ADSS ePassport Server

Common Criteria Certified ePassport Server

ADSS ePassport Server is a proven standards based, certified product that can be deployed on premise or as part of a cloud service. It offers high availability, scalable throughput to meet the most demanding needs. This is a strategic product for Ascertia providing support for the latest Windows and Linux operating systems, databases and HSMs from the major vendors.

Digital Trust Overview

Digital Business defines the transition of analog processes to the digital world, this global movement has seen the digitization, streamlining and improvement of digital interactions. In order to conduct digital business, you must be able to trust the identity of the person, application or service you are communicating with, this requires digital trust.

Digital Trust and transformation extends to the digitization of passport holder biographical information and biometrics to enable passport issuers and border officials the ability to verify a passport holder at border control, ensure authenticity of a passports contents, and prove the identity of a passport holder.

ADSS PKI Server is core to providing digital trust, used to provide trust and authenticity to electronic machine readable travel documents, and to provide protection to travel document holder secondary biometrics. ADSS ePassport Server delivers a highly secure and scalable trust services platform upon which can be built services to issue X.509 digital certificates compliant to ICAO 9303 part 12 to form part of the passport manufacture process to digitally sign the Logical Data Structure that is written to the passport chip, and to offer the essential digital services to ensure Border Control is automatically updated to be able to verify signatures when presented with a passport.

ADSS ePassport Server can also be used to deliver ISO 7816 digital certificates compliant to BSI TR-03139 v2.2, this PKI enables border management to issue digital certificates to border inspection systems to authorize domestic and international border officials to access and read the secondary biometric that is stored on the chip within electronic passports.

ADSS ePassport Server can also provide the optional Single Point of Contact, National Public Key Directory and Master List Signer to projects to further enable automation, international exchange and additional security to passport and border management projects.

Key Features

- **Standards Compliance**: Fully compliant with ICAO 9303 pt 12, BSI TR-03110, BSI TR-03139 v2.2, BSI TR-03129 and ČSN 36 9791.
- **Third Party Certifications**: Common Criteria EAL 4 certified, meeting the requirements of the NIAP Protection Profile for Certification Authorities Version 2.1 (2017)
- **Automated Certificate Lifecycle Management:** Includes support for Certificate Management over CMS, ICAO PKD Download/Upload, International Certificate exchange via SPOC
- **High-Availability**: Is easily configured to offer high scalability and availability to meet the most demanding infrastructure needs. Multiple load balanced servers can work concurrently, and resilient secondary sites can also be established.
- **Distributed Architecture:** ADSS PKI Server can be deployed to offer a fully distributed digital trust issuance model.

ADSS PKI Server Architecture

Ascertia's ADSS ePassport Server provides a modular framework that delivers all of the components required to issue, protect and validate ePassports as well as an SDK that can enable border control to inspect ePassports and digitized passport holder biometrics.

Electronic passports are electronic machine-readable travel documents with many security features, Public Key Infrastructure provides the key components to deliver electronic security to the solution. The International Civil Aviation Organization (ICAO) and the European Union introduced standards to provide security to these documents, this has helped to deliver superior border security to countries globally.

ADSS ePassport Server includes Country Verifying Certification Authority (CVCA), Document Verifying CA (DVCA), Master List Signer, National Public Key Directory (NPKD), Single Point of Contact CA and Single Point of Contact (SPOC), that can be deployed by Passport Issuance Offices and Border Management agencies to create, manage and verify passport holders and their biometrics both domestically and via SPOC, enable international travel document verification. ADSS PKI Server is Common Criteria EAL 4 Certified and meets the requirements of the National Information Assurance Partnership Government Approved Protection Profile for Certification Authorities v.2.1 (2017), this means that ADSS PKI Server is certified to the very latest CA protection profile and to a high assurance level.

ADSS PKI Server provides full support for the certificate profiles required to support Passive Authentication in support of Basic Access Control and Terminal Authentication in support of Extended Access Control.

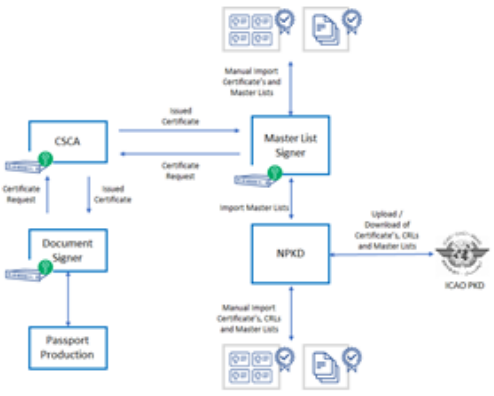
Ascertia Basic Access Control PKI

Core CSCA Infrastructure

- Country Signing Certification Authority (CSCA)
- National Public Key Directory
- Master List Signer

Passport Production Infrastructure

- Document Signing Service



Ascertia Extended Access Control PKI

Core Infrastructure

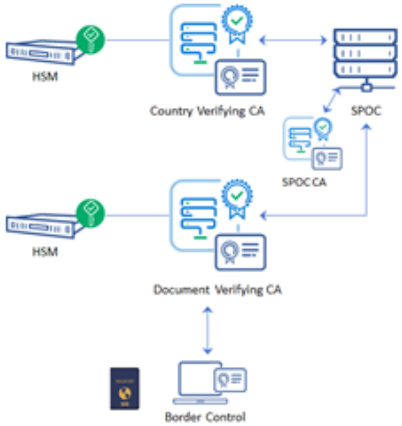
- Country Verifying CA (CVCA)
- Document Verifier (DV)

Border Control

- Inspection System SDK

International Certificate Management

- Single Point of Contact (SPOC) CA
- Single Point of Contact (SPOC)



Ease of Use

Product installation is simplified, using a wizard to guide operators to configure the database, main operator account(s), trust model(s) and HSM details, plus the CAs, their validation policies, the CRL monitoring and event reporting.

Administration is provided by an intuitive browser-based administration console, each operator is authenticated via a client TLS certificate and only provided access to product functions according to their role within the product.

Advanced Features

Performance Tuning: ADSS PKI Server provides the ability to fine tune the deployment to make best use of the platform on which the product is operating, this in turn enables the fine tuning of performance to meet business needs.

ePassport Options:

Ascertia SPOC

Ascertia's Single Point of Contact (SPOC) module enables countries to securely exchange certificates and certificate requests automatically for their EAC PKI with their international counterparts to enable secure and authorised access to citizen biometrics stored within the ePassport.

Ascertia National Public Key Directory Server

National Public Key Directory (NPKD) provides fully automated download and upload to the ICAO PKD and offers countries the ability to manually import BAC validation materials obtained through diplomatic exchange or that have been downloaded from ICAO.

Ascertia Master List Signer

Master List Signer is an optional component that digitally signs a list of CSCA certificates, this provides a secure list of trust anchors at border control as well as supporting a secure distribution mechanism for CSCA certificates via the ICAO PKD.

Management Control and Reporting: Detailed role-based access controls makes it easy to give staff the rights they need, for instance allowing help-desk staff to access log information so they can help customers whilst ensuring that they cannot view or change any configuration data.

ADSS PKI Server creates detailed event and transaction logs that can be used to create usage reports and identify high demand users, certificates or IP addresses. Advanced management reporting is provided as a standard feature.

ADSS ePassport Server is an advanced trust services platform that provides support for Basic Access Control, and Extended Access Control PKI to support the issuance and validation of ePassport documents and authenticate border inspection systems to enable access to passport holder secondary biometrics.

Secure web-based management is provided as standard together with advanced management configuration options and detailed reporting.

Supported Operating Systems:

Microsoft Server 2022, 2019, 2016
Linux RedHat, SUSE, CentOS, Ubuntu

Supported Databases:

Microsoft SQL Server 2022, 2019, 2017
Oracle 19c, 18c
Azure SQL Database (Database-as-a-service)
PostgreSQL 14, 13, 12, 11
MySQL 8, 5
Percona-XtraDB-Cluster 8, 5

Supported Security Modules

Thales Luna and Protect Server
Entrust nShield
Utimaco Security Server
Microsoft Azure Key Vault
Amazon AWS Cloud HSM (Linux Only)

Mike Hathaway | Chief Product Officer

About Ascertia

Ascertia provides digital trust for people, devices, data and documents for everybody from individuals to Enterprises and Governments. Ascertia's PKI and digital signature technologies serve a global customer base and partner network via direct and indirect sales channels.

For more info

info@ascertia.com

www.ascertia.com