

EAC and EAP: The Differences

EAP (ISO/IEC 18013-3) is a protocol closely based on EAC (BSI TR-03110 Version 1.10). WG10 has made every effort to make EAP compatible with EAC to the extent possible. This document lists the remaining differences between the two.

Certificate Format

EAP builds on the certificate format of EAC which in turn is an application of card-verifiable certificates as defined in ISO/IEC 7816-8. EAP certificates use the same basic structure as EAC certificates, using an OID to convey the actual formatting. They differ in the following three areas:

Object Identifiers

EAP uses object identifiers assigned to ISO/IEC 18013 for the public key format, whereas the object identifiers used in EAC are under the exclusive control of BSI. Reliance on EAC object identifiers may have led to future inconsistencies within ISO/IEC 18013-3 or to requirements (by reference) that would not have been synchronized with the unique nature of the driving licence environment.

Subject Key Identifier (SKI)

Note: In EAC terminology, the SKI is called "Certificate Holder Reference".

In EAC, the SKI must be a Latin-1 encoded string of not more than 16 characters. It consists of the ISO ALPHA-2 country code of the issuer, followed by the name of the issuer, and a key sequence number. WG10 concluded that this method does not provide sufficient collision resistance, especially in the more complex context of driving licenses where there is no 1:1 mapping of countries and certificate issuers.

EAP allows the SKI to be a binary string in the spirit of RFC 3280 (X.509 PKI), derived from the public key, or another method that generates unique values. This method offers the stronger collision resistance required by the large expected number of PKI participants. The length of the SKI is limited to a maximum of 16 bytes to match the length in EAC certificates.

Path Length Constraint

EAC requires a fixed three-tier hierarchy (CVCA > DV > IS). WG10 concluded that such a constrained hierarchy will not suit the heterogeneous environment of driving licenses, where many participants from both public and private sector are expected.

The EAP certificate structure includes a path length constraint in the certificate holder authorization field, a widely used mechanism in X.509 infrastructure to allow a flexible PKI.

As a consequence, the coding of the certificate holder authorization is different.

Implicit Key Selection

EAC requires a key to be selected using an MSE command before any PSO command can be executed.

EAP uses implicit key selection, where the key to be used in subsequent PSO commands is automatically selected after a successful PSO command; however, explicit key selection is allowed to allow compatibility with existing terminals.

Implicit key selection simplifies the verification process and may enhance performance.

Command Chaining

EAC does not allow command chaining.

EAP allows command chaining if the chip does not support extended length APDUs.

Command chaining allows EAP to work with chips and/or terminals that do not support the extended length mechanism, which are generally available at a lower cost.

Comment [LJN1]: by?

Comment [LJN2]: Why is this not a problem for ICAO? I.e., why is this a problem in the driving licence environment but apparently not in the passport environment?

Comment [mku3]: The BSI document does not really have a reputation for being stable. Using the same OIDs would result in having to support any further change they make to the PK format.

Comment [LJN4]: Certificate holder reference? If correct as stated, it may be helpful to also state the EAP equivalent.

Comment [LJN5]: Why did BSI not go this route? I.e., why is this a need in the driving licence environment but not in the passport environment?

Comment [mku6]: I presume the reason why BSI did not go this route is because G&D's card OS doesn't. This feature is a remnant of my original "keep it simple" approach. There is no technical reason for using explicit key selection, but it's not a major issue either.

Comment [LJN7]: Because we expect a more diverse driving licence environment that is found in the passport environment?

Comment [mku8]: Driving licenses are issued in considerably larger volumes and frequency as passports//ID cards are hence more const-sensitive. BTW, this was cause of a large dispute between NL-FR vs DE in BIG, but of course DE dictated that chaining will not be allowed. Again, this was not for technical, but for political reasons and also to gain "competitive" advantage.