Qwilt Open Caching Service Security Principles

v.2.6.0
15 Feb 2022
22-298260-000

Table of Contents

1. Introduction

1.1. Purpose

This document describes the Qwilt Open Caching Security principles, processes and policies, enabling Qwilt to provide a secure solution to its customers and partners.

1.2. Contacts

Support – Email: support@qwilt.com
US Toll-Free Number: 1-888-684-5785
Sales – Email: sales@qwilt.com

1.3. References

Table 1 lists documents and other references that are essential for understanding the topic of this document.

Table 1 References

No.	Designation	Title
2.	CheckPoint Cloud Guard	https://www.checkpoint.com/cloudguard/
3.	Center of Internet Security	https://www.cisecurity.org/
4.	Common Vulnerability Scoring System	https://www.first.org/cvss/specification-document
5.	ISO 27001	http://www.27000.org/iso-27001.htm
6.	ISO 27017	https://www.iso.org/standard/43757.html
7.	Tenable Nessus	https://www.tenable.com/products/nessus/nessus-professional

1.4. Abbreviations and Acronyms

Table 2 provides a glossary of acronyms and terms used in this document.

Table 2 Terminology

Term	Definition
API	Application Programmatic Interface
AWS	Amazon Web Services
ATP	Acceptance Test Plan
BW	Bandwidth
CDN	Content Delivery Network
CP	Content Provider
HTTP/S	Hypertext Transport Protocol / Secure
HW	Hardware
ISP	Internet Service Provider
ISO	International Organization for Standardization
Qwilt Cloud	Open Cache Controller
OCN	Open Caching Node
OCS	Open Cache System
PT	Penetration Test
QC	Qwilt Cloud Service Suite
QN	Qwilt Node
SVA	Streaming Video Alliance
SW	Software
VOD	Video on Demand

2. Background

2.1. Qwilt Open Edge Cloud

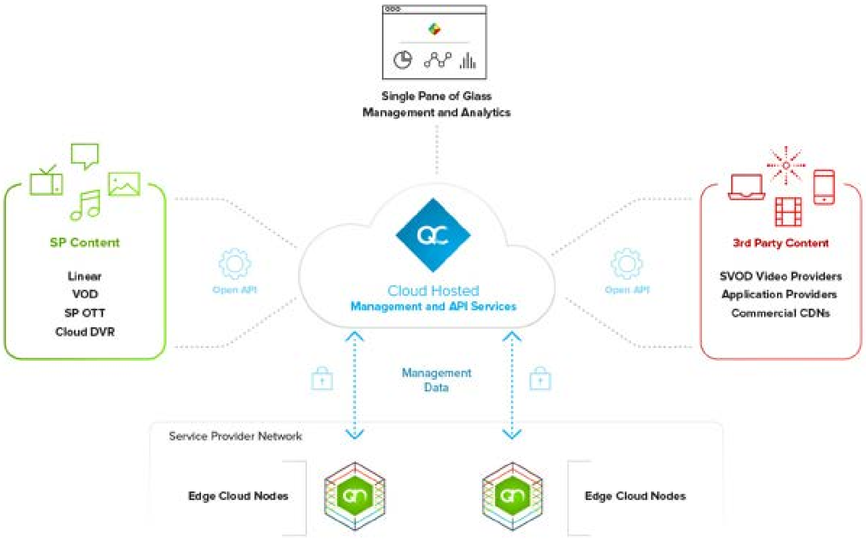


Figure 1 - Qwilt Open Edge Cloud

Today’s applications are increasingly dependent on low latency and high bandwidth input, output and processing. New applications such as virtual and augmented reality as well as 4K and higher quality videos are increasingly being delivered over fixed and mobile networks. Internet of Things (IoT) sensors and autonomous vehicles are examples of applications that depend upon localized processing at the very edge of the network to facilitate low latency response to inputs. Due to these trends, fixed and mobile Internet Service Providers (ISP) are increasingly deploying their processing capabilities at the edge of their networks, typically by building new hardware platforms based upon common off-the-shelf (COTS) compute and storage and by supplying virtualized software infrastructure for running 3rd party as well as their own services.

Qwilt has developed the Open Edge Cloud platform to facilitate the deployment of content caching at the edge of the ISP network, at the closest possible location to the users of these services. Qwilt's Open Edge Cloud architecture leverages cloud management and connectivity, open APIs and powerful small-form-factor software nodes to deliver true edge content delivery capabilities built for tomorrow's application and content delivery demands. Qwilt builds the software that unlocks the potential of this ISP edge by deploying hundreds/thousands of software nodes at any point in an ISP network, from the core to the metro, and even to access networks. Qwilt software is simple to operate as it is 100% cloud-managed. Qwilt software packs maximum performance into a small form factor that is elastic and resilient at the same time.

The Qwilt Open Edge Cloud connects applications to their edge services. Not only does the Qwilt Open Edge Cloud enable ISPs to manage all content delivery services from a single pane of glass, but it also supports standardized Open Caching interfaces to enable the common delivery of managed partner content at the edge of their network.

Qwilt is a founding member of the Streaming Video Alliance (SVA) and is the leader of the Open Cache working group. SVA has developed an ecosystem where CDNs can work together with Internet Service Providers (ISP) to cost-effectively deliver content at the very edge of the ISP network, regionally maximizing end-user bandwidth, without a corresponding increase of load on the ISP’s central network or backbone. The Open Cache Ecosystem defines standard roles, responsibilities and interfaces by which content providers via their content delivery networks (CDNs) may delegate content caching responsibility to the ISP edge.

2.2. Qwilt Open Caching Architecture and Components

2.2.1. Qwilt Cloud (QC)

The Qwilt Cloud (QC) is the existing Cloud Connectivity Service Suite hosted by Qwilt in AWS. Qwilt will implement a specific ISP tenant in AWS, including secure and isolated databases.

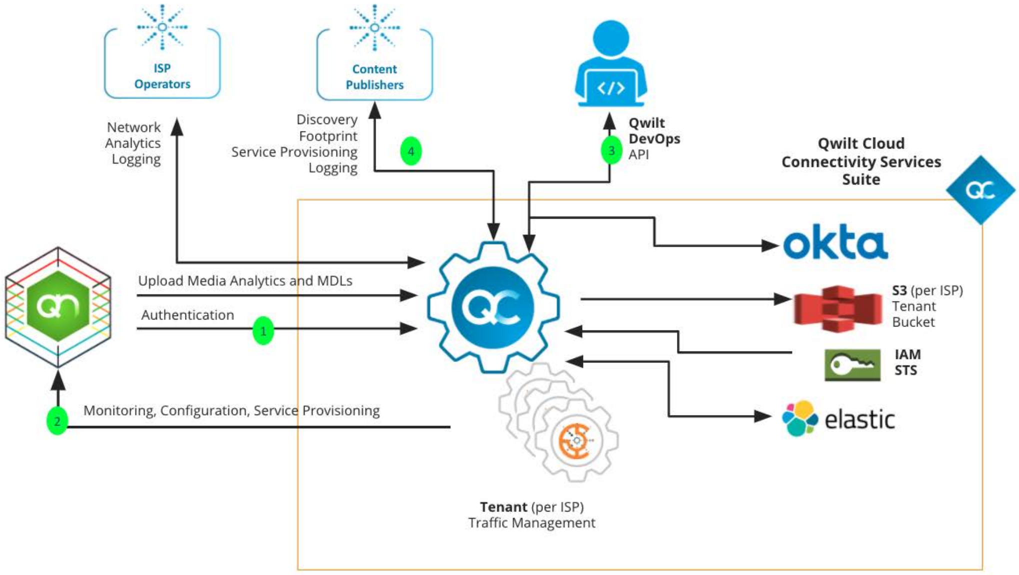

ISP Operators
Content Publishers
Network Analytics Logging
Discovery Footprint Service Provisioning Logging
4
3
Qwilt DevOps API
Qwilt Cloud Connectivity Services Suite
okta
Upload Media Analytics and MDLs
Authentication
1
S3 (per ISP) Tenant Bucket
IAM STS
elastic
2
Monitoring, Configuration, Service Provisioning
Tenant (per ISP) Traffic Management

Figure 2 Qwilt Cloud Architecture

2.2.2. Qwilt Node (QN)

Qwilt Nodes are distributed widely within a service provider network, forming a content delivery service that enables localized delivery of the most popular content in any given market. Securing Qwilt's solution and the ISP customers' networks is top of mind.

Qwilt's end-to-end security architecture has attained ISO 27001 certification for security. Qwilt's end-to-end security architecture is designed to protect Qwilt's 4 in 1 service including ISP CDN, Open Caching, Transparent Caching and Multicast ABR.

The Qwilt Node's Operating System (known as QwOS™ software) has implemented a security architecture consisting of six different security mechanisms working in unison to ensure individual elements are never compromised as depicted in the image below:

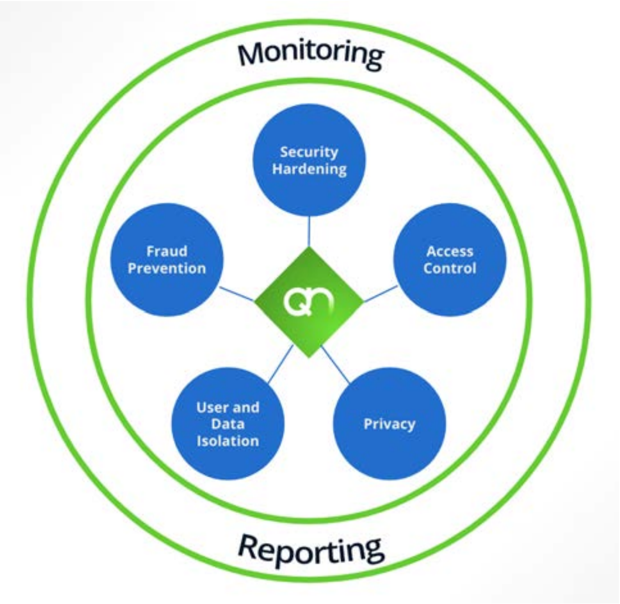


Figure 3 Qwilt Node Security Principles

3. Information Security Measures

The following activities and policies are performed by Qwilt personnel in order to ensure the security of the solution and privacy of the users and data:

3.1. Secured Development

Information security is integrated into Qwilt's agile development process and tools. It is part of Qwilt's user story and planning processes. Qwilt maintains a secure version control system to track all changes to ensure that the code will remain consistent and manageable.

Security is part of Qwilt's ongoing testing efforts: in the QA, code-reviews, automated regression suites, vulnerability assessments and penetration testing.

3.2. QC DevSecOps

Qwilt practices what is commonly referred to as "DevSecOps". DevSecOps incorporates the security team and their capabilities into Qwilt's DevOps delivery practices to ensure that security is incorporated into all production releases.

Figure 4 - DevSecOps

Continuous security validation is added at each step - from development through production - to ensure that the application is always secure. The outline of the process is as follows.

From Dev to DevOps:
Once the quality of the new code is verified, the application is deployed to a new environment also known as Staging. The Staging process verifies that there are no security vulnerabilities in the running application. This verification is accomplished by executing automated penetration tests against the running application to scan for vulnerabilities.

The Amazon Inspector (reference 2) is utilized for all existing Qwilt Cloud services that have been implemented using AWS resources. The Amazon Inspector has been optimized for AWS resource security assessments.

Amazon Inspector is an automated security assessment service that automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

Amazon Inspector incorporates a built-in library of rules and reports. **These include checks for best practices, common compliance standards and vulnerabilities.** These checks include detailed recommended steps for resolving potential security issues.

The two leading compliance standards are:

- Common Vulnerability Scoring System (CVSS) (reference 3)
- Center of Internet Security (CIS) (reference 4)

3.3. QN DevSecOp

Each release of Qwilt's QwOS software is hardened against known security threats (threat analysis).

Qwilt performs vulnerability scans using Tenable Nessus (reference 7) and Whitesource for code analysis in order to ensure the security of the QwOS software and the underlying Linux OS, addressing all known and relevant vulnerabilities. In cases where new vulnerabilities are published in between scheduled scans, Qwilt publishes immediate software updates as necessary.

Qwilt's agile DevOps methodology enables rapid implementation of security updates for all of our software components: Linux kernel, distribution and packages. In the same manner, it manages secure communication with QC and OS-level QN server protection. Identified vulnerabilities are being mitigated by their severity. Critical severity founding is handled with no delay whereas lower severity founding is being mitigated and prioritized along with the other product features.

3.4. Auditing Processes

Qwilt has successfully passed multiple tier-1 security and vulnerability scans by some of the world's leading service providers.

We conduct an external and internal audit on a yearly basis.

Qwilt utilizes CloudGuard by Checkpoint Software Technologies for ongoing audit and compliance validation of Qwilt's cloud assets and configuration.

3.5. Penetration Testing

For pro-active security tests, Qwilt conducts periodic penetration tests performed by third-party experts. In addition, Qwilt consistently runs DAST-based (Dynamic Application Security Testing) tests.

4. Hardening

4.1. QN Hardening

The QwOS software implements topology validation and enforcement including interface control and routing table enforcements. The system secures its management sub-system, isolating root and performance processes and securing process initialization.

QwOS software utilizes the following mechanisms to ensure continuous operations of the system while minimizing attack vectors:

- Enforce allocation of system resources per process (i.e. CPU, memory, etc.)
- Each process is using specific users with minimal granted permissions
- Enforce allocation per usage (i.e. dedicated storage for system application vs. content management storage)
- No root user usage
- Ongoing process monitoring and proactive trouble handling – the system can identify each of the processes' status and take required actions

4.2. Service Isolation

Network policies authorize Qwilt Node (QN) content delivery and service operational needs only. Any other communication to and from QN is restricted by default.

Content Delivery

QN enables subscribers to fetch static content using common HTTP and HTTPS protocols.

Accessing from QN to any other ISP services and machines is blocked by default at the QN level and at the ISP switches layers.

Service Management

QNs within the service provider network communicate with QC Services outside of the service provider network using HTTPS for all operational needs: configuration updates, monitoring and software updates.

The communications between QN and QC are whitelisted on the QNs and in the ISP’s switches. QN within the service provider network always initiates communications to the QC outside of the service provider network.

Qwilt’s Operation team may securely access QC & QNs for maintenance & troubleshooting.

5. Securing ISP Data

5.1. Subscribers Privacy

5.1.1. QN Privacy

Qwilt's QwOS software maintains security isolation between users of the service.

Each QN node is capable of anonymizing all user information ensuring that privacy and confidentiality are never exposed. Personally identifiable information such as IP addresses may be obfuscated prior to inclusion in Media Delivery Logs (MDL) whether stored locally on the QN or streamed to the QC.

User and Data Isolation

The QN node software maintains a clear separation between the control (authentication, statistics, logging, etc.) and data planes (content stream). Additionally, content security is maintained by storing content in the SHA-256 Cryptographic HASH algorithm while protecting against unauthorized access to content retrieval.

5.1.2. QC Privacy

As a rule, the QC does not handle any Personal Identity Information of the ISP subscribers.

Data Isolation

QC is a multi-tenant environment and as such data handling is engineered to allow access of each tenant to their data and only to their data.

For example, MDL logs are kept per device per tenant S3 bucket and the authorization is managed so the access of the customer is only to logs within their buckets, and the old MDLs are removed after a pre-agreed time.

5.2. In-transit Data Encryption

All Data is encrypted in transit between QC services. Control and Log Data is encrypted in transit between QN and QC.

Delivered Content requests may be encrypted between origin and QN or between QN and the subscribers.

- QC leverages TLSv1.2 with AES_128_GCM_SHA256 cipher for data in motion.
- QN leverages VPNs, HTTPS, FWs, ACLs to enforce in-transit data encryption

Copyright © 2021 Qwilt. All Rights Reserved.

6. Securing Content Providers data

Securing CP content delivered from the Qwilt Edge Cloud is a responsibility shared by the Content Publisher, the Internet Service Provider as well as Qwilt. Security includes protecting the Qwilt Edge Cloud platform, the streaming management flows as well as securing the data at rest and in transit.

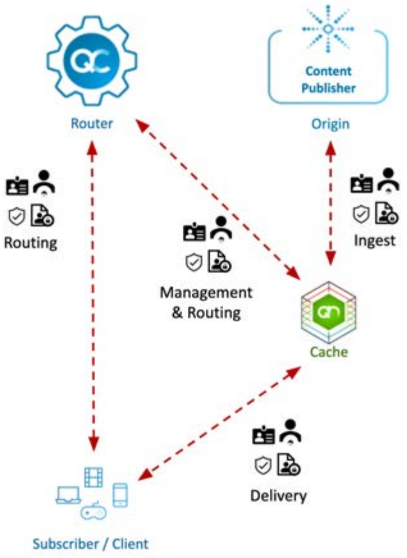


Figure 5 - Open Caching Streaming Security

Open Caching streaming between content publishers and service providers is protected through the use of identification, authentication, confidentiality and integrity.

- **Identification** is enabled through the use of shared information - whether in the form of the asymmetric Public Key Infrastructure (PKI) certificates and keys or through the use of symmetric shared secrets
- **Authentication** is enabled through the use of cryptographic algorithms such as SHA-256 encryption as well as PKI public/private key pairs
- **Confidentiality** is maintained through the combined use of identification, authentication and encryption. Confidentiality ensures the privacy of the communications, whether from user to cache or from the cache to the origin
- **Integrity** is also similarly maintained through the combined use of identification, authentication and encryption. Integrity ensures that

communications such as content requests, whether from user to cache or from the cache to origin, are tamper-proof

The Qwilt Edge Cloud supports a number of protocols that are shared with content publishers as well as client devices to maintain Open Caching security. Some examples include:

- **SSL/TLS** - Secure Sockets Layer / Transport Layer Security ensures the privacy and integrity of HTTPS communications between clients, the Content Publisher and the Qwilt Edge Cloud
- **G2O** - Ghost 2 Origin, an authentication protocol originated by Akamai, authenticates content delivery requests. Typically G2O is used by the content publisher (or their CDN) to authenticate that the open caching node is permitted to relay requests from a specific client
- **QSEC** - Qwilt Secure URL Signing is a “cookie-less” ABR security algorithm that enables signatures to be prefixed at any point in the URL path. Qsec uses JWT for signaling the signature and metadata (which includes a token). URL Signing provides authentication of the source as well as integrity for the message that is shared between client and server

During onboarding to the Qwilt Edge Cloud, the Content Publisher specifies the security requirements which are defined within the Open Caching Service profile that is then provisioned globally to open caching nodes throughout the Qwilt Edge Cloud.

7. Authentication, Authorization & Accounting

7.1. QC AAA

Users of QC APIs can be one of two types: humans or machines, and belong to one of the following three logical groups (organizations): Service Providers, CDNs or Qwilt engineering team. In no case, can a user be of both types simultaneously, nor belong to more than one logical group.

7.2. User Statuses

A user (any kind of user) can be in one of the following statuses:

- **Active** - User may log in to QC and perform permitted operations
- **Inactive** - User is registered in QC, but cannot log in not perform any operations
- **Blocked** - A status of an Active user becoming temporarily inactive (due to recurrent login attempts, license enforcement, etc.). This case cannot be set manually (change to block), only unset manually (change to active or inactive)

NOTE: A user cannot change his own status. Such an operation requires a different user with higher privileges

QC UAA system is based on Okta identity management (reference 8) for user authentication purposes. This includes:

- HTTPS only protocol
- OAuth 2.0 compliant API
- Encryption, salting and hashing of passwords
- JWT Token-based authentication, including:
  - SHA-256 signing algorithm
  - Short-lived access tokens
- Protection against website attacks (SQL injections, CSRF, XSS)
- Cross-Origin Request Sharing (CORS) limits JavaScript access to whitelisted QC endpoints

- Secured cookie management (no JavaScript access, sent only on secured connections)
- QC user management:
    - Private platform - no automated “signup” functionality;
    - New users are created by Qwilt Customer Care personnel and assigned to appropriate tenants following human validation of identity
    - The customer is required to formally update Qwilt’s Customer Care on the need to remove users from this customer’s tenant.
    - Tenants and all of their users are removed soon after the expiration of the business agreement with the tenant entity.
- Account initial registration and recovery (forgot password) is done via the user’s email address
- Self-service user credentials management - password is never stored in plain text, nor are ever visible to any Qwilt personnel

QC credential types

- Human credentials are username and password
- Machine credentials are an API key and secret

7.3. QN AAA

Qwilt’s QwOS software implements advanced AAA, including local CLI as well as remote TACACS+ management of all users. QwOS software includes multiple user groups with a hierarchy of privileges. Accounting of QwOS CLI and Linux access is logged and available via Syslog.

The QwOS system enables the creation of multi-layer ACLs including media delivery ACLs which leverage Qwilt’s robust policy table. Delivery policy table and configuration allow service provider users to define a variety of required limitations (e.g. IP sessions, Subscriber Subnets, Origin Server Subnets, Content Site) which can be associated with all or a subset of the system functionality.

7.4. Secured Access

QC & QNs can be accessed via company VPN with a user-protected password and 2FA.

7.4.1. QN Access

To access the QNs, additional authentication is required using an internal AAA system. Any access is logged and available via Syslog.

7.4.2. QC Access

Cloud VPC and Firewall isolates all communication by default, specific endpoints are opened for external requests via Cloud Load Balancers and restricted via Security Groups.

8. Certifications

The current landscape for information security standards specifically targeted for cloud computing environments is maturing. There are several cloud-specific security standards initiatives that have recently been published, including ISO/IEC 27017 and ISO/IEC 27018, that provide more detailed guidance and recommendations for both cloud service customers and cloud service providers.

The current best practice for cloud service security assessments is a combination of ISO 27001 and ISO 27017 implementation and certification of ecosystem security requirements.

ISO 27001

The objective of the standard itself is to "provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS)". Further, "The design and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization".

ISO 27017

ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

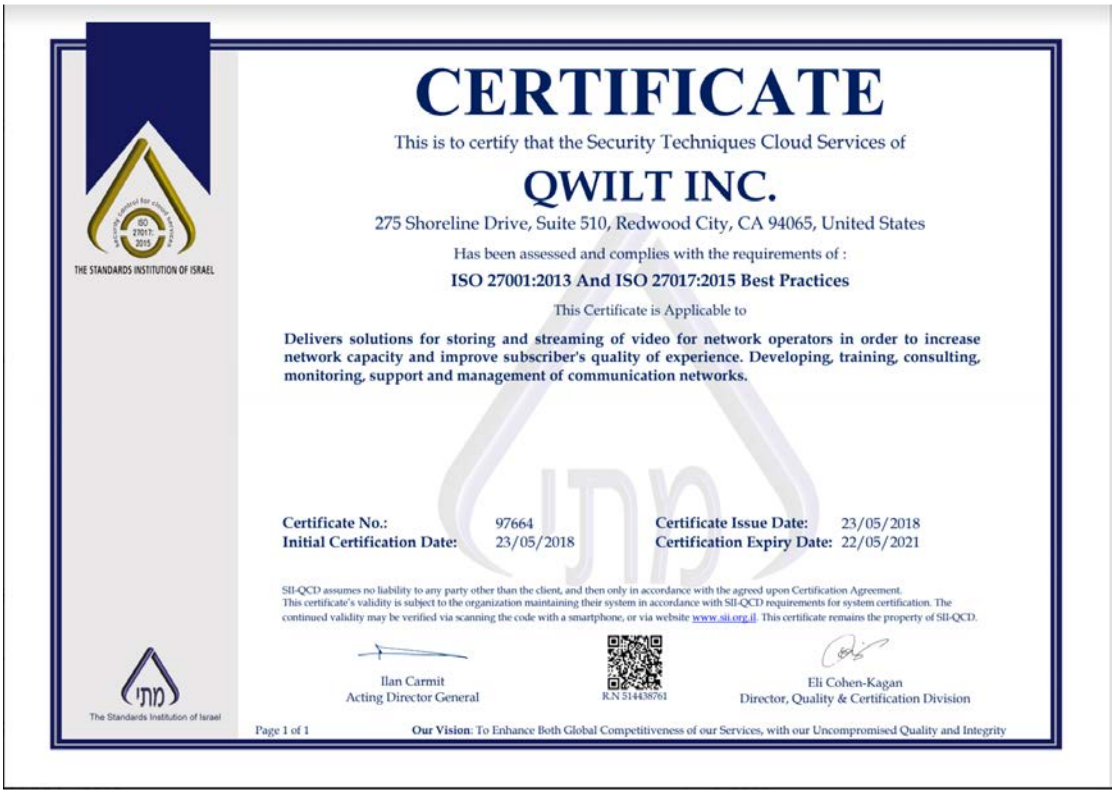
- additional implementation guidance for relevant controls specified in ISO/IEC 27002
- additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation - International Standard - provides controls and implementation guidance for both cloud service providers and cloud service customers.

ISO 27701

The objective of the standard itself is to provide guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.

Qwilt has been certified for ISO 27001, ISO 27017,ISO 27018 and 27701.



security control for cloud services ISO 27017: 2015

THE STANDARDS INSTITUTION OF ISRAEL

CERTIFICATE

This is to certify that the Security Techniques Cloud Services of

QWILT INC.

275 Shoreline Drive, Suite 510, Redwood City, CA 94065, United States

Has been assessed and complies with the requirements of :

ISO 27001:2013 And ISO 27017:2015 Best Practices

This Certificate is Applicable to

Delivers solutions for storing and streaming of video for network operators in order to increase network capacity and improve subscriber's quality of experience. Developing, training, consulting, monitoring, support and management of communication networks.

Certificate No.: 97664
Initial Certification Date: 23/05/2018
Certificate Issue Date: 23/05/2018
Certification Expiry Date: 22/05/2021

SII-QCD assumes no liability to any party other than the client, and then only in accordance with the agreed upon Certification Agreement. This certificate's validity is subject to the organization maintaining their system in accordance with SII-QCD requirements for system certification. The continued validity may be verified via scanning the code with a smartphone, or via website www.sii.org.il. This certificate remains the property of SII-QCD.

Ilan Carmit
Acting Director General

R.N 514438761

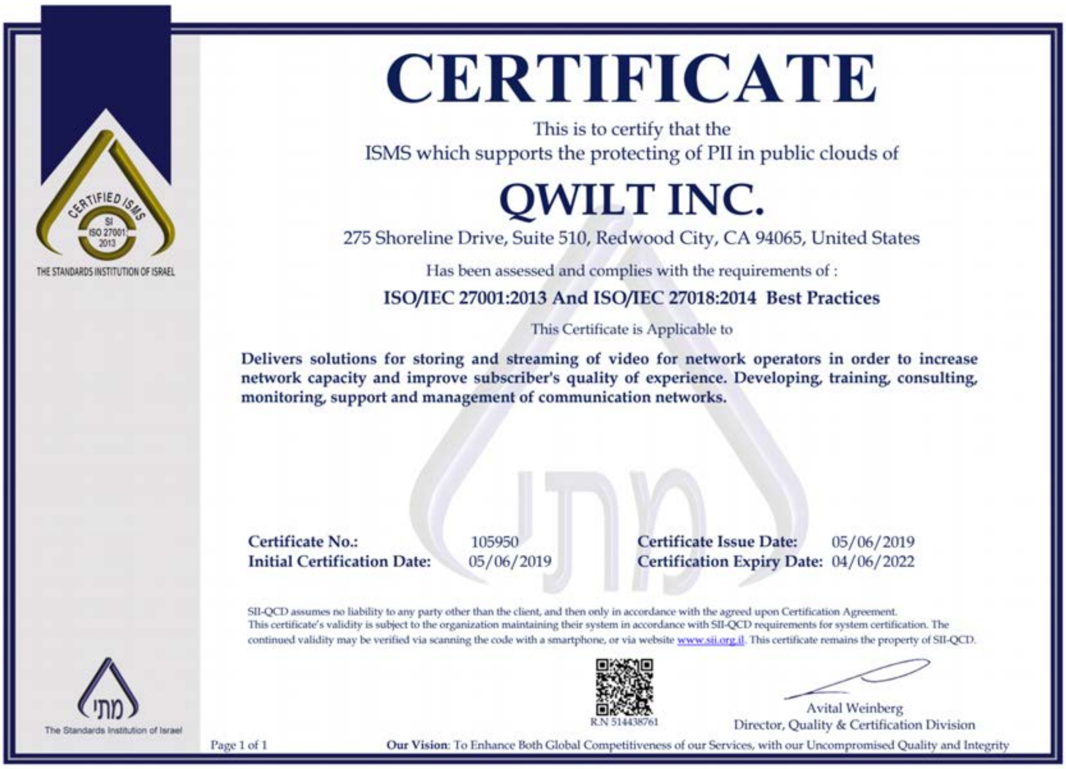
Eli Cohen-Kagan
Director, Quality & Certification Division

מתי
The Standards Institution of Israel

Page 1 of 1

Our Vision: To Enhance Both Global Competitiveness of our Services, with our Uncompromised Quality and Integrity

Figure 6 - Qwilt ISO 27001 and 27017 certification



CERTIFIED ISMS
SI
ISO 27001
2013
THE STANDARDS INSTITUTION OF ISRAEL

CERTIFICATE

This is to certify that the
ISMS which supports the protecting of PII in public clouds of

QWILT INC.

275 Shoreline Drive, Suite 510, Redwood City, CA 94065, United States

Has been assessed and complies with the requirements of :

ISO/IEC 27001:2013 And ISO/IEC 27018:2014 Best Practices

This Certificate is Applicable to

Delivers solutions for storing and streaming of video for network operators in order to increase network capacity and improve subscriber's quality of experience. Developing, training, consulting, monitoring, support and management of communication networks.

Certificate No.: 105950
Initial Certification Date: 05/06/2019
Certificate Issue Date: 05/06/2019
Certification Expiry Date: 04/06/2022

SII-QCD assumes no liability to any party other than the client, and then only in accordance with the agreed upon Certification Agreement. This certificate's validity is subject to the organization maintaining their system in accordance with SII-QCD requirements for system certification. The continued validity may be verified via scanning the code with a smartphone, or via website www.sii.org.il. This certificate remains the property of SII-QCD.

מתי
The Standards Institution of Israel

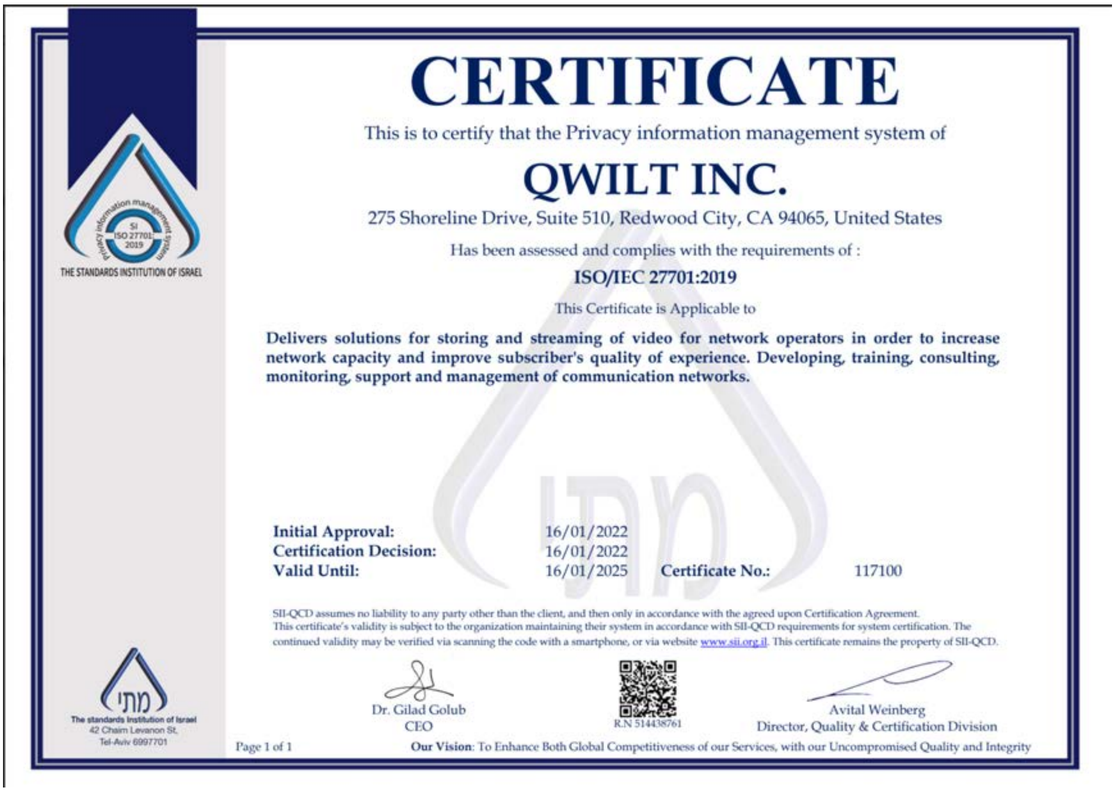
R.N 514438761

Avital Weinberg
Director, Quality & Certification Division

Page 1 of 1

Our Vision: To Enhance Both Global Competitiveness of our Services, with our Uncompromised Quality and Integrity

Figure 7 - Qwilt ISO 27001 and 27018 certification



Privacy information management system
SI
ISO 27701
2019
THE STANDARDS INSTITUTION OF ISRAEL

CERTIFICATE

This is to certify that the Privacy information management system of

QWILT INC.

275 Shoreline Drive, Suite 510, Redwood City, CA 94065, United States

Has been assessed and complies with the requirements of :

ISO/IEC 27701:2019

This Certificate is Applicable to

Delivers solutions for storing and streaming of video for network operators in order to increase network capacity and improve subscriber's quality of experience. Developing, training, consulting, monitoring, support and management of communication networks.

Initial Approval: 16/01/2022
Certification Decision: 16/01/2022
Valid Until: 16/01/2025
Certificate No.: 117100

SII-QCD assumes no liability to any party other than the client, and then only in accordance with the agreed upon Certification Agreement. This certificate's validity is subject to the organization maintaining their system in accordance with SII-QCD requirements for system certification. The continued validity may be verified via scanning the code with a smartphone, or via website www.sii.org.il. This certificate remains the property of SII-QCD.

מתי
The standards Institution of Israel
42 Chaim Levanon St,
Tel-Aviv 6997701

Dr. Gilad Golub
CEO

R.N 514438761

Avital Weinberg
Director, Quality & Certification Division

Page 1 of 1

Our Vision: To Enhance Both Global Competitiveness of our Services, with our Uncompromised Quality and Integrity

Figure 8 - Qwilt ISO 27701 certification

9. On-going security updates

Qwilt constantly improves the solution's information security capabilities and updates the solution infrastructure from time to time in order to incorporate security vulnerability fixes.

End of Document