Security by Design

WHITE PAPER

Trilliant helps leading utilities and energy retailers achieve their smart grid visions through the Trilliant Communications Platform, the only communications platform purpose-built for the energy industry that integrates disparate systems of systems into a unified whole. The Trilliant Platform is deployed with more than 200 utilities worldwide to enhance energy efficiency, improve grid reliability, lower operating costs, integrate renewable energy resources and electric vehicles, and empower consumers to better manage their energy consumption.

1100 Island Drive
Redwood City, CA 94065
t 650-204-5050
f 650-508-8096
www.trilliantinc.com

Security by design

Trilliant has built its Platform around security from the start. We put security and data privacy at the heart of our product, and have developed an ethos throughout our business of putting security first. Our communications platform includes security by design. Trilliant plays an active role in developing new security standards and models for smart energy, meaning that our products are always ahead of the game.

Driving forward standards

Trilliant plays an active role in multiple standards organizations and other bodies who are developing new security standards and models. We are pushing the agenda for smart energy security and data privacy forward, and ensuring that the Trilliant® Communications Platform is the strongest there is on the market. Trilliant sits on the management committee of the Smart Specifications Working Group (SSWG), who are responsible for designing and delivering security specifications for the UK smart metering rollout to the UK government. We are playing an active part of delivering the security infrastructure requirements for the British Smart Meter System, covering diverse areas including security for Home Area Networks, Wide Area Networks and Pre-Payment. As well as providing end-to-end security for our own Trilliant Platform, we work together with our partners; we are ensuring that the end-to-end security of any infrastructure containing Trilliant products and services is secure for use by GB plc.

Combining the best to make them stronger still

Trilliant has studied the different protocols that are available today for Smart Metering solutions and have tied them together into a strong, flexible and secure protocol for the WAN. We call this the Dual Protocol.

The Dual Protocol architecture is an open, interoperable WAN specification published by the SSWG, in conjunction with BEAMA that provides the smart metering system with improved meter data collection and with the ability to send communications to devices in the home. It also provides network management services that make the administration of the overall system more efficient. The communications architecture used by Trilliant, connects two separate networks together to form one system. The WAN connects the remote head end system to the communications hub located in a customer's home. The HAN is a network that establishes connections between in-home devices, including meters, with the communications hub acting as a gateway between the HAN and WAN.

The application presentation layer of the Dual Protocol employs the ZigBee GRIP standard. The application layer uses DLMS/COSEM, and ZigBee standards. The current version of the Dual Protocol specification's HAN support is based on open IEEE802.15.4 2.4 GHz DSSS radio and MAC, as well as ZigBee's network stack and Smart Energy Profile Specification version 1.1 R16 application layer with SSWG extensions. Other HAN networks can be accommodated by extensions to the Dual Protocol's attributes and commands.

In the reference architecture, the Communications Hub establishes secure HAN links between:

- The Gas meter and the hub – for communicating gas data and meter management data during scheduled periods when the battery powered Gas meter turns on its radio
- The Electric meter and the hub – for communicating Electric meter data and for managing the Electric meter
- The in-home display and the hub – For communicating Gas meter data and Unity information to the customer and for managing the in-home display.
- The in-home display and the Electric meter. – For communicating Electric meter information directly to the customer.

The Dual Protocol WAN communication architecture is designed to use a selection of established communication protocol standards at various layers. The current selection has a GSM/GPRS/SMS physical and media access layer, a IPv4 network layer and both a UDP/Digital envelope and a TCP/TLS transport layer. The Dual Protocol specification is designed to be extended to support other physical, media access and network mechanisms. The design allows the specification to optimize the WAN performance and head end system's resources to take into account characteristics of the underlying network. The Dual Protocol specification provides a set of technologies that are efficient for the head end system and hub and efficient for the WAN network. They supply WAN services that include:

- Reliable delivery
- Security
  - Mutual device authentication
  - Data integrity
  - Data privacy
  - Data operation authorization
  - Key management
  - End-to-end security

- Device commissioning and decommissioning
- Coordinated multiple firmware Image transfers for multiple devices on the HAN and the hub.
- Alarm and event configuration and reporting
- Meter reports
- Clock management
- Head end system to HAN device communication

The Dual Protocol optimizes the meter reporting and time synchronization operations that account for the bulk of a smart metering system's actions.

There are a number of benefits to a Dual Protocol over using a single, stand-alone metering protocol such as DLMS/COSEM.

- The Dual Protocol does not require translation in the communications hub from WAN to HAN, whereas a single protocol does, which blocks the ability to support end-to-end security. This creates a weak point in the end-to-end security model for operations such as credit and prepayment delivery.
- Dual Protocol supports a reliable, secure session-less reporting of meter reads and alarms, leading to improved WAN performance and head end system efficiency.
- By removing protocol translation, translation errors and complexity are avoided.
- Also, by removing translation, translation updates in the firmware are no longer needed, meaning that the overall system efficiency is improved.
- The Dual Protocol specification uses certificate based WAN key management which is more efficient and secure than key wrapping management systems such as DLMS/COSEM.
- The non-translated, native transport of ZigBee commands and data is more flexible than a system that translates between DLMS/COSEM and ZigBee. As more consumer devices need to attach to the HAN, the dual protocol will be able to talk to, and manage them, even if they are nothing to do with the metering infrastructure in the home.

End-to-End Security

One of the most important security considerations in a smart meter infrastructure is that of the end-to-end data security. Thus, ensuring that there are no weak points, no uncontrolled remote devices, no area uncovered by security policy and provision of trust throughout the network. The end to end system includes the energy meters, in-home displays and other equipment on the HAN, the Communications Hub, the Communications Networks and the head end system, as well as the processes and procedures that surround the installation, operation and support of the system. The simplest way to ensure end-to-end security is through deploying the Trilliant Platform in its entirety, as we have built and linked security by design throughout the entire architecture. However, as important as the technical security elements, is the design and deployment of processes and management surrounding the operation of the system. There are a number of considerations that Trilliant recommends evaluating when deploying an end-to-end smart metering system to ensure smooth management and strong process deployment. The selection of a proper system design, devices and security procedures will ensure security from every angle and from every person with a system relationship.

- Secure cipher material configuration
- Key distribution
- Private and public key administration
- Private key locations and storage in devices
- Centrally administered secure key storage in the head-end system
- Key usage policies and procedures to ensure key integrity
- Defense in depth policies and procedure that provide robust security and limit the consequences of a security failure
- Limited trust policy of the system
- Detecting and reporting attacks
- Measures that can be taken to counteract an attack
- Data privacy policies and their coverage
- Data integrity policies and their coverage
- Command authentication policies and their coverage
- Denial-of-service and replay attack policies and their coverage
- Key rotation policies and methods
- Access authorization policies and their coverage
- Security tests the licensee plans on running to test the effectiveness of the system before deployment and to monitor it after deployment

Third party access devices

A key part of the smart meter system, and one that can impact its end-to-end security is the addition of third party HAN access devices in the home. These could be energy information display devices, home appliances or any number of additional in-home products needing access to the metering system for energy or other data. The attachment of these devices to the HAN needs to be carefully controlled so as to maintain end-to-end security. Without verified attachment and access to defined data sets, weaknesses could easily be introduced. There are a few ways of pairing a third party device to the network.

- Key-code Entry: The home-owner is issued with a unique key to their smart metering system, which they can type into a device to pair to the network, in much the same way as a wi-fi passcode works today.

- Remote pairing: the key-codes are held remotely for a wide range of third party devices, and a message from the home-owner to the system provider is needed to remotely pair the HAN and device, in much the same way as a SIM card is activated on a cellular network.
- Physical attachment: The third party device can by physically attached to the HAN trust center, by USB cable or suchlike, to allow authentication to be completed.

Each of these are valid ways of connecting and authenticating devices on the HAN, each with their own positives and negatives. The key thing to remember is that even with the most secure access mechanism, if the access device is not certified to access and utilize the smart metering system in the recommended way, then end-to-end security can still be breached. This can be avoided by partitioning the data and system into separate logical sets. Separate access for third party devices, and separate access for trusted energy operators can be achieved simply, so long as the definitions and class groups are defined before deployment begins.

Security assessments and audits

The best way of managing security risks within the smart meter infrastructure is to take a holistic approach and ensure that all risks are identified, assessed and subsequently tackled. This can be achieved through carrying out a thorough risk assessment. Ideally, a risk assessment should be carried out at regular intervals through the infrastructures lifespan, not just at the beginning of deployment, as the nature of security threats changes over time, and what is not a threat today may become so in the future. By basing a security assessment against an appropriate security standard a framework for identifying and categorizing risk can be established. Trilliant recommends a six-month audit be performed initially; if the system passes the audit, it will then be performed on an annual basis.

The security assessment should look at both security policies and procedures using the established process as well the consideration of the specific points important to the individual deployment. Any periodic security audit should focus on determining how well the management of the system is working and the overall effectiveness of the system in maintaining security. As such the audit should focus on three main topics:

1. Compliance to the policies implemented, including:
- A review of the management records
- A review of administration failures with an analysis of the cause and the remedial steps taken to correct the failure

2. A review of all security breaches
- Their cause, their impact on the system
- The immediate steps taken to mitigate the attack
- The effectiveness of the mitigation
- The recommended remedial actions, if any, to improve security
- Open security issues and actions

3. A review of the security tests that have been run and their results. These tests can include such things as the introduction of unauthorized devices and the generation of unauthorized commands.

Once the risks are identified and understood appropriate safeguards can be put in place. Security deployment and management should be seen as a continually evolving environment requiring regular management and review. By taking this approach, and by also running concurrently with other policies such as disaster recover, risk can be managed and breaches resolved without serious consequential damage to data and reputation.

Data Privacy

By implementing a robust security framework, data privacy can also be assured. Ironically, the best approach to building confidence in Data Privacy policy is to be as open about it as possible. Data Privacy is achieved through strong security tools and procedures and not through obscurity. The best way of avoiding objections to data privacy from the smart meter community is to demonstrate to them how seriously security and data privacy are taken.

Data Privacy is something that affects the user of the system, not the manager of the system, and as such any data privacy policy must be user-centric. By designing security in a methodical manner, and publishing the steps taken to ensure data privacy, the user has no surprises hidden around the corner on how their personal data is managed and examined. In addition to this, each authenticated device on the network must adhere to a strict set of rules, ensuring that access to personal data via third party devices cannot be achieved, without the relevant permissions. A user-centric data privacy policy must:

- Put the user at the heart of the data security design
- Offer simple options and choices for how data is handled, allowing the user to feel in control
- Not compromise on data security for the sake of consumer engagement
- Publicize the security steps, both physical and virtual, being taken to protect user data
- Take user's data privacy concerns seriously and implement changes that will make them more likely to engage with the service.
- Ensure that any third party organizations that may handle the user data adhere to the same security models and methodology as the parent company.