Security within DLMS – A Summary

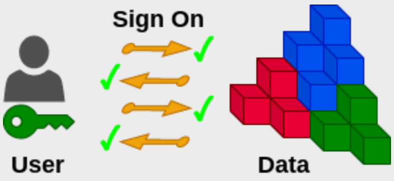
DLMS – Secure as Standard

DLMS COSEM is a transport independent application protocol that provides complete application layer security, ensuring sensitive and sometimes critical data, is fully protected end to end. Application layer security is the **only** method to ensure complete data privacy and comply with the latest GDPR requirements.

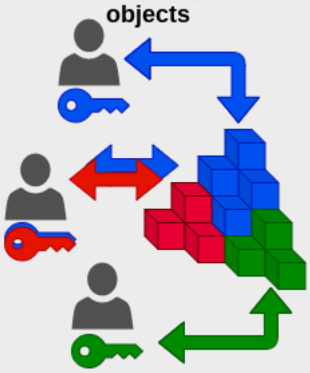
In order to secure data at the application level, DLMS utilises industry standard Secure sign on with Role Based Access (RBAC) combined with full end to end data protection techniques.

Secure sign on with RBAC

Secure sign on with Role Based Access Control (RBAC) is a mechanism to prove a person or device (i.e. the Client) is actually who they say they are and have the appropriate access rights to the other party (i.e. the Server).



Users can be granted access to one or more group of objects

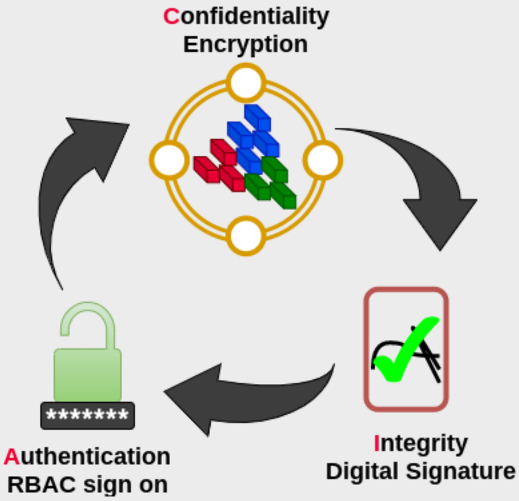


In DLMS, secure sign on is part of a mechanism or process called Application Association (AA), in which both the Client and Server mutually authenticate one another, providing access to a particular set of data objects depending on the access rights of the Client. The access rights specify the operations that can be performed by the user (e.g. read data, write data or commands) and the required protection level (encryption and/or authentication) required for the message datagrams. A DLMS server can simultaneously support several AAs with different clients, designed such that each AA can access selected data according to its role. Should authentication fail, the AA cannot be established and data exchange cannot take place.

RBAC is essential for practical applications, such as where an installation engineer may require access to data pertaining to configuration, but be blocked from accessing sensitive customer data that an only an operator should have access to for aiding in customer service enquiries. RBAC makes this possible, as the installation engineer would be required to sign in with different credentials than the operator and thus only be granted access to the appropriate data.

Message protection

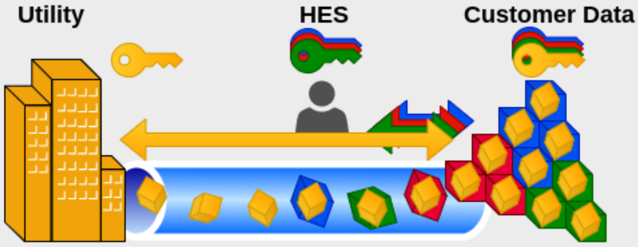
Once a Client has authenticated itself with a Server, messages can be exchanged. Message protection is provided through a number of industry standard techniques to ensure complete protection, these being encryption for confidentiality (to prevent eavesdropping) and digital signatures for non repudiation and integrity (ensure data is not tampered with).



The level of protection to be applied to each message is determined by the Application Association (AA) during the initial sign on process.

In order to provide a total solution, DLMS not only supports protection of the message (or datagram) but also the data contained within. This layering of protection allows sensitive data to be truly secure end to end.

Layering of protection is critical for large smart meter deployments where sensitive data has to be transferred from a Utility all the way to a meter and back, without any person or device en route being able to intercept it. However, common with such large deployments, the data collection software (or HES) where the data collection Client resides, is actually remote from the utility systems. This can present a challenge for many application protocols, as it is normal for the messages (and thus data within) to be deciphered by the Client in the HES hence breaking the end to end protection. However, as DLMS supports layering, the data within a datagram message is further secured, thus allowing the sensitive data within the message datagram to be transferred all the way to the Utility without the risk of it being compromised.



Security suites

DLMS provides secure logon with RBAC and message protection through NSA Suite B that allows three levels of security up to 256bit Symmetric and 384bit Asymmetric cryptography to satisfy all market requirements. Two of the suites support V.44 compression for use on networks with limited bandwidth.