

Gridstream Advanced Security



Defense-in-Depth Protection for the 21st Century Utility

Overview

Today's connected world requires expertly designed processes and solutions to maintain data integrity from the grid's edge to the back office. As a provider of advanced metering and smart grid solutions Landis+Gyr, in partnership with world-class security experts RSA and Safenet, offers Gridstream® Advanced Security. This solution provides additional defense-in-depth mechanisms that complement the robust security measures already fully integrated end-to-end within Gridstream Standard Security. Advanced Security further strengthens your smart grid solution by including additional root of trust, authentication and encryption security methods integrated into a utility's smart grid business processes and smart grid technology.

Gridstream Advanced Security guards against unauthorized access and continuously monitors devices throughout the Gridstream network and meter mesh. In addition, Gridstream Advanced Security extends to advanced Grid Management applications for signs of anomalous or nefarious activity. When unusual or improper activity occurs, Gridstream Advanced Security provides

necessary events and alarms enabling proper escalation of security incidents to protect your smart grid.

The Features of Gridstream Advanced Security include:

- **Device Specific Encryption Keys:**
Each device is provisioned with unique encryption keys used to protect the privacy and integrity of data and commands sent to and from the device.
- **Secure Command Broadcast:**
Commands broadcasted to groups of devices are also secured with unique segment keys that provide confidentiality, integrity and authentication for the command.
- **Downstream Message Authentication:**
Verify messages using a digital signature to ensure commands originated from a trusted source.
- **Bi-Directional Message Integrity:**
Validate 2-way network messages using additional key mechanisms and hashed message authentication code to ensure message integrity.

GRIDSTREAM ADVANCED SECURITY BENEFITS:

Why Landis+Gyr makes a difference.

- Protects utility shareholders from financial or reputation loss due to security breach of the Advanced Metering or Grid Management hardware, network or head-end system.
- Provides utilities with immediate, tangible security for data in transit for Gridstream Advanced Metering and Grid Management applications.
- Aligns with current regulatory technology standards and guidelines from NERC and NIST and evolves with changing requirements.
- Enables IT security teams to incorporate world-class encryption and authentication solutions into your smart grid without significant software customization expense.
- Allows customers to benefit from SafeNet and RSA's product enhancements to proactively address new cyber-attack risks.

Product Specifications: Gridstream Advanced Security

■ Mutual Authentication:

Authenticate upstream and downstream messages and check for integrity in the receiving device.

■ Field Tool Authentication:

Authenticate and secure communication between network devices and field tools.

■ Certified Root of Trust:

Store and maintain a Utility Signing Key within certified security appliances in a high-availability environment.

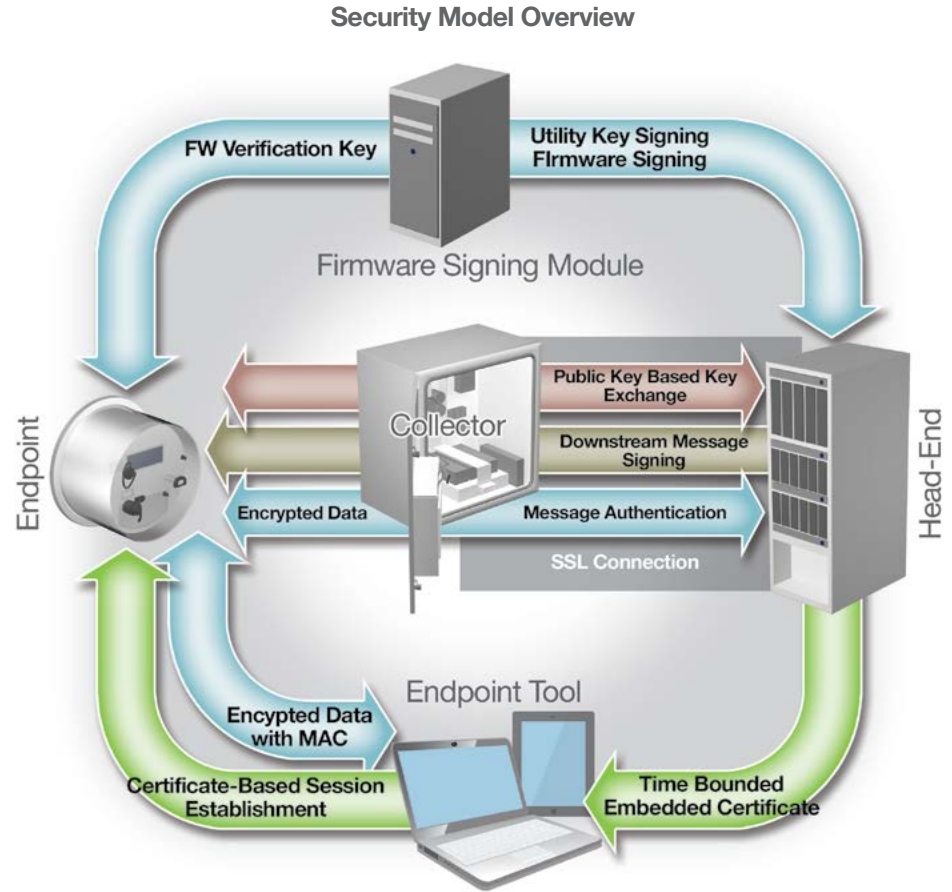
■ Vaulted Key Management:

Store and manage encryption keys with dedicated, high-availability key management appliances.

The elliptical curve cryptography found within Gridstream Advanced Security is offered by RSA and follows open standards for encryption that have been repeatedly validated across multiple industries that also require world-class cyber-security such as financial services, healthcare, retail as well as the Department of Defense among many other government agencies.

Further, Landis+Gyr aligns Gridstream Advanced Security with leading utility industry security regulatory standards and guidelines as driven by organizations such as NISTIR, NERC, IEEE, ANSI and ZigBee®.

Gridstream Advanced Security integrates components designed by security market leaders RSA and Safenet. The result is a defense-in-depth that aligns with the



security standards embraced by the utility industry. The solution is proven at-scale at multiple utilities requiring state-of-the-art authentication and encryption solutions for their smart grids.

To validate the Gridstream security solution set, security partner Lockheed Martin performed a risk assessment using NISTIR-7628 guidelines and the NERC-CIP standard. Further, on an ongoing basis, Landis+Gyr performs risk

assessments and penetration tests to identify vulnerable assets and implements mitigating security features for emerging security threats. World-class penetration testing partners include Lockheed Martin, IBM and Wurdtech among others on a rotating basis. These assessments provide perspective that Landis+Gyr directly incorporates into our Research and Development process to consistently improve smart grid security.

Specifications

Cryptography	FIPS 197 AES256, FIPS 180-3 SHA256, FIPS 186-3 ECDSA, FIPS 198-1 SHA256 HMAC – NSA Suite B
Key Vaulting	Oasis KMIP provides interoperability at key manager
Hardware Security Module	PKCS#11 provides interoperability at trust center
Key Provisioning	Public Key Interchange using Elliptical Curve
Firmware Integrity	NEMA SG-AMI-1 Meter Upgradeability Standard

Phone: 678.258.1500

FAX: 678.258.1550

landisgyr.com

4.23.14