka_sri_lanka_statistics.html, [Accessed: May 25, 2009]

[16] W3C, "XML Signature Syntax and Processing", June 2008. [Online]. Available: http://www.w3.org/TR/xmldsig-core/, [Accessed: January 8, 2009]

[17] Sun Microsystems, Inc. , "Java Card 3.0.1 Platform Specification", 2008. [Online]. Available: http://java.sun.com/javacard/3.0.1/specs.jsp, [Accessed: January 8, 2009]