

DLMS/COSEM Security Enhancement- Latest Updates

By Vinoo S Warriar

The DLMS/COSEM specification is fully described in the DLMS UA coloured books. The latest updated releases of the colored books (The DLMS-UA standards), are the Blue Book -10th edition, Green Book -7th edition (with an Amendment 1), Yellow Book-4th edition. While the latest releases also show much progress on various aspects of DLMS/COSEM, which includes security enhancements, incorporating the FSK-PLC profile etc., the primary thrust has been on Security.

The security specific enhancements to the standards now provide:

- a) Data access security: Definitions for authentication mechanisms, for high-level-security signon process. These were left to user in earlier editions.
- b) Data transport security: Definition of a security context with a security policy, security suite and the security material elements. Definition of the ciphered application context PDUs to carry the ciphered services.

DLMS/COSEM provides two categories of security services:

- I. Data access security related to authentication of the sign-on process between clients and servers and
- II. Data transport security related to authentication and encryption of the actual DLMS data communications between clients and servers.

The latest releases have achieved the following major objectives:

1. Data access security procedures were addressed by lowest, low and high level security requirements. Lowest level was no-security, low level was password-protected access (one-way authentication), and high level security was a four pass two way authentication that uses encryption technologies in the last two passes. However, the actual high level security mechanism was left to the user in earlier editions. The latest editions, define three standard mechanisms to process the encryption in the final two passes, by clearly defining three of the authentication mechanism choices
2. Data transport security procedures were defined as being carried out under ciphered application contexts, but the exact mechanisms and services were not defined earlier. The current releases specify and define the transport security procedures as a combination of authentication of messages as well as encryption

of messages. The standards now define a security policy, a security suite and the security material.

Security policy defines the following possibilities:

- No authentication or encryption
- All messages are authenticated
- All messages are encrypted
- All messages are authenticated and encrypted

The security suite currently defines one mechanism, namely the Galois Counter Mode (GCM) of AES-128 to provide the authentication and encryption, with a possibility to add other mechanisms later to the suite.

The security materials relevant to the above are the block cipher key, an authentication key and the initialization vector.

3. The standards also now flesh out the structure of the ciphered-APDU and the services to transport encrypted and/or authenticated APDUs
 - a) The ciphered application context APDU contains a Security Header. The Security header consists of a concatenation of a Security Control (SC) byte and a Frame Counter (FC). The SC byte contains the security suite id (currently only the value 0 is defined standing for the AES-128 GCM mode), and a bitmask that identifies the security policy in force (whether the APDU is encrypted or authenticated or both or neither). The resulting APDU can contain a plain text xDLMS PDU with an authentication tag appended at the end, may be an encrypted xDLMS PDU or may be an encrypted xDLMS PDU followed by an authentication tag
 - b) The COSEM Application Process requests and responses primitives contain a Security_Options parameter that tells the underlying layers what security procedures are to be implemented in the PDU. Similarly, the COSEM indications and confirmation primitives received from the underlying layers contain the corresponding Security_Status information.

Vinoo Shankar Warriar, US Director-Product Management, Kalkitech), is a member of DLMS working committees and has been actively involved in framing DLMS based companion specification for Indian markets. He is one of the chief architects behind Kalkitech's DLMS solutions.