secunet
eID PKI Suite N-PKD

National Public Key Directory

More than just a mirror of the ICAO-PKD

secunet.com

The secunet N-PKD offers not only comprehensive collection and distribution of certificates but also guarantees that only trusted certificates are in use – thus providing more efficient border control.

CSCA certificates issued by a nation's certificate authority are the trust anchor to ensure the authenticity and integrity of the electronic data stored in eID documents. These certificates must be accessible and trustworthy in order to establish a chain of trust. A national Public Key Directory (N-PKD) is needed to enable the verification of the eID document's authenticity at the border through checking their electronic signature.

The role of passive authentication at border control

The content of the chip in electronic ID documents is secured with a digital signature. During electronic document verification at border control, the electronic signature used to protect the data stored on the chip is verified against the Document Signer (DS) certificate of the issuing authority in the country of origin (Passive Authentication). To determine whether the DS certificate is genuine an inspection system performs Passive Authentication. But how do inspection systems get access to the certificates they need and how do they know they are trustworthy? One of the means used here is the concept of Masterlists, which are exchanged internationally via the ICAO PKD. Since not all nations are participating in the ICAO PKD, countries may choose to assign individual trust levels to certificates not covered by the ICAO PKD.

To address this, the solution is a national Public Key Directory (N-PKD) as counterpart to the ICAO PKD. The N-PKD is required for communicating with the ICAO PKD. It exchanges certificates and Masterlists as well as Deviationlists with the ICAO PKD and allows countries to merge this data with certificates from other sources.

The N-PKD manages individual trust levels for each certificate allowing distinct control of which certificate to trust at border control. Masterlists are then used by the N-PKD to communicate this information. secunet offers an integrated solution for checking the quality of certificates and ensuring that only trustworthy certificates are stored in Masterlists.

The N-PKD component of the eID PKI Suite represents the national layer of the ICAO PKD and performs the following use cases:

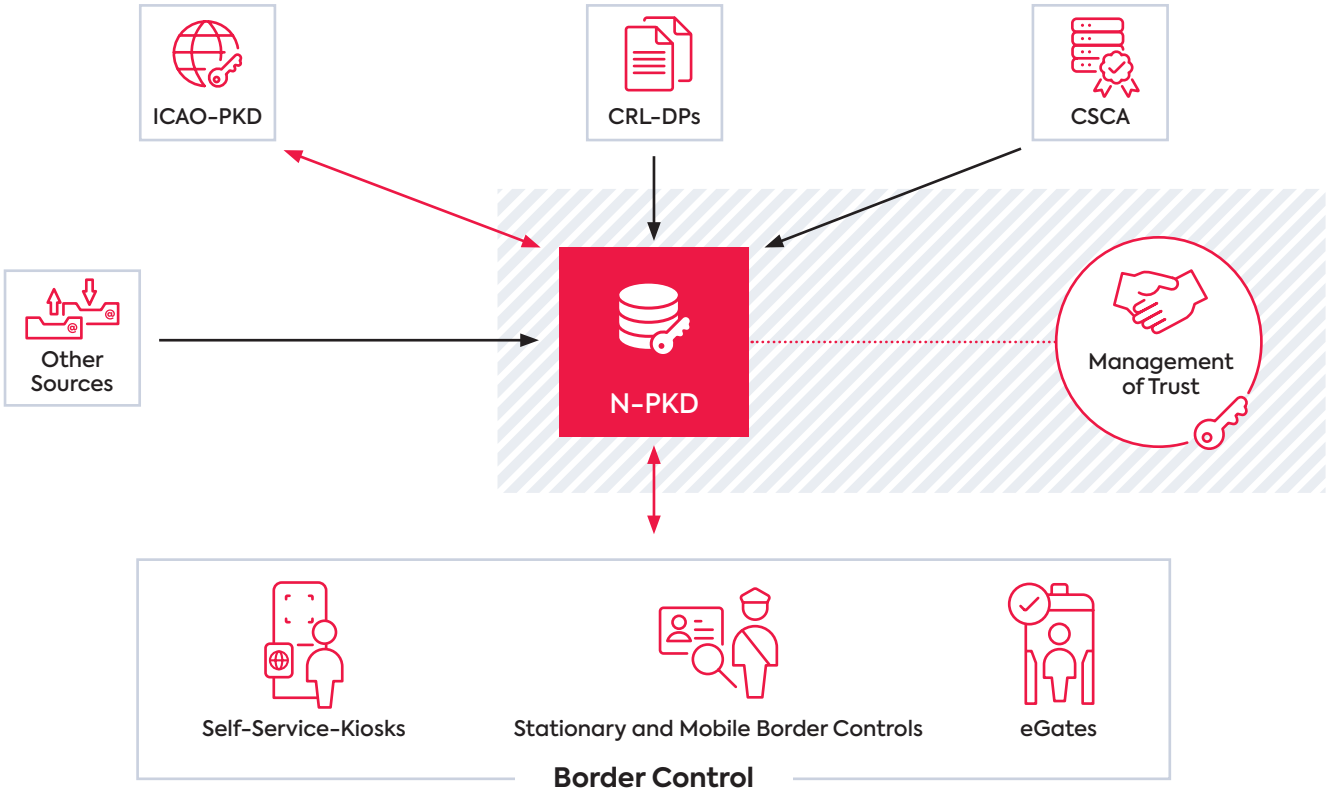
Data collection

Supports automated ICAO PKD Interface

- Download of DS certificates, Masterlists and Deviationlists
- Upload of certificates and lists

Keeps revocation information up to date

- Collect Certificate Revocation Lists
- Automatically receive CRLs from ICAO PKD and from all other known CRL distribution points



Supports manual, customer-specific options for the import of:

- Certificates (CSCA, DS)
- Masterlists, Defectlists and Deviationlists
- Revocation information (CRLs)

Managing Trust

Automated evaluation of imported objects

- Compliance to ICAO profile
- Link certificates to already trusted objects available
- Signature validation
- Customisation

Estimating the new trust status of objects

- Create Masterlists on trusted CSCA certificates
- Create Defectlists containing at least the revocation information for DS certificates
- Distribute Masterlists and Defectlists to the inspection systems (BSI TR-03129)

Benefits

- Automated collection and verification of certificates
- Provision of Masterlists, Defect-/Deviationlists, DS certificates, Revocation Information according to ICAO Doc 9303 respectively BSI TR-03129
- Efficient certificate validation based on customer needs

“Besides the excellent performance and usability of the PKI system during operation, secunet’s service concept as well as the profound expertise of the whole team are remarkable. In this complex project, we always had someone at our side who immediately solved the challenges to our complete satisfaction – even on-site at short notice when it was necessary.”

Þorvarður Kári Ólafsson,
Programme Manager ID and Travel Documents,
Registers Islands

Why secunet?

secunet offers the experience of more than 350 PKI projects of various sizes and complexities. secunet is a trusted partner for complex PKI systems of – among others – the German Federal Police, the Latvian Ministry of Interior, the Norwegian Police Force and Registers Iceland.

secunet’s eID PKI Suite solution offers high-quality modules, such as the N-PKD, that are well established and fulfil the latest requirements towards PKI in the eID and border control sector. Due to the flexible, modular and interoperable approach, our customers benefit from a smooth integration into their systems. secunet’s holistic, high-performance and high-security PKI solution automatises and thus optimises our customers’ processes.

Why is it more than just a mirror of the ICAO PKD?

The secunet N-PKD manages trust anchors. Besides the import of all trusted foreign and domestic ICAO PKI information, the N-PKD is also able to import not trusted, defective and fake single certificates and lists. The data on certificates that are not trustworthy is verified against newly imported certificates and lists. This prevents repeatedly imported certificates from being inadvertently classified as trusted. Thus, it ensures that untrusted certificates are denied for publication and are therefore neither used for the ICAO PKD upload nor at national border control.

Step 1 of the evaluation of certificates is the technical inspection of the certificates:

- The inspection of certificates start with validating the encoding and the signature
- Furthermore several properties of the certificates are determined
- Evaluation criterions can be extended by customer needs
- Evaluation criterions will be maintained by secunet
- The ratings can be recalculated manually or automated

Step 2 of the evaluation of certificates is the calculation of a suggested trust status:

- Defining a ruleset based on the ratings
- Evaluation of the estimated trust status according to the object ratings
- Ruleset can also consider customer-specific ratings
- Standard ruleset will be maintained by secunet

The suggested trust status allows the operator two alternatives:

- Automated acceptance of suggested status
- Indicative suggestion to be approved by the operator

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen · Germany
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com

More information:
secunet.com/pki-for-border-control

secunet N-PKD_EN_03/20