HJP CONSULTING.

الشركة الإماراتية الألمانية
للطباعة الأمنية ذ.م.م.
Emirates German Security Printing LLC

Giesecke & Devrient

secunet

BUNDESDRUCKEREI

PRESS RELEASE

German expertise leads the implementation of the National PKD solution in the United Arab Emirates

Tamper-proof and efficient e-passport verification: EGSP delivered the solution in collaboration with HJP, Bundesdruckerei, secunet and G&D

Paderborn, 9 March 2015 – Abu Dhabi–based Emirates German Security Printing LLC (EGSP) delivered the complete infrastructure for the establishment of a National Public Key Directory solution. The system is used at border control checkpoints in the United Arab Emirates (U.A.E.) to ensure tamper-proof and efficient verification of domestic and foreign electronic passports. For the implementation of the "Made in Germany" security solution, EGSP was supported by its partners HJP Consulting GmbH, Bundesdruckerei GmbH, secunet Security Networks AG and Giesecke & Devrient GmbH.

Emirates German Security Printing, a joint venture in which Bundesdruckerei holds a 49 percent stake, is the prime contractor for the National Public Key Directory (NPKD) project initiated by the Ministry of Interior of the United Arab Emirates. EGSP's project partners delivered the solution. HJP Consulting (HJP) worked closely with the relevant departments in the Ministry of Interior of the United Arab Emirates and provided all services related to system integration, including planning, testing and project management. G&D Dubai, a subsidiary of the Munich-based technology group Giesecke & Devrient (G&D), provided the NPKD software, which is part of the *secunet eID PKI Suite* by the G&D subsidiary secunet Security Networks. The Bundesdruckerei delivered the software for the expansion of existing border control systems.

Proof of authentic and tamper-proof electronic passport data

Electronic passports are embedded with a chip that prevents the undetected manipulation of the personal data of the passport holder. Using the Public Key Directory of the International Civil Aviation Organization (ICAO), border control authorities can verify the authenticity of the passport data. They rely on having access to prequalified certificates, called Document Signer Certificates, and other public key infrastructure (PKI) data from active ICAO member states.

The Ministry of Interior of the United Arab Emirates has now introduced the National PKD system to examine the data obtained from the ICAO PKD and from other sources and to forward the appropriate certificates and certificate revocation lists (CRLs) to all document verification systems (so-called "Inspection Systems") at border control posts in the U.A.E. In September 2011, the United Arab Emirates became the first country in the Middle East to join the ICAO PKD as an active member. Now it is the first country in the Middle East that implemented a National PKD solution.

Background: Public Key Infrastructure (PKI) and Public Key Directory (PKD)

A public key infrastructure (PKI) enables participants to exchange encrypted information with each other on a public communication network such as the Internet without having to use a different trustworthy channel to exchange a shared secret key. Instead, participants just need to share their public keys in order to exchange encrypted messages. The encrypted messages can be decrypted only by a recipient with the associated secret key (private key). The same mechanism can be used to generate a digital signature (also called an electronic signature) that shows whether a message is indeed from the sender or whether it has been modified by an unauthorized person. In the area of e-passports, digital signatures are used to determine that the data on an electronic passport was stored there by the appropriate authority and has not been falsified.

Authentication of the sender is essential to prove that the issuer of a public key really is who it claims to be. This is where the public key infrastructure comes into play. The basic principle is that a trustworthy authority confirms the identity of the sender of a public key, thus assuring the participant that the data is tamper-proof and originated with the sender. Therefore, the trusted authorities establish public key directories (PKD), in which are recorded both the currently valid and the compromised public keys of its participants.

For electronic passports, the ICAO provides the exchange platform (ICAO PKD) for PKI data of the operators of National PKD solutions.

For more information, please contact:
HJP Consulting GmbH
www.hjp-consulting.com

Mr. Markus Hartmann, Managing Director
Mrs. Anke Larkworthy, Marketing Director
Hauptstrasse 35
33178 Borchen
Germany
info[at]hjp-consulting.com

Emirates German Security Printing
https://www.bundesdruckerei.de

Bundesdruckerei GmbH
https://www.bundesdruckerei.de

Giesecke & Devrient GmbH
http://www.gi-de.com

secunet Security Networks AG
http://www.secunet.com/de/