Landis+Gyr

# Gridstream® Connect Advanced Security

Enhanced end-to-end security from the meter to the head end and everywhere in between

landisgyr.com

# Overview

Today's connected world requires expertly designed smart grid processes and solutions to maintain data integrity from the grid edge to the back office. Events of recent years show that it is critical to have a strong plan around cybersecurity, whether it is to thwart cyberattacks, prevent unauthorized commands affecting service, or ensure the privacy of consumer data. With the advent of new threats and increasingly sophisticated attacks, it is vital that utilities continue to invest in a security solution that provides best-in-class end-to-end security, ensuring authentication, encryption, and integrity across the system, from devices to network to applications.

With Gridstream Connect, Landis+Gyr offers a highly flexible, interoperable, and adaptable platform capable of supporting an ever-increasing list of utility applications and connected devices. To help utilities safely realize the potential of this platform, Landis+Gyr provides an Advanced Security architecture that strengthens end-to-end protection against cyber-attacks.

# Gridstream Connect Advanced Security Benefits:

### Device-specific encryption keys limit risk of exposure from a single key compromise

Each device is provisioned with a unique encryption/decryption key to protect the privacy and integrity of data and commands sent to and from the device. With each endpoint having a unique key, information gained from a single endpoint compromise can't be used to further disrupt the network.

***Key Automation Minimizes Operational Impact***
*Key rotations are fully automated and can be scheduled in advance or triggered manually, minimizing administrative overhead.*

### Time-bound field tool authentication reduces threat of unauthorized access

Field tool access is protected by time-bound authentication certificates. This limited-time access ensures sessions do not remain open and prevents the subsequent use of field tools to make unauthorized changes.

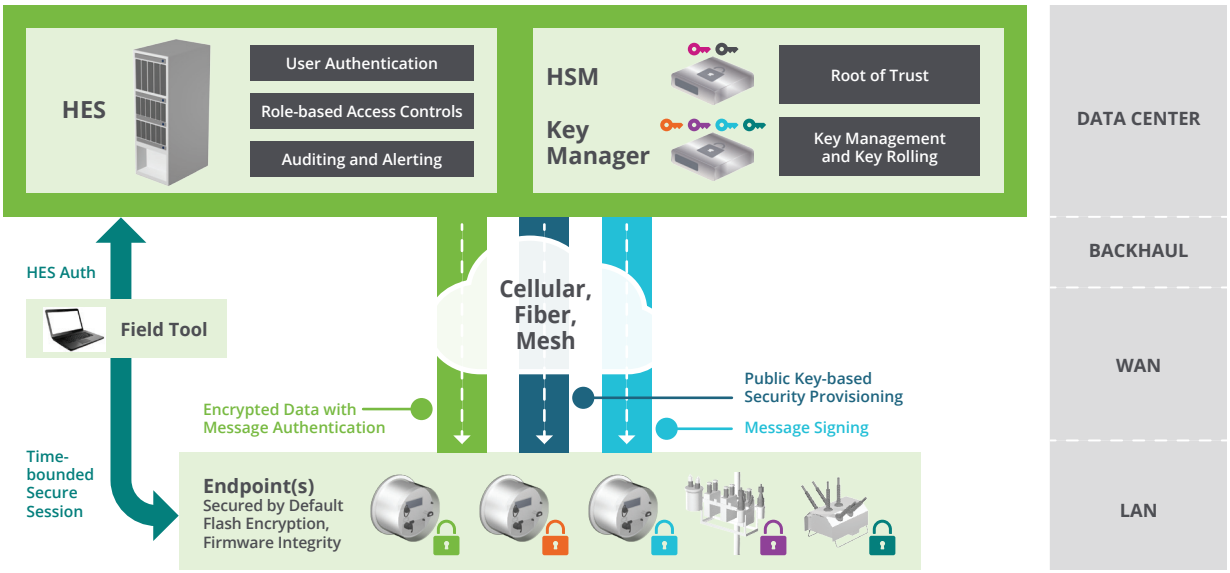
### Downstream message authentication protects against rogue commands

Endpoints verify messages using a digital signature to ensure commands originated from a trusted source, and adding proof-of-origin and receipt to each downstream message to prevent unauthorized commands, such as service disconnects and load control commands, from impacting operations.

### Hardware-based root-of-trust security provides maximum protection against theft

The cryptographic keys (root of trust) are inherently relied upon, and therefore must be secure by design and protected from theft. The most secure implementation of a root of trust is through hardware that makes it immune from malware or other cyberattacks. Landis+Gyr's Advanced Security uses Thales Hardware Security Modules (HSMs), which feature FIPS 140-2 and Common Criteria Level 4 certifications, providing strong protection for the root of trust.

## Interoperable Standards-based Security Architecture




*Landis+Gyr's Advanced Security architecture features device-specific encryption keys, time-bound field tool authentication, downstream message authentication, and hardware-based root of trust security.*

## Risk Considerations

Landis+Gyr's Advanced Security uniquely provides enhanced protections across five key areas of risk that utilities should seriously consider when evaluating security needs.

**Ensures trusted sources, reducing potential liability** arising from illicit access resulting in unauthorized disconnects, outages from network attacks, and breaches of consumer confidentiality.

**Prevents reputation damage** and erosion of consumer confidence by guarding against security breaches.

**Lowers potential compliance costs** associated with certification and remediation, by providing a NERC-CIP compliant solution with ongoing risk assessments and penetration tests to ensure security.

**Protects against revenue loss** – due to disruption of meter-to-cash processes, loss of usage or billing data integrity, or a widespread denial-of-service attack – by thwarting cyber-attacks at both the meter and broader network level.

**Ensures consumer privacy,** protecting against the growing threat of malicious third-party access to smart grid technology and associated real-time consumer data.

## Industry Standards and Requirements Methodology

Landis+Gyr has actively participated in the creation and evolution of many smart grid security standards and requirements, having been involved in standardization committees such as the NIST Cyber Security Working Group (CSWG), and having contributed to the NISTIR 7628 Guidelines for Smart Grid Security. These activities led to the creation of our standards-aligned Advanced Security offering and enabled us to develop a ground-floor perspective as to the various threats and vulnerabilities that utilities must be prepared to address when deploying a smart grid solution.

Based on this solid foundation, our Advanced Security solution follows open standards for encryption that have been validated across multiple industries that require world-class cybersecurity, including the financial services and military sectors. It utilizes proven, scalable, non-proprietary cryptographic software and key management appliances. Thales HSMs and FIPS-validated cryptographic libraries are used to generate an individual key for each device in the network, and each communication packet contains strong integrity mechanisms based on these keys.

## Gridstream Connect Advanced Security Specifications

| Purpose | Algorithm and Key Length | NIST / FIPS Specification |
|---|---|---|
| Encryption | AES256 Counter Mode | FIPS 197 |
| Integrity | Keyed SHA256 | FIPS 198-1 |
| Message Signing | ECDSA (Elliptical Curve Digital Signing Algorithm) 256-bit prime curve | ANSI X9.62:2005 – per FIPS 186-3 |
| Hashing | SHA2 | FIPS 180-3 |
| Random Generation | SHA256 HMAC DRBG | ANSI X9.82:2005 – per NIST 800-90 |
| ECC Key Generation | Prime filled 256 bit | NIST 186-3, D1.2.3 |

## Let's build a brighter future together.

To learn more about partnering with Landis+Gyr or Gridstream Connect, visit **landisgyr.com**, email us at **marketing@landisgyr.com**, or call us at **888-390-5733**.