Belgian Electronic Identity Card (applet 1.7) content addendum

Table of content

Scope

This standard describes the change in specifications of the Belgian Electronic Identity Card files and objects for applet 1.7 eID cards that will have undergone a rekeying to benefit from the newer, more secure, ECC certificates.

Applet 1.7 cards that will be re-keyed will now get certificates (authentication and non-repudiation) signed by citizen and foreigner CA's that have an EC key, and which in turn will be signed by an EC Belgian Root CA.

The RRN certificate is now an EC RRN certificate that falls under an EC Belgian rootCA.

The signature files (EF SGN#ID and EF SGN#Address), that will be re-created during the re-keying on the eID card, will now be in the EC format like on the applet 1.8 eID cards.

Changes

EF(SGN#Address)

This transparent elementary file contains the signature of the ***EF(ID#Address)*** by the National Register.

EF(SGN#ID) is first appended to ***EF(ID#Address)*** before signing, in order to ensure the consistency with the file ***EF(ID#RN)***. If zero bytes are present at the end of ***EF(ID#Address)***, they need to be removed first.

Signature format: ECDSA P-384 with SHA-2-384

EF(SGN#Address) has a fixed length. If the EC signature (in asn.1 format) it contains is smaller than this fixed length, it will be padded by zero bytes.

Remark: The length of the asn.1 encoded signature can be found by adding 2 to the value of its second byte.

EF(SGN#ID)

This transparent elementary file contains the signature of the ***EF(ID#RN)*** by the National Register.

As the ***EF(ID#RN)*** file contains the hash of the picture, the picture is also implicitly signed.

Signature format: ECDSA P-384 with SHA-2-384.