

ECMA-138, Security in Open Systems – Data Elements and Service Definitions

SCOPE

This ECMA Standard defines a number of abstract security services for use in a distributed system. For each of the abstract security services identified in this document, a service definition is given. These service definitions are intended to be used in contexts such as:

- Open Systems Interconnection where they may be used as references for the development of security related protocols or elements of other protocols,

- Open Distributed Processing where they may be used as references for the development of secure systems architectures,

- Applications Standards developments (e.g. Distributed Office Applications) where they may be used to specify security functionality embedded in specific applications.

The security requirements of distributed applications that are specific to the nature of these applications (e.g. access controls to the objects owned by a given application such as a database manager) are addressed here only with regard to the interactions of such applications with the security services.

This ECMA standard is structured as follows:

Clause 1 (this Clause) gives a general introduction, references, and definitions of terms.

Clause 2 describes a model of security based on the abstract Security Facilities in ECMA TR/46. A set of security services and the requirements for security information are described.

Clause 3 describes the most important piece of security information used in the application layer: the Security Attribute. Methods for passing attributes between security services, and between application processes, are suggested. A standard format for packaging together and sealing attributes for transmission is given.

Clauses 4 to 9 outline the individual security services, their semantics, service interfaces, and management interfaces.

Clause 10 shows how the components described in this ECMA Standard should be used in other standards for productive applications.

Appendix A contains the full ASN.1 for the data elements defined in the main text. Appendix A is part of this standard.

Appendices B to F contain additional descriptive material which may help the reader to interpret the standard in their own environment. A reader interested in security for distributed systems should read the document as laid out. A reader who is looking for help on providing security in a new application standard should read clause 10, then refer back to the earlier clauses as required.