The Offer for Public Institution “Public Services Agency” (Republic of Moldova)

Warsaw, 16 February 2022

Table of Contents

The personalization system for Identity Documents and National Passport System

Warsaw, 16 February 2022

1 Solution description

1.1 Definitions and abbreviations

Abbr	Description
Batch	Group of document applications for card/document personalization
Blank	Non-personalized card/document
CMS	Card Management System
HSM Tools	Backend component acting as a facade of HSM operations
CA	Certification Authority
Document application	Request to produce a single card/document. It contains all the data necessary for personalization of the card/document. The request is identified by unique number.
HA	High Availability
ICAO	International Civil Aviation Organization
OCR	Optical Character Recognition
QA	Quality Assurance
PKI	Public Key Infrastructure
RSA	Rivest-Shamir-Adleman algorithm
WSQ	Wavelet Scalar Quantization (fingerprint image compression algorithm)

1.2 Purposes of system implementation

THE PERSONALIZATION INFORMATION SYSTEM is a solution that allows to issue identity documents, passports, driving licenses, registration certificates and other documents with or without electronic layer. This type of documents can be used not only to present personal and identification data in graphical form but also to store additional data like facial image and fingerprints in its electronic chip that is embedded into document's physical structure. Facial image and fingerprints are biometric data and their usage gives authorities extended possibilities of confirming person's identity in more secure ways. Documents with electronic layer greatly support decrease in identity frauds and other actions that pose threat to public and national safety. They can provide at the same time highly convenient way of accessing various public and commercial services and easy ways of travel as they meet international standards and requirements of ICAO. Electronic layer on a document can also be used as a storage for digital certificates in extension to proposed solution.

Solution described in this document offers modern design, wide customization, high performance and very high level of security.

1.3 Functional scope of the System

Functions of the system can be divided into the subsequent modules:

1.3.1 Card Management System

The Card Management Module, which is part of the Personalization System, provides business services in the following scope:

- Receiving certificate generation requests from Personalization System and generating certificate requests passed to PKI (being proxy between Personalization System and PKI).
- Storage of information about certificates embedded in the document.
- Receiving the electronic layer status change and status change for requests generating certificates wchich is passed to PKI (being proxy between Authority System and PKI).
- Transmission of activation PIN codes and PUK codes
- Mass revocation of certificates

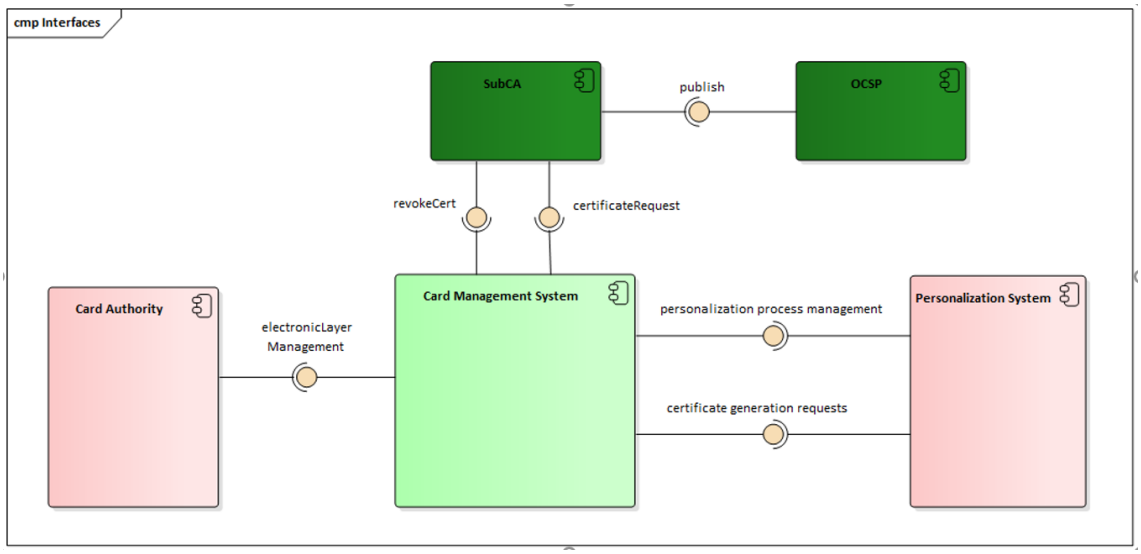
The Card Management System module, which has a database schema separate from other Personalization System modules, communicates with:

• a Personalization System through the SOAP interface issued by the Card Management System

• a PKI module through the SOAP interface provided by the PKI

• a Card Authority system through the SOAP interface issued in the Card Management System

Communication is secured with the SSL protocol.



1.3.2 HSM Tools

HSMTools – backend component acting as a facade of HSM operations, and management.It consist of two moduls:

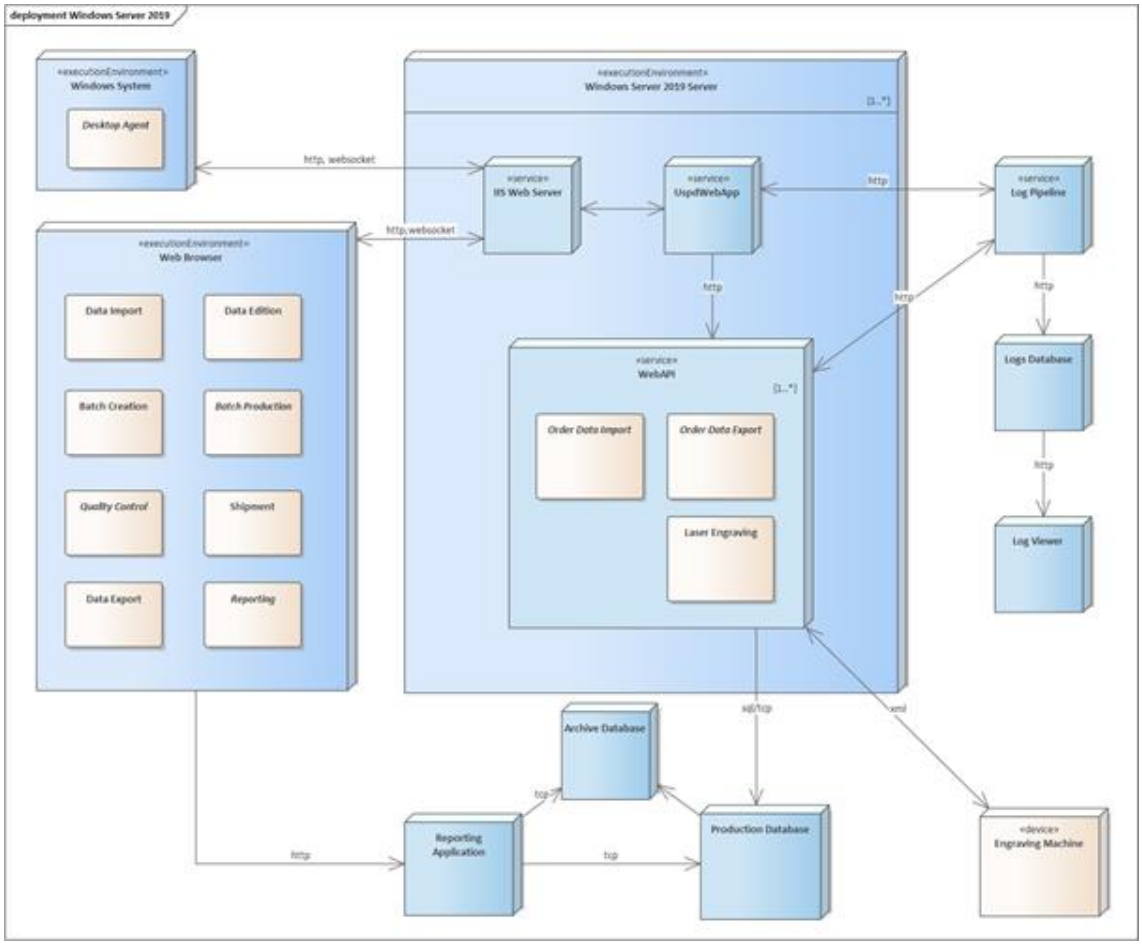
- one for other components of the system - simplifying signing, decryption, authentication, and object exporting operations.

- second for administrators – enabling key generation, certificate request generation, certificate import(X.509 and CVC), and secret key import.

Although component uses standard interface(PKCS#11) for accessing HSM, it functioning is highly dependent on the vendors(Thales) implementation of the standard, and may not work properly with other vendors HSMs. In that case additional adjustment, and testing will be needed.

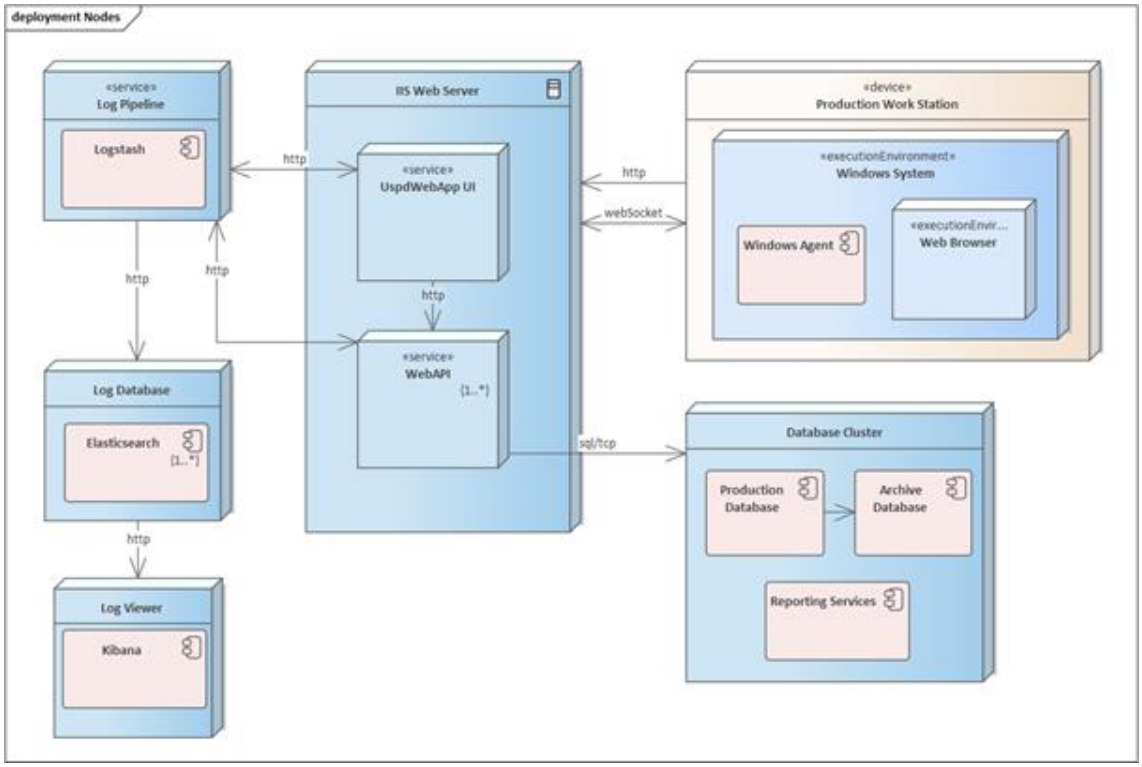
1.3.3 Personalization process management

Components of the system are shown in the diagram below. All of these modules help business process to provide production ability. Elements on the left side (Desktop Agent, all Web Browser modules) provide user interface into the system. The WebAPI component allows the user interface to drive business cases. Other components like log pipeline, log database, log viewer, active database, archive database, reporting services, web server are backend services used by the system.



The next diagram shows the logical deployment of the personalization system with main components. The deployment of the production system consists of the following elements:

- Web Server node delivers WebAPI and web application services, this node can be scaled by adding resources like processor cores and RAM memory. It is also possible to scale by adding nodes running web server instances and creating a web farm, in such case load balancer is necessary.
- Database Cluster nodes run database instances for production and archive purposes. Production database works in high availability mode to ensure required system performance.
- Log pipeline (Fluentd, Elasticsearch, Kibana) integrates all the system logs into one place (Elasticsearch) and makes them easily viewed using Kibana. Thanks to extensibility of the selected solution it is possible to connect external log sources, for example engraving machines, to the log pipeline.



The complete process of document personalization is comprised of the following steps:

1.3.3.1 Personalization data acquisition

Data acquisition, in the context of personalization system, is a matter of importing data into the system. Document applications are created outside of the system boundaries and imported to the system in offline or online mode. To ensure high product quality, validation is applied, and all not compliant data are held back by quality check. Data which is invalid for document production is rejected and the ordering party is notified about rejection reasons. Correctly validated personalization data is stored in the system repository and ready to be produced.

1.3.3.2 Production management

System helps to manage production tasks by providing accountability - personalization process of individual document is tracked and monitored. To manage a large number of applications, they are grouped together into production batches. Grouping of applications can be done in accordance with business requirements, for example, grouping applied according to the priority of the application or the ordering source (e.g. territorial office). Then batches of documents are taken for personalization and for the next production steps.

1.3.3.3 Batch personalization

Personalization is part of the process where documents are produced, and depending on the specific technology the process may differ. System supports technology of a specific process by providing modules for processes like laser engraving, chip programming, chip validation, quality control. During batch personalization the existing PKI infrastructure is utilized to perform operations such as certificate issuance, certificate revocation, data signing.

1.3.3.4 Quality assurance

Quality control is performed after a batch of documents is produced. The system support QA by providing a module helping operators to check the final quality of the product. The Quality Control module allows to search and visualize documents, moreover it enables to validate chip personalization. For many reasons, document personalization may not be successful, in such case QA operator marks applications to be personalized again.

1.3.3.5 Documents shipment

All produced documents have to be sent to the place specified in their applications. System provides an accountable and secure way to manage the shipment of produced documents to their destination. Document shipping is confirmed by sending a notification to the ordering party. Documents are sent in secure and tracked envelopes, and delivery to the destination is acknowledged.

1.3.3.6 Production accountability

Accountability for document production is ensured by logging of business operations to the system repository for operational use. Logging of business operation is based on the system log of all operations. The system supports accountability by providing users with the data required to validate production process.

1.3.3.7 Reporting

The system supports production process by providing different kinds of reports needed in production, shipping, etc.

1.3.3.8 System administration

Configuration of the system is managed by the administrator. System configuration is possible in the following categories: user management, production configuration, machine configuration, document layouts, system setting.

1.3.4 Personalization of documents

1.3.4.1 Laser engraving process

The system supports document personalization using laser engraving machines equipped with its own software. The process of laser engraving on blank or pre-personalized cards is as follows.

Operator configures engraving machine to specific settings according to production technology. When the machine is ready, operator inserts blank cards to be personalized into it. Engraving begins with operator's action. The engraving equipment processes the production batch of documents until the batch is finished. Each engraved document goes to the next stage of the personalization process.

The system and the engraving machine are integrated and able to exchange data about the engraving process. The system feeds the engraving machine with personalization data for production batch. After engraving system receives and analyzes reports from the engraving machine. Based on the results of the reports, documents are passed or rejected from production.

1.3.4.2 Chip programming

Electronic personalization of the document is performed after engraving. Depending on the chip specification a different program is launched for chip programming. The chip programming time also depends on the chip type. The results of this process are transferred to the document engraving report.

1.3.4.3 Automatic Vision Inspection

The engraving machine system is equipped with a vision inspection system that can check the quality of the documents and read personalized data using OCR for comparison. Configuration of the vision inspection system is independent of the personalization system. Vision inspection results can be used to guide the flow of production process, for example failure of a specified inspection test will change document's status.

The results of the visual inspection are transferred to the document engraving report. After inspection, the report is available for the personalization system.

1.3.4.4 Manual quality control

The manual step of quality control is after laser engraving, chip personalization and vision inspection. Batches of personalized documents are manually verified one by one by quality

assurance operators - they compare the data engraved on the document with application data presented by the system. Each document is validated using eMRTD reader. Several validation steps are performed to confirm the validity of the document, for example, the engraved MRZ is compared with the stored data on the chip, also the DG checksum on the chip is validated. If validation fails at any stage, it can be repeated when the operator decides to do this. In case of manual control failure this event is stored in the system repository, the status of such a document is set to ‘rejected’ or ‘reproduction’. When all documents in the batch are validated during quality control, the batch status is changed and it’s ready for the next step in the process.

The system supports quality control by providing easy validation using eMRTD readers and visualization of application data. In case the document fail the quality control, in most cases, it is reproduced in another production batch with a higher priority, if the operator decides to do so.

1.3.5 Card profile

1.3.5.1 e-Passport

ICAO application description

The ICAO application is used to store the data of the owner of the document (including his personal data) and the data of the document.

Preparation for use

The ICAO application will be personalized prior to delivery, i.e. all files will be created and the file access conditions will be set.

The file access conditions will be automatically activated after the personalization is completed.

After receiving the card (before handing it over to the end user), the issuer of the travel document should perform the following operations:

- authentication using a transport key,
- specifying the sizes of used files (for unused files, this step should be skipped, they will be unavailable in the Use phase),
- saving data to files,
- uploading BAC/SAC keys,
- uploading the Chip Authentication key,
- uploading Terminal Authentication initialization data: CVCA certificate, current date, document number, EF.CVCA file identifier,
- ending the personalization by switching to the Use phase.

Transport keys

The transport key for the production cards will be safely handed over in accordance with the procedure agreed between the parties.

ICAO files

The ICAO application includes the files EF.DG1, EF.DG2, EF.DG3, EF.DG14, EF.CVCA, EF.SOD and EF.COM. The general characteristics of the files are shown below. Details of the content are described in the document:

"ICAO Doc 9303 - Machine Readable Travel Documents, Part 3, Eighth Edition - 2021".

EF.DG1

Name	EF.DG1
FID	’0101’
SFI	‘01’

Length	Determined by the issuer of the travel document during personalization.
Access conditions	Read: BAC / SAC Write: None

EF.DG2

Name	EF.DG2
FID	’01 02’
SFI	‘02’
Length	Determined by the issuer of the travel document during personalization.
Access conditions	Read: BAC / SAC Write: None

EF.DG3

Name	EF.DG3
FID	’01 03’
SFI	‘03’
Length	Determined by the issuer of the travel document during personalization.
Access conditions	Read: EAC Write: None

EF.DG14

Name	EF.DG14
FID	’01 0E’
SFI	‘0E'
Length	Determined by the issuer of the travel document during personalization.
Access conditions	Read: BAC / SAC Write: None

EF.CVCA

Name	EF.CVCA
FID	’01 1C’
SFI	‘1C’
Length	Determined by the issuer of the travel document during personalization.
Access conditions	Read: BAC / SAC Write: None

EF.SOD

Name	EF.SOD
FID	’01 1D’
SFI	‘1D’

Length	Determined by the issuer of the travel document during personalization.
Access conditions	Read: BAC / SAC Write: None

EF.COM

Name	EF.COM
FID	’01 1E’
SFI	‘1E’
Length	Determined by the issuer of the travel document during personalization.
Access conditions	Read: BAC / SAC Write: None

1.4 Business processes

These main business processes are executed in order to prepare and issue documents with electronic layer:

1.4.1 Personalization

This process begins with receiving a request of issuing document to CMS. Next, this process includes warehouse services, preparation of production series, graphic personalization by laser and electronic personalization. Then the documents are given for quality control and preparation of shipment personalized documents.

1.4.2 Document issuance

In this process personalized document is issued to citizen. Data from document are read and used for verification of citizen’s identity.

1.4.3 Document revocation

This process provides support for certificate: revocation, suspend and renewing previously issued certificates.

1.5 Solution architecture

1.5.1 General concept

The main assumption of the project based on two environments. Production and test environment. The proposed solution has been divided into two parts.
A personalization center includes:

1. CMS - Card Management System. Production part wchich is handling certificate requests

2. Personalization Center - Production part containing e-document personalization machines.

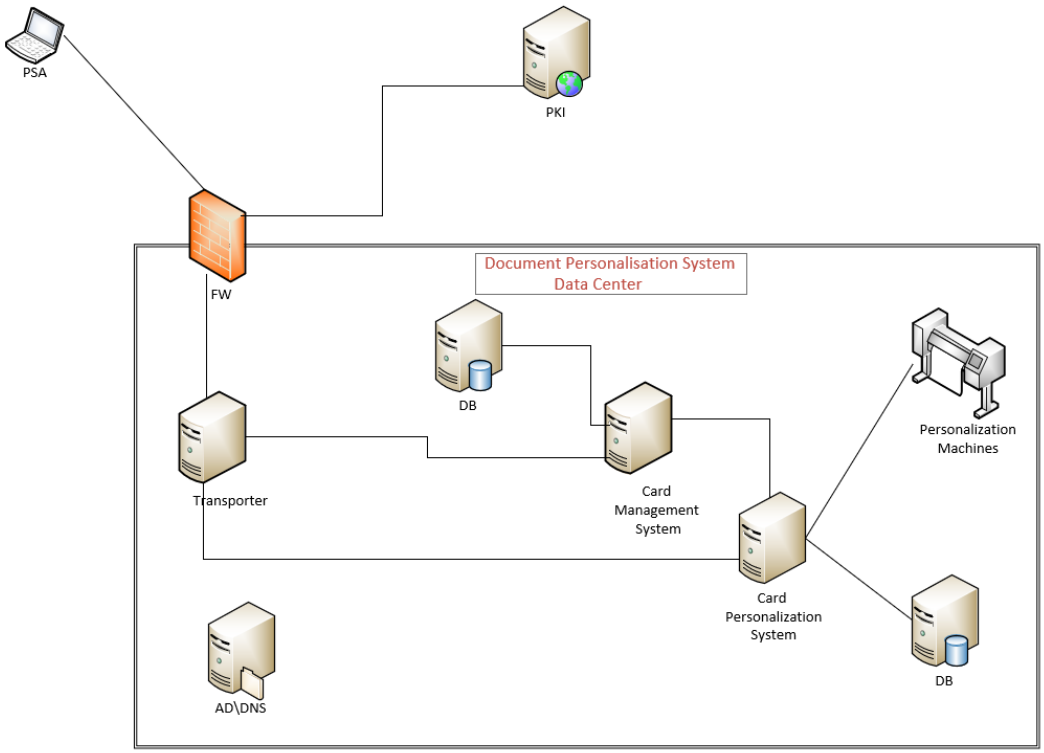
This is the main part of the whole system. This is a centralized system built in HA architecture. For the best protection against failures and disasters there should be ensured a redundancy of all modules constituting the Personalization System.

1.5.2 Physical architecture

Primary data center includes the following components:

1. CMS - Card Management System
2. Personalization Center - Contains Personalization Machines
3. Active Directory Servers and DNS servers

The picture below shows the overall structure of the system for production and test enviroment:



2 Quotations

2.1 System software

The table below contains pricing of modules of e-documents system:

#	Module
1.	CMS - Card Management System
2.	PC - Personalization Center

2.2 Software License

Licenses/subscriptions of third-party COTS software are listed in the following table:

#	License/Subscription
1.	Backup Networker
2.	MS Windows Server
3.	MS SQL Server
4	Elasticsearch
5	Redis
6	Nagios

2.3 Service prerequisites and boundaries of the offer

- It is assumed that service support will be based on remote access (VPN). In case of lack of possibility to remove failure remotely PWPW engineers will present on site,
- It is assumed that L1/ L2/L3 service support will be provided by PWPW in English language
- PWPW ensure service support maintenance of the system for the entire period of operation- 42 months
- It is assumed that software installation will be done by PWPW (PaaS)
- PWPW ensure to removal of errors detected in the operation of the system
- PWPW ensure restoring the operation in case of the system crash
- The offer does not cover any construction works related to enrollment and central sites preparation (power supply, network connectivity and air conditioning appliances/systems, fire system, security system, extraction system). The Purchaser should provide conditions and sites necessary for personalization machines in central site
- The offer does not cover security audit,
- The offer does not certified trainings
- PWPW does not procure hardware with the exception personalization machines

2.4 Trainings

- PWPW will provide necessary trainings concerning the functionality of the System,
- PWPW will provide necessary trainings concerning about backup and restore data from backup,
- PWPW will provide necessary trainings materials in English language in electronic version (*.pdf, *ppt),
- In case it is allowed to perform trainings remotely. PWPW will do it. The tool used for the communication will be agreed by the Parties before trainings,
- The level of the trainings will be prepared in a way that allows full personalization process to be carried out independently by a trained team of the Ordering.

2.5 Yours sincerely,

……

Grażyna Renata Rafalska

Elektronicznie podpisany przez Grażyna Renata Rafalska
Data: 2022.02.28 09:25:04 +01'00'