The Saudi Arabian Smart Card

ID2

White Paper

Summary Version

Author: Jacob P. Kremer
# TABLE OF CONTENTS

1. INTRODUCTION ........................................................................................................................................... 3  
   1.1. DOCUMENT OUTLINE .......................................................................................................................... 3  
   1.2. OBJECTIVE .............................................................................................................................................. 4  
   1.3. HISTORY ................................................................................................................................................... 4  
   1.4. WHY CENTRALIZED? ............................................................................................................................... 5  

2. ID2 PROJECT .................................................................................................................................................. 6  
   2.1. PROJECT BACKGROUND ......................................................................................................................... 6  
   2.2. PROJECT SCOPE ..................................................................................................................................... 9  
      2.2.1 Project Approach ................................................................................................................................. 9  
      2.2.2 Project Phases .................................................................................................................................... 10  
   2.3. SYSTEM COMPONENTS .......................................................................................................................... 12  
      2.3.1 ID2 Card ............................................................................................................................................ 14  
      2.3.2 Card Management System (CMS) ..................................................................................................... 24  
      2.3.3 Central Personalization System (CPS) .............................................................................................. 25  
      2.3.4 MULTOS independent KMA (iKMA) ................................................................................................. 26  
      2.3.5 MULTOS ............................................................................................................................................ 28  
      2.3.6 Enrolment Management System (EMS) ............................................................................................ 30  
      2.3.7 SAMIS (Central Data Infrastructure – DB2) ...................................................................................... 31  
      2.3.8 SAMIS Gateway ................................................................................................................................. 31  
      2.3.9 CLEB (Card Lifecycle Event Broker) ................................................................................................ 33  
      2.3.10 Certificate Authority (CA) .............................................................................................................. 34  
      2.3.11 CA Gateway ...................................................................................................................................... 34  
      2.3.12 Card Update and Validation Gateway ............................................................................................. 35  
   2.4. OVERALL LOGICAL ARCHITECTURE ....................................................................................................... 38
1. INTRODUCTION

1.1. Document Outline

Chapter 1 provides an overview of the purpose of the Kingdom of Saudi Arabia (KSA) smartcard based Identity Cards being Phase 1 and Phase 2. This document further on provides information about the Identity Card Project Phase 2 (ID2).

Chapter 2 provides an overview of the ID2 Project and includes information about the project structure and the overall ID2 Systems Architecture with all of its major components. This chapter also includes a section about the project achievements as well as its unique design as to Card Data Security and Availability.
1.2. Objective

With the launch of the initiatives towards e-government and e-commerce, the Ministry of Interior of the Kingdom of Saudi Arabia (MOI) has recognised the need for technological change. As these initiatives are implemented, the MOI will face new challenges involving much more than just delivering services to citizens and businesses electronically.

Main Objectives:

- Enhance National Security
- Provide strong authentication of citizens by law enforcement officers (police, border control, etc)
- Provide service to citizens/residents
- Enable e-Government
- Enable innovative services for card holders in cooperation with other Ministries and Private Sector
- Provide and efficient and secure as well as reliable identity card
- Provide infrastructure for other types of ID-solutions in the future

1.3. History

The Card Printing Project Phase 2 (ID2) is the follow up project for the Phase 1 ID Card Project. Both Cards are Smart Chip based (Smart Cards) and have the format/size of the TD1 (Credit Card Size) ICAO standard while other ICAO size/standards defined are the TD2 which is a slightly larger size identity specification and the TD3 which is the specification for the e-passport page which holds the Micro Chip.

- TD-1 85.60 × 53.98 mm Most banking cards and ID cards
- TD-2 105 × 74 mm Netherlands and German ID cards issued prior to Nov 2010
- TD-3 125 × 88 mm Passports and Visas
- TD-000 25 × 15 mm SIM cards

Both Cards have an Infineon microchip (Contact) running the MULTOS Operating System. Differences between the Phase 1 and Phase 2 cards are:

- Phase 1 card single application and is 32 KB EEPROM, Phase 2 is 68 KB EEPROM
- Phase 1 has a single data container application while the Phase 2 card has:
  - MOI Data Container with:
    - Facial and fingerprint biometrics
    - Full Family (40) Member Data
    - Drivers License
    - Passport
o MOH Data Container
o Signing Application with PKI Certificate
o Secure Channel application with PKI Certificate
o Role based PKI certificate for access control
o Phase 1 card is PVC while Phase 2 is a high quality PC Card
o PIN Application to utilize and manage user identified PIN Code

The Phase 1 Card was issued starting early 2005 and issuance has been discontinued while all MOI User Sites now only issue the new Phase 2 cards. The Phase 2 Card started rollout in January 2008 and is now issued at all MOI User Sites. Another difference between the Phase 1 and Phase 2 ID Projects is that the Phase 1 Project was a distributed approach where all cards are enrolled, printed and issued at the User Sites, while the Phase 2 Project is a Centralized Approach where the enrolment is done at the User Sites and all Personalization of the card is done centrally.

1.4. Why Centralized?

The centralized solution provides a much security environment where the printing/personalization is performed in a high secure Operations Floor with full biometrics access control and separate security zones in the Personalization Area. All produced cards go through a rigorous QA Process and all cards are shipped to the User Sites under strict security processes. Another reason is that the “Distributed” approach can only be performed using “Table Top” Smartcard Printers which produce a lower quality card with less security features and lower life cycle expectation. Also the “Table Top” Printers can only do D2T2 (Ink Printing) which requires a protective lamination which also reduces the life cycle expectation.

The Central Printing Systems are high capacity personalization systems which can perform virtually any printing requirement such as Laser Encoding, Card Surface Security features (See also Section 2 of this document) and although Laser Encoding as for now, only support Black and White Graphics the usage of Laser Encoding provides a high quality and secure engraving of the card and does not require a lamination layer.

MOI HQ Building
2. **ID2 Project**

2.1. **Project Background**

The ID2 Contract was awarded to Logica in 2004 and actual work based on a “Scope of Work” agreement, started early 2005. The diagram below depicts the Logica Project Organization Chart.
Logica was the Prime Contractor and used GemAlto as the subcontractor to provide:

- High Volume Card Personalization Systems
- Cards based on LaserCard Infineon chip and 1 MB Optical Stripe
- Card Surface Design and Laboratory Quality Tests
- MULTOS masking
- Printing/Personalization Management Software

Logica as the prime contractor provided all remaining elements of the agreed Scope of Work such as:

- All Hardware and Systems Software
- Requirements Definition Documents
- Network Design and delivery of all components
- Complete Systems Design and Development
- Testing (Unit, Integration and Acceptance)

The project started in 2005 with the Requirements Definition Phase which completed with a final sign off around the end of 2005. The Design and Development phase completed early 2006 and after a few rounds of MOI/NIC changes to the technical solution the final products started being delivered and tested around the end of 2006.

During 2007 a comprehensive round of Integration and Acceptance Tests were performed which resulted in additional changes and enhancements. First Pilot Sites were implemented during 2007 and a complete Kingdom wide rollout started at the end of 2007.

More than 50 Technical Position Papers were produced and several key decisions were made during the Requirements and Design Phases.
The ID2 (Identity Card Phase 2) replaces the Phase 1 ID Card and is issued to all Male Saudi Citizens 15 years and older. The diagram above provides a conceptual overview of the ID2 System Components.

The Card Enrolment and Handout is performed at all MOI User Sites while all other processing is performed centrally at the MOI IT Division (National Information Center – NIC).
2.2. Project Scope

2.2.1 Project Approach

The high level overview of the total project is given in the next diagram.

The horizontal axis represents the project phases and the vertical axis represents the work streams. The high level activities on all cross points for project phase and work stream are listed in the diagram.
Activities with *Italic* text, white filling and thin lines are in scope for MOI/NIC.
Activities with **Bold** text, colored filling and thick lines are in scope for LogicaCMG.

### 2.2.2 Project Phases

**Mobilization & start-up**

During mobilization & start-up the project team was formed and project and quality plans written and agreed. The intention of this phase was to be fully prepared for the start of the project.

**Detailed Requirements Specification**

During the detailed requirements specification phase detailed specifications of the scope will be produced. The output is the exact specification of the solution (i.e. the Controlling Specification).

**Development & unit test**

After the detailed specifications were agreed with MOI/NIC, the development of the solution started based on the Controlling Specification (Functional Requirements Specifications (FRS). Subsequent changes to specifications were made through an agreed change control process. After development each component was unit tested.

**Integration & Acceptance test**

During the integration test the solution was tested in the acceptance environment linked to all other systems (like the Central Personal Database (SAMIS)). This to ensure the solution developed supported all agreed requirements. After this, during acceptance, MOI/NIC verified that the developed solution did meet the agreed requirements. This phase ended with the Preliminary Hand over of the solution to MOI/NIC.

**Deployment**

During Deployment users were trained and deployment commenced to other user sites in the country.

**Warranty & Maintenance**

During the warranty & maintenance period of three years Logica provided warranty & maintenance on all deliverables, both hardware and software. Logica did implement a support desk to facilitate this support.

Warranty and Maintenance Structure see diagram below:
The process of application and issuance of cards is visualized in the interaction diagram below.
2.3. System Components

The ID2 solution comprises of the following main components:

- ID2 Card
- Card Management System (CMS)
- Central Printing System (CPS)
- MULTOS Independent KMA (iKMA)
- Enrolment Management System (EMS)
- SAMIS (Central Database (DB2))
- SAMIS Gateway
- CLEB (Card Lifecycle Event Broker)
- CA (Certificate Authority) (PKI ENTRUST)
- CA Gateway
- Card Update and Validation Gateway
For a high level overview of all ID2 components see diagram below.
2.3.1 ID2 Card

The ID2 card has an embedded microchip as per ISO 7816 standards which as an internal structure as presented below.
The chip is an Infineon SLE66CX680PE with RAM – 6KB, ROM – 244KB, EEPROM 68KB

The diagram above shows how the micro chip is embedded in the card.
The chip “data structure” is shown below and can be compared with a MS Windows Folder-File Structure
The ID2 card applications are graphically represented on the diagram below:

The base card is a Poly Carbonate (PC) material card which is described in the diagram below. Further in this section an overview of the different card materials available with their advantages is described.

A polycarbonate identity document, such as an ID card, is created by fusing together multiple layers of polycarbonate in a glue-free process, using temperature and pressure.
Each layer has a specific role:

- The central layer is generally opaque and white. It can house an antenna to enable contactless reading of an electronic chip.
- Intermediate layers carry the security imprint and specific security features, such as holograms and screen-printed OVIs.
- A carbon-enriched intermediate layer supports laser-personalization.
- The outer layer bears the tactile embossing and the CLI.
MOI/NIC Requirements for the ID2 card includes:

- Support for multiple types of cards with different configurations in parallel
- Strong physical and logical security features in order to prevent fraud
- Flexibility to extend card functionality
- Multiple types of cards with different configurations are supported in parallel
- All existing ID cards (Citizens) and Iqama cards (Residents) will eventually be replaced by ID2 cards
- Durability
- NIC as the card issuer controls the card and its functionality; other organizations could deploy functionality if NIC agrees
- Strong life cycle management of the cards, the card applications and the corresponding key material
- Local enrolment and issuance; central personalization
- Automation where possible
- Strong authentication, signing and biometric verification are core functionalities of the cards.
- A shadow copy of relevant citizen data is available on the card and needs to be synchronized when possible
- The cards can be used offline and online
- Cards should be usable for border control in GCC
- Third parties will be provided with the means to integrate with the card

The card surface personalization is performed by using the Laser Engraving methodology. Other matters of personalization is D2T2 which is used by the Malaysian Smart Card (See my White Paper for this Project)
Why Poly Carbonate (PC)

What sets polycarbonate apart from other materials is the fact that it is non-de-laminable. When used in pure form and not mixed with other plastics, the different layers of polycarbonate that make up the identity document fuse together to form a single, solid card body. All security features, including irreversible laser-engraved personalization information, are safely located within and protected by the 100% polycarbonate card body.

In addition to traditional security features, such as security printing, screen-printing with optically variable inks (OVIs), holograms and diffractive optically variable image devices (DOVIDs), polycarbonate is unique in supporting highly fraud-resistant level-one security features; that is to say those visible to the naked eye. These features, which are easily authenticated by the relevant authorities, include changeable laser images (CLIs), clear windows and irreversible laser-engraved information personalization.

Moreover, polycarbonate’s durability allows for the production of long-lifespan identity documents, which can last for over ten years, and it is available in a choice of interfaces including chip-less, contact, contactless and dual interfaces (whether with one shared or two distinct microprocessors).

Polycarbonate has won the trust of governments around the world and is used in the production of at least 14 national identity card programs, ten national passport programs and 13 national driving license programs. In addition, the majority of national electronic identity cards deployed worldwide are made from Polycarbonate.
Why Laser Engraving versus D2T2

Laser engraving on a polycarbonate identity document results in the formation of a permanent black mark and this mark is precise and non-reversible.

This technique is used to personalize a blank document with the holder’s information using text and a photograph of the holder.

The letters and figures are deep black, and may have a distinctive texture. The photo is black and white, with shades of grey and high contrast.

Personalized engravings are made within the solid polycarbonate card body frame and are therefore irreversible.

The Laser Sealer process combines guilloches and a photograph in such a way that any attempt to perform additional laser engravings subsequent to the official personalization of the document is easily detected.

This technology has been used in Europe for more than a decade for high security documents. Only disadvantage is the Photo engraving can only be done in Black & White

D2T2 (Dye Sublimation) (sometimes called dye diffusion thermal transfer – or D2T2) uses heat to transfer dyes to a substrate. Used for high quality color printing, the process creates continuous tone colors by varying the amount of heat applied. Typically a 3- or 4-color ribbon (cyan, magenta, yellow and black) is passed under a thermal print-head and heat is applied to deposit dye. Ribbon dyes can be applied:

a. Direct - printed directly to a card surface; or,

b. Retransfer - printed to the backside of a clear retransfer ribbon which is then fused to the card surface. Frequently used to personalize smart cards which may have irregular surfaces.
A disadvantage of this technology is the supply cost for the multi-panel ribbon. Another limitation is that the dyes need to be protected from degradation that may result from chemical or ultraviolet radiation attack. The required protection called lamination is another added cost factor as well as an issue as to the life cycle duration (de-lamination) of the card.

ID2 Card Applications

PIN Application

The PIN application serves as an authentication mechanism between the card holder and the card. Its aim is to make sure that card holders authenticate themselves to the card before using applications where PIN authentication is required.
SIGN Application

The Sign application serves as an authentication mechanism between the card holder and the e-services provided by MOI or other external parties. Further it acts as secure certificate storage for storing X.509 certificate and its associated key pair. Functionality such as mutual authentication (through delegation), data signing and non-repudiation are provided by this application as well.

PIN Application

PIN Application

PIN Unblock Code etc...
Generic Data Container Application

The Generic Data Container application serves the functionality of storing and managing various sets of data. This application will be cloned on the card to provide a data container application for MOI (MOI-DC) and another data container application for MOH (MOH-DC).

Secure Channel Application

The secure channel application serves as a provider of mutual authentication, data confidentiality and data integrity from the card and the central system and vice versa.
2.3.2 Card Management System (CMS)

The MOI/NIC Card Management System is provided by ACI using their Smart Chip Manager (SCM) product.

NIC has the Card and Application Management System to issue and track all kinds of official documents.

ACI Smart Chip Manager is a multi-issuer and multi-application smart card management system that manages the complete workflow within a chip card scheme. Smart Chip Manager consists of solutions for chip card issuance and management, application parameter management, card personalization management, and post-issuance services.

Smart Chip Manager offers a complete chip card issuance solution — from single-application EMV cards to multi-application chip cards. Acting as the central repository for all card parameter values, it retains application, personalization and parameter data for future real time updates or card re-issuance.
2.3.3 Central Personalization System (CPS)

CPS is an existing server side component provided by Gemalto. The CPS consists of several subcomponents such as the central Map Server and the Site Servers at each printing site. The card printers are also part of the CPS.

The purpose of the CPS is to personalize the raw smartcards. All cards manufactured for MOI are directly transferred from the manufacturer to the central printing site and personalized in batches on request. Personalization entails both the printing of the cover and the initialization of any smart cards with initial smart card applications and encryption keys.

The CPS registers the raw cards with CMS upon arrival. Subsequently the cards are personalized in batches as requested by the CMS. The status of each personalization request is communicated with CMS. Detailed reports of the card production sites are generated such that this process can be controlled.

Below is an overview of the CPS system architecture.
CPS contains two (2) personalization printers from Mühlbauer. Both of the two printers are functional and capable of producing all card types (e.g. ID, Family Card, Driver License and Iqama (Resident Card)).

2.3.4 MULTOS independent KMA (iKMA)

The iKMA is the Independent Key Management Authority which is the Key Management System for the MULTOS environment. MULTOS is the secure Card Operating System running on the ID2 Card. See for more details Section 2.3.5.

iKMA Main Components

The iKMA hardware includes proprietary and non proprietary hardware components described in the following sections.

iKMA System Proprietary Hardware:

The proprietary hardware includes:

- **Crypto cards (NCC cards)**: The iKMA system delegates all the cryptographic operations (key generation, ALC/ADC signatures, etc.) to the NCC cards.
- **Safe alarm kits**: Hardware and wiring used to protect the iKMA safe. Crypto Alarm cards (referred to as NCA cards) constitute the main components of safe alarm kits. These cards are used for environmental and tamper protection of the iKMA safe.

iKMA System Non-Proprietary Hardware:

The non-proprietary hardware includes printers, smart card readers, servers (i.e. industrial computers) and personal computers.

The iKMA system safe is also part of the iKMA non-proprietary hardware. It is used to house the iKMA computers chassis and includes mains for power distribution cabling, fans for system cooling, etc.

The main components of the iKMA system are:
- The MULTOS Key Management Vault System (KMVS)
- The Combined Outer Office System (COO) and
- The MULTOS Service Provider Interface (M-SPI).
ROM - Read Only Memory protection Key
MISA - Used for generating a unique transport key which makes the card unusable until the card has been “enabled”
MSM - Data Enablement Key

ALC – Application Load Certificate
Used for key management for loading applications in the card EEPROM, the certificate is part of the ALU (Application Load Unit) which contains application and data for card personalization

ADC – Application Delete Certificate
Certificate with keys needed to delete an application from the card EEPROM

2.3.5 MULTOS

MULTOS (which stands for "Multiple Operating System") is an operating system that allows multiple application programs to be installed and to reside separately and securely on a smart card.

Each program is isolated by the operating system so that no application can interfere with another one. Whereas earlier smart card systems did not allow new applications to be installed or old ones deleted, MULTOS makes this possible. Updates or patches can also be installed as needed. Each application is platform-independent due to the implementation of a virtual machine.

Developers write applications for MULTOS smart cards using the MULTOS Executable Language (MEL).
MULTOS AAM is Application Abstract Machine which is similar to the JavaCard Virtual Machine.

The diagram below shows the process of card manufacturing and personalization:
Comparison MULTOS and JavaCard

2.3.6 Enrolment Management System (EMS)

The EMS enrolment modules provide web-based services to enroll new cardholders (KSA citizens). The enrolment modules integrate with the existing SAMIS to pull data from the existing citizen database. Pictures can be taken and Quality assured. After completion and validation card requests are generated for the Card Management System (CMS). The system is rule and role based to support the sequence of events and of activities of the various employees involved.

The EMS Check-In modules provide web-based services to support the logistic process receiving personalized cards that were shipped by the CPS and storing these cards at the User Site. The Check-In modules interface with the card stock tracking modules of the CMS, and can cater for support of “Automated Card Dispenser” card delivery processes at the (larger) collection sites.
The EMS Hand-Out modules provide web-based services to support the logistic process of the delivery of new card to cardholders (KSA citizens and residents). The Hand-Out modules interface with the card stock tracking modules of the CMS, and can cater for support of “Automated Card Dispenser” card delivery processes at the (larger) collection sites.

2.3.7 SAMIS (Central Data Infrastructure – DB2)

The SAMIS system can generally be described as an infrastructure holding IBM Mainframes and the DB2 Database holding all Citizens and Residents Demographic and Biometric data. SAMIS basically is the NIC legacy system controlling and saving all citizen / resident data. As the ID2 project needs the citizen / resident data the SAMIS gateway was developed to communicate with the SAMIS mainframe. All host functions are deployed in the mainframe and all clients are deployed on the SAMIS Gateway.

2.3.8 SAMIS Gateway

The SAMIS Gateway (SAMISGW) is a server side integration component.

The SAMIS Gateway hides the details of accessing the SAMIS host System from the other CSCI. SAMIS is an existing Main Frame application system for resident’s data. The SAMIS Gateway decouples the National ID system from the SAMIS application, ensuring that a change in the SAMIS does not necessarily mean the National ID system needs to be changed as well (and vice versa).

The SAMIS gateway does not need any persistence other than necessary for ensuring the correct completion of current transactions. Current updates will remain in the (persistent) queues of the source systems until correctly delivered to the SAMIS or the internal subsystems. Semi-Synchronous messages, that have a limited lifetime are not persisted and will be removed by the hosting systems after a proper timeout has been exceeded.

The SAMISGW provides citizen data to SCM for the enrolment of new Cards, status updates initiated by the SCM are communicated with SAMIS. The SAMIS GW will also communicate Card data updates initiated by SAMIS for enrolled citizens to the Card Update Gateway. The technically asynchronous communication with the mainframe is synchronized for the clients when the request and responses are correlated.

The SAMIS gateway consists of highly available WebSphere MQ Software for its integration with the other subcomponents of the solution. WebSphere Application Server is used for the validation and the conversion of messages between SAMIS and the subsystems. The IBM application server also acts as an MQ client for the queues hosted on the mainframe.
A new Mainframe application has been developed (Advantage:GEN/CICS) to provide the data that is required by the Card Printing Phase II system. This application will be developed and integrated according to SAMIS guidelines and is considered to become an integral part of the existing SAMIS application. Connectivity with the SAMISGW from Tuxedo based queues is ensured by using a Tuxedo based Tuxedo to MQ adapter. The gateway also acts as an MQ client for the queues hosted on the mainframe.
2.3.9 CLEB (Card Lifecycle Event Broker)

The CMS is authoritative source of card status and card status linked to certificate status. For flexible system design CLEB was developed to notify associated systems about card status upon important events in lifecycle of card.

The Card Lifecycle Event Broker (CLEB) is a server side integration component specifically developed for the MOI Card Printing Phase II system. The life cycle of the card is managed by the ID2 Card Management System and as more and more systems become ‘ID Card aware’ they are interested in card status changes as this will impact their functioning as well.

A clear example is the CA who needs to know when a card is created, blocked and destroyed as this should be reflected in the status of the accompanying certificates. These interfaces will be implemented as part of this change request and will be based on the CLEB architecture.

The main purpose of the Card Lifecycle Event Broker is to provide standardized message broker architecture between the ID2 and external systems currently identified and systems that will be identified and added in the future. This will then provide a common interface between the ID2 solution and other MOI-NIC systems as well as other Government Systems such as other e-Government Portals etc.

This does not imply that new system interfaces can be added without changes, but the changes would be implemented at the common interface level which makes the messaging system easier to maintain and extend. It will also simplify the addition of messaging services based on Web Services.

Before distributing a card status change to all interested subscribers the Card Lifecycle Event Broker (CLEB) will provide updated card status in the database. No history will be kept of card status for a card, so only the last card status changed for a card will be persisted.

![Card Lifecycle Event Broker Diagram](image-url)
2.3.10 Certificate Authority (CA)

The Certificate Authority is based on the ENTRUST PKI Solution.

2.3.11 CA Gateway

CA Gateway function is for transactional access to CA services for ID2 project. CA Gateway interface is standards driven (i.e. PKIX-CMP, RFC 2510).

The CA Gateway (CA-GW) is a server side integration component specifically developed for the ID2 Project system. The CA-GW acts as a bridge between the Entrust CA and other (sub) systems. It shields off the proprietary Entrust API, by providing a PKIX-CMP (RFC 2510) compatible interface over MQ. Authenticity and integrity of messages between the other (sub) systems and the CA Gateway will be guaranteed by implementing a secure (mutually authenticated) channel on middleware level.

The CA Gateway will store information about pending transactions like transaction ID’s and serial numbers of not yet confirmed (but handed out) certificates. Basically the system will store all the information about transactions to be able to prevent actions that violates pending transactions. For example it will not allow doing a certificate request for a initialized end entity that is not confirmed yet. The CA Gateway consists of a clustered WebSphere Application Server, connected to an Oracle database. The integration with CMS and the CA-GW is based on PKIX-CMP compliant ASN.1 DER encoded binary messages over a clustered WebSphere MQ instance and conforms to [IDD_CA-GATEWAY].

The CMS uses the CA Gateway (CA-GW) in two ways:

- It sends a PKIX-CMP certification request directly to the CA-GW (using the Xebia Tuxedo Bridge). The CA-GW sends a response message back. Finally the CMS will send a confirmation message back to confirm the certificates were received.
- The CMS sends a card lifecycle notification XML message to the CLEB. The CA-GW subscriber of the CLEB will if necessary send a PKIX-CMP revocation message or a confirmation message to the CA Gateway, and will also handle the response message from the CA-GW.
2.3.12 Card Update and Validation Gateway

**Validation Gateway**

The Validation Gateway (VG) is a server side integration component developed. The functions of the VG are accessible from the MOI Service Portal and User Sites.

The purpose of the VG is to provide online chip card related services that can be used by ASPs (most notably MOI) to determine the validity of the smartcards and their contents. It also decouples external systems accessing the cards (the portal and the kiosks) and the card applications from the SCM. In each online interaction of a card through the MOI service portal the VG is involved.

The SCM, however, is shielded from this interaction as much as possible. Any relevant card status change is pushed from the SCM to the VG. As soon as a card gets online to be used for e-services provided by the Application Service Providers (ASP), its validity will be checked by means of the VG. The VG will also indicate that a card needs to be blocked, unblocked or whether its data or card applications need to be renewed.

The VG manages all interaction during the initial phase of a card coming online (either at a user site or through the MOI Service Portal). This means that the CUG provides services to the VG.

The VG has to store the status of all blocked or unblocked cards and whether hard or soft blocked. Also pending hard blocks will be stored. The VG also stores an indicator whether post issuance is required for a specific Card. The VG will also keep track of the last time that a card was used online and whether errors occurred during authentication, post issuance or card update.

The Validation Gateway consists of a WebSphere Application Server, connected to an Oracle database. The internal integration is based on WebSphere Message Queues. The client applications all have to be authenticated using certificates. Network based (Host Security Modules (HSM) will be used for validating signatures and other cryptographic functions.

The HSM’s are accessed using the Secure Access Layer (SAL) component. Client interaction is browser based. Because of technological resemblance the hard- and software infrastructure is shared with the Card Update Gateway (CUG), which is described below. The Validation Gateway also provides a GUI based ability to configure the Post Issuance process.
The Post Issuance process can be activated when changed applications are available in the CMS. The CMS will notify the Validation Gateway if this occurs. When new applications are available the Validation Gateway can also be configured by this GUI to set a “configurable time delay” for performing these checks against the CMS.

Validation Gateway Diagram

Card Update Gateway

The Card Update Gateway is a server side integration component. The functions of the CUG are accessible from MOI Service Portal and User Sites.

The purpose of the CUG is to prepare and accumulate data updates for the chip cards. SAMIS is the source of all data updates although the CUG will be designed in such a way that it can be enhanced to facilitate other sources of card data. The CUG formats the acquired information and provides online services such that the data can be written onto the card. The access rights of the data sets will be taken into account.

An indicator for each pending update is pushed from the SAMIS to the CUG and stored. The actual data remains at the SAMIS. When a card comes online, it is
checked in the (local) database whether an update is pending at the SAMIS, and if that’s the case, a request is done to SAMIS to retrieve the updated data and is written to the card.

The issuer private key is stored in the HSM.

The software infrastructure of the VALGW is shared by the CUG. HSM access is provided for by a shared SAL component.
2.4. Overall Logical Architecture