secunet

Three letters to ease inspection of electronic identity documents: PKI

Written by Author: Heiko Bihr, Principal, secunet Security Networks AG, Division Homeland Security

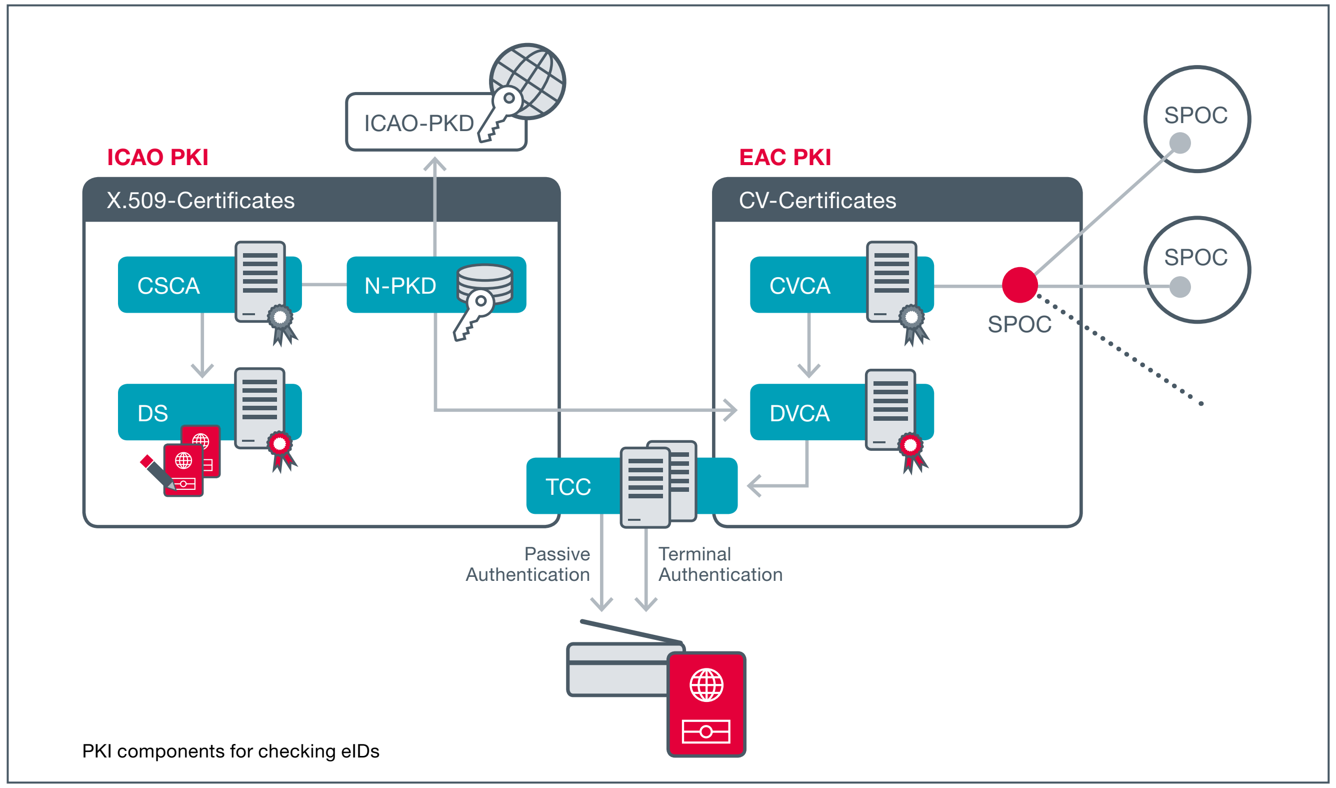
Introduction

PKI might be considered an "old hat" as certificates have been around for a long time. Secure certificates can nowadays be issued without problems. The new aspect is that PKI instances are located in different authorities and these instances have to communicate with each other. Many countries still have to do some homework with regards to their infrastructure: While systems for document issuance do exist, the background infrastructure for comprehensive electronic document checks at the border is lacking – in many countries the checks are therefore confined to the optical level. However, in order to secure international borders, it is not sufficient to only issue electronic ID documents they also have to be reliably and comprehensively checked at the border.

Challenges for adding comprehensive checking of eIDs to border control processes

When establishing a comprehensive security infrastructure to check electronic eIDs based on PKI authorities still face three key challenges.

Firstly, **managing trust anchors** is important. During electronic document verification, 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). DS certificates are issued by a nation's certificate authority (CSCA). This makes CSCA certificates the trust anchors to ensure authenticity and integrity of electronic data stored in eID documents. Each border control station must be equipped with a list of trustworthy CSCA certificates. Quality assurance is key in order to manage these lists. One of the means used here is the concept of Masterlists, which are exchanged internationally via the ICAO PKD. However, this concept provided by ICAO is not complete as not all nations are participating in it and countries may want to assign individual trust levels to certificates. The solution is a national Public Key Directory (N-PKD) as counterpart to the ICAO PKD. The N-PKD exchanges certificates and Masterlists 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 used by the N-PKD to distribute the list of trustworthy certificates to border control systems.



PKI components for checking eIDs

Secondly, **establishing communication interfaces** between countries to enable or support verification of fingerprints is crucial. In order to access fingerprints stored on an electronic ID document at border control, an Extended Access Control (EAC) authorisation certificate is needed. The issuance and exchange of prerequisites for EAC requires communication via designated aligned interfaces to handle incoming and outgoing certificate requests (SPOC). While there is already an existing specification for the SPOC communication interface, some difficulties still ensue, for example in the area of interoperability. The problem is comparable to the instance when two people with different dialects are trying to understand each other. The issues can occur when setting up the encrypted communication (where TLS is used) or during data transmission via this communication channel. The SPOC therefore has to be highly flexible in understanding and speaking all different possible dialects – not many solutions available at the market offer this capability.

Last but not least **high availability of central systems** is essential. To assure an efficient border control process, above mentioned tasks are performed by central systems. Their availability is mandatory during border control check. The effort to equip each border control system with certificate exchange capabilities would be enormous and is not very efficient. A central system is needed to provide the respective functionality. This type of system must be highly available and reliable since access to certificates is essential to perform electronic document authentication at border control. Such centralised document verification infrastructure that allows the connection of various distributed terminals is called Terminal Control Center (or TCC). A secure centralised certificate and key storage is part of this solution allowing the TCC to take over authentication procedure for authorised document readers. Several European countries, such as Germany, Czechia and Norway for example use a TCC for their border control and benefit from the fully comprehensive document check as the security level rises significantly.

Is it soon the norm for countries to establish a PKI infrastructure for border control?

While the challenges as outlined above exist, they can be tackled using high-performance, easy to operate PKI components. Countries and respectively issuance and border control authorities simply need to embrace this technology and make use of it. Many still seem to fear interconnected PKIs for border control as extremely complex and unfathomable. However, it truly is not that difficult as secunet's current projects have proven.

www.secunet.com/pki-for-border-control