System Design Document

CNWIS-G2

Project eID

Version: 1.0

Revision Date: 04/09/2008

www.project-eid.org

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

Table of Contents

Section 1. Introduction

1.1. Purpose

This is the System Design Document (SDD) of the project eID (electronic identity). The SDD will break down the project into domains and the domains into components to describe in detail what the purpose of each component is and how it will be implemented. The SDD will also serve as a tool for verification and validation of the final product.

This document is intended towards the general audience with interest about the eID project. Specifically the government authorities and policymakers would find useful information about the eID project. Also the staff members of the Department of Computer Science and Engineering, University of Moratuwa, mainly the project supervisor, project coordinator, project evaluation panel, and the development team of the project could be using this for various purposes. The supervisor will refer to the SDD whenever needed during the progress of the project.

1.2. Electronic Identity

Electronic Identity is the electronic replacement for traditional ID cards. This will be the electronic counterpart to the existing national identification card (NIC), with more diverse uses other than functioning as a mean to prove identity of a person. Electronic identities will be the basic tool for authentication and identification in future. This will serve as a medium in the physical world and also in the connected online world. But the use of such electronic identity devices such as electronic identity cards brings in a serious issue of user privacy. We are researching to figure out solutions to these issues and to implement an electronic identity system which preserves a user's Anonymity, Unobservability and Unlinkability.

1.3. Scope of Project eID

The scope of the eID System includes its distinct features, its benefits, and its limitations. The system's distinct features permit the holder to authenticate himself offline and to access any e-government services and several other services from various service providers. While proving the authentication offline the system lets the law enforcement authorities to validate the eID card, then validate the person and check with the POI (Person of interest) database to see the person is entitled for committing any crimes or any unlawful actions. System allows the eID holder to access the online services with protecting his/her privacy. We strongly concerned about preserving Anonymity, Unobservability and Unlinkability properties of the users. We are researching about implementing Anonymous credential Systems[4] in the service side considering the privacy issues.

Section 2. Overall System Architecture

2.1. Architectural Design Approach

We are using Service Oriented Architecture (SOA) for service side implementation. SOA is an approach to loosely coupled, protocol independent, standards-based distributed computing where software resources available on the network are considered as Services. We'll have our authentication application published as a web service and there would be several other service providers to publish their own service. They can use the authentication service for certification and then offer the service. The potential of SOA was realized in this context as it would greatly help easy integration of several other applications with the eID system.

Further we understand the privacy concerns of the users with Anonymity, Unobservability and Unlinkability properties. We value their apprehension on this issue and have decided to use Anonymous Credential Systems (also called pseudonym system) in which linkability can be avoided. In such systems different service providers and credential issuers know the users only by pseudonyms. A user can not be linked with his different pseudonyms. Yet, an organization can issue a credential to a pseudonym, and the corresponding user can prove possession of this credential to another organization (who knows him by a different pseudonym), without revealing anything more than the fact that the user owns such a credential.

Users can 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. We've developed a policy for data collection in this circumstance considering the privacy concerns of users. It will ensure that anybody's information will not be revealed without the permission of law authorities. The policy will be implemented in such a way so that *you can stay anonymous until you don't commit any forbidden action*.

We are using internationally recognized standards for service implementation, secure data management, cryptographic techniques and algorithms, mainly for the PKI implementation, eID card design, signature schemes and web services. There are several other standards for eID card specification, key size for encryption and the data format standards, which also will be considered.

Seven laws of Identity specify the required properties for an identity providing application. We're more concerned about complying with those rules because they are the building blocks of identity infrastructure. Failing to incorporate with those rules would never get positive feedbacks from the normal people.

2.2. Architecture Design

The following figure depicts the overall system architecture.

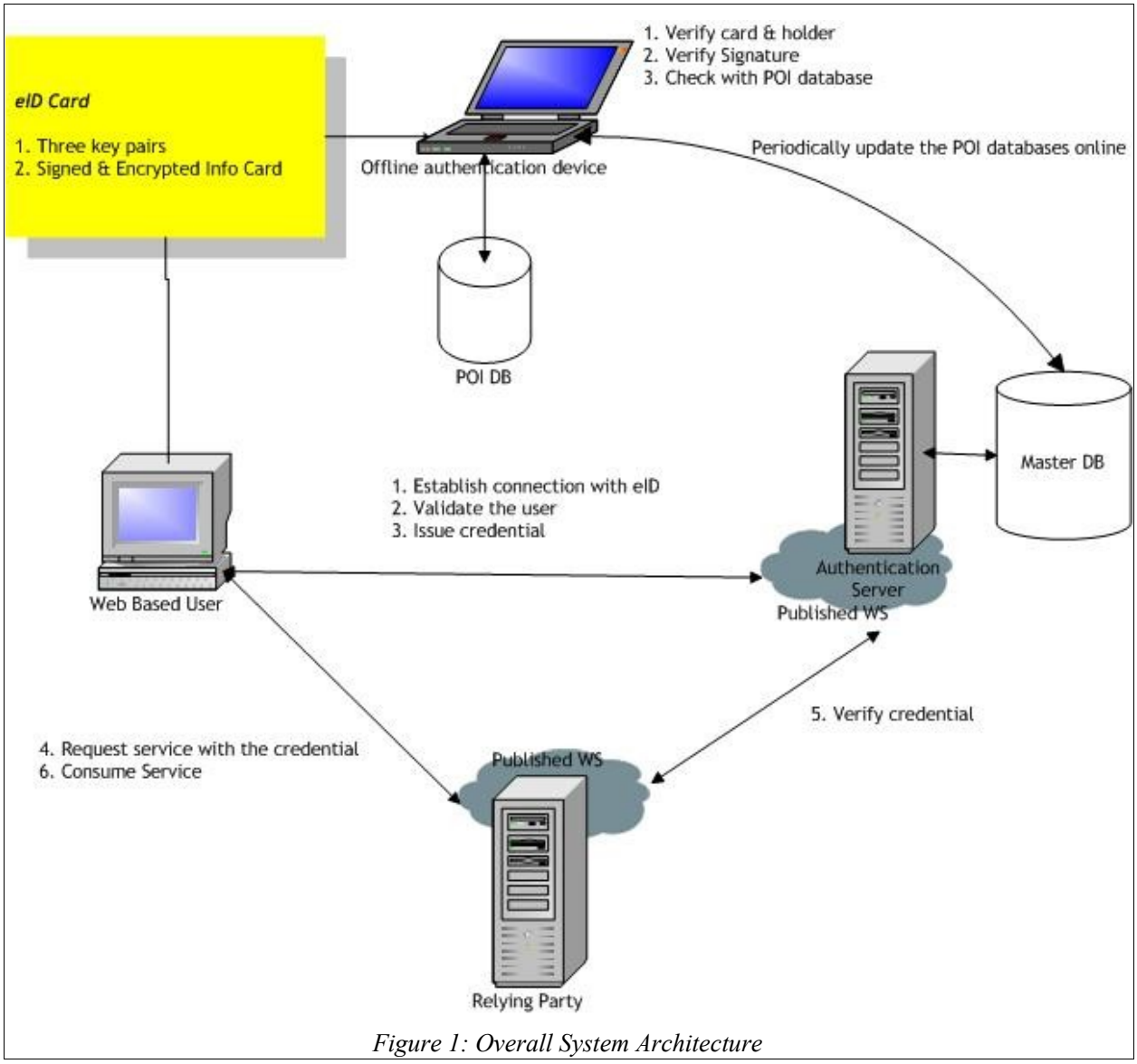

Figure 1: Overall System Architecture

The eID system can be used in offline mode as well as in online mode for authentication. The eID container will be a Smart Card with USB interface which is easy to be used with all computers having a USB port. There is no need to have a smart card reader at each point whenever the eID has to be used. But there is a flexible option to simply change to smart card based eID if requested.

2.2.1. Offline Authentication

The eID card will be validated at first with the eID identifier and the key. Then the user will be validated, while doing this, the Personal Identifiable Information (PII) will be checked with the Person of Interest (POI) database. If the person is not in the list then he's authenticated and this certified information will be collected according to the following policy.

The PII will be processed inside the USB smart card. There will be designated group of juries and they'll be configured with group signature scheme. There will be a common public key for the group and different private keys for each jury. This public key will be used to encrypt the PII. Before that PII will be signed by the officer who checks the identity for security purposes. This will ensure that the eID was checked by some authorized person. This encrypted data will be updated to the main database when the device goes online. The POI databases in the remote devices also will be periodically gets updated.

2.2.2. Online Authentication and Service access

We are using web services to implement the Service Oriented Architecture. For protecting the privacy of the users we're using the Anonymous Credential Systems (also called as Pseudonym systems). Our authentication service will act as credential issuer and the service providers will act as credential verifiers.

We're also concerned about strong privacy enhancing access control enforcement; we'll implement these concepts wherever appropriate. Clear separation between Access Control Decision and Access Control Enforcement will help for efficient access control to data.

Section 3. Component Architecture

3.1. Online Web Services

eID Web Service is one of the main part of the eID system, which is providing online authentic and identity facilities. In here we define a protocol that allows a service provider to generate an authentication request for an eID card holder and receive an authentication assertion in response. For secure and reliable functioning of web service, integrated it with a J2EE servlet container. In all of these cases, the authentication results in a SAML assertion being used to communicate the authentication event. In eID system there are four main components working in concert.

- **Authentication -** handles service requests, that are need to be are authenticated
- **Identity -** subsequent to authenticate the user by requesting web service, RP can claim to know the identity of that user.
- **Malicious Protection Mechanisms –** protect against the malicious attacks that can be harmful to the system, user and Reliant party.
- **Offline Authentication Logs Handler** – Process the logs entries in online that are saved in offline authentication process, which will be orchestrate offline and online log records.

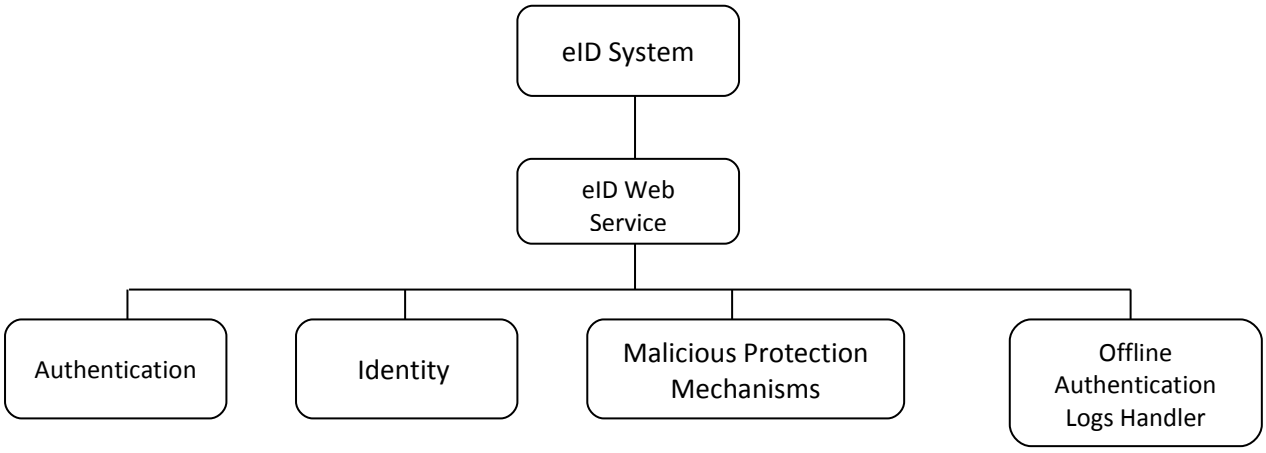

Figure 2: Components of eID Web Service

3.1.1. Authentication

Authentication component is handles authentication requests from Reliant Parties, those are need to be are authenticated eID card holders. Authenticate component authenticate the reliant parties before handle the requests send by them. That will be ensure that any data belongs to the user want be provided to a malicious activity and gather the access level of the Reliant Party. Also authentication request are send through Malicious Protection Mechanisms component to ensure that

request will not be performed a malicious activity in the system. Then Authentication component directly validate the cardholders authentication using special applet that will sent to card holder.

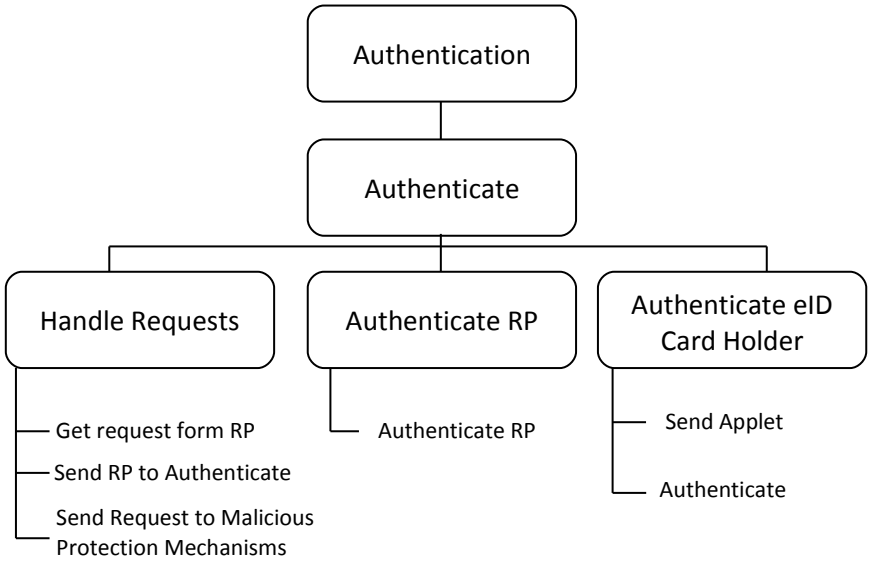

Figure 3: Authentication Module

3.1.2. Identity

Subsequent to authenticate the user by requesting web service, Reliant Party can claim to know the identity of that user. So if they have request for identity of the card holder, authentication component let that to be handle by the identity component of the eID web service. Identity component will provide identity of the card holder depend on the Reliant Parties access level. That will ensure that only necessary portion of data have been provided to the Reliant Party.

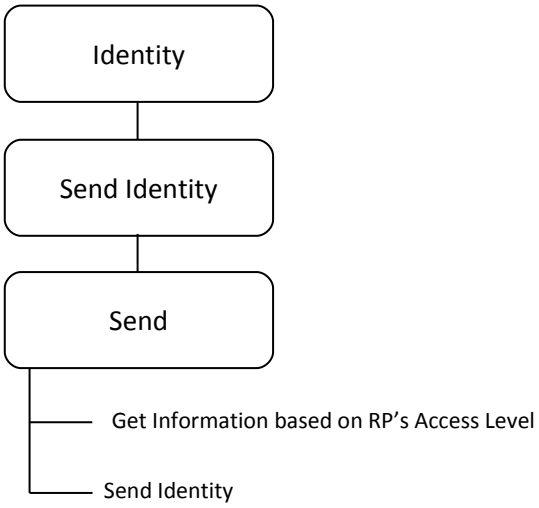

Figure 4: Identity Module

3.1.3. Malicious Protection Mechanisms

This component protects eID system against the malicious attacks that can be harmful to the system, user and Reliant party. This component perceives malicious activities, send with authentication requests and reject them. That ensures that privacy data of card holder of Reliant Party want misused by malicious attacker.

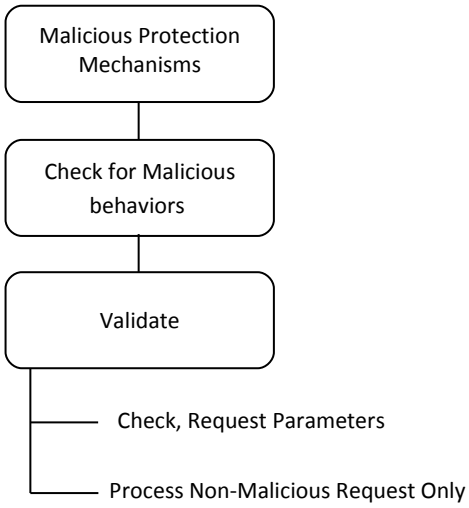

Figure 5: Malicious Protection Mechanism Module

3.1.4. Offline Authentication Logs Handler

Process the logs entries in online that are saved in offline authentication process, which will be orchestrate offline and online log records. In offline authentication also offline authentication devices keep logs record in secured manner. So that is very important to upload offline authentication log record in to data warehouses. This all process handles by the offline Authentication log handler component in the eID web service.

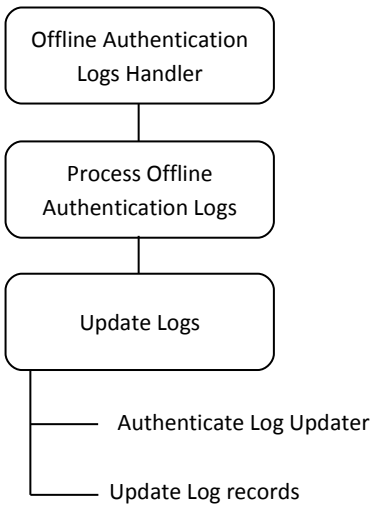

Figure 6: Offline Authentication Logs Handler Module

3.1.5. Use case Diagram

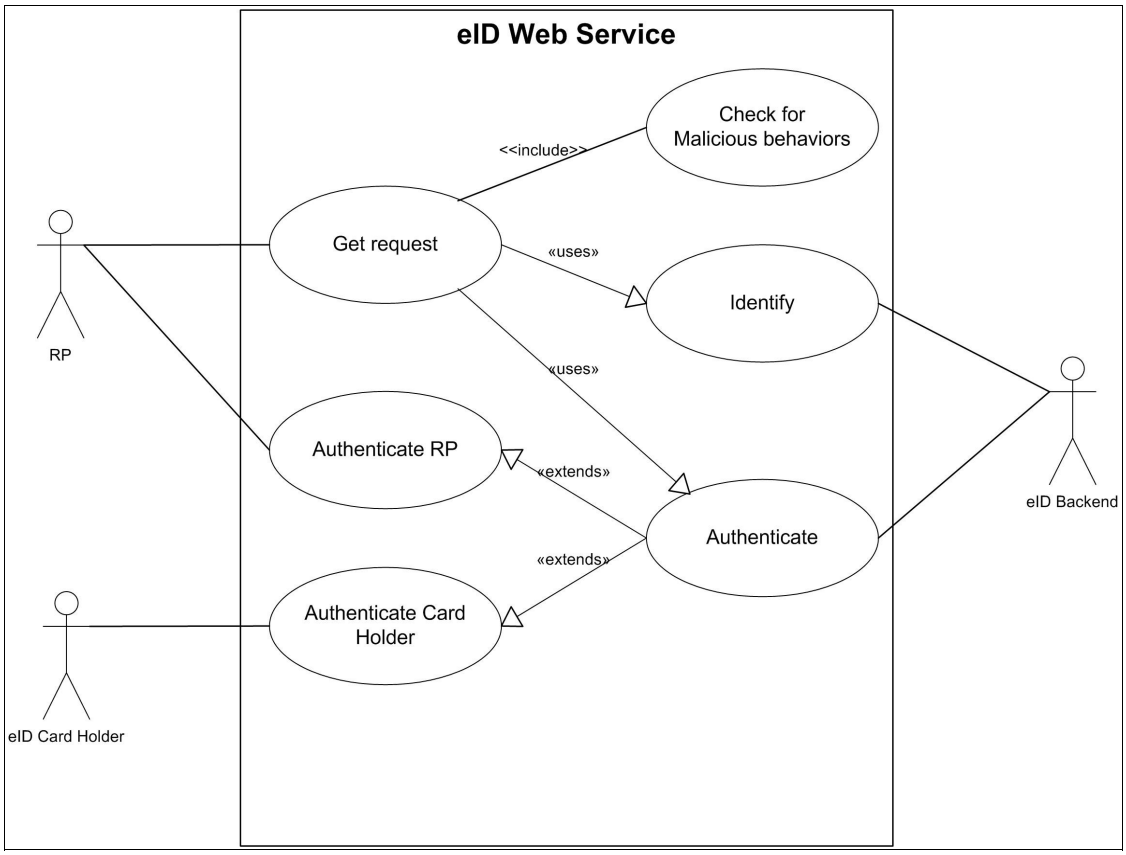

Figure 7: eID Web Service Use case diagram

3.1.6. Sequence Diagram

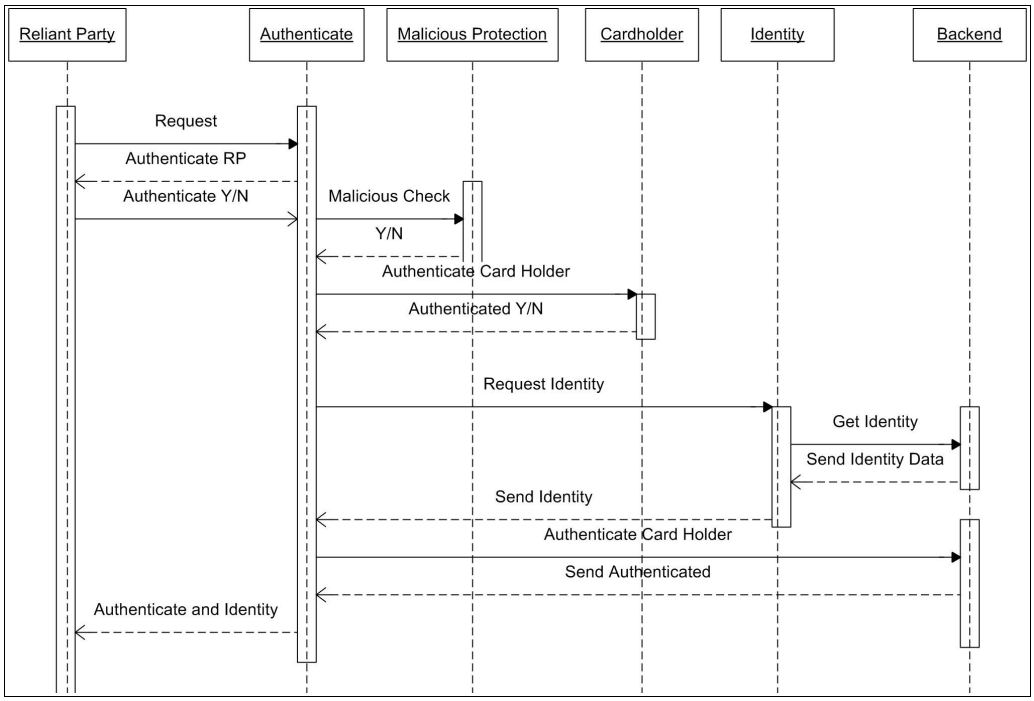

Figure 8: eID Web Service Sequence Diagram

3.1.7. Activity Diagram

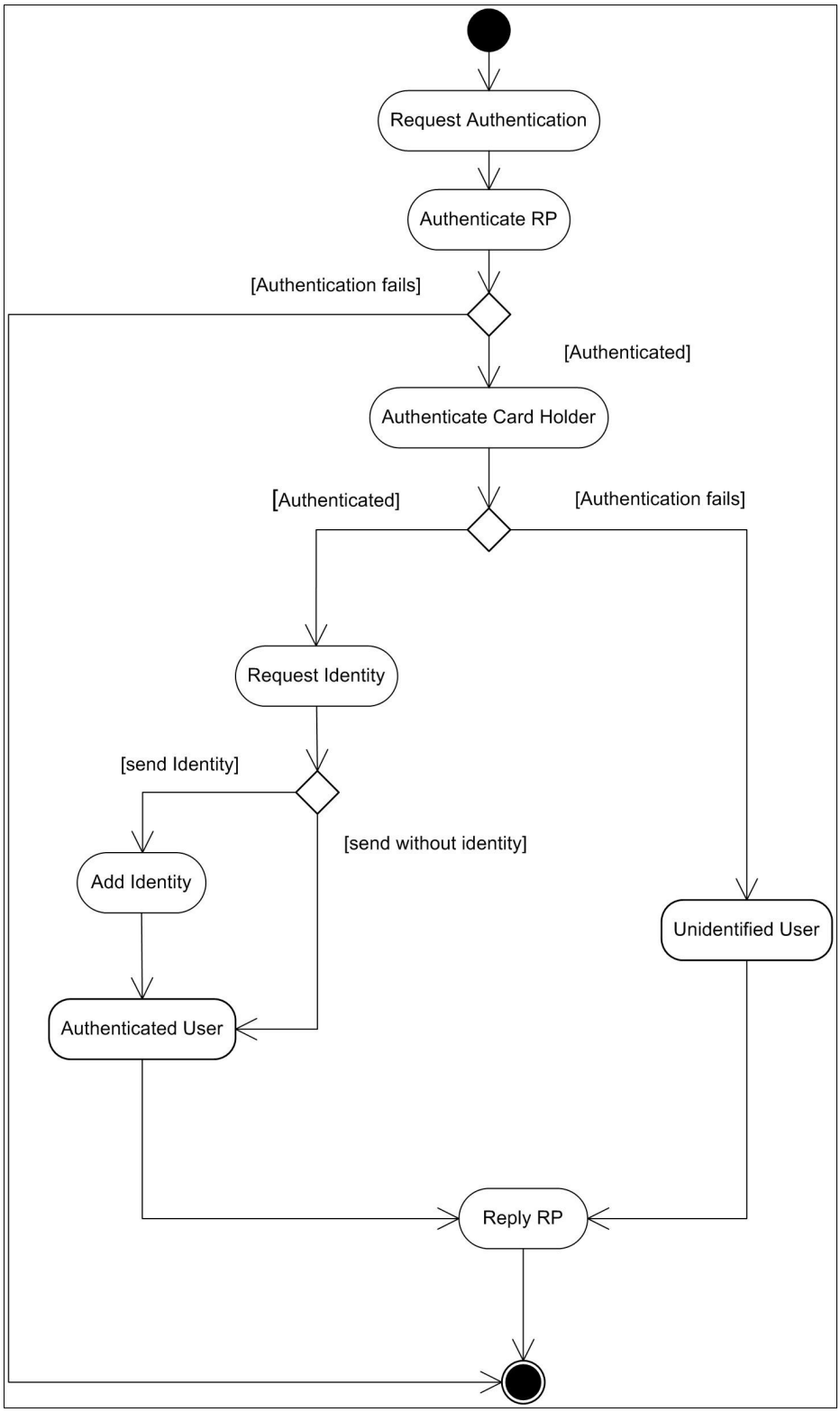

Figure 9: eID Web Service Activity Diagram

3.1.8. Data Flow Diagram

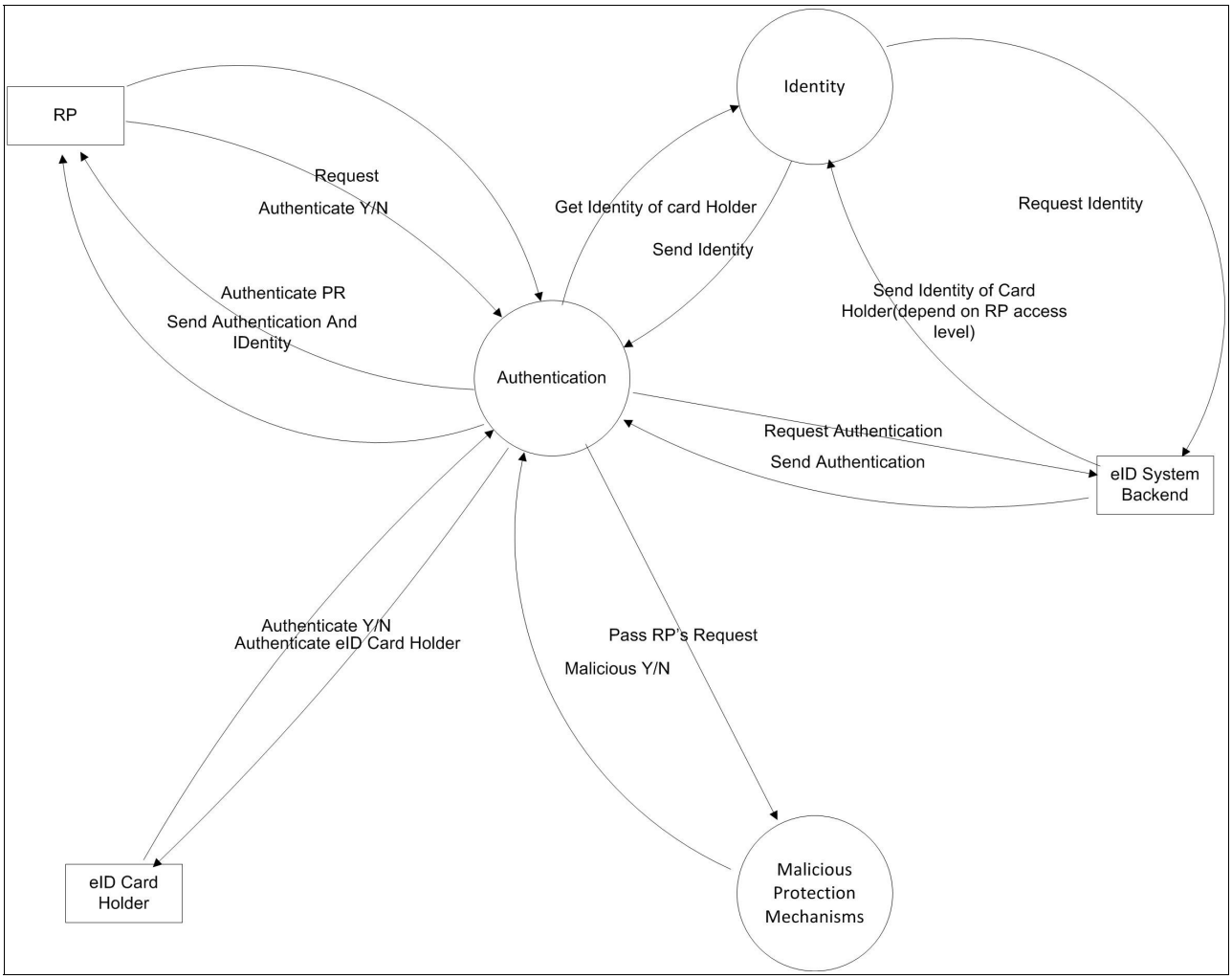

Figure 10: eID Web Service Data Flow Diagram

3.1.9. Constrains

eID web service, which is providing online authentic and identity facilities to the eID system, performed under lots of constrains. Due to system mainly consist of a web server and a servlet container, eID web service is exposing to threat, so there are some security constrains which we have to consider while implementing the web service. Web service's Malicious Protection Mechanisms acts on the security constraints defined and enforce the security constraints accordingly. The security constraints of authentication request shouldn't be violate the security constrains of the eID web service, if not request is denied. Because SOAP message does not include the integrity specified in the request constraints.

System should have set of proper defined set of policies to protect the system form vulnerable attacks. Also web service should not violate security laws define by law of the country and the international institutes. There are some other important things we have to consider regarding the

authentication web service used in the eID system. Web Services implement interoperability Message Exchange Patterns across multiple systems. So, the security architecture must deal with how identity data protected as it is ported across organizational and technical domains.

Also when we are providing identity information to the Reliant Parties, system should provide minimum amount of identity information to them. Maximum level is the "access level" which is defined for that Reliant Party by the system. So in here system should act in the proper manner, which only minimum size of dataset will return to the Reliant Party, depends on request. Web Services are frequently used in peer to peer and ESB scenarios where messages may traverse many directions in the system. So it is difficult to have a control on SOAP/XML message according to the policies defined by the System.

3.1.10. Extendibility

eID system is designed based on the SOA architecture, which will provide more extendibility features for the eID system. In this SOA architecture eID web service acts a big role. Also eID web service is designed in loss coupling manner, which will be provide the more extendibility feature to the system. Malicious Protection Mechanisms which protect system against malicious attacks will be design with more extendible features. Because of depend on the fast changing security threats Malicious Protection system updated and extended. Due to fast changing e-commerce world, there will be new authentication requirement day by day. So authentication system also designed in extendible manner.

3.2. Offline Authentication Applications

3.2.1. Introduction

This Offline Authentication Application is required to be used mainly by law enforcement authorities such as police for authenticating the citizens. There will be similar situations where the user will have to prove his/her identity to show that he is an authenticated citizen.

The eID card will be validated at first with the eID identifier and the key. Then the user will be validated, while doing this, the Personal Identifiable Information (PII) will be checked with the Person of Interest (POI) database. The POI database will have the list of persons who are facing lawful actions or to be taken into the custody. If the person is not in the list then he's authenticated and this certified information will be collected according to the following policy.

The PII will be processed inside the USB smart card. There will be designated group of juries and they'll be configured with group signature scheme. There will be a common public key for the group and different private keys for each jury. This public key will be used to encrypt the PII. Before that PII will be signed by the officer who checks the identity for security purposes. This will ensure that the eID was checked by some authorized person. This encrypted data will be updated to the main database when the device goes online. The POI databases in the remote devices also will be periodically gets updated.

3.2.2. Interfaces/Interfacing

The interfacing with the eID is via the USB interface as it is proposed in Project eID. We are using USB smart cards for easy interfacing with PCs and wireless handheld devices. But it could be a smart card reader in case of normal smart cards. Earlier we were researching about using normal USB memory sticks as eID holders. But it formulates serious privacy violations regarding the handling of private keys. We had the necessity of using the PKI for implementing online service access using eIDs.

3.2.3. Constraints

This application needs to synchronous periodically with the POI master database whenever it goes online for accurate performance in catching the crooks. We'll have the problem with synchronizing with online databases periodically because all the devices cannot go online frequently. This kind of problem can only be solved by improving the network access technologies.

3.2.4. Extendibility Mechanisms

The OCP (Open Closed Principle) principle will be used for the application development. So it will be easy to extend the program with additional features.

3.2.5. Use Case Diagram

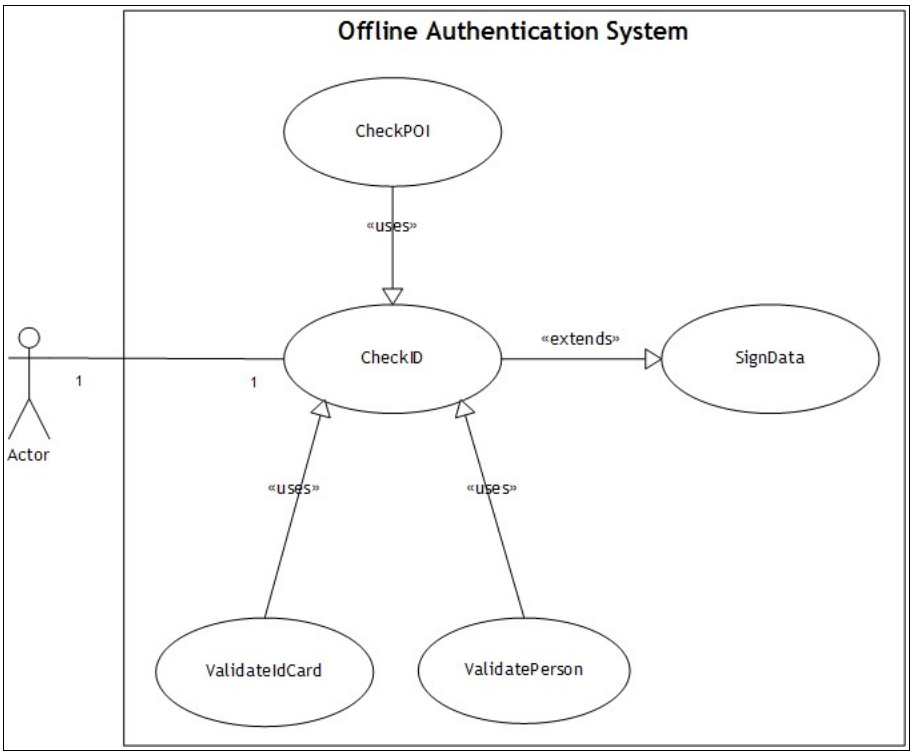

Figure 11: Offline Authentication Applications Use case diagram

3.2.6. Sequence Diagram

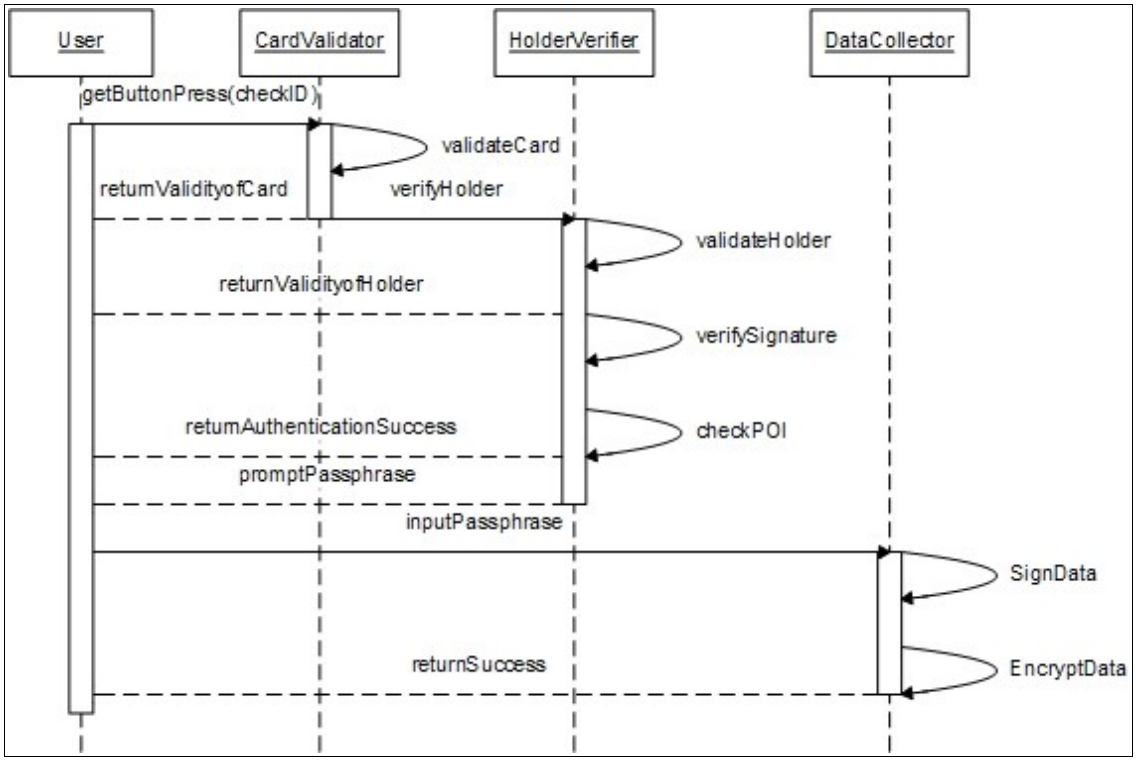

Figure 12: Offline Authentication Applications Sequence diagram

3.2.7. Activity Diagram & Class Diagram

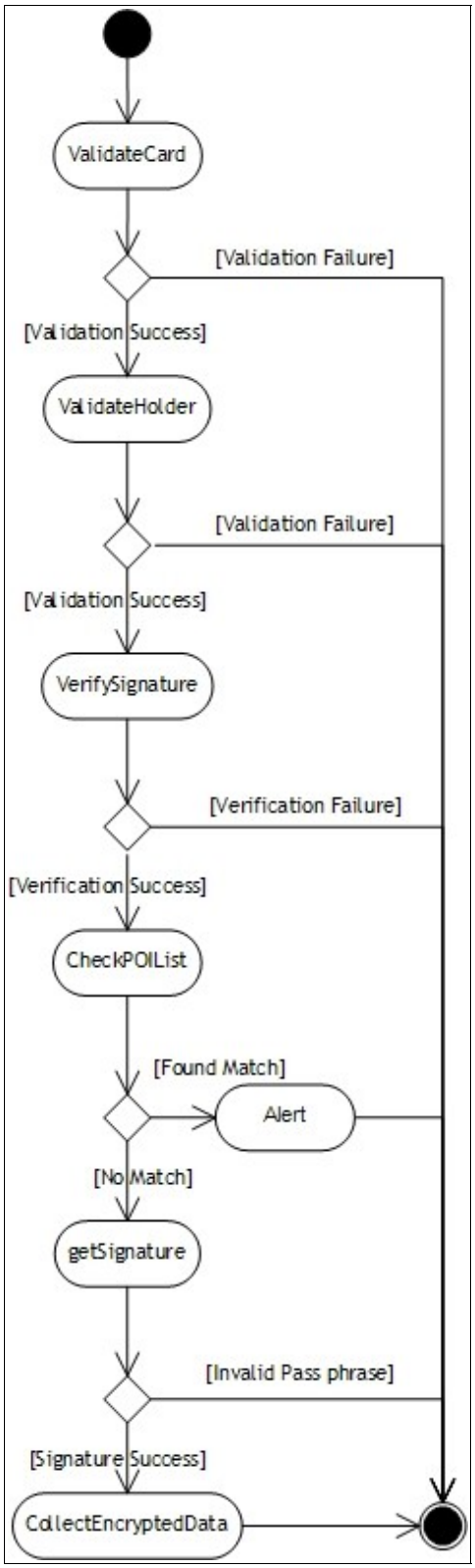

Figure 14: Offline Authentication Applications Activity diagram

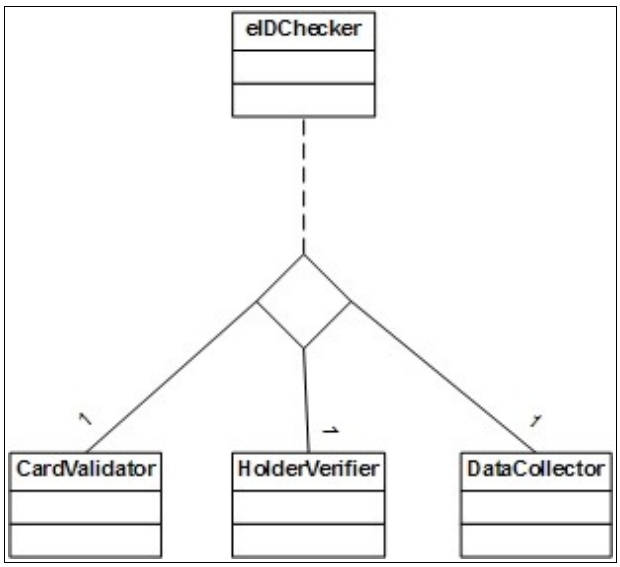

Figure 13: Offline Authentication Applications Class diagram

3.3. Back End Infrastructure

eID card creation process is the main back end process in the eID system architecture. Here we are illustrating the three important phases which are involving in the Physical card creation process.

1. Get the relevant data from the eID applicant – In this process phase authorized person get the eID applicant identification data, biographical data and the Key data. This is normally getting with the application form.
2. Authorized person digitally sign the digital data of the applicant – Here Authorized person digitally sign the applicant's digital data by using his private key.
3. Burn those data in the physical eID card – Those digitally signed data then burn in the eID card by using some chip burning equipment.

The second phase is the backbone in the above processes. Because its handle many back-end components in the eID system.

3.3.1. Details of the components

When an Authorized person needs to digitally sign the applicant eID card then he needs to login to the eID a card issuing service which is provided by the eID system through a Client side application. This application is a Web services client application which is run in the card issuing department. And the eID Login services and Card issuing services is a WEB SERVICES which are run in the eID system's web server. And another important component is the eID centralized database. Here all the details of an eID card holder are maintained in much secured manner.

3.3.2. Use case Diagrams

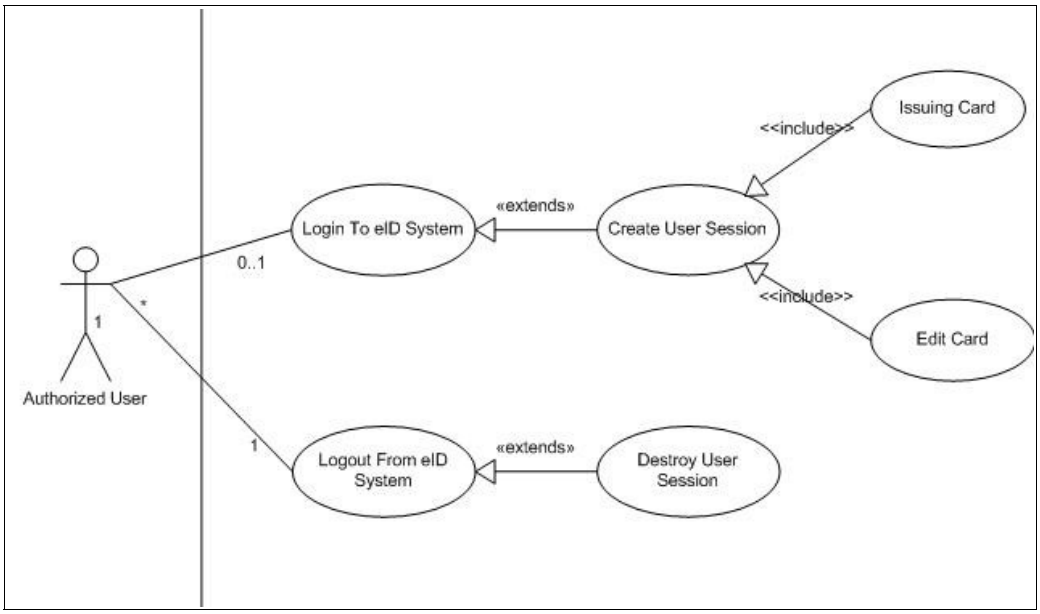

Figure 15: eID Card Issuing System - Card creation use case

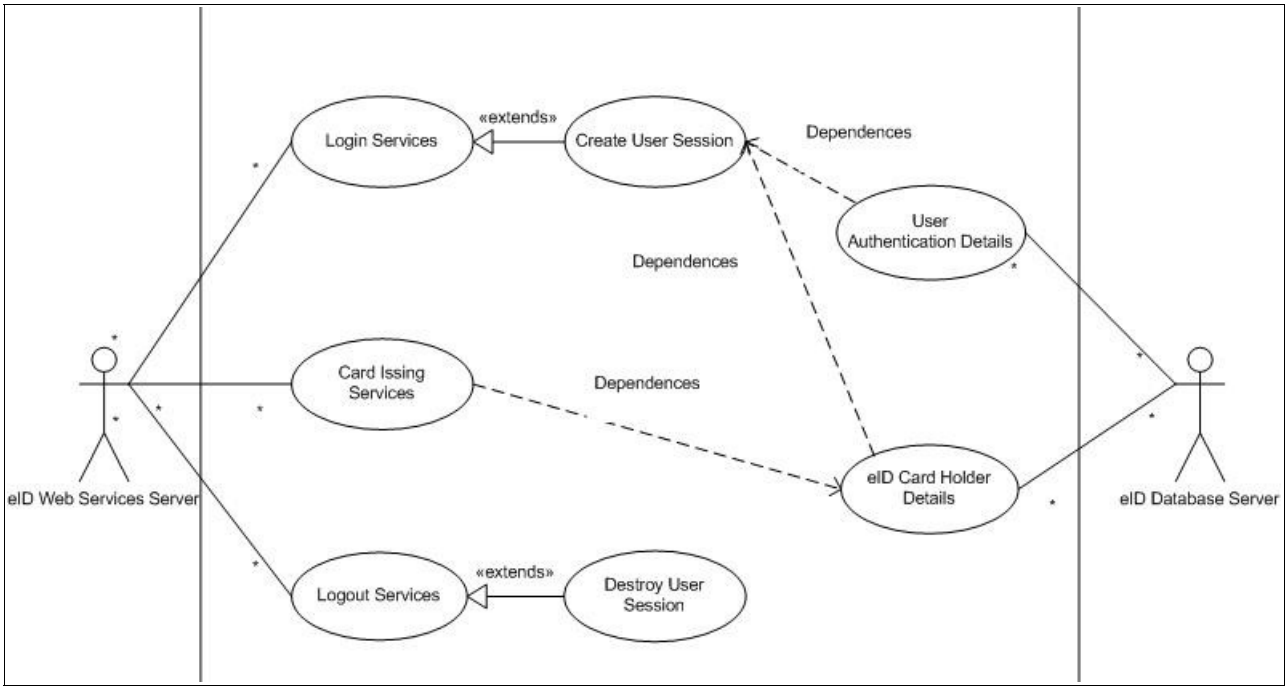

Figure 16: eID Card Issuing System - Backend process use case

3.3.3. Interfacing

The interface between the eID system and the client application is designed through the web services. Following Sequential diagram will describe it clearly.

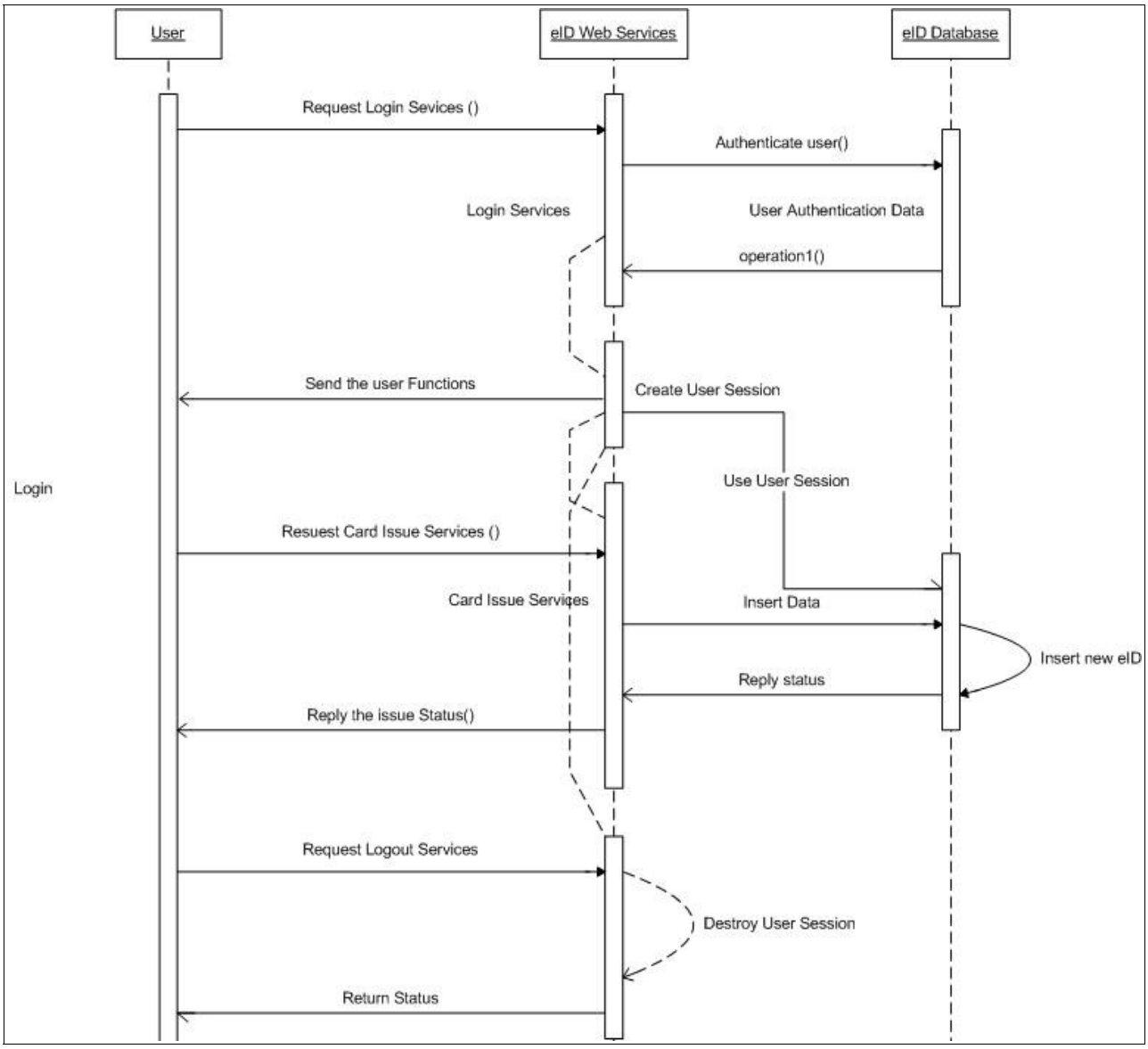

Figure 17: Backend sequence diagram

3.3.4. Activity Diagram

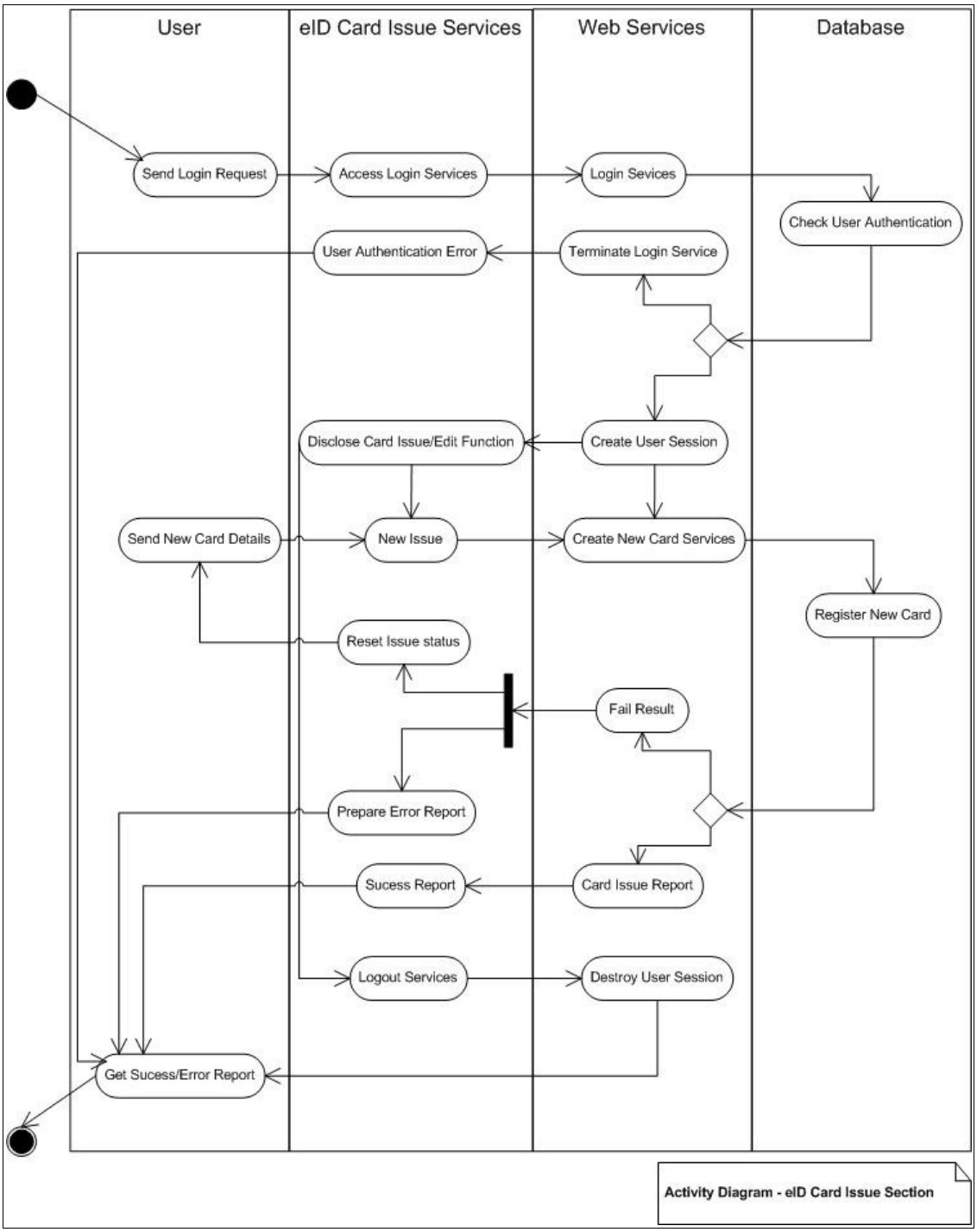

Figure 18: Backend Activity Diagram

3.3.5. Extendibility Mechanism

By using the web services in the eID system we can easily let the system to extendable. When we need to establish a new card issuing section, then we can extend the eID card issuing system without affection the entire eID system.

3.4. eID card specification

The eID card will be a smart card with a USB interface, thus it will not require any special card reader for use. This card will follow the sizes specified by the ISO/IEC 7810:2003 ID-1 standard[5], which specifies a size of 85.60 × 53.98 mm (3.370 × 2.125 in). Due to the restricted printable area of the card, all data are written without labels. This approach allows a multilingual solution if needed. On the first side are the name of the authority releasing the card, the personal data of the cardholder (surname, name, place and date of birth, photo and sex), and a unique card ID number. On the other side are the cardholder's address and the card's validity period. The eID card will have a Micro-USB interface[6] for easy connectivity to many devices.

The eID card will contain three key pairs, one to authenticate the card, next to authenticate the person and the other to signing purposes. It is not recommended to use the private key for signing which will be used for person authentication. These will follow the PKCS#7 standard[7] of non-repudiable electronic signatures. Then we'll have an Info Card that would contain Personal Identifiable Information and images of the citizen's fingerprint (not mandatory), which would've been signed by an authority and encrypted. The eID will have an identifier which will not imply any information about the user. The sole purpose of having this identifier is to identify the eID card.

Figure 19: eID Card Front Design (Sample)

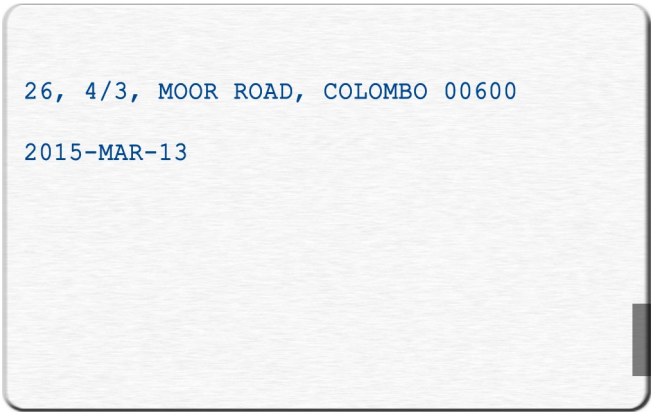

Figure 20: eID Card Back Design (Sample)

Section 4. Important design parameters

We consider security and privacy as the two important design requirements of the eID system. Security includes both the secure mechanisms for data stored in the card and the back end system security. Card level data security is provided by cryptographic mechanisms. This includes signed information stored in the card and authorized devices with limited access to the card. Back-end system security needs to be ensured both by network security mechanisms and physical security mechanisms. Also the eID web service inherently includes malicious access control mechanisms.

Privacy will be another key issue in Project eID. Privacy of user and system data is of crucial importance for an eID system. Privacy is not just another pluggable feature but one of the main system requirement of an eID system. Privacy should be ensured while the information is on the move between two parties, as well as while the data is stored in some central location. As we discuss in [1], we understand ensuring privacy is a very complicated task but it is an essential part of the eID system. Thus we are focused on this research area and we hope to make eID system as an anonymous credential system. This will give us a leap in the whole project topic.

Section 5. System Implementation Plan

We plan to implement the eID system by both using existing software components and developing other framework specific components. One of our main criteria is to use existing open source tools and software for possible requirements and then develop out one software and hardware to match open standards.

5.1. Software development

For the software system framework development we plan to reuse the following software components:

- Apache Axis2/WSAS – For eID Web Service
- OpenSC – Multi platform smart card solutions
- Java Card API
- MySQL

We will also develop the following develop software components for the eID framework:

- Offline authentication application
- Online authentication web service, using Axis and J2EE
- Smart card programming
- Implementation of anonymous credential system

5.2. Hardware development

We will be using a standard Smart Card with USB interface in the development phase. Then we will be proposing a new eID card specification which will follow the ISO/IEC 7810:2003 ID-1 standard for the physical dimension of the card, but this will also include a Smart Card with a Micro-USB interface.

Section 6. References

[1] ***Privacy Enhanced Data Management for an eID System,*** B. A. Malalasena, S. Nimalaprakasan, S. Ramanan, K. Shayanthan, Department of Computer Science and Engineering, University of Moratuwa, Sri Lanka

[2] ***Italian Electronic Identity Card - Principle and Architecture,*** Mario Gentili

[3] ***Privacy Features of European eID Card Specifications,*** Ingo Naumann, Giles Hogben

[4] ***A Security Model for Anonymous Credential Systems,*** Andreas Pashalidis and Chris J. Mitchell, Information Security Group, Royal Holloway, University of London

[5] ISO/IEC 7810:2003, Identification cards -- Physical characteristics

[6] Micro-USB Cables and Connectors Specification 1.01: Released in April 2007.

[7] Non-repudiable electronic signatures (PKCS#7)

[8] IEEE Recommended Practice for Software Design Descriptions

Section 7. Glossary

- eID Electronic Identity
- ESB Enterprise service bus
- IEC International Electrotechnical Commission
- ISO International Organization for Standardization
- J2EE Java 2 Platform, Enterprise Edition
- NIC National Identification Card
- OCP Open Closed Principle
- PII Personally identifiable information
- PKCS Public-Key Cryptography Standards
- PKI Public key infrastructure
- SDD System Design Document
- SOA Service Oriented Architecture
- USB Universal Serial Bus

Section 8. Revision History

Version	Date	Description
0.1	01-Sep-2008	Draft 1
1.0	04-Sep-2008	Submission