3.1 REFERENCE MODEL DEFINITIONS

This Part of the Standard is based on the concepts developed in ISO 7498-1 and makes use of the following terms defined in it:

a. Application Entity
b. Service or Layer Service

c. Key Management

The definition is “the generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.”
3.9 CHARACTER HANDLING DEFINITIONS
This part of the standard makes use of the following terms defined in ISO/IEC 2011-2022:1994:

a. Coded character set; code.
b. Code extension;
c. Escape sequence.

3.14 REFERENCE MODEL SECURITY ARCHITECTURE DEFINITIONS
This Part of the Standard makes use of the following terms defined in ISO 7498-2:

a. Digital Signature

Note: The definition is “Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of that unit and protect against forgery e.g. by the recipient.”

b.c. Data Confidentiality

Note: The definition is “the property that information is not made available or disclosed to unauthorized individuals, entities or processes.”

d.e. Data Origin Authentication

Note: The definition is “the corroboration that the source of data received is as claimed.”

c.d. Data Integrity

Note: The definition is “the property that data has not been altered or destroyed in an unauthorized manner.”

d.e. Key Management

Note: The definition is “the generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.”