Reference

danish national police biometric authentication

Enrolment client and gateway for second generation ePassports (PAS 1.1)

The Danish National Police along with local government and the Foreign Services are all responsible for the enrolment of ePassport applicants, whereas the National Police has sole responsibility to accept and distribute biometric data to the physical ePassport (booklet) vendor.

In accordance with current EU regulations, all EU Member State passports must contain biometric identification elements. The first generation ePassports contains biometrics in an embedded RFID chip in the form of a document holder facial image and additional document holder data protected by Basic Access Control (BAC) via the document MRZ information. The second Generation ePassports supported by this new solution - in additional to using larger capacity RFID chips - also contain fingerprint images – protected by Extended Access Control (EAC), using Certificates via integration to the national PKI (Document Issuer). All Danish passports issued on or after January 1st 2012 now contain the required biometric information stored on RFID.

The project

The total Project covers the areas:

- Atos Homeland Security Suite Fingerprint Module (HSS FPM)
- Fingerprint scanners
- Software development and System Integration
- Hosting & Operations (Managed Services)
- Software Maintenance and support services (Application Management)

The solution elements

The solution is made up of a variety of elements.

1.: Interface specification – An agreed interface specification has been developed in the very early stages of the project. This specification is written in XML and defines the data structures for transmission and retrieval of all types of ePassport applications (metadata as well as biometric information (holder image, signature and fingerprints) as well as defines the required security features that must be implemented by all vendors interacting with the ePassport processes.

2.: Biometric Gateway - A series of applications has been developed to facilitate enrolment, administration and delivery of ePassport applications containing biometric data. These applications have been deployed using application servers and web servers, and use latest technology in terms of security and application interaction. All application data – regardless of vendor origin – are transmitted to the gateway. Access is protected by signing and encryption (Web Services Security), as well as certificate validation of all biometric clients. Data is validated for schema compliance and – upon success – a unique reference number is returned to the caller. Data is stored in a central database (encrypted) and made available for the ePassport booklet vendor. The Gateway also services central and local administrators enabling them to maintain the solutions and perform event and audit inspections as and when needed.

3.: Enrolment Client – A java based enrolment client – built upon HSS FPM – supports the data capture required by the ePassport process. The client is able to operate in (normal) online mode as well as in offline mode for contingency purposes. Security is handled by the use of the Public certificate based Single-Signon solution (SSO "NemLog-in") to handle the generation and delivery of valid SAML tokens, as well as the use of application-specific role based access control. The enrolment client is modularised, making it easy to support new requirements; adding e.g. a new process for handling lower-than-normal quality fingerprints according to latest standards.

The HSS FPM, has been enhanced, to support the use of Citrix Presentation Server based environments as well as Microsoft remote Desktop Services configurations. This means, that the client can operate in all the different environments used by the enrolment authorities.

The software platform for the client is build on Java in the shape of applets, executed in the clients browser.

The server solution is based on a Microsoft Windows Server 2008 operating environment with MySQL as the database engine. Application environment is provided by JBoss while Apache manages webservice requests.

Cost savings in the maintenance and operations

Benefits for the National Police

A biometric enrolment client is now available to support the capture of biometric data from passport applicants. This client is rolled out to all Police stations in Denmark, as well as in the Faeroe Islands and Greenland.

The Police can use the same client for central administration, thus controlling which municipalities have authorisation to deliver enrolment data, which local administrators are allowed to create and maintain new caseworkers, as well as view all event and audit information captures by the Gateway.

The National Police now have a uniform, well defined and robust solution for eID vendors to connect and retrieve enrolment data, regardless of origin (multiple client vendors are used for ePassport enrolment clients in Denmark). Based on industry-leading biometric software, along with the extensive use of Open Source solutions (Databases, Application Servers, Java and XML) the Police can realize cost savings in the maintenance and operations, as well as when new requirements due to new legislation or new enhancements in the enrolment processes are implemented.

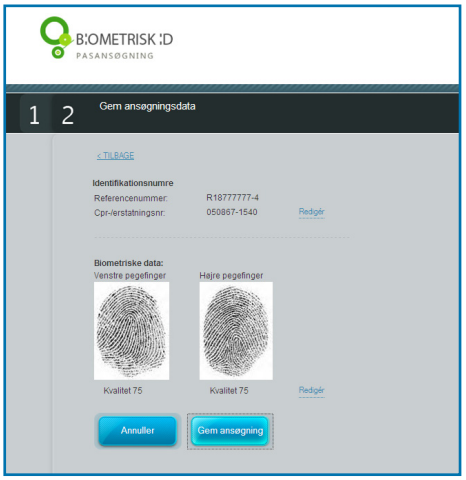
Benefits for the Municipalities

The municipalities that also have chosen to use the ePassport enrolment client provided by the Police, have a robust and centrally managed and maintained enrolment client available with full support. Hence they do not need to acquire infrastructure and software to adhere to MRTD related rules and guidelines.

The support and documentation are provided by the National Police free of charge to the municipalities; the investment is limited to hardware (fingerprint scanners) and HSS FPM licenses in the number they need individually.

Due to the lightweight enrolment client, and the use of standard components, the municipality can quickly and easily adapt to variations in enrolment volume; they can quickly setup additional workstations in periods of heavy usage patterns.

Since the solution has been developed for the National Police, the municipalities have a guaranteed legal compliance in case of changes to MRTD structures, as well as an automatic adherence to security requirements; thus they can focus on citizen services instead of security and technical issues related to the handling of biometrics.



Client screenshots

Fore more Information please contact: shss.at@atos.net