ISO/IEC 7816-15 Identification cards — Integrated circuit cards — Part 15: Cryptographic information application

return to the ISO Standards

Table 1: Data sheet for Identification cards — Integrated circuit cards — Part 15: Cryptographic information application

Title	Identification cards — Integrated circuit cards — Part 15: Cryptographic information application
Acronym	
Version	2016
Document Number	7816-15
Release Date	2016
Reference	https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-15:ed-2:v1:en

> **Note**: The following is an excerpt from the official ISO catalog. It is provided here as a convenience and is not authoritative. Refer to the original document as the authoritative reference.

Scope

This part of ISO/IEC 7816 specifies an application in a card. This application contains information on cryptographic functionality. This part of ISO/IEC 7816 defines a common syntax and format for the cryptographic information and mechanisms to share this information whenever appropriate.

The objectives of this part of ISO/IEC 7816 are to

- facilitate interoperability among components running on various platforms (platform-neutral),
- enable applications in the outside world to take advantage of products and components from multiple manufacturers (vendor-neutral),
- enable the use of advances in technology without rewriting application-level software (application neutral), and
- maintain consistency with existing, related standards while expanding upon them only where necessary and practical.

It supports the following capabilities:

- storage of multiple instances of cryptographic information in a card;
- use of the cryptographic information;
- retrieval of the cryptographic information, a key factor for this is the notion of “Directory Files”, which provides a layer of indirection between objects on the card and the actual format of these objects;
- cross-referencing of the cryptographic information with DOs defined in other parts of ISO/IEC 7816 when appropriate;

- different authentication mechanisms;
- multiple cryptographic algorithms (the suitability of these is outside the scope of this part of ISO/IEC 7816).

This part of ISO/IEC 7816 does not cover the internal implementation within the card and/or the outside world. It is not mandatory for implementations complying with this International Standard to support all options described.

In case of discrepancies between ASN.1 definitions in the body of the text and the module in Annex A, Annex A takes precedence.