# Gridstream solution security

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>5</td>
</tr>
<tr>
<td>Integration</td>
<td>6</td>
</tr>
<tr>
<td>Meter reading</td>
<td>7</td>
</tr>
<tr>
<td>Field tools and data collection system applications</td>
<td>8</td>
</tr>
<tr>
<td>Communication</td>
<td>9</td>
</tr>
<tr>
<td>Data storage</td>
<td>10</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>11</td>
</tr>
<tr>
<td>Encryption techniques</td>
<td>12</td>
</tr>
<tr>
<td>Integrity</td>
<td>13</td>
</tr>
<tr>
<td>Availability</td>
<td>14</td>
</tr>
<tr>
<td>Authentication</td>
<td>15</td>
</tr>
</tbody>
</table>

# IDIS security using DLMS-COSEM

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>16</td>
</tr>
<tr>
<td>Security policy</td>
<td>17</td>
</tr>
<tr>
<td>Security suite</td>
<td>18</td>
</tr>
<tr>
<td>Key generation and distribution</td>
<td>19</td>
</tr>
</tbody>
</table>
The Gridstream system is a powerful energy management service based on two-way data communication. It enables a wide range of applications, such as remote meter reading, customer relationship management and demand-side management. It provides functions to assist utilities with load control, reporting power outages and monitoring power quality. Vast amounts of information flow through a Gridstream system every day, and the security of this data is a top priority. It is vital to protect the system against unauthorized users or ‘hackers’ and to ensure the integrity and confidentiality of the data.

The data flowing through the Gridstream system is exposed to various risks, such as intrusions in the field network, the data centre or even at system level. The security architecture for Gridstream ensures system and network availability, while at the same time meeting critical security objectives, such as confidentiality, integrity and authentication of data. By using a system like Gridstream that focuses on these objectives, a utility can effectively manage its security risks.

Figure 1 – Example Gridstream AIM infrastructure using sub-networks and zones
In overview, the key elements of the Gridstream security approach include:

- **Access control**
  The servers in the head end system platform are all protected using hierarchical access control mechanisms. For example, these mechanisms allow an administrator to assign an available network for each user, and offer an easy way to assign access rights (roles) within that network to the user. Within a role definition, an administrator can define access rights to user-specific AIM applications. The internal network of AIM system platform servers is typically protected from external access using firewalls and multiple levels of network access control mechanisms.

- **Integration**
  In a typical project, the integration of the Gridstream system into the utility's information technology environment is carried out after the evaluation of existing systems and security requirements. Particularly when the utility system resides in a different location than the head end and meter data management systems, the security enforcement mechanisms between the two are carefully planned and enforced.

- **Meter reading**
  Remote reading of metering values from a point-to-point metering device (i.e. a device that communicates with the head end system using a mobile network) by the data collection system is typically protected using a virtual private network (VPN) tunnel between the internal Gridstream network and security enforced by the communication service provider and network-provider. In the case of a local area network (LAN) connected meter, a VPN with firewall may be enforced between the LAN meter and the AIM internal network.

- **Field tools and data collection system applications**
  For operating the AIM Site Manager application, the Site Manager typically runs on a server in a de-militarized zone (DMZ) and is connected via a VPN tunnel to the telecom operator network with an optional HTTPS connection between the field tool device application and the Site Manager server.

  For AIM Dashboard, it is advisable to run the Dashboard server in the DMZ, and that HTTPS connections are enforced between the user terminal and the Dashboard server. The data transfer between the AIM Dashboard server and the AIM system platform server may also use the HTTPS protocol.

- **Communication**
  AIM supports various communication methods, and regardless of the method selected, Gridstream ensures secure and reliable data transfer at all system levels. Communication is secured by various methods (as outlined above) to prevent, for example, unauthorized connections or system monitoring.

  Gridstream includes automatic repeat functions at different system levels to enable smooth recovery and to solve any possible communication problems. The communication protocols used have automated control and correction functions.

  Communication between the measurement and display device and the data collection system is typically via either mobile telephony or power line communication (PLC). Message security over the mobile telephony network is typically provided by the wide-area networking VPN functionality of the network provider, in conjunction with the use of HTTPS on the transport layer.

  Providing message security over power line communications has been a subject of work in the IDIS consortium and in DLMS-COSEM standardization. Confidentiality, integrity and authentication is provided by using AES encryption and key distribution services throughout the measurement, switching and display system itself, and at the interfaces to the data collection system.

  Communication within a meter is done by using an internal bus. For instance, meter values are read directly from the meter’s measurement integrated circuits by using the meter’s internal bus. The internal bus is only accessible by breaking the meter cover seal, which sends a system alarm to the data collection system, making such security attacks easy to detect and locate.

- **Data storage**
  In addition to securing communication, Gridstream ensures that all data is safely stored and transferred. Each metering value coming from the meter has a status indication with the assured time of measurement, to show whether the user can trust the value or not. It shows,
for example, if there were power cuts or if the device’s time was adjusted during the measuring period. This information helps the user to locate the details of the device in question, if necessary. The Gridstream logging and auditing functions ensure that all modifications to the system data are carefully traced in the system.

- **Confidentiality**
  Gridstream protects confidential information through the use of security standards for interoperable solutions, as well as various encryption techniques at the multi-energy endpoint and network levels.

  Secure communications are imperative for data transfer between devices in the measurement, switching and display system and the data collection system components, such as a data concentrator or the head end system. The DLMS-COSEM protocol provides several security features for authenticating and transporting data. Data transport security provides privacy and authentication of data as it travels from a multi-energy meter point to the next system instance. Gridstream meters use the security features that have been defined by the DLMS-COSEM standard.

- **Encryption techniques**
  Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing the ‘key’. To ensure confidentiality in metering data transfer, the following encryption techniques are used by Gridstream devices.

  The Advanced Encryption Standard (AES) is an encryption method that uses unique keys at the endpoint to protect home or business information from interception that could lead to potential privacy and operational exploits.

  Secure Sockets Layer (SSL) protocol is designed to protect data transported over internet protocol (IP) based networks, as well as secure sockets for HTTP and web services.

- **Integrity**
  Data integrity is ensured while data is stored in the meter, and also as data is transmitted to the next system component. Gridstream protects access to stored data against unauthorized access, modification, removal or destruction. This is done using checksums, which ensure

<table>
<thead>
<tr>
<th>Objective</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Confidentiality | Preserving unauthorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.  
  *A loss of confidentiality is the unauthorized disclosure of information.* |
| Integrity | Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.  
  *A loss of integrity is the unauthorized modification or destruction of information.* |
| Availability | Ensuring timely and reliable access to and use of information.  
  *A loss of availability is the disruption of access to or use of information or an information system.* |
| Authentication | Ensuring that access to resources is given only to entities whose identity and right to access the resources has been verified. |

Table 1 – Security terminology
**Availability**

Gridstream is able to use, and is compatible with, standard IT infrastructure. This means that utilities can employ traditional data centre technologies to solve availability challenges. A unique challenge particularly in power line communication implementations is susceptibility to interference. Systems using Gridstream can reduce jamming and interference issues through the design and function of the network implementation.

**Authentication**

Authentication takes place when a user logs on to the systems interface. Gridstream is protected using hierarchical access control mechanisms. The internal network in a project installation is typically protected from external access using firewalls and multiple levels of network access control mechanisms.

Gridstream can allocate access permits to users. As different users, such as supplier staff, utility staff, the grid operator, or the multi-energy utility, have different interests, they also have different rights to the data in the system and metering point. Assigning access privileges ensures that users only have rights to the information that they require.

All users of external connections should be authenticated inside a secure data connection protocol. This is especially important for protection against signals from an unauthorized meter or a computer that emulates a meter. The authenticity of a meter that is sending data is ensured using the DLMS-COSEM high level security authentication protocol.

The DLMS-COSEM protocol ensures secure access to the electricity meter’s data. Data access security is based on assigning different access rights. The next system component is required to be correctly authenticated to access data.

Other features used by Gridstream to provide authentication and integrity include:

- Role Based Access Controls (RBAC) within the head-end system enabling the utility to restrict operational and data access on a granular basis to both individuals and systems with an explicit need

- Native and Lightweight Directory Access Protocol (LDAP) with user authentication mechanisms at the head-end. The native authentication mechanism is based on User IDs and hashed passwords. LDAP support enables the utility to implement extremely elaborate multifactor and even multi-person access controls using standard third-party systems

- Hash Message Authentication Codes (HMACs) to guarantee the authenticity of a message

- Mobile administration software makes use of digital certificates issued by the head-end to authenticate field tools.
IDIS security using DLMS-COSEM

Gridstream measurement, switching and display devices as well as the interface between these devices and the data collection system over power-line communications use the specifications defined by IDIS and DLMS-COSEM. These standards have been elaborated to include specifications for providing secure communications in the data collection process. As part of the IDIS interoperability consortium, Landis+Gyr is committed to implementing security functionality according to the DLMS-COSEM specification.

The following section summarizes, the main cornerstones of DLMS-COSEM security.

- **Authentication**
The DLMS-COSEM specification defines three levels of authentication. An implementation can use either No, LLS or HLS depending on the level of protection required. IDIS security uses HLS. (Table 2)

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Server</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>No authentication</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>LLS (Low level security)</td>
<td>—</td>
<td>Password authentication</td>
</tr>
<tr>
<td>HLS (High level security)</td>
<td></td>
<td>Challenge/response authentication</td>
</tr>
</tbody>
</table>

Table 2 – Authentication types used in DLMS-COSEM

- **Security policy**
DLMS-COSEM defines the concept of different available security policies, of which there are four types:

1. Security not imposed
2. All messages are authenticated
3. All messages are encrypted
4. All messages are authenticated and encrypted (IDIS security)

- **Security suite**
The security suite defines the cryptographic algorithm used for message security. DLMS-COSEM specifies one specific security suite using Galois Counter Mode (GCM) with AES-128. (Table 3)

<table>
<thead>
<tr>
<th>Security suite ID</th>
<th>Authentication algorithm</th>
<th>Encryption algorithm</th>
<th>Key transport method</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>AES-GCM-128</td>
<td>AES-GCM-128</td>
<td>Key-wrapping using AES-GCM-128</td>
</tr>
<tr>
<td>All other reserved</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

Table 3 – Security suite defined in DLMS-COSEM
## Key generation and distribution

The IDIS security specification references the key scheme of DLMS-COSEM, which is based on a single set of unique symmetric keys per meter. Each key type has a specific purpose (e.g. key encryption, authentication, message encryption) within the DLMS-COSEM communication protocol.

Note: In DLMS-COSEM the term global means valid over multiple associations, and not system-wide

<table>
<thead>
<tr>
<th>Key type</th>
<th>Use</th>
<th>Generation</th>
<th>Delivery</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Symmetric keys</strong></td>
<td><strong>Symmetric keys</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master key (MK)</td>
<td>Key encryption key for global keys</td>
<td>Landis+Gyr production system</td>
<td>From Landis+Gyr production system to HES using signed messaging</td>
<td>Production system • HES • Meter</td>
</tr>
<tr>
<td>Global unicast encryption key (GUK)</td>
<td>Global encryption of unicast xDLMS APDUs</td>
<td>HES</td>
<td>Wrapped with master key, invocation of global_key_transfer method by HES or the DC</td>
<td>HES • DC • Meter</td>
</tr>
<tr>
<td>Global broadcast encryption key (GBEK)</td>
<td>Global encryption of broadcast xDLMS APDUs</td>
<td>HES</td>
<td>Wrapped with master key, invocation of global_key_transfer method by HES or the DC</td>
<td>HES • DC • Meter</td>
</tr>
<tr>
<td>Global broadcast authentication key (GAK)</td>
<td>Authentication of xDLMS APDUs</td>
<td>HES</td>
<td>Wrapped with master key, invocation of global_key_transfer method by HES or the DC</td>
<td>HES • DC • Meter</td>
</tr>
<tr>
<td>Dedicated unicast encryption key (DUEK)</td>
<td>Dedicated encryption of unicast xDLMS APDUs</td>
<td></td>
<td>Transported as part of the xDLMS Initiate Request APDU, which is encrypted and authenticated using the AES-GCM-128 algorithm, the global unicast encryption key and the authentication key</td>
<td></td>
</tr>
</tbody>
</table>

Table 4 – DLMS-COSEM key types
Landis+Gyr generates master key and initial global keys (one unique set per meter)

Landis+Gyr sends a copy of the key information to Utility

Figure 2 – Overview of key management in Gridstream
The main steps in the Gridstream IDIS security key generation and management process are as follows:

1. The Landis+Gyr manufacturing facility uses a secure key manager software and secure key storage hardware to generate an initial unique key set for each meter consisting of a master key (a key encryption key) and initial global keys (GUK, GBEK, and GUEK).

   Note that the DLMS term “global” means valid over multiple communication associations, and not system wide.

2. The global keys are then encrypted using the master key and written to the meter.

3. The Landis+Gyr production system sends a copy of the key material to the utility AIM system using signed secure based on the Landis+Gyr public key infrastructure.

4. The utility AIM system stores and manages the key material using its local secure key manager and secure key storage hardware.

5. As each meter is registered to the AIM system as part of the installation process, AIM securely distributes the key material to appropriate data concentrator (using TLS over mobile communications) and initiates communication with the meter.

6. As part of the communication initialisation process, AIM renews the meter’s global keys and distributes them to the data concentrator and meter.

7. All communication from the head end system to the meter via the data collection system is authenticated and encrypted using the renewed meter-specific keys.

Figure 3 - Simplified process flow for Gridstream secure communications
Gridstream Solution Security Overview

Figure 5 – DLMS-COSEM message cryptography

Additional authenticated data (Associated data) contain:
- Authentication only: SC-A II AK II xDLMS APDU
- Encryption only: Null
- Authenticated encryption: SC-AE II AK

A = Additional authenticated data
AK = Authentication key
C = Ciphertext
EK = Encryption key
FC = Frame counter
IV = Initialization vector
P = Plaintext
SC = Security control (A, E, AE)
Sys-T = System title
T = Authentication tag