Cloud-based provisioning of qualified certificates for the German ID card

Marcel Selhorst, Carsten Schwarz

Bundesdruckerei GmbH
Oranienstr. 91, 10969 Berlin
marcel.selhorst@bdr.de, carsten.schwarz@bdr.de

Abstract: In November 2010 the German government introduced a new national ID card. The Bundesdruckerei GmbH was the responsible company for designing and producing the ID card including its highly sophisticated security features. Besides traditional means for visual identification, the card contains a wireless smartcard chip enabling online usage of the ID card. Thus citizens are now able to prove their identity, age or place of residence to an online service provider, e.g., through a web application. Additionally, the chip contains an inactive application for the generation of digital signatures based on elliptic curve cryptography (ECDSA) which - upon activation - can be used to digitally sign electronic documents (online as well as offline).

The Bundesdruckerei GmbH is currently the only party able to perform online post-issuance personalization of qualified electronic signature certificates on the ID card. In order to do so, a new web application called "sign-me"[1] has been developed enabling citizens to activate the signature application on the ID card. In order to diminish the technical challenges for the citizens, "sign-me" takes over the required steps of

- performing the required online identification of the citizen according to the German signature law by using the eID-application provided by the new ID card,
- generating a fresh signature key pair on the ID card,
- exporting the according public key to the certificate service provider "D-TRUST GmbH", the trustcenter of the Bundesdruckerei GmbH, which is then responsible for binding the citizen's identity to the generated signature key pair by issuing the according X.509-certificate, and finally
- storing the issued qualified certificate on the citizen's ID card.

This invited talk briefly introduces the German eID system and focuses on the organizational process as well as the infrastructure required for secure online issuance and management of the certificates. We will introduce the "sign-me" web application and show how citizens can activate the signature application on their ID card, how quickly it is possible to issue and store a qualified certificate on the ID card and how it can be used to finally sign documents. An outlook on envisioned further extensions of "sign-me" concludes the presentation.

[1] http://www.sign-me.de