ICAO Public Key Directory

ICAO PKD White Paper – System Specification for participants

Update for ICAO PKD Service 2020

Table of Contents

1 Introduction

In a world that gets more and more digital, trust is a central concern. Manipulations of physical travel documents can be discovered forensically, while changes to digital information stored in an electronic travel document cannot. It is important to have a trustable public key infrastructure (PKI) in place to reliably check the integrity of digital information through the verification of digital signatures.

The Public Key Directory (PKD) solution provided by the Bundesdruckerei GmbH to ICAO and the PKD participants enables them to give trust to verified digital information stored in electronic travel documents issued by the participating states.

The following document describes the architecture of the provided solution – including, but not limited to, components, role definitions and interface descriptions of the system provided by the Bundesdruckerei GmbH.

The provided ICAO PKD service also contains a pre-production environment that is supplied to the participating states to test their integration with the ICAO PKD service and to check their PKD data for conformance before uploading them to the live system.

Within the document the terms “PKD data” and “CSCA registry information” are used. PKD data stand for document signer certificates, master lists, certificate revocation lists and deviation lists. CSCA registry information stand for contact information of eMRTD personnel.

2 System overview

The following chapter describes the general system architecture including operational models, a component list, an interface list, and a list of user roles, a description of the network zones, a description of the LDAP structures and a description of the data procession within the system.

2.1 Logical operational model

The following sub-chapters present the logical operational model of the ICAO PKD service. The logical operational model displays the logical components of the system including their respective position in the different locations as well as communication directions between single components.

The provided ICAO PKD service itself is hosted in identical systems within two geographically separate sites (location A being located in Berlin, Germany and location B being located in Abu Dhabi, United Arab Emirates). An operator location is additionally provided within the ICAO headquarters (being located in Montreal, Canada). The two hosting sites are designed so that each of them can take over the work of the other site should one of them fail.

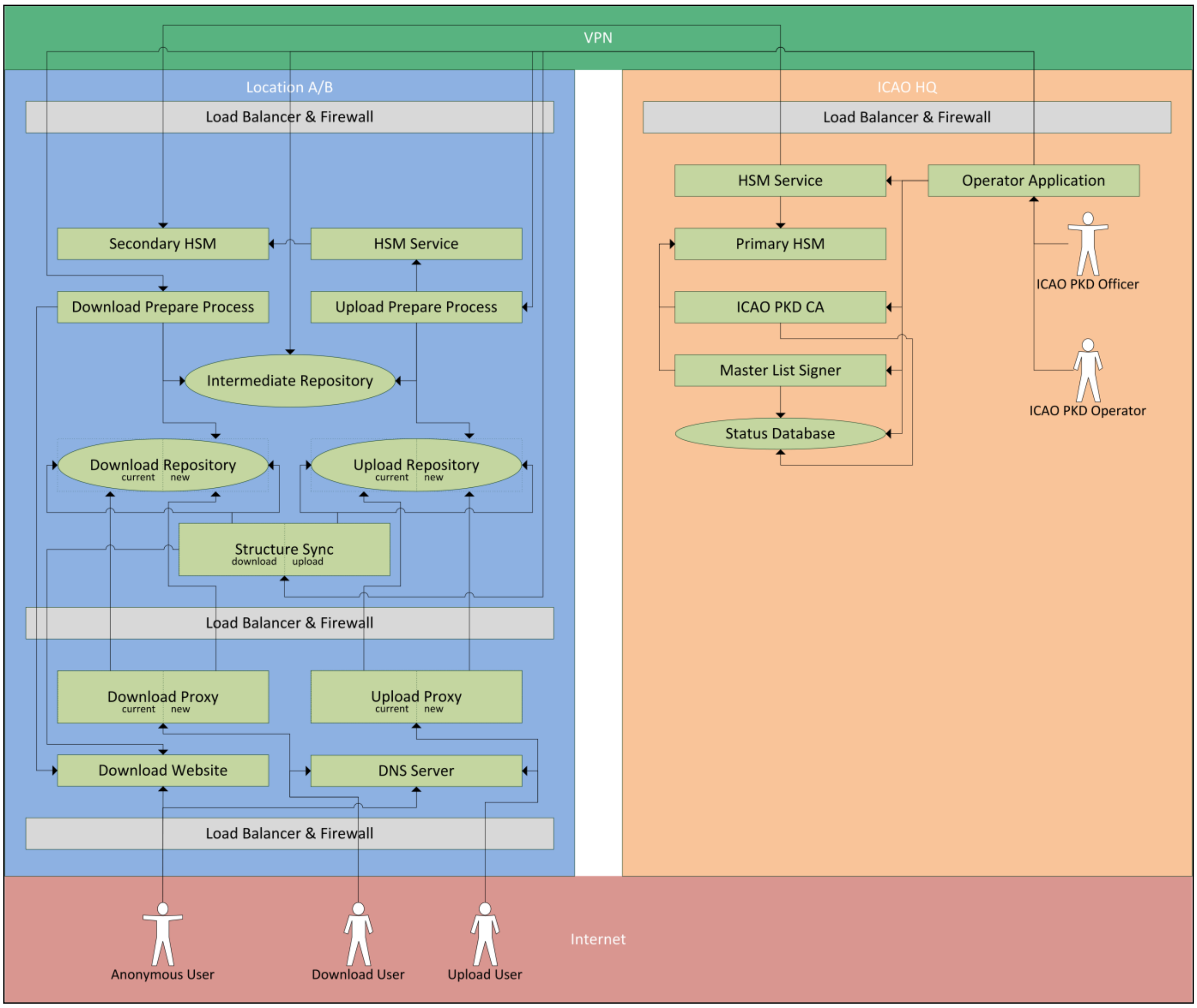

Figure 1: Logical Operational Model – Production Environment

2.2 Network zones

The ICAO PKD service is separated into three different network zones: the demilitarized zone, the internal zone and the operator zone.

2.2.1 Demilitarized zone

Each hosting site contains a demilitarized zone where the services are located and can be accessed through the internet. This zone contains the most endangered components as those can be attacked from the outside. Therefore this zone contains well-proven and industry-leading components including Apache HTTP servers and Oracle Directory Server LDAP servers. The demilitarized zone is separated from the internet by two firewall layers. Firewalls of two different vendors are used.

2.2.2 Internal zone

Each hosting site contains an internal zone where the data preparation takes place and where the PKD data are stored in repositories. In addition, the secondary HSMs are located in this zone. The internal zone is separated from the demilitarized zone by one firewall layer.

2.2.3 Operator zone

The operator zone is located within the ICAO headquarters and contains the operator application as well as the primary HSM, the master list signer, the ICAO PKD CA and the status database. The operator zone contains the most sensitive system components. Therefore all network connections to the internal zone are initiated from within the operator zone.

2.3 User roles

This sub-chapter contains the list of user roles with the ICAO PKD service together with a description of each role and the components the corresponding role assignees will access within the system.

Name	Components	Description
ICAO PKD Operator	Operator Application	ICAO PKD Operators access the operator application to manage the ICAO PKD system. Data published through the ICAO PKD system are managed by the ICAO PKD Operators on their own. Changes to the data stored in the HSMs and rejection of non-conformant PKD data are initiated by the ICAO PKD Operator and have to be acknowledged by an ICAO PKD Officer. ICAO PKD Operator role is assigned to ICAO staff members.
ICAO PKD Officer	Operator Application	ICAO PKD Officers access the operator application to manage the ICAO PKD system. The ICAO PKD Officer acknowledges changes to the data stored in the HSMs and rejections that are initiated by an ICAO PKD Operator. ICAO PKD Officer role is assigned to ICAO staff members.
Upload User	Upload Repository through Upload	Upload users access the upload repository through the upload proxy to import PKD data and CSCA registry information which will be published

	Proxy (Conformance Website)	through the ICAO PKD system after they have been checked and accepted. They use access certificates issued by the ICAO PKD CA to authenticate against the upload repository. (Within the pre-production environment, upload users are also able to access the conformance website. They use access certificates issued by the provider to authenticate against the conformance website, which is part of the pre-production environment. TLS client authentication is used as the authentication mechanism of the conformance website.)
Download User	Down-loadRepository through Download Proxy	Download users access the download repository through the download proxy to extract PKD data and CSCA registry information which are published in the ICAO PKD system. There are two types of download users: certificate-based download users and password-based download users. Certificate-based download users use access certificates issued by the ICAO PKD CA to authenticate against the download repository. In contrast, password-based download users use a username/password combination to authenticate against the download repository.
Anonymous User	Download Website (Checksum Download)	Anonymous users access the download website to retrieve the published PKD data in the form of LDIF exports. To do so they have to accept the terms and conditions of the ICAO and they have to solve a CAPTCHA. Anonymous users do not have to pass an authentication.
System Support	Upload Proxy Upload Repository Upload Prepare Process Intermediate Repository Download Prepare Process Download Reposi-	The system support is the personnel of the provider that implements, configures, monitors and maintains all components of the ICAO PKD system. There are certain tasks that require the work of the system support in cases that should not appear in the day-to-day work. System Support role is assigned to staff members of the provider / service operator.

	tory Download Proxy Download Website HSM Service Primary HSM Secondary HSM Operator Application Status Database ICAO PKD CA Master List Signer Pre-Production Prepare Process Structure Sync Logging Server Monitoring Server Pre-Production HSM	

Table 1: List of user roles

3 LDAP structure

This chapter describes the handling of the LDAP structure within the provided ICAO PKD service. This includes the description of the LDAP structure.

3.1 LDAP structure

The ICAO PKD service provides a LDAP structure with clearly defined attribute type definitions, object class definitions and an unique directory root “dc=pkd,dc=icao,dc=int”. The attribute types and object classes of the LDAP structure are described in the separate document “ICAO PKD Interface Specification for Participants”.

Within the provided ICAO PKD service there are three different repositories, providing different sub-trees of the unique ICAO PKD directory root – the upload repository providing the writable upload sub-tree structure for the participants, the download repository providing the read-only download sub-tree structure for the participants and the intermediate repository providing the working sub-tree for the ICAO PKD Operators and ICAO PKD Officers. Each repository contains separate access user accounts.

3.1.1 Upload Repository

The upload repository in the “dc=upload,dc=pkd,dc=icao,dc=int” subtree contains during the upload step the data uploaded by the participating states, which is their PKD data in the “dc=data” subtree and their CSCA registry information in the “dc=registry” subtree. Each participating state gets its own writable subtree.

The certificate-based upload user accounts are located in the “dc=meta” subtree.

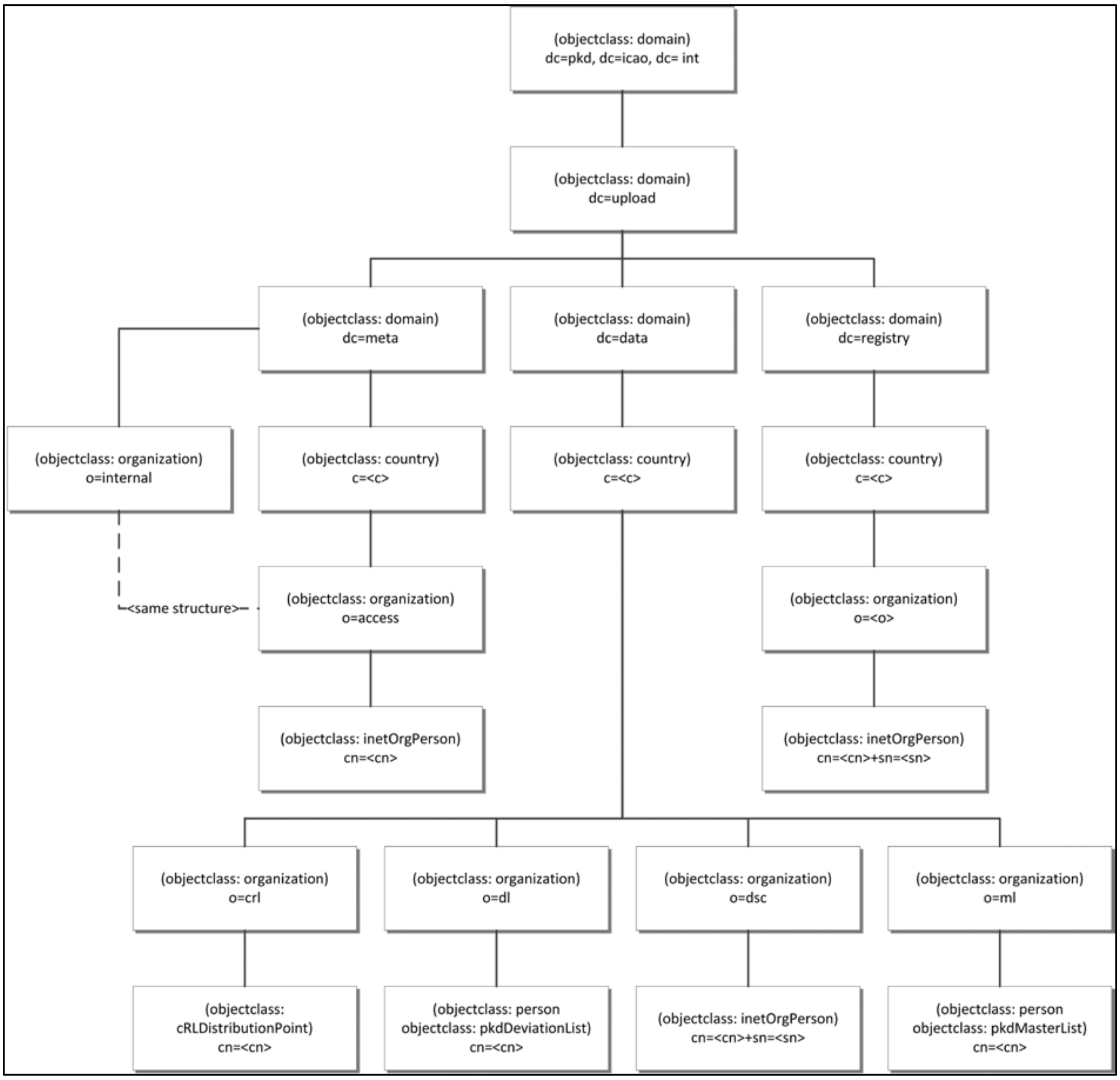

Figure 2: Directory Information Tree – Upload Repository

3.1.2 Intermediate Repository

The intermediate repository in the “dc=intermediate,dc=pkd,dc=icao,dc=int” subtree contains all data that have been processed by the upload prepare process, but have not been processed for download or alternatively rejected. Processed PKD data are stored in the “dc=ul-data” subtree, while processed CSCA registry information are stored in the “dc=ul-registry” subtree. This repository also holds data that have been accepted and that have not already been published to the download repository (i.e. data are held during the implemented cool down period). The intermediate repository is also used to create new upload user accounts and download user accounts.

3.1.3 Download Repository

The non-writable download repository in the “dc=download,dc=pkd,dc=icao,dc=int” subtree contains all PKD data and CSCA registry information that have been accepted, that have passed their cool-down period and that have been processed by the download prepare process. Processed PKD data are stored in the “dc=data” or in the “dc=nc-data” subtree, depending on their conformance check results and depending on the decision made by the ICAO. Processed CSCA registry information are stored in the “dc=registry” subtree.

The certificate-based download user accounts and the password-based download user accounts are located in the “dc=meta” subtree.

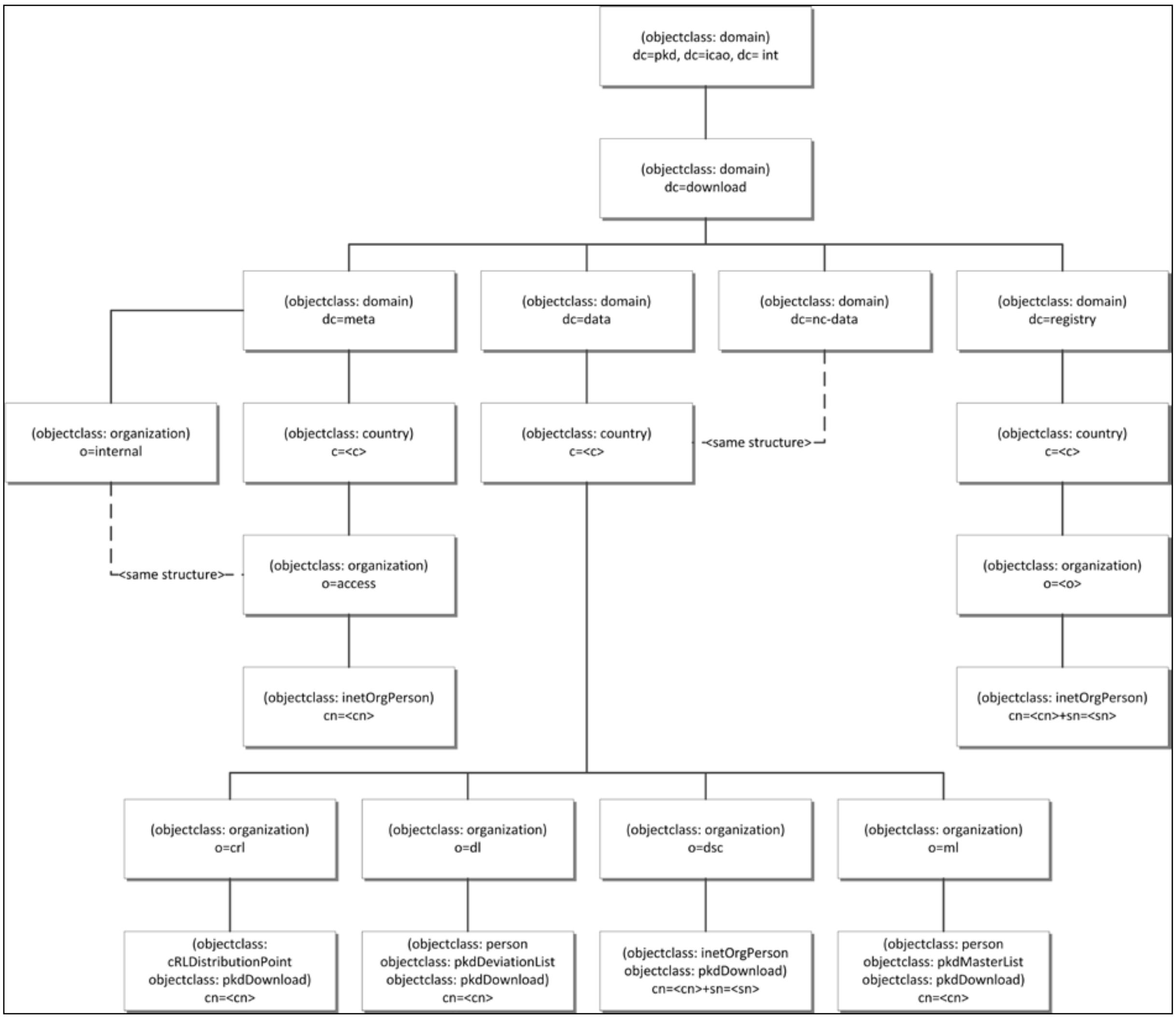
(objectclass: domain)
dc=pkd, dc=icao, dc= int
(objectclass: domain)
dc=download
(objectclass: domain)
dc=meta
(objectclass: domain)
dc=data
(objectclass: domain)
dc=nc-data
(objectclass: domain)
dc=registry
(objectclass: organization)
o=internal
(objectclass: country)
c=<c>
(objectclass: country)
c=<c>
<same structure>
(objectclass: country)
c=<c>
<same structure>
(objectclass: organization)
o=access
(objectclass: organization)
o=<o>
(objectclass: inetOrgPerson)
cn=<cn>
(objectclass: inetOrgPerson)
cn=<cn>+sn=<sn>
(objectclass: organization)
o=crl
(objectclass: organization)
o=dl
(objectclass: organization)
o=dsc
(objectclass: organization)
o=ml
(objectclass: cRLDistributionPoint
objectclass: pkdDownload)
cn=<cn>
(objectclass: person
objectclass: pkdDeviationList
objectclass: pkdDownload)
cn=<cn>
(objectclass: inetOrgPerson
objectclass: pkdDownload)
cn=<cn>+sn=<sn>
(objectclass: person
objectclass: pkdMasterList
objectclass: pkdDownload)
cn=<cn>

Figure 3: Directory Information Tree – Download Repository

4 Data preparation

This chapter describes the data preparation processes from the upload by a participating state, through the upload preparation, acceptance and download preparation to the download by participating states and anonymous users in more detail. The flow of the data during the data preparation is shown in the dataflow diagram below.

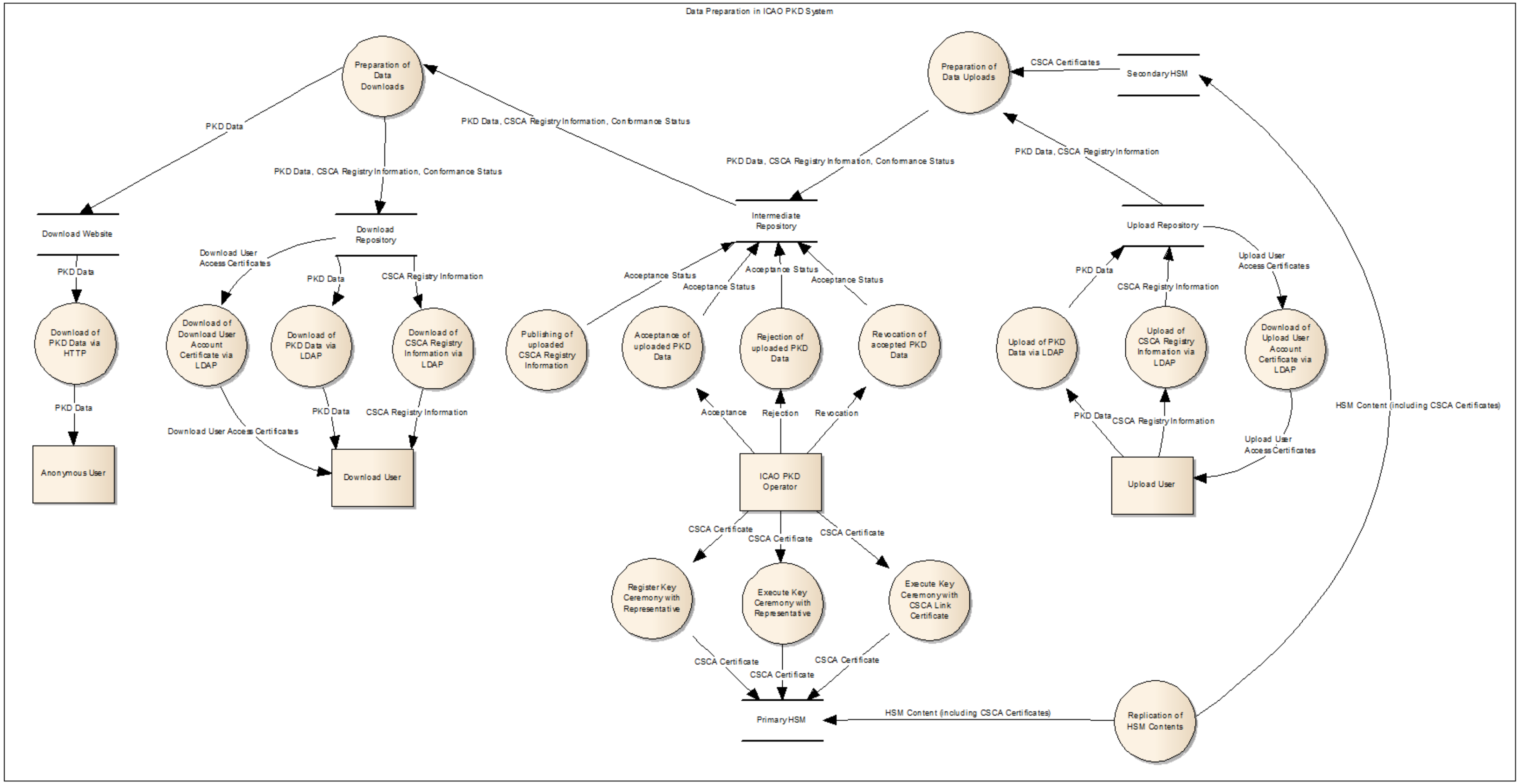
Data Preparation in ICAO PKD System
Preparation of Data Downloads
PKD Data
PKD Data, CSCA Registry Information, Conformance Status
PKD Data, CSCA Registry Information, Conformance Status
Download Website
Download Repository
PKD Data
Download User Access Certificates
PKD Data
CSCA Registry Information
Download of PKD Data via HTTP
Download of Download User Account Certificate via LDAP
Download of PKD Data via LDAP
Download of CSCA Registry Information via LDAP
PKD Data
PKD Data
CSCA Registry Information
Download User Access Certificates
Anonymous User
Download User
Preparation of Data Uploads
CSCA Certificates
Secondary HSM
PKD Data, CSCA Registry Information, Conformance Status
PKD Data, CSCA Registry Information
Intermediate Repository
Upload Repository
Acceptance Status
Acceptance Status
Acceptance Status
Acceptance Status
Publishing of uploaded CSCA Registry Information
Acceptance of uploaded PKD Data
Rejection of uploaded PKD Data
Revocation of accepted PKD Data
Acceptance
Rejection
Revocation
ICAO PKD Operator
CSCA Certificate
CSCA Certificate
CSCA Certificate
Register Key Ceremony with Representative
Execute Key Ceremony with Representative
Execute Key Ceremony with CSCA Link Certificate
CSCA Certificate
CSCA Certificate
CSCA Certificate
Primary HSM
HSM Content (including CSCA Certificates)
Replication of HSM Contents
HSM Content (including CSCA Certificates)
PKD Data
CSCA Registry Information
Upload User Access Certificates
Upload of PKD Data via LDAP
Upload of CSCA Registry Information via LDAP
Download of Upload User Account Certificate via LDAP
PKD Data
CSCA Registry Information
Upload User Access Certificates
Upload User

Figure 4: Data preparation dataflow diagram

4.1 Data upload

Data uploaded to the ICAO PKD system contain PKD data and CSCA registry information. There are certificate-based upload user accounts that have to be used to access the corresponding LDAP interface to be able to upload new data to the ICAO PKD system. The data are uploaded to one of the two redundant sites hosted by the provider. The data are replicated to the other site. Data uploaded to the ICAO PKD system stay in the upload repository until they have been handled by the upload prepare process.

4.2 Upload preparation

The upload prepare process handles the data uploaded to the upload repository. During the upload preparation the uploaded PKD data are checked for conformance with DOC 9303. The PKD data are also cryptographically checked against the CSCA certificate of the corresponding participating state. The key material needed to execute the cryptographic checks is read from the secondary HSMs. The prepared data are moved to the upload branches of the intermediate repository and are thus deleted from the upload repository.

4.3 Acceptance and rejection

Data that went through the upload preparation are located in the upload branches of the intermediate repository where they are accessible by the operator application for further handling. CSCA registry information are automatically accepted by the operator application to reduce the work load of the ICAO PKD Operator. PKD data that are conformant to DOC 9303, and only have acceptable variations, and that passed the cryptographic checks are automatically accepted by the operator application to reduce the work load of the ICAO PKD Operator.

All PKD data that are not conformant and thus have variations that are not allowed or that did not pass the cryptographic checks have to be manually reviewed by the ICAO PKD Operator through the operator application. Manually accepted PKD data can either be marked as conformant or as non-conformant.

PKD data that are not conformant may alternatively be rejected by the ICAO PKD Operator through the operator application. Rejected PKD data are removed from the intermediate repository to prevent further procession.

Accepted data are moved from the upload branches of the intermediate repository to the download branches of the intermediate repository. There is a separate download branch for non-conformant PKD data to keep these apart from the conformant PKD data.

4.4 Cool-down and revocation

Accepted PKD data will not be published directly to the download repository and to the download website. Instead there is a cool-down period (48h for DSCs, MLs, DLs and 24h for CRLs) in which those accepted data are held back before they are published. In this time period the ICAO PKD Operator has the possibility to revoke the acceptance of PKD data. This may be necessary when PKD data have been falsely uploaded by a participating state or in cases where PKD data have been falsely accepted.

When acceptance of PKD data is revoked, the data are moved from the download branches of the intermediate repository to the upload branches of the intermediate repository so that they can be either accepted or rejected afterwards.

4.5 Download preparation

The download preparation reads the accepted data from the download branches of the intermediate repository that have passed the cool-down period – and are thus ready for publication – and moves them to the download repository. The data are deleted from the intermediate repository. The static LDIF files for the download website are also generated during the download preparation.

4.6 Data download

When the download preparation has finished the current set of PKD data can be downloaded manually from the download website which is accessible for anonymous users. Participating states can use certificate-based download user accounts or password-based download user account to access the download repository from which the PKD data can be downloaded automatically. In addition, participating states have the possibility to download the CSCA registry information.

5 Availability

This chapter describes the steps taken to provide an ICAO PKD service with a high level of availability.

5.1 Redundant sites

Most of the ICAO PKD service components will be set up in two redundant locations (with the exception of the primary HSM, the master list signer, the ICAO PKD CA, the status database and the operator application which are located in the ICAO headquarters). The first location is hosted in Berlin, Germany and the second location is hosted in Abu Dhabi, United Arab Emirates.

5.2 Automatic site selection

A DNS-based load balancing will be used to automatically select an available location upon connecting to the ICAO PKD service, while providing an equal load distribution. In cases where one of the two redundant locations fails this DNS-based load balancing will also take care of the failover. The automatic site selection requires that the demilitarized zone of each hosting site contains DNS servers.

5.3 Manual site selection

In addition to the automatic site selection provided for the ICAO PKD service each participant has to possibility to manually select the location that shall be used to connect to the service. This allows for even more sophisticated load balancing and failover scenarios that may be implemented by the participating states (e.g. based on the geographical location of the national PKD).

5.4 Redundancy within sites

Within each site – including the ICAO headquarters – all services will be deployed redundantly to provide a load distribution between servers. Additional the network hardware is deployed redundantly as well to avoid single point of failures.

5.5 HSM replication

The provided ICAO PKD service consists of a writable primary HSM in the ICAO headquarters and two read-only secondary HSMs – one secondary HSM is located in Berlin, Germany and the other secondary HSM is located in Abu Dhabi, United Arab Emirates. Data written to the primary HSM will be regularly replicated to the secondary HSMs. Those secondary HSMs are used during the upload preparation to cryptographically check the uploaded PKD data but also serve as a backup of the primary HSM.

5.6 Repository replication

The multi-master replication features of the selected directory server product are used to regularly synchronize the contents of the repositories (update repository, intermediate repository and download repository) between the two redundant locations. This is a necessity for providing the load balanced and geographically redundant service but also serves as a backup of the repositories’ content.

6 Pre-Production Environment

Most of the logical components of the pre-production environment and most of the structure of the pre-production environment are equivalent to the production environment. This chapter describes where and how the pre-production environment differs from the production environment.

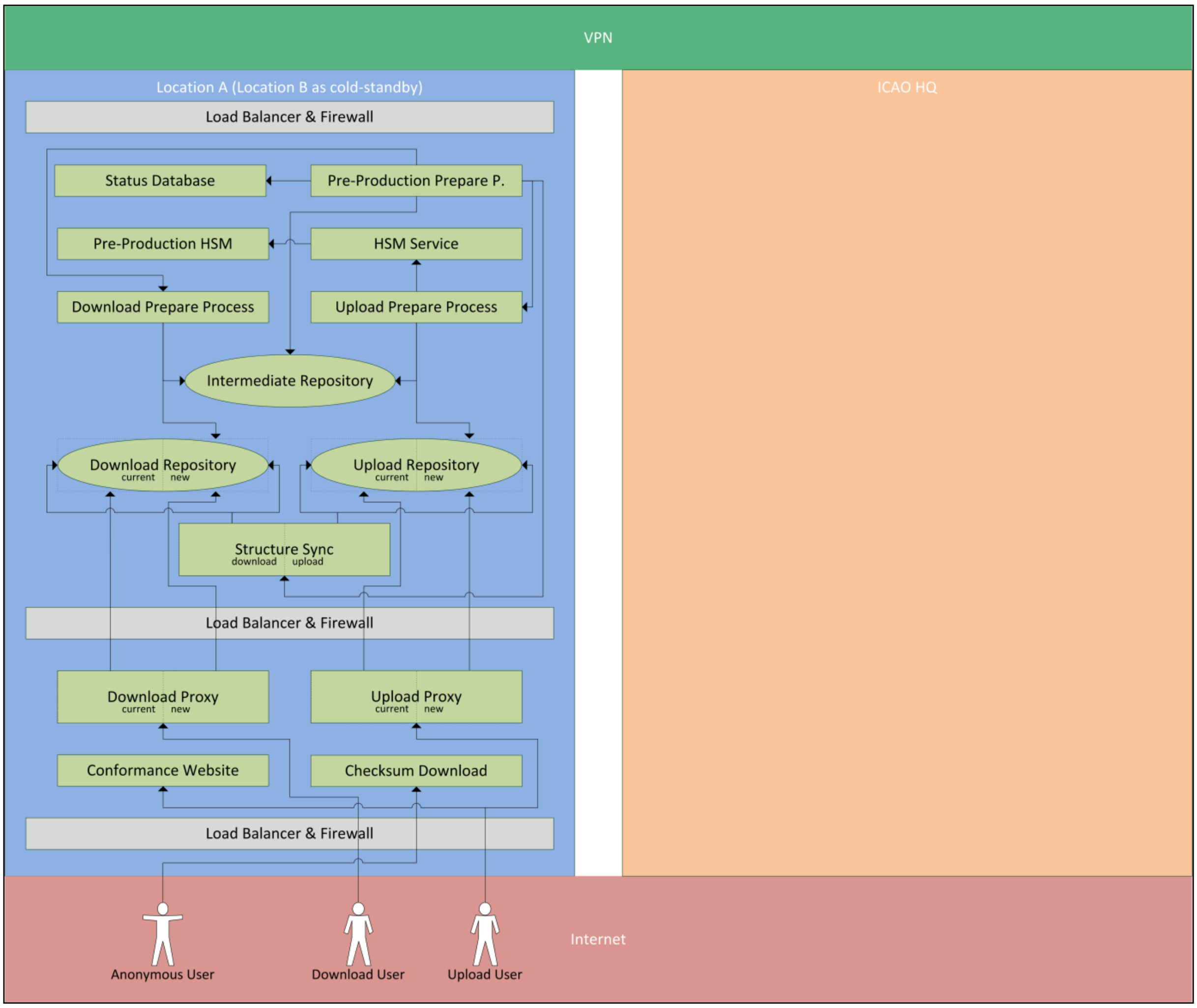

Figure 5: Logical Operational Model – Pre-Production Environment

6.1 Cryptographic checks

To execute cryptographic checks on uploaded data within the pre-production environment the upload prepare process needs access to the CSCA certificates of the participating states. This is achieved by means of a separate Pre-Production HSM component where also non-productive CSCA certificates of the participants can be imported for testing purposes.

6.2 Fully automatic acceptances and rejections

The pre-production environment does not contain the operator application (and also not the primary HSM, not the secondary HSMs, not the ICAO PKD CA, not the master list signer and not the status database). To replace the operator application, a different logical component – the pre-production prepare process – is used to trigger all other processes (upload prepare process, download prepare process and structure sync) and to automatically accept uploaded data as either compliant or non-compliant. The decision will be based entirely on the conformance check results generated by the upload prepare process. The acceptances will take place without user interaction.

6.3 Availability

Due to the reduced availability requirements of the pre-production environment the logical components are not installed in a geo-redundant load balancing manner. Instead a cold-standby is provided, meaning that should the location providing the pre-production environment fail to work, the other location has to be started manually to take over the tasks of the pre-production environment. This also means that the data stored in the pre-production environment may be different when the backup site has to provide the pre-production environment.

6.4 Creation of download users and upload users

Download user accounts and upload user accounts within the pre-production environment will be created by the provider. A corresponding request for the creation of a new user has to be given by the requesting participating state to the provider.

6.5 Access credentials

The access credentials for the pre-production environment will be issued and provided by the provider of the ICAO PKD service. An internal CA of the provider will be used to issue the corresponding access certificates for download users and upload users. The access credentials of the production environment will not work in the pre-production environment.

6.6 Download website

No download website will be provided for anonymous users within the pre-production environment.

6.7 Conformance website

To check the conformance of PKD data and CSCA certificates prior to uploading them to the production environment, the participating states may use the upload user credentials of the pre-production environment to access a separate conformance website. This website allows the upload user to upload PKD data and CSCA certificates to be checked for conformance. The conformance checks executed on the uploaded data and the conformance results generated by the conformance website will be equivalent to the checks executed and the results generated by the data preparation processes within the production environment except for inter-object checks like cryptographic checks.

7 Other considerations

This chapter contains information to other topics that do not fit into the previous chapters.

7.1 TLS Certificates used externally

All external communication of the ICAO PKD system will be TLS-secured. Therefore TLS certificates are required for all externally available components of the system. The extended validation TLS CA of the D-Trust will be used to issue these TLS certificates.

7.2 TLS Certificates used internally

All internal communication of the ICAO PKD system is required to be TLS-secured. Therefore TLS certificates are required for all internal components of the system. An internal CA operated by the provider will be used to issue these TLS certificates. The corresponding CA root certificates will also be deployed by the provider to all internal components of the system.

7.3 ICAO PKD Operator and ICAO PKD Officer credentials

Credentials for the ICAO PKD Operators and the ICAO PKD Officers are provided in the form of smartcards. These have to be requested by an ICAO PKD Operator and an ICAO PKD Officer and will be issued by a CA of the provider. The new user of the operator application will also be created by the provider within the intermediate repository.

7.4 Form of notification of ICAO PKD Operator and participating states

A web-based service portal of the provider will be used to provide status notification information of PKD uploads to the participating states. The same service portal will also be used to notify the ICAO PKD Operator about new tasks in the operator application (e.g. the upload of PKD data that did not pass the cryptographic check or that did not pass the conformance check). Notifications will only be used in the production environment.