SEAL SQ
semiconductors + quantum

Whitepaper

Seal SQ
Protecting Data At Rest

SEAL SQ
semiconductors + quantum

Contents

About SEAL SQ

SEAL SQ is a pure play cybersecurity company, with over 20 years of experience in providing digital trust and cryptographic protection. SEAL SQ delivers secure semiconductors, digital certificates, digital IDs, as well as SaaS platforms for proof-of-provenance, lifecycle management and blockchain-driven traceability. SEAL SQ customers are typically IoT vendors servicing smart buildings, smart cities, smart agriculture, drones, health care monitoring, logistics and Industry 4.0. SEAL SQ has even been able to successfully extend its Trust model to non-connected objects. Such objects connect through NFC or a plug when needed, and include luxury goods, health care consumables, appliance accessories, cold crypto wallets, and pieces of art.

SEAL SQ's certificate Authorities, Security Brokers, management systems and tamper resistant secure microcontrollers are regularly audited and accredited with highest grade WebTrust, Common Criteria and FIPS certifications.

Abstract

It has been said that “Data is the new oil” and it is true in the sense that they have similarity in how value is extracted. Raw data, like oil, is valuable because it can be refined into useful products. Raw data can be used to train AI, and refined into actionable data. Refined data is useful to give insights into the behaviors of systems and businesses.

Cybersecurity, and cyberattacks are all over the news. Whether the cyber attacks are ransomware or data breaches they involve compromising data in some way. This is due to the inherent value of data. Data protection is therefore a significant aspect of cybersecurity.

When we consider ways of protecting data, we need to understand the various states of data and use the appropriate protection mechanisms and techniques based on that state. Data states are “At Rest”, “In Motion”, or “In Use”.

We will look at the various security technologies that are provided by SEAL SQ to secure data when it is in each of these states. The technologies that are used to protect data when it is in each of these states include identity, authentication, access control, encryption, and data integrity. The SEAL SQ products that implement these mechanisms include secure semiconductors in the form of secure elements, secure MCUs and card reader chips. SEAL SQ’s trust services provide identities with our Certificate Authority (CA) for Public Key Infrastructure (PKI), and Certificate Management Services (CMS)

For IoT applications, there are a few unique considerations that need to be taken into account and we will see that securing the IoT node with hardware secure elements and using PKI can provide the highest level of security available.

States of Data Overview

The state of data will influence the protection techniques that will be employed to secure the data. This section will provide a description of the state, the vulnerability of the data in that state, and security mechanisms that can be employed to protect the data in that state. Since most of the time, data is either at rest or In Motion, cyber criminals will often target these two states.

Data At Rest

Data at rest is not being actively transmitted or used. It is in static storage. This storage can be long term or offline storage, Network Active Storage (NAS), cloud storage, encrypted external storage, or hard drive. The format of storage can be in the form a database, structured, unstructured, or file system. The specific storage will depend on how the data will be used.

If the data is to be archived and used infrequently, then the data can be in an archival backup. If there are retention requirements or regulations, then the archival backup can be actively managed so the data is deleted or moved to offline storage at the appropriate time.

If the data is At Rest, but there is a requirement to access the it on an ongoing basis, then the data needs to be available in NAS, Cloud, hard disk, or some accessible storage.

At Rest is generally considered the most secure and easiest to protect since access can be tightly controlled

Data In Motion

Data In Motion (or In Transit) is data that is being transferred from one place to another. Examples of In Motion include transferring files over an internal private network or the Internet, database replication, and transferring measurements from an IoT device.

When data is gathered by an IoT device it is In Motion, similar to mining for oil. Data is also In Motion when it is being consolidated for refining and aggregation into useful reports or for applications, when it is being used for dynamic control in systems, and when it is being prepared for archival.

Data In Motion is generally considered less secure than data at rest due to the increased exposure introduced by transmission.

In order to be useful, data must enter the In Motion state.

Data In Use

Data In Use is data that is currently being accessed, updated, processed or displayed. This includes data that is being aggregated for reports, and data being used in user applications. One prerequisite to In Use is that it is decrypted and in its useful format. It needs to be decrypted so that user applications can work in a context that is useful to the user. In Use data will typically be in program memory or cached in short term storage.

Due to the fact that this data is decrypted for use, the In Use data is most vulnerable to compromise and / or corruption.

Data In-Motion Security

Vulnerability

The primary vulnerability of At Rest data is compromised access. The first step in compromising the data will involve gaining access to the computer, external drive, or network where data is stored. Once the attacker is on the computer, they will then attempt to access the data.

Access can be obtained in a variety of ways. Vulnerabilities include a disgruntled insider, unauthorized physical access to an on site workstation, WiFi access vulnerabilities, and an online breach of the network. If the data is stored on the cloud, then access to the cloud account and the trustworthiness of the cloud provider become potential vulnerabilities.

When an attacker has access to the computer where the data is stored, they will then attempt to access sensitive data. Usually there are additional security measures to access sensitive data. Vulnerabilities include unprotected or superficially protected data, unencrypted data or unprotected encryption key, and unrestricted read/write.

Once the data is breached, there are multiple ways that hackers will use the data to mount an attack. Among the common attacks are encrypting the data and holding it for ransom (ramsomware), publicly exposing the data, covertly using the data to attack the company, corrupting the data, or crippling the products and/or services of the company.

Protection

An important factor in securing data At Rest, is protecting the computer, external drive, or network where the data can be accessed. If the attacker can get to a place where the data is exposed, then they can read or compromise it. However, even in the case where the computer is breached, all sensitive data should have additional security measures that protect it from being exposed or corrupted.

Security measures for protecting data At Rest include encrypting the data, categorizing the data according to the required protection level and structuring the data storage for appropriate security and access. Structuring the data according to protection level saves costs for secure storage and allows security policies to be more targeted by leveraging Access Control Lists (ACLs) and Multi Factor Authentication (MFA)

There are a few different ways to accomplish encryption, for example you can encrypt the data into normal file storage on a hard disk, NAS, or in the Cloud. When encrypted data is stored in this way, it should also protect file system access and protect read / write rights. Also, when encrypting the data, it

is important to also implement a sound key management strategy. Part of this strategy will be to store the keys securely in a hardware device like a SEAL SQ VaultIC secure element.

Another example of accomplishing secure storage is to use encrypted external storage. This approach has the advantage of combining relatively easy access to the data with a sound key management strategy. There are several examples of secure storage using the MS600x and the VaultIC from SEAL SQ.

SEAL SQ Security Building Blocks

VaultIC Secure Elements

The VaultIC secure elements VaultIC408 and VaultIC292 combine hardware-based key storage with cryptographic accelerators to provide a wide array of cryptographic features including identity, authentication, encryption, key agreement and data integrity. The hardware security is Common Criteria Evaluation Access Level 5+ (CC EAL5+) certified to protect against hardware attacks such as micro probing and side channel. Additional certifications and capabilities include FIPS140-3 Level 3, NIST SP800-90B, and NIST CAVP.

The fundamental cryptography of the VaultIC family includes the NIST recommended algorithms and key lengths (ECC, RSA, and AES). Each of these algorithms is implemented on chip and uses on chip storage of the secret key material, so the secrets are always protected in the secure hardware.

The secure storage and cryptographic acceleration make them an ideal solution for use cases like network/IoT end node security, platform security, secure boot, secure firmware download, secure communication/TLS, data confidentiality, encryption key storage, and data integrity.

MS600x Secure MCUs

The SEAL SQ MS6001 and MS6003 secure MCUs are based on the low power, high performance ARM SecurCore 300 32 bit architecture. The accompanying ROM features the storage of low level drivers, bootloader, wear leveling and cryptographic code. The cryptographic accelerator is dedicated to perform fast encryption or authentication functions. The MS600x family is certified CC EAL5+ to provide the highest standard of hardware security.

The security features and large Flash memory for firmware and data of the MS600x family of MCUs are a perfect fit for use cases like external secure storage, encryption key storage, USB hardware authentication tokens, FIDO, and full IP protection for embedded systems.

Smart Card Reader Chip

SEAL SQ has more than 20 years of design and research experience in secure products for the smart card industry. SEAL SQ's comprehensive and highly competitive portfolio of Smart Card Reader chips enables customers to obtain secure, high-performance chips for any application.

Offering stand alone hardware platforms, or third-party integrated applications allows customers to quickly build smart

card readers without requiring custom development. SEAL SQ's Smart Card Reader chips are EMV-CO compliant enabling a wide spectrum of use cases from financial to user authentication.

The smart card reader increases the security for user authentication. This higher confidence of user identity will provide better security for data in the At Rest and In Use states

PKI

SEAL SQ offers a full portfolio of standards based technologies to manage digital identities for people, applications, and IoT devices. SEAL SQ offers enterprise level PKI to scale the number of certificates from hundreds to millions. SEAL SQ has a long history as a PKI technology provider and a Trusted Certification Authority (CA). SEAL SQ managed PKI (mPKI) service is called INeS CMS. INeS provides certificate management, CA management, public cloud integration, Role Based Access Control (RBAC), and APIs for custom implementations.

These PKI technologies support the use cases of At Rest and In Motion, and In Use. The At Rest and In Use use cases require reliable user authentication and strict access control. The end points of data In Motion will require certificates to establish their identities. The INeS CMS platform will provide a secure, scalable, and manageable trust model.

Use Case

External Secure Storage

A good use case to demonstrate data At-Rest is external secure storage. It covers the essential elements of controlled access, encrypted storage, controlled by a secure MCU.

Advantages to storing critical data in an external secure storage are:

1. External secure storage drives are not always attached, making it harder for remote online attacks
2. External secure storage encapsulates the security into a secure hardware encrypted drive.
3. Flexible storage capacity can be achieved surpassing 25 TB
4. The external secure storage is portable and can be attached to any computer or network. Including computers that are not connected to any network ("air gapped").

The design for the external secure storage with USB interface will use a MS6003 for a secure MCU. This MCU will securely store the encryption keys and perform the encryption and decryption in a Trusted Execution Environment (TEE). The TEE allows for flexibility in the cryptographic algorithms used for encryption / decryption. Access control will include a user certificate generated and managed by the INeS CMS. The certificate along with a password and a Personal Identification Number on the USB storage device combine to achieve Multi Factor Authentication for accessing the stored data.

Conclusion and Key Takeaways

Data is a valuable commodity and needs to be protected. We have identified the various states of data and have focused on the description, the vulnerabilities, and the security for data At Rest.

Encryption, identity, access control, and hardware security have been shown to be the building blocks of data At Rest security. These elements are supported by secure elements, secure MCUs, card reader chips, certificate management and CAs. SEAL SQ has security technologies of VaultIC Secure Elements, MS600x secure MCUs, Smart Card Reader chips, and PKI infrastructure enable data protection for At Rest, In Motion, and In Use data states.

SEAL SQ security will protect data throughout the data life cycle as it goes through it's various states.

Acronyms and abbreviations

AES	Advanced Encryption Standard
ACL	Access Control List
AI	Artificial Intelligence
API	Application Programing Interface
CA	Certification Authority, entity that signs digital certificates
CC	Common Criteria
CISO	Chief Information Security Officer
CMS	Certificate Management System
CSR	Certificate Signing Request
DDOS	Distributed Denial of Service
EAL	Evaluation Assurance Level Used with CC certification to specify the level of verification (e.g. CC EAL5+)
ECC	Elliptic Curve Cryptography, a public Key cryptography algorithm
ECDH	Elliptic-curve Diffie–Hellman
ECDHe	Elliptic-curve Diffie–Hellman ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
ICA	Issuing Certificate Authority
IoT	Internet of Things
IP	Intellectual Property
MCU	Micro Controller Unit
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OISTE	Organization for the Security of Electronic Transactions https://oiste.org/
PIN	Personal Identification Number
PKCS#11	Public-Key Cryptographic Standards
PKI	Public Key Infrastructure https://en.wikipedia.org/wiki/Public_key_infrastructure
RBAC	Role Based Access Control
REST	Representational State Transfer
ROT	Root of Trust. The foundation for cryptography.

RSA	Rivest Shamir Adleman, a public Key cryptography algorithm
SaaS	Software as a Service
SE	Secure Element
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer. Secure transportation protocol replaced by TLS
TB	Terra Byte
TEE	Trusted Execution Environment
TLS	Transport Layer Security. A secure transportation protocol
WiFi	Wireless Fidelity

References

[NIST] NIST SP 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018

[FIPS] NIST FIPS 140-3: Security Requirements for Cryptographic Modules, March 2019

[CC] CC:2022 Release 1

[VIC408] SEAL SQ: VAULTIC408 Summary Datasheet, March 2022

[VIC292] SEAL SQ: VAULTIC292 Summary Datasheet, xxx 2022

[AWS] Device Manufacturing and Provisioning with X.509 Certificates in AWS IoT Core

[AppNote] SEAL SQ: Secure IoT Device to Cloud Solution

Disclaimer

Information in this document is not intended to be legally binding. SEAL SQ products are sold subject to SEAL SQ Terms and Conditions of Sale or the provisions of any agreements entered into and executed by SEAL SQ and the customer.

The products identified and/or described herein may be protected by one or more of the patents and/or patent applications listed in related datasheets, such document being available on request under specific conditions. Additional patents or patent applications may also apply depending on geographic regions.

For more information, visit www.SEAL SQ.com

Release date: December 2022

Contacts

SEAL SQ SA
Avenue Louis-Casaï 58
1216 Cointrin
Switzerland
Tel: +41 22 594 3000
Fax: +41 22 594 3001
SEAL SQ Semiconductors
Arteparc Bachasson • Bât A
Rue de la carrière de Bachasson
13590 Meyreuil • France
Tel : +33 (0)4 42 370 370
Fax : +33 (0)4 42 370 024

Email: sales@SEAL SQ.com
Stay connected with @SEAL SQ