QUANTIFY
truly intelligent buildings

Security Overview

White Paper

Version 1.0

SECURITY OVERVIEW

PROBLEM STATEMENT

With many technologies, including the Internet of Things (IoT), often security is an afterthought. This failure to recognise and invest in security leads to disconnected product sets creating a complex chain of devices and software. The weakest link in this chain may therefore be manipulated by malicious actors to compromise the entire chain.

Quantify Technology's vision is to produce the world's first Truly Intelligent Building Platform. Truly Intelligent is not merely repackaging lighting or building automation, but fundamentally transforming the way buildings interact with their tenants to deliver improved lifestyle, safety and additional business value.

Only by baking in security as a critical component in all parts of product design, and by viewing them as essential components of the chain or system, can the system protect itself from the ever-increasing attacks by malicious actors. This system should understand that parts of the system, whether hardware, software or process, may come from many different sources and can dynamically change. However, regardless of the source, the system components or the age of the system, or the use of the system, the system should always support the principle of "baked in" in security.

This document describes the various methodologies that can be used to secure the qDevice (Hardware), Mobile Applications and the Quantify Cloud. The material is intended to be read by those, internal or external, with a moderate level of security knowledge.

QUANTIFY TECHNOLOGY SYSTEM OVERVIEW

Shown in figure 1 is a high-level overview of the Quantify Technology platform. The platform consists of many key elements, each with security requirements; each element underpinning a holistic security approach.

At the top of the diagram is the Quantify Cloud, Quantify Technology's cloud service that provides registration, enablement, activation, configuration and reporting path for the Quantify Technology qDevices, Quantify Cloud is designed to interact with other 3rd Party value-added applications and services via a published API. qDevices connect to the Quantify Cloud using standards-based protocols, the internet and wireless technologies.

Mobile applications are also supported, permitting secure, intuitive interaction with qDevices. These applications provide secure direct access to qDevices to action configurations. Additionally, the mobile devices allow users to change settings, provide software updates to qDevices and synchronise with the central Quantify Cloud service.

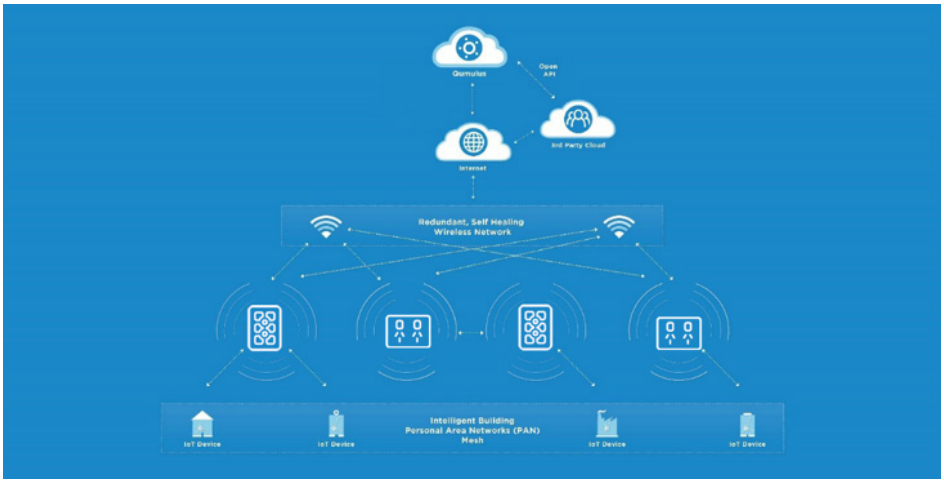

Figure 1: **High-Level System Overview**

Figure 2 shows a logical diagram of the main components of the Quantify Technology Platform. Devices are the physical components of the system that interact directly with the user environment. These include qDevices, optional Quantify Technology gateways, mobile devices, 3rd Party gateways and other 3rd party IoT devices. These devices are interconnected using industry stand networks and protocols to the services, including the Quantify Cloud and 3rd party applications. Application Programming Interfaces (APIs) are also deployed to allow easy and secure integration between different components of the system. Together these components of the system connect to deliver specific business objectives such as home automation and energy management.

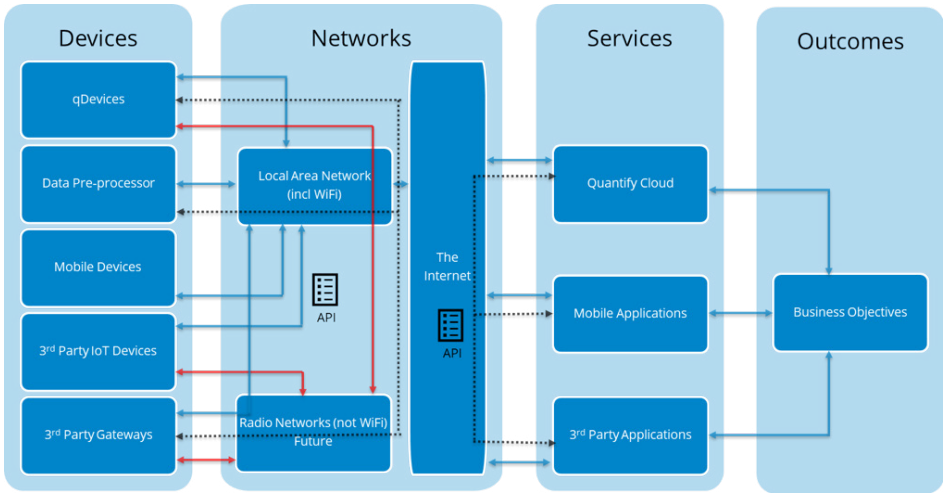

Figure 2: **Logical System Overview**

QUANTIFY TECHNOLOGY SECURITY PRINCIPLES

Based on the industry framework AAA, Quantify Technology's security principals are:

- **Authentication – Identify and validate**
  Individual users, devices (qDevices and 3rd Party), services (mobile applications and cloud applications) must securely identify themselves to the system and each other. The system may revoke these identities, and this allows the removal of a component of the system. Devices are identified via a secure signed certificate, while applications are identified via OAuth. These security measures allow the revocation of any device or application from interacting with the system.

- **Authorisation – determine if specific tasks are permitted (CY 2020)**
  Individual authenticated components of the system are given privileges and capabilities to interact with other parts of the system. For example, a 3rd party application may only be available to specific paying users of that application; particular users may be able to configure qDevices, but some users may be able to obtain reporting from qDevices; some applications may onboard 3rd Party IoT devices, while some applications may not.

- **Accounting – measure the resources consumed (CY 2020)**
  The system logs all successful and unsuccessful actions of authentication and authorisation. Logging provides the ability to determine if malicious actors are present and adjust security posture appropriately. Accounting also provides a capability for 3rd party application or device providers to monetise access to the Quantify Technology platform.

Increasingly the AAA framework is supporting a new A, AI or Artificial Intelligence. AI can be used to analyse the data produces through AAA to deliver actionable Intelligence with regards to possible breaches. Quantify Technology's architecture is designed to collate these statistics and supply these statistics to AI.

Figure 3 shows a sample security flow for a service communicating with a device. The reverse flow is also supported, that is when a device communicates back to services.

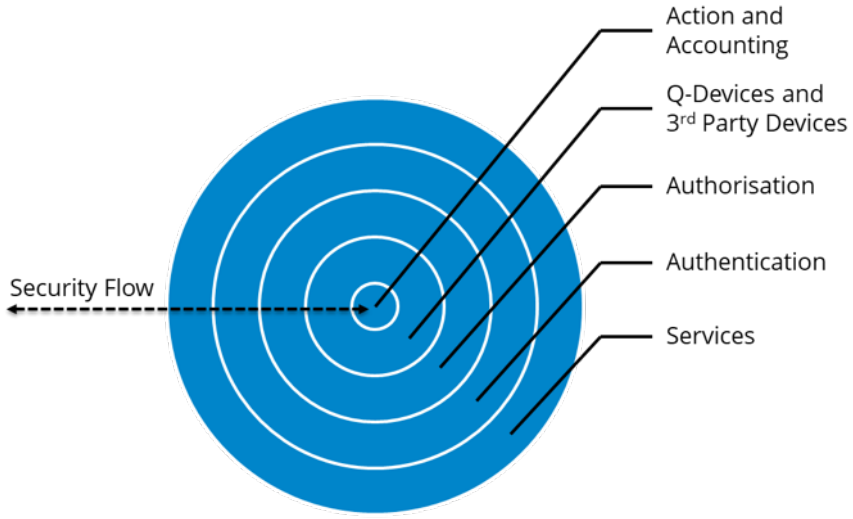

Figure 3: **Security Flow to/from a Service to a device**

qDevices have a manufacturers certificate installed at production. This certificate allows the qDevice to pass the first stage of AAA, authentication, this process is performed using Public Key Infrastructure (PKI) and X.509. These certificates and keys allow a qDevice to participate in a "tree of trust" with the MQTT (messaging system) of the Quantify Cloud. Through this trust relationship, the Quantify Cloud can first test a qDevices legitimacy to participate with the system.

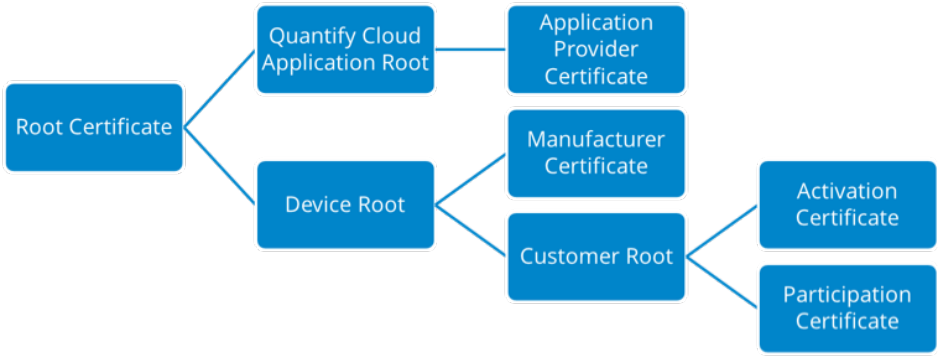

Figure 4: **Example security model**

PKI uses a public and private key pair. Decryption of a message encrypted by the public component is only decryptable by the private competent and vice versa - it is a one-way process. Similarly, digital signing tests to see if a certificate is legitimate by using a one-way hash. Any modification of the certificate results in a different hash, rendering the certificate invalid. Certificates always contain the public key, but can also contain some other useful information such as dates the certificate is valid or whether certain actions are permitted or determining device ownership – Authorisation.

At a rudimentary level, using PKI principles, a public certificate or message can be signed by an issuer's private key. A recipient can then use that issuer's public key to test the validity of the certificate or message. In the future, a mobile application attempting to connect to a qDevice could first test to see if it is authorised to talk to that qDevice. Figure 4, shows a high-level example of possible use of this tree of trust for the system. Using certificates, we can build the implicit trust of components within the system. Note, that certificates can also contain expiry information, this creates an ability to request that critical components periodically reconnect with the Quantify Cloud for update and validation purposes.

Note that the entire certificate chain may require validation all the way back to the original Certificate Authority root certificate (such as Verisign) shown in Figure 5. Note that in the case of a qDevices, the qDevice verify back to the AWS IoT intermediate CA certificate.

Where communication across an open network is required to remain confidential, components use the industry standard Transport Layer Security (TLS). TLS allows these components, with the aid of X.509 certificates, to negotiate a onetime session-based encryption key for secure communication. As this key is random and changes every time these components communicate, it allows those conversations to remain confidential.

On an open network, with a risk of messages in open text, the system employs digital signing techniques. These techniques use PKI certificates or previously securely shared secrets (using TLS), to sign a message with a unique hash. Hashes are one-way cryptographic functions, that is, having the hash does not allow you to determine the secret or certificate used. The validity of the message is determined by the recipient, by examining the hash and computationally recalculating and comparing that hash using the previously shared secret. It is essential that the system periodically rolls said secrets using a methodology such as TLS in figure 6, and that any messages detected with incorrect details are also Accounted for, as those may be indicators of a malicious actor or incorrectly configured devices.

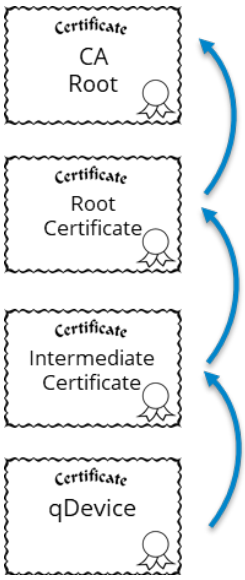

Figure 5: **The formation of trust back to the Root Certificate**

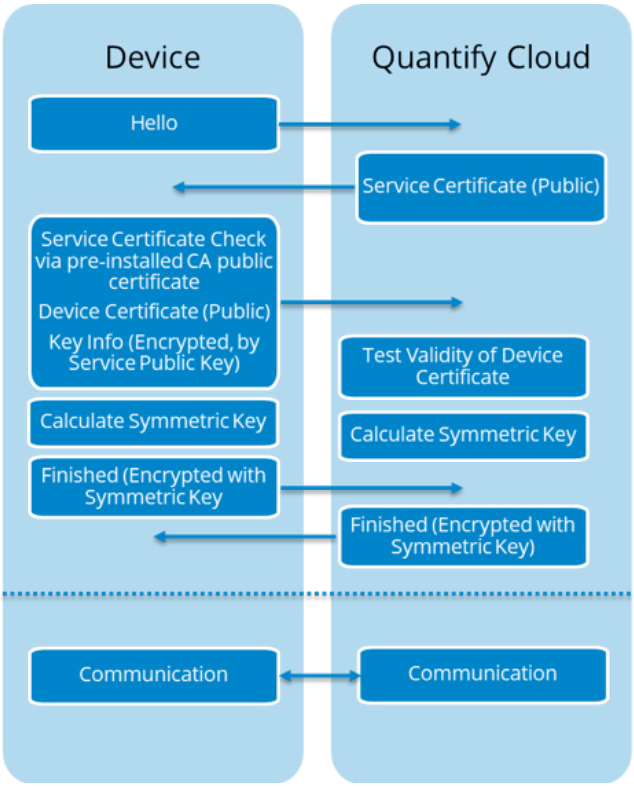

Figure 6: **Example Device to Service Secure Communication**

Where different components of the system manufactured by different parties need to communicate, secure APIs are defined. These APIs act as secure, controlled and measurable doorways between these components of the system and allow multiple parties to collaborate without detailed knowledge of the internal workings of any component of the system.

APIs are authorised via a valid username and password. However, to hide the users password from 3rd party applications OAuth is used to generate an application token. When a user authorises an application, the user enters their username and password and the OAuth service then creates a token for that service. Tokens are then used for the purpose of authentication, removing the necessity for the user to login each time.

The system protects itself against a replay attack, that is someone obtaining access to a legitimate message and resending that message for malicious purposes. As messages contain timestamps, and the physical qDevice has access to a real-time clock, they can determine if a message is outside a valid timeframe. Additionally, on the transmission of a message, the message contains a unique session identifier. If a malicious actor modifies the timestamp or session identifier, the signature will not match, and that message will be deemed invalid.

Future implementations may support 802.1x, to ensure that qDevices belong to a customer and are permitted to connect to the customers' network. This standard, supported by enterprises, allows the challenging of qDevices by an organisations RADIUS identity server. Once the challenge is successful, the qDevice can then legitimately connect to the customers' network, as shown in figure 9.

The final “A” in AAA stands for Accounting. It is essential to not only account for legitimate messages and actions but also log invalid ones. If too many invalid messages or actions occur, the devices can collate this information to perform analysis via Quantify Cloud. Quantify Cloud can then instruct devices in the field to change behaviour, such as shun a connection, rotate security keys or actively inform the user of possible attacks.

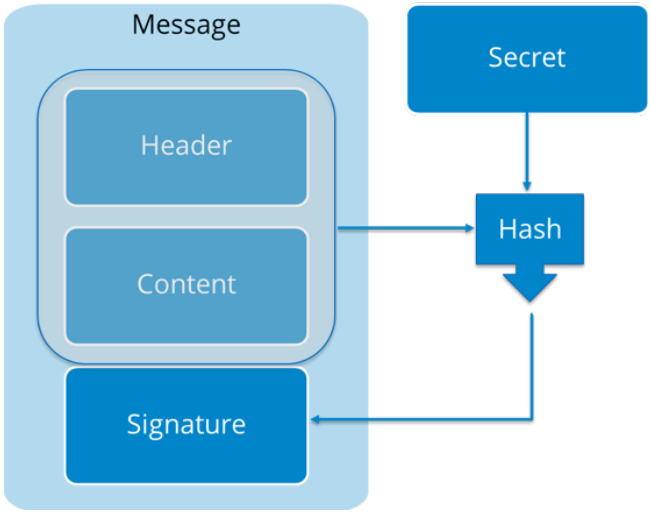

Figure 7: **Example Digital Signing Technique**

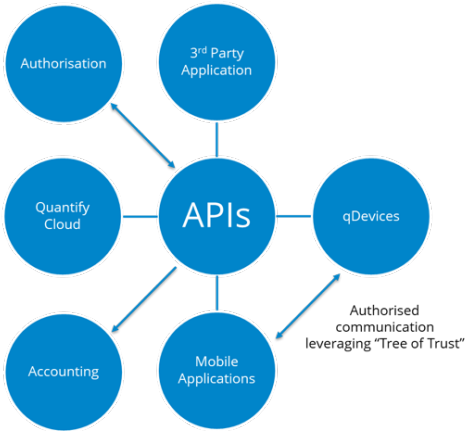

Figure 8: **Example of API Structure**

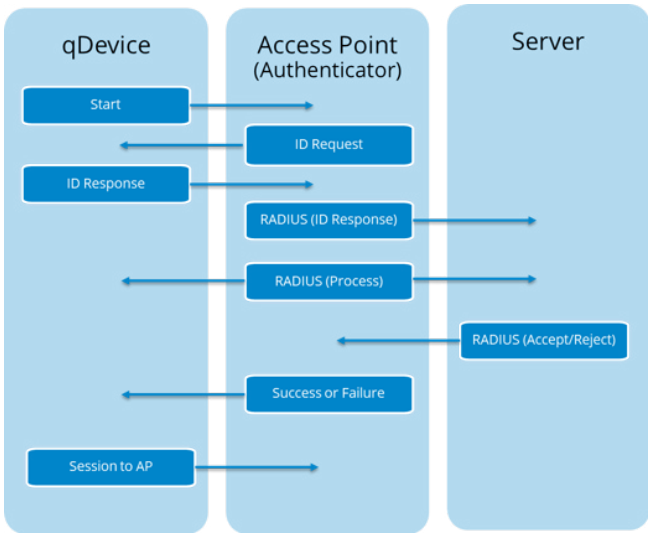

Figure 9: **Overview of 802.1x Process**

The system utilises standard network security protocols, for example, WiFi WPA2 encryption. It is highly recommended to activate these standards on a qDevice network. These protocols deliver security by obscurity layer, as passwords are effectively in the control of the end user. Unlike most other IoT widgets, the system does not inherently rely on these techniques but uses their availability to enhance security.

As added protection, the system allows a user to provide encrypted credentials to an installer, via the installer App. In this case the installer never sees the actual details of those credentials and only extracts those credentials into device memory when the device wishes to connect to the WiFi network. This methodology reduces the number of people that require access to the actual credentials, further reducing the risk of credential leakage.

The AC Controller is electrically wired into the wall and sealed. To gain access to this device and the secured data requires an obvious amount of physical effort. The removal of such a device can be detected by Quantify Cloud or by physical security personnel, alerting the customer to a possible breach. Any possible breach can result in WiFi credential changes, PKI key changes and secret changes, effectively rendering the obtained information useless. The Quantify Cloud platform can identify this rogue device being reconnected to any network and alert systems to act appropriately.

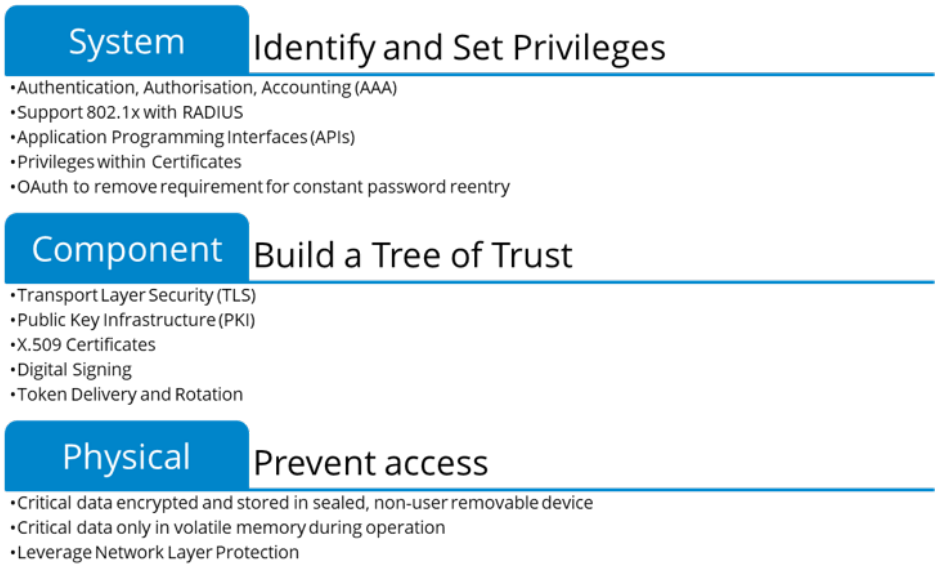

Figure 10: **Summary of Security Principals**

Figure 10 summarises the Key Security Principals described in this document. By viewing the Quantify Technology solution as a holistic platform and not just a series of disconnected components in a chain, the system becomes stronger. Each link in the chain is supported by each other link, creating a more robust and ultimately secure, scalable platform.

Each component should only trust another component once they have authenticated each other. Authentication may be via username/passwords, certificate tree of trust or by signing via a mutual secret, preventing a malicious attacker from illicitly joining or impersonating the system.

Once authenticated, components must then be authorised to perform specific actions. Testing authorisation of actions ensures that compromised components cannot perform escalation of privileges to disrupt the entire system. This model is known as the principle of least privilege. At all times all actions within components of the system, whether legitimate or illegitimate, are logged. Logs are then analysed to determine if the system is exhibiting signs of malicious attack or compromise.

+61 (0)8 6254 0200

sales@quantifytechnology.com

Suite 2, 6 Brodie-Hall Drive, Bentley, Western Australia 6102

www.quantifytechnology.com