

Standard ECMA-235

The ECMA GSS-API Mechanism

(March 1996)

Following on from Standard [ECMA-219](#), that defines services, data elements and operations for authentication, Privilege Attribute and key distribution applications (the APA-Application), this Standard ECMA-235 defines the syntax of the tokens that enable distributed applications implementing the APA-Application and related data elements specified in Standard [ECMA-219](#) to interwork.

The tokens defined in this Standard are :

- Tokens for Security Association establishment
- An error token for communicating a failure to establish a Security Association
- Tokens for message protection
- A token for Security Association deletion

In order to provide a basic set of implementation options, this Standard also defines some key distribution schemes based on symmetric and asymmetric cryptographic technologies. These include specification of the encryption algorithms and methods to be used.

The following files are provided in this set of CD-ROMs:

File name	Size (Bytes)	Content
ECMA-235.PDF	214'253	Acrobat PDF file
ECMA-235.PSC	717'960	Corresponding PostScript file

Printed copies of this Standard can be ordered, free of charge, from document@ecma.ch .
