Trilliant Communication Solution: Security by Design

White Paper by Trilliant Holdings, Inc.

Trilliant Holdings, Inc.
1100 Island Drive
Redwood City, California 94065

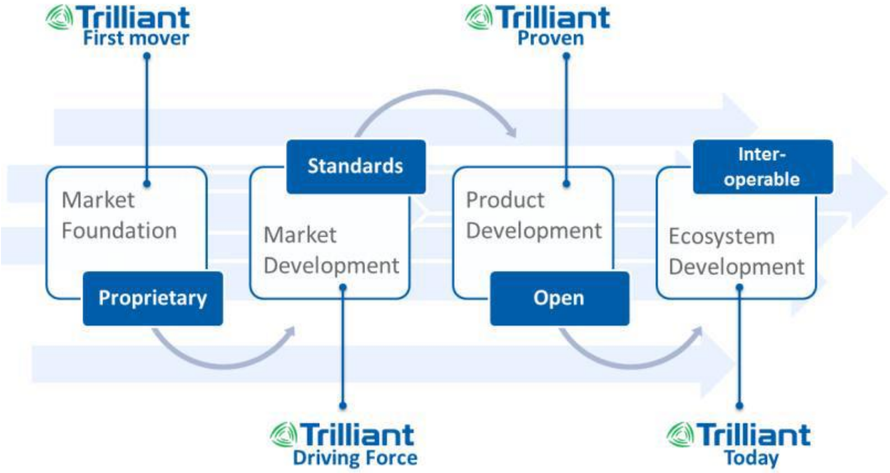
Table of Contents

Security by Design

Trilliant has built its Platform around security from the start. We put security and data privacy at the heart of our solution, 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 Industry Standards

Trilliant plays an active role in multiple standards organizations and other bodies that 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 experts are playing a significant part in the work of the management committee of the Smart Specifications Working Group (SSWG), which is 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 for the UK Smart Meters rollout, which covers 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 to ensure that the end-to-end security of any infrastructure containing Trilliant products and services is secure.



Combining the Best to Make Them Stronger Still

Trilliant has studied different protocols that are available 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, which provides the smart metering system with improved meter data collection and with the ability to send messages 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 first part of the system is the WAN, which connects the remote head end system to the communications hub located in a consumer’s home. The HAN is the second part of the system, which is a network that establishes connections between in-home devices (including meters) with the communications hub (that acts as a gateway between the HAN and WAN).

The application layer protocol uses DLMS/COSEM with UK SSWG extensions v2.11, and ZigBee Cluster Library with ZigBee Smart Energy Profile protocol version 1.1b R18 with UK SSWG extensions v2.3.1. The Dual Protocol combines GRIP over the TCP/IP TLS or Digital Envelopes over UDP protocol stacks to deliver either DLMS or ZigBee messages. The current version of the HAN protocol is based on the open IEEE 802.15.4 2.4GHz DSSS radio and MAC, as well as ZigBee’s network stack and cluster library.
Stub APS presents Trilliant invention we added to the ZigBee standard. This part adds additional security to the InterPAN communication.
See the illustration of the Trilliant Communication Solution Stack (Figure 1) for more details.

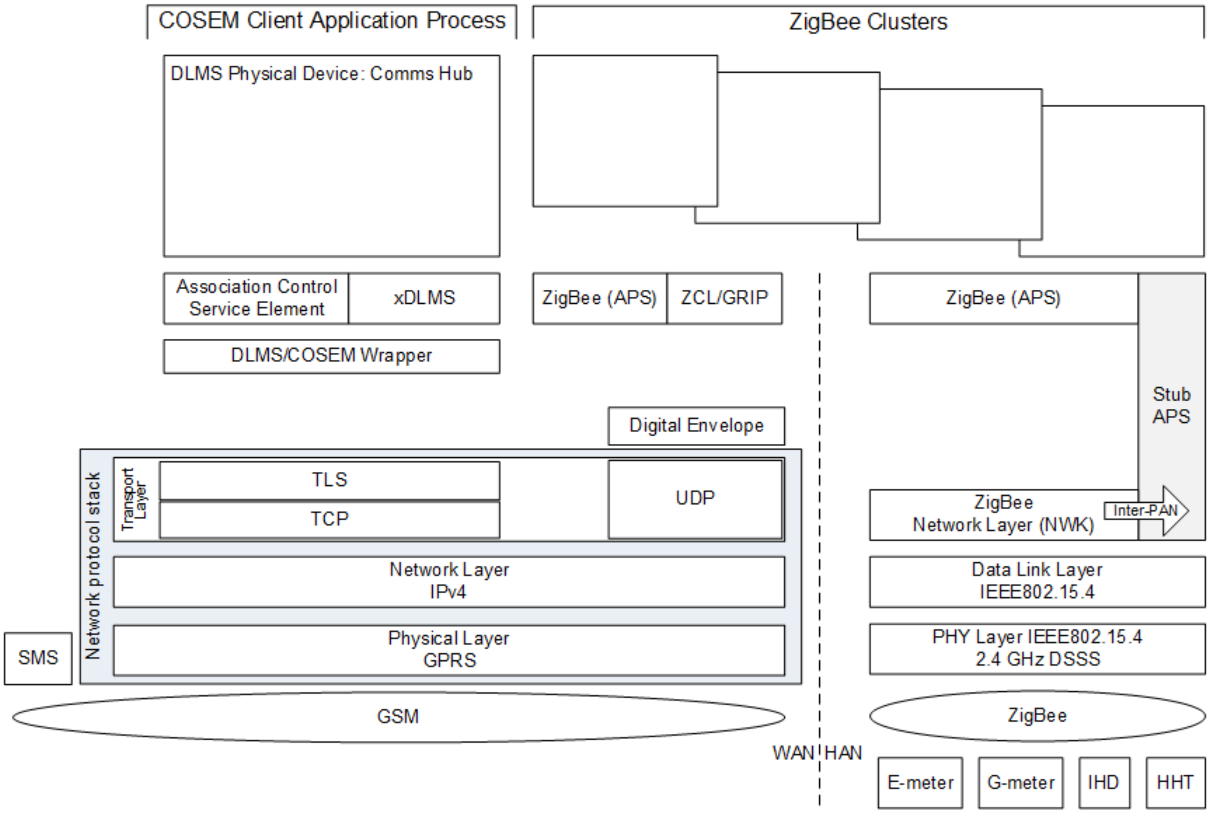
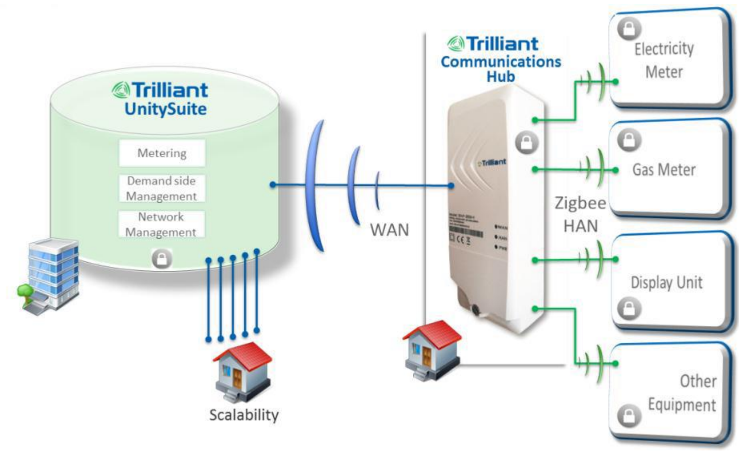


Figure 1. Trilliant Communication Solution Stack

The Dual Protocol 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 data link layer, an 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, data link, 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 data delivery
- Security
  - Head End system controlled device authentication
  - Mutual device authentication
  - Cryptographic data integrity
  - Data privacy
  - Key management
  - End-to-end security
- Secure device commissioning and decommissioning
- Coordinated multiple firmware image transfers for multiple devices on the HAN (including 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. 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 prepayment vends delivery and similar.
- 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 (for example when adding new features to the meters). This improves the overall system efficiency.
- The Dual Protocol specification uses certificate-based WAN key management, which is more efficient and secure than key wrapping management systems such as those that are used by many DLMS/COSEM meters.
- The non-translated, native transport of ZigBee commands and data is more flexible than a system that translates between DLMS/COSEM and ZigBee.

End-to-End Security

One of the most important security considerations in a smart meter infrastructure is that of end-to-end data security. This ensures that there are no weak points, no uncontrolled remote devices, and 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 installing, operating, and supporting 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 system operation. 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. Selecting a proper system design, devices, and security procedures ensures 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 procedures that provide robust security and limit the consequences of a security failure
- Limited trust system policy
- 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

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 addressed. This can be achieved through carrying out a thorough risk assessment. Ideally, a risk assessment should be carried out at regular intervals over the infrastructure's 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 initially audit; if the system passes the audit, it should then be performed on an annual basis.

The security assessment should look at both security policies and procedures using the established process as well as consider the specific points important to the individual deployment. Any periodic security audit should focus on determining how well system management 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 and 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 recovery), risk can be managed and breaches can be resolved without serious consequential damage to data and reputation.

About Trilliant

Leading utilities and energy retailers are under increasing pressure to deal with supply limitations, environmental mandates, intermittent renewables, and changing demand with the growing popularity of plug-in electric vehicles, distributed generation, and consumers’ desire to use energy more efficiently. They are also faced with the daunting technical complexities of unifying disparate information from the many systems resulting from the evolving landscape of systems, energy devices, and applications.

Trilliant helps savvy utilities and energy retailers achieve their smart grid visions through the Trilliant Smart Grid Platform, the only purpose-built communications platform that integrates these disparate systems of systems into a unified whole. Only by using a smart grid platform purpose-built for the energy industry can utilities and energy retailers unify the information from their disparate systems of systems to achieve their smart grid visions and enjoy the benefits of having done so.

Trilliant understands that a particular utility’s smart grid business needs may be different from those of other leading utilities and energy retailers. For example, some utilities may seek to satisfy regulatory mandates while also increasing reliability and improving operational efficiencies. Others may seek to empower consumers to use energy better and offer differentiated services. Still others may seek to integrate more renewables, distributed energy resources (such as electric vehicles, storage, and solar panels), or be able to reduce non-technical losses. Whatever a utility’s smart grid business needs are, the Trilliant Communications Platform offers utilities and energy retailers the widest range of options and flexibility -- tailored to the business’ particular goals, regulatory model, and service territory -- to solve their unique smart grid business needs, today and tomorrow.

In the UK, Trilliant is currently deploying its Smart metering (SMETS1) communication solution, which includes the first generally available Communication Hub designed to support the Foundation stage of smart meter deployment. Trilliant’s solution was the first to address issues of multi-supplier and multi-device interoperability.

The Trilliant Communications Hub is a corner stone of an open and interoperable communications platform that securely connects to the Trilliant UnitySuite™ Head-End Software using secure private GPRS networks. The Communications Hub creates a secure communications link to electricity meters, gas meters, and in-home displays, with a potential to connect to other in-home energy management products using DLMS/COSEM and ZigBee Smart Energy Profile communications standards.