Judicial Information Service
Ministry of Security and Justice

WHITE PAPER

A National
Public Key Directory

Version 1.0 definite
Date 21 July 2015
Author Jeen de Swart
Judicial Information services
Ministry of Security and Justice, Netherlands

ABSTRACT

This white paper is about a possible setup of a National Public Key Directory (NPKD) containing Certificates for all kind of e-documents (like e-MRTD, e-Residence Permit, e-Driver License, et cetera). The responsibility for such a NPKD is a National Government. As national trustworthy source these certificates can be provided to the national borders for checking e-documents like Automatic or Assisted Border Control (ABC) gates. Beside the national borders these certificates could also be provided for (Military) Police Control, Immigration Services or Commercial Purposes. This document describes a possible infrastructure with some components without any vendor named or commercial influences.

The benefit of a NPKD is the fact that a responsible government is in charge of providing necessary certificates as a trustworthy source to national- and commercial bodies with the purpose of checking the genuinity of the e-document chips' content. It's up to the national government to decide to which bodies these certificates – or part of the certificates - are provided.

A NPKD is part of a total (private) infrastructure which serves different domains (for different inspection bodies or organizations) each disclosed by a National Single Point of Contact (NSPOC). Not only the NPKD but also the Verification PKI – necessary for the private sensitive information on the e-document chip – can be disclosed through a NSPOC and even the possibility of necessary registers or databases.

Terminals (devices with an e-document reader) can be managed by a Terminal Control Center (TCC). These TCC's are connected to the domain's NSPOC and have a specific interface specification to provide all the necessary functionality to the terminals – like providing the certificates from the NPKD.

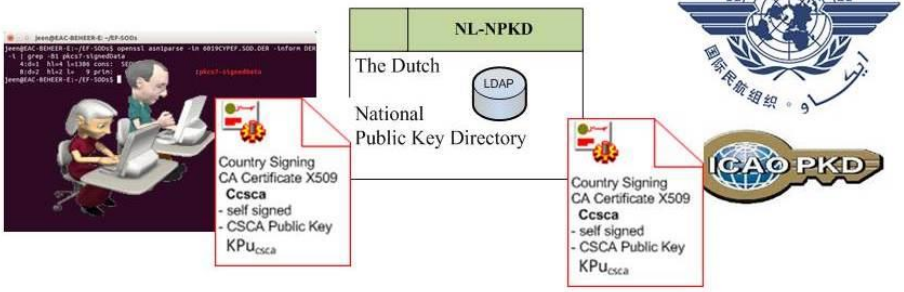
To be a trustworthy provider of certificates through a National Public Key Directory a government must have an organization of trustworthy employees with enough skills, awareness and knowledge. Procedures must be in place before adapting certificates into the NPKD. To be trustworthy, Risk Management must be an overall adaption.

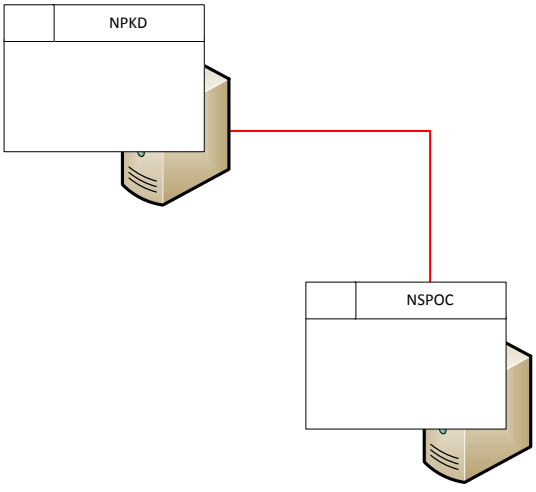
Invited and encouraged by the ICAO PKD Border Engagement Subgroup (as mentioned in the ICAO PKD paper B-Pub/56) the delegation of the Netherlands was delighted to create this white paper. The Netherlands will present this paper with examples on the ICAO PKD meeting of October 2015 in Montreal.

INDEX

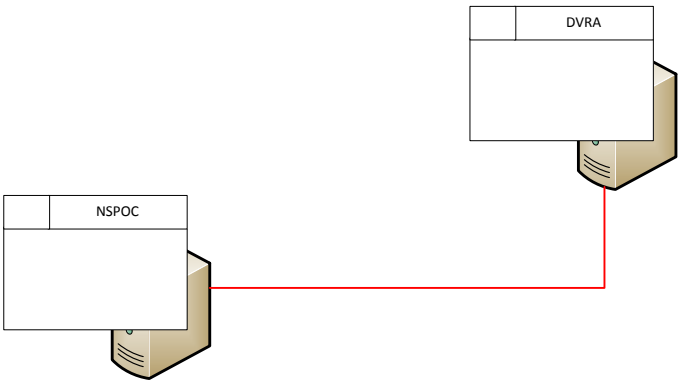
THE ARCHITECTURE

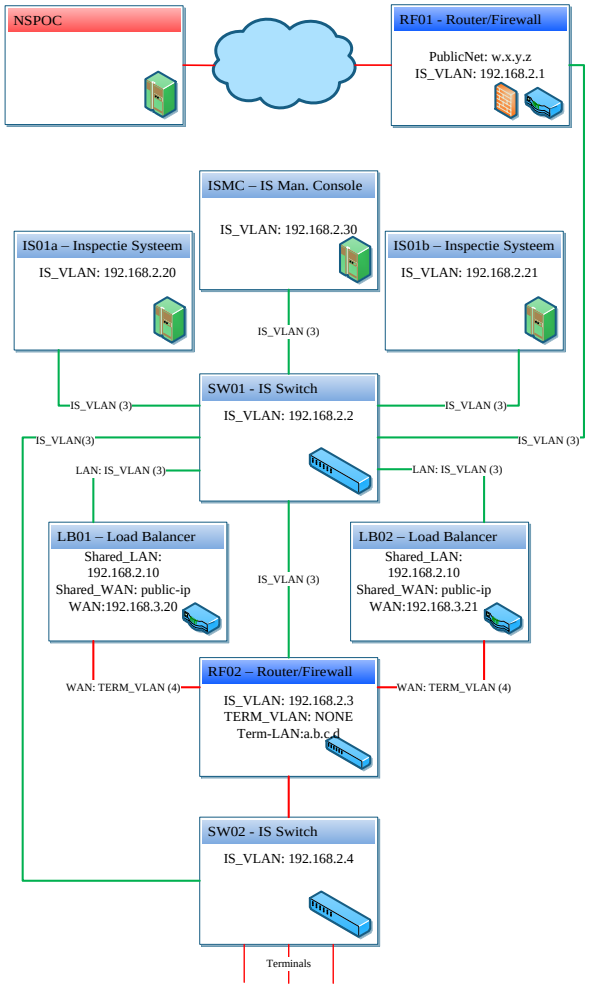
A National Public Key Directory (NPKD) is a LDAP Directory containing national and international certificates from the signing hierarchy of e-documents. These certificates are necessary for terminals (devices with e-document readers connected) to check the genuinity of e-documents (called Passive Authentication). A NPKD can contain certificates (CSCA certificates and DS certificates), Certificate Revoke Lists (CRLs), Masterlists and Defectlists. Masterlists and Defectlists can be seen as a signed container of certificates. The responsibility of a NPKD is a National Government. The National Public Key Directory is a trustworthy source for the Inspecting Bodies like Border Control. The process of importing certificates into the NPKD is never automatic. There is a role of a NPKD Manager who is responsible for the import of certificates. Masterlists and Defectlists are available from trustworthy sources (like ICAO PKD) but it is the NPKD Manager (as Governmental Employee) who decides which certificate will be imported. The same responsibility is there for importing certificates from bilateral sources or websites. A Government should have a Policy Authority as a responsible body who has the governance for the process of importing and how the NPKD Manager should handle the certificates. With these procedures the NPKD Manager is able to import certificates. A part of this procedure is to check the certificates against the ICAO 9303 specifications. It is the NPKD Manager who decides within the NPKD for which Inspection Body the certificates are available. A NPKD is part of a total (private) infrastructure which serves different domains (groups of inspection bodies with a same functionality) each disclosed by a National Single Point of Contact (NSPOC). For example: Border Control as inspection bodies are connected to one NSPOC and National Police Force as inspection bodies are connected to another NSPOC both getting different or the same certificates. NSPOC's can be seen as virtual querying users to the NPKD. The communication to and from the NPKD is always secure using special certificates. The NPKD is manageable through a Graphical User Interface (GUI) which can be a web interface with a connection for the NPKD management. This is also a secure connection using special certificates. For the purpose of all secure connections the responsible Government could produce TLS certificates them with an own, so called, CONNECTCA. A possible solution for such a CONNECTCA is given in Appendix 1. This solution is part of the security and input for a Risk Analysis.





If in a domain (group of inspection bodies with a same functionality) verification of private information (like fingerprints) in the chip is necessary for inspection purposes then the NSPOC can also be connected to the Document Verifier Registration Authority (DVRA). From this server the necessary certificate chain for the Inspection Systems (IS) will be provided. The connection between the NSPOC and DVRA is a secure connection with TLS certificates from the CONNECTCA, see Appendix 1. The NSPOC delivers a secure web service with SOAP messages which can provide the Signing Certificates (CSCA's and DS'), CRL's, Masterlists and CA Chains (for verification PKI). Within this document we will not describe the complete functionality of the Verification PKI. From this point the white paper describes the example of Border Control with Terminal Control Centers (TCCs) which are connected to the NSPOC. In fact there are mostly two possibilities of terminals (devices with e-document readers connected, like ABC gates) for Border Control. The manufacturer of the terminals delivers his own TCC or the manufacturer of the terminals depends on a central TCC, see Appendix 2. In both cases there is an Interface Specification for the necessary SOAP messages. A dedicated TCC consists at least two Inspection Systems (IS) and a Management console for the Inspection Systems (ISMC). The IS' contains a certificate store of CSCA's and CRL's (synchronized with the NPKD) and can contain Hardware Security Modules (HSM) for the verification chain (EAC PKI). The most common practice is that the ABC systems only needs the Country Signing Certificates (CSCA's) and for secondary inspection the Verification Chain (for fingerprint inspection). A TCC is a secure "black box" with two Router/Firewalls, one with a secure connection to the NSPOC and the other with secure connections to the terminals (devices with e-document readers connected, like ABC gates). These secure connections are using TLS certificates from the CONNECTCA, see Appendix 1. Which functionality per terminal is allowed (in SOAP messages) can be managed by the ISMC. In the case of ABC systems there are two possibilities for getting the CSCA's and CRL's. There is a "pull' mechanism: the ABC gates implemented the interface specifications and asked (pull) for the certificates and CRL's every half an hour, or there is a "push" mechanism: the ABC gates are Web Service activated, implemented the interface specifications and

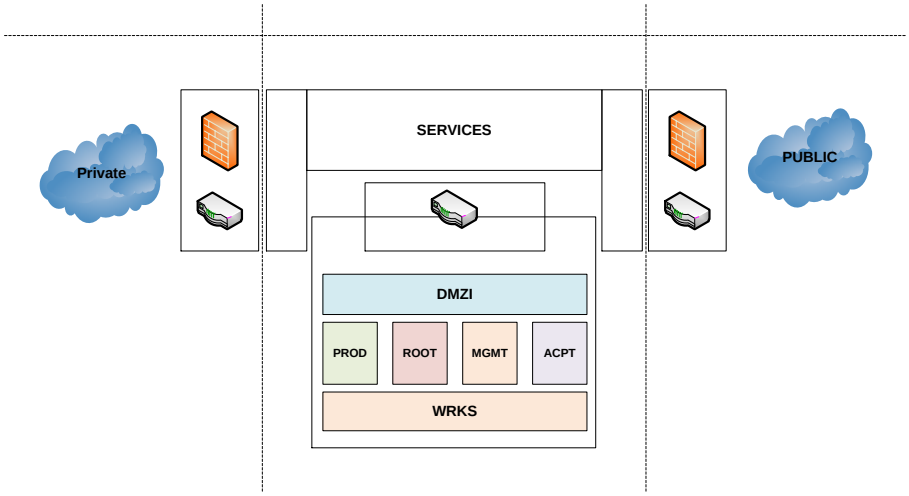




besides asking (pull) for the certificates, from the NPKD the certificates can be pushed to the ABC systems. It depends on the manufacturer of the ABC gates which mechanism can be implemented.

THE INFRASTRUCTURE

The systems described in the Architecture (see Appendix 2) needs to be placed in a secure environment. This can be done by creating several segmented and separated environments by VLAN's (Virtual Local Area Networks). VLAN's are mutually isolated and can only be accessed by Routers and Firewalls. This solution is a part of the security and input for a Risk Analysis. Within this architecture there is a demilitarized zone (DMZ) for the systems connecting to the private or public network (for example the NSPOC), a ROOT environment for example the Root CONNECTCA, a Production environment (PROD) for the NPKD, a Management environment (MGMT) for the Monitoring and Administrating systems and a Preproduction environment (ACPT). Besides these environments there is a Specimen environment (TEST) for creating, testing and developing. The VLAN's as environments can be stretched over a wide geographical area. Where possible the systems, as described in the Architecture (see Appendix 2), are virtualized (virtual machine) using servers with hypervisors. For systems needing a HSM there is a choice of using network attached HSM (netHSM) or within the server installed HSM (PCI-HSM). The benefit of netHSM's is that all the systems can be virtual machines. For storage the virtual machines can use the Storage Area Network (SAN). The final solitary virtual environment for PKI services depends on governmental security procedures regarding networks (firewalls and routers).



THE ORGANIZATION

Depending on the Governmental Organization there are different roles and responsibilities for the different systems as described in the architecture, see Appendix 2. The overall governance is a Policy Authority giving direction to the Signing – and Verification – PKI (including the CONNECTCA) and authorization to the TCC for connections of terminals and providing certificates. This white paper doesn't describe in detail all the responsibilities and roles for all the systems but gives a global view

as presented in Appendix 3. The roles must be seen as descriptive and can be combined within employees. The total solution is a part of the security and input for a Risk Analysis. Very important is that there is enough knowledge within the Governmental Organization for managing and operating the different systems as described in Appendix 2. Furthermore the role of architect is necessary to keep track of all the changes worldwide and implementing these changes into the organizational architecture.

THE SETUP AND COSTS

In this white paper the estimate of costs will be given in time, personal and necessary devices and will be restricted to the architecture given in Appendix 2 (without terminals and EAC-PKI). The first step in the development must be an architecture, for example something like Appendix 2. The necessary (and possible future) functionality must be described for every system in this architecture. The setup of this architecture and the description of the systems will take approximately three to six months for one architect. The architecture will be input for own development or a tender. To develop the systems (applications), as described in the architecture, two developers need approximately six to twelve months. If it is a tender then it takes approximately eighteen to twenty-four months. During the setup an auditor and security officer should be involved. The infrastructure is also part of the architecture and must be setup with IT Management. Setting up the physical servers, storage, implement the hypervisor and setting up the virtual machines will take approximately one to two months. Together with IT Management, in the same months the Security Officer and Network Management will deal with the virtual network setup and firewall and router rules. To manage all this setup it should be a project with a project manager and Policy Authority already in place. There will be costs of physical hardware (servers), storage (SAN), Hypervisors, Firewalls and Routers. Extra costs will be HSM devices when necessary for CONNECTCA, Inspection Systems and future EAC-PKI. The virtual machines needs an Operating System (OS) which can be a free or paid OS. Depending if the Governmental Organization wants to tender there will be costs of the functional software releases to build the system (applications) as described in Appendix 2. For own development there will be costs of databases, middleware and application software (Web Services and GUI). With a tender the costs are hard to predict. There will be extra costs for training personal.

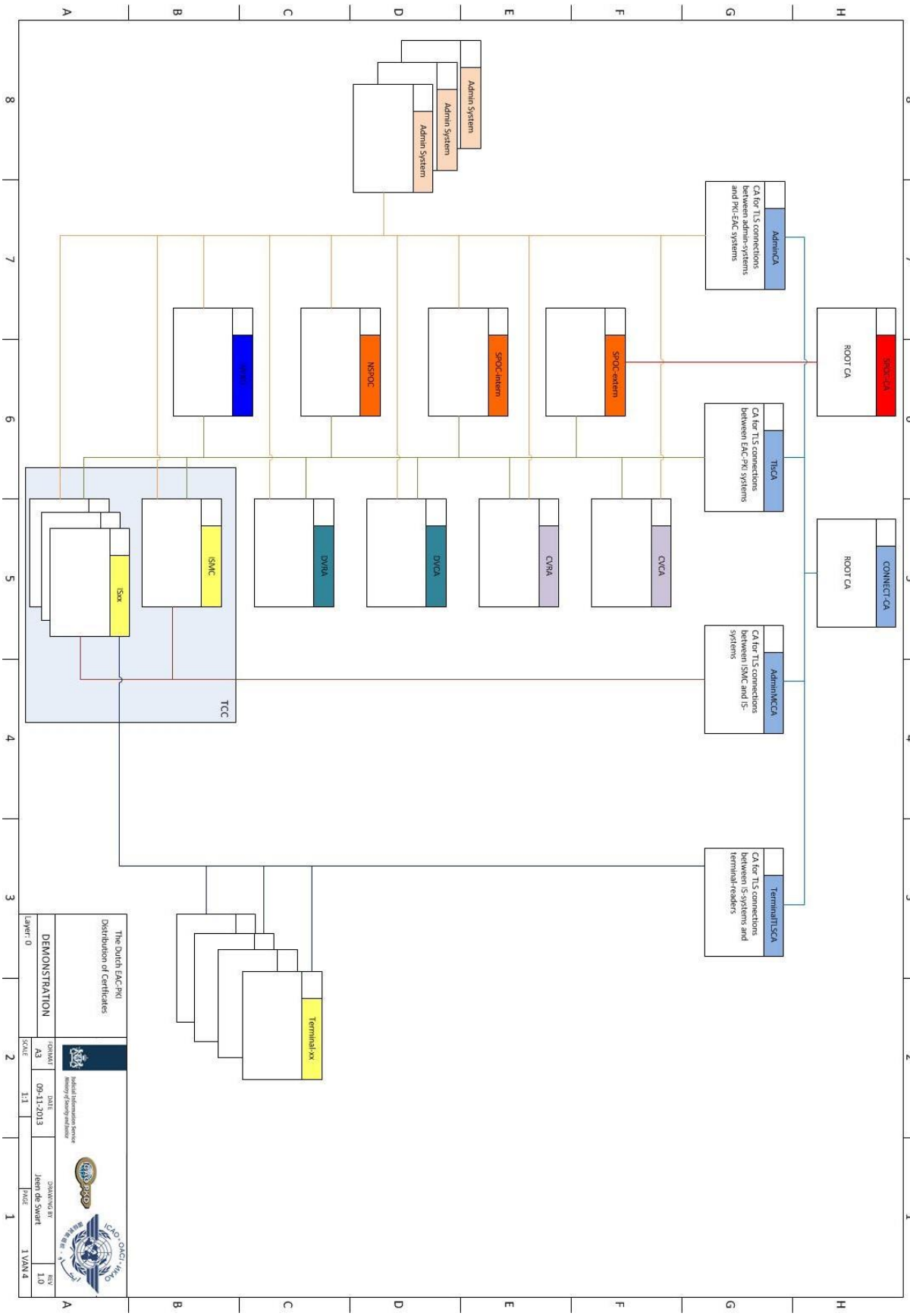
APPENDIX 1, CONNECTCA

The CONNECTCA is the Root Certificate Authority (CA) of the Connect PKI. The Public Keys of the CONNECTCA are contained in self-signed CA certificates. The CONNECTCA issues CA certificates to its Subscribers, the Subordinate CA's (Sub-CA's). A Subordinate CA issues TLS client and server certificates to a group of Managed Systems that share a specific purpose. A Subordinate CA has a self-signed (Root) CA certificate and a CA certificate signed by the CONNECTCA.

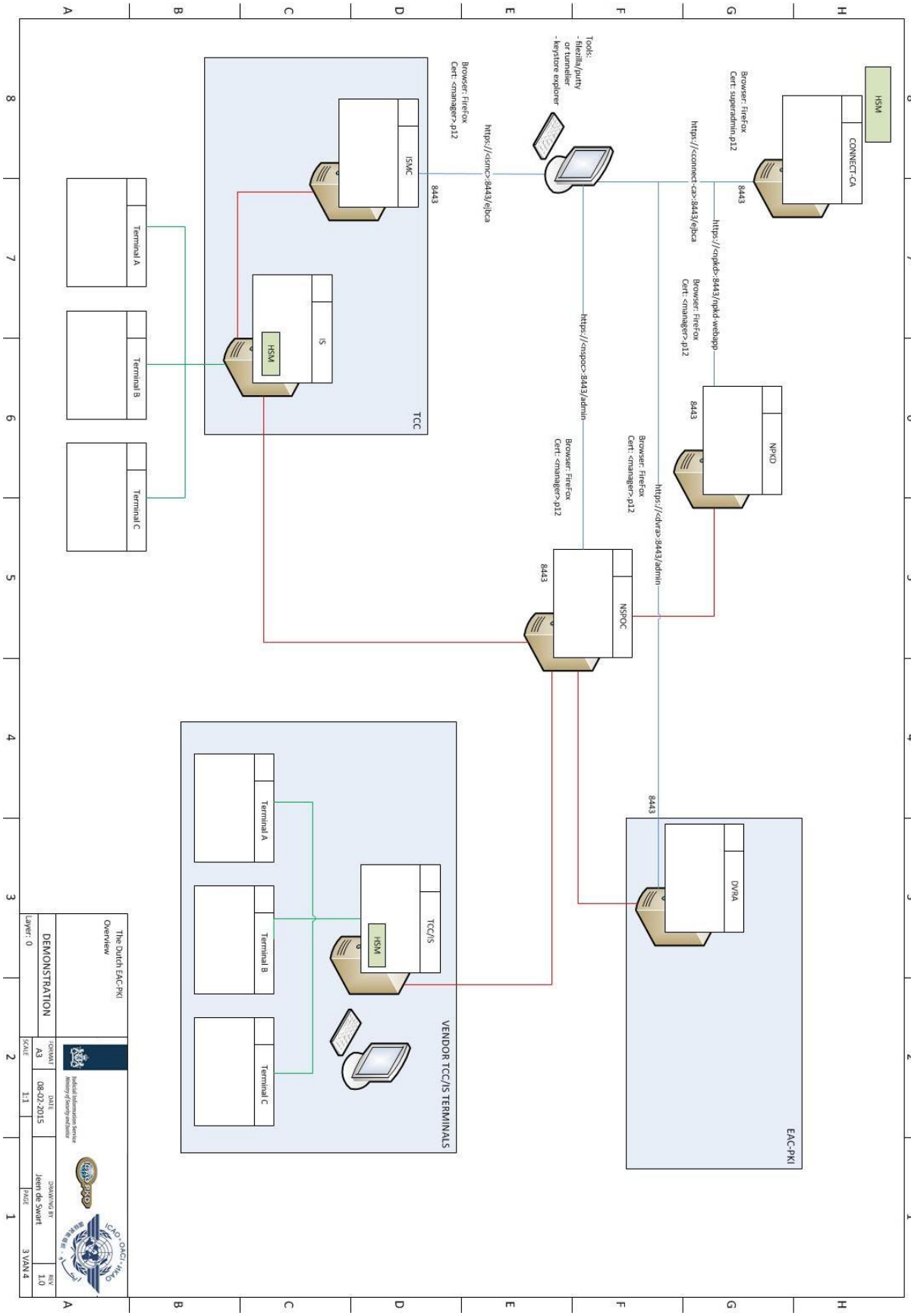
The following Subordinate CA's can be defined: TLSCA, ADMINCA, TERMINALTLSCA and ADMINMCCA.

The ADMINCA is the Subordinate CA for issuing TLS certificates for secure connection for admin-systems (server and GUI), the TLSCA is the Subordinate CA for issuing TLS certificates for the secure connections between the servers. The ADMINMCCA is the Subordinate CA for issuing TLS certificates between the Inspection Systems and the Management of these Inspection Systems. For the secure connection of the Terminals (devices with an e-document reader) there is a TERMINALTLSCA as a Subordinate CA.

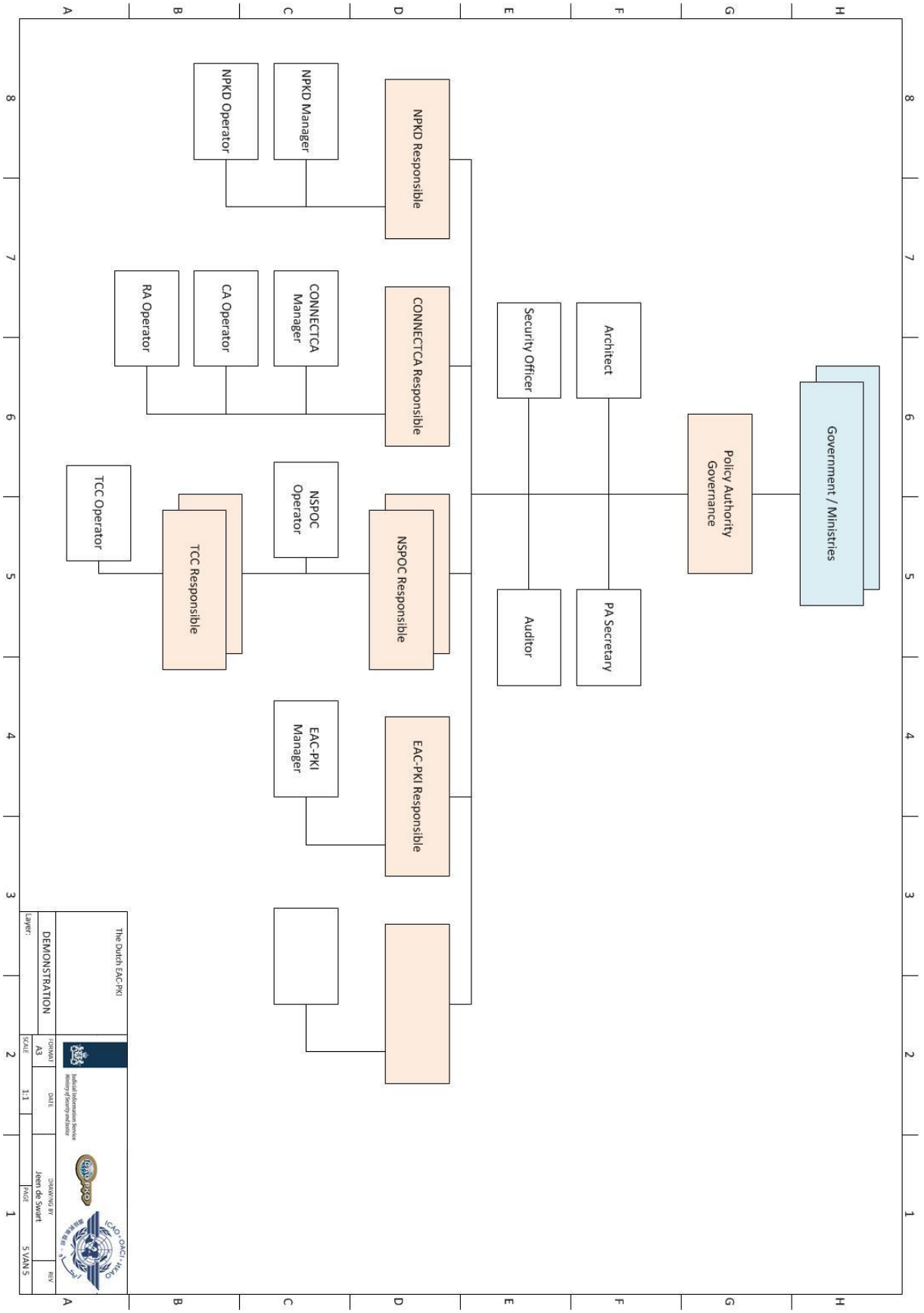
There is a SPOCCA mentioned in this architecture. This is a special CA for the Verification PKI functionality within Europe. The SPOC functionality is not further described in this white paper.


ROOT CA
SPOC-CA
ROOT CA
CONNECT-CA
AdminCA
CA for TLS connections between admin-systems and PKI-EAC systems
ThCA
CA for TLS connections between EAC-PKI systems
AdminMCA
CA for TLS connections between ISMC and IS-systems
TerminalTLSCA
CA for TLS connections between IS-systems and terminal-readers
Admin System
Admin System
Admin System
SPOC-extern
SPOC-intern
NSPOC
CVCA
CVRA
DVCA
DVRA
ISMC
ISoc
TCC
Terminal-xx
The Dutch EAC-PKI
Distribution of Certificates
DEMONSTRATION
Layer: 0
FORMAT
A3
SCALE
1:1
DATE
09-11-2013
DRAWING BY
Jeen de Swart
REV
1.0
PAGE
1 VAN 4

APPENDIX 2, OVERVIEW NPKD



APPENDIX 3, GOVERNANCE RESPONSIBILITIES AND ROLES



APPENDIX 4, TERMS AND ABBREVIATIONS

ABBREVIATION	Full Form
ABC	Automated / Assisted Border Control
CA	Certificate Authority
CRL	Certificate Revocation List
CSCA	Country Signing CA
DMZ	Demilitarized Zone
DS	Document Signer
DVRA	Document Verifier Registration Authority
EAC	Extended Access Control
e-MRTD	Electronic Machine Readable Travel Document
GUI	Graphical User Interface
HSM	Hardware Security Module
ICAO	International Civil Aviation Organization
IS	Inspection System
ISMC	IS Management Console
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NPKD	National Public Key Directory
NSPOC	National Single Point of Contact
OS	Operating System
PA	Policy Authority
PCI	Peripheral Component Interconnect
PKI	Public Key Infrastructure
RA	Registration Authority
SAN	Storage Area Network
SOAP	Simple Object Access Protocol
TLS	Transport Layer Security
VLAN	Virtual Local Area Network

TERM	Definition
Certificate application	An application for the issuance of a certificate to a subscriber. The certificate application is submitted to the RA by a representative of the subscriber that is responsible for the intended Certificate Holder. A certificate application includes a certificate request and other data required for the validation of the application by the RA.
Extended Access Control Public Key Infrastructure (EAC-PKI)	The infrastructure required to control access to fingerprint biometrics on Passports and Travel Documents utilizing Extended Access Control.
Hardware security module (HSM)	A hardware module for the safe storage of keys and the safe performance of cryptographic operations.
International Civil Aviation Organization (ICAO)	An United Nations organization tasked with fostering the planning and development of international air transport. In this

TERM	Definition
	role it sets international standards for MRTD's.
National Public Key Directory (NPKD)	The National Public Key Directory (NPKD) is a domestic PKD. The NPKD is responsible for the delivery of certificates and CRLs for Passive Authentication.
Registration Authority (RA)	The Registration Authority is responsible for identification and authentication of certificate applicants, approval or rejection of certificate applications and managing revocation of certificates.