UNBOUND

(MATH OVER MATTER)

Integrate a virtual secure enclave directly into any app to enable secure transactions from insecure devices.

The Secure-as-Hardware Software with a Mathematical Proof

Unbound has decoupled trust from infrastructure. Based on **cryptographic breakthroughs** that draw strength from math (not matter), Unbound Crypto of Things (CoT) let's you virtually embed a secure enclave to protect keys and certificates on any and every device. Built upon Unbound's platform-agnostic FIPS validated **vHSM technology**, Unbound CoT lets developers simplify and strengthen the identity and authentication crypto layers of their mobile apps in heterogenous environments. CoT unbinds the crypto layer from the hardware devices, so you don't have to secure every device make or model.

Unbound Crypto of Things is the only lightweight software key protection solution that enables every endpoint device to have a virtual secure enclave (vSE), where private keys can be stored securely with a trust level comparable to dedicated secure hardware – creating a consistent level of security among all BYOD devices that connect to your applications.

Breaking the Boundaries of Traditional Key Management & Protection

Traditional management of cryptographic keys on the endpoint side requires holding them in a physically secure boundary such as a smartcard, hardware token or a secure element, as they often appear in the clear during their lifecycle, e.g. while being generated or used. Thus, locking keys within physical boundaries has, until now, been the generally accepted safest method of key protection because it could protect against this single point of failure. This is especially important in endpoint devices, that are inherently untrusted and operate in an insecure environment

Eliminating the Single Point of Failure

Unbound CoT eliminates this single point of failure by ensuring that your most sensitive **keys never exist in the clear at any point in their lifecycle – not even when generated or while in use**. With Unbound CoT, key material is never whole. Rather, each key exists as two random key shares. All operations are carried out without ever uniting the key shares. By eliminating the single point of failure, Unbound CoT can stretch the secure boundary far beyond the traditional physical casing.

Benefits & Features

- Mathematically proven security guarantee – the key material never exists in the clear throughout its lifecycle including creation, in-use and at-rest
- Virtual root of trust for any device and application, rendering cryptographic keys immune to malware and client-side attacks
- Unparalleled central management, control and audit capabilities on cryptographic assets bound to devices
- Support all industry standard crypto algorithms
- Intuitive and easy to use SDK in various development languages for superb developer experience

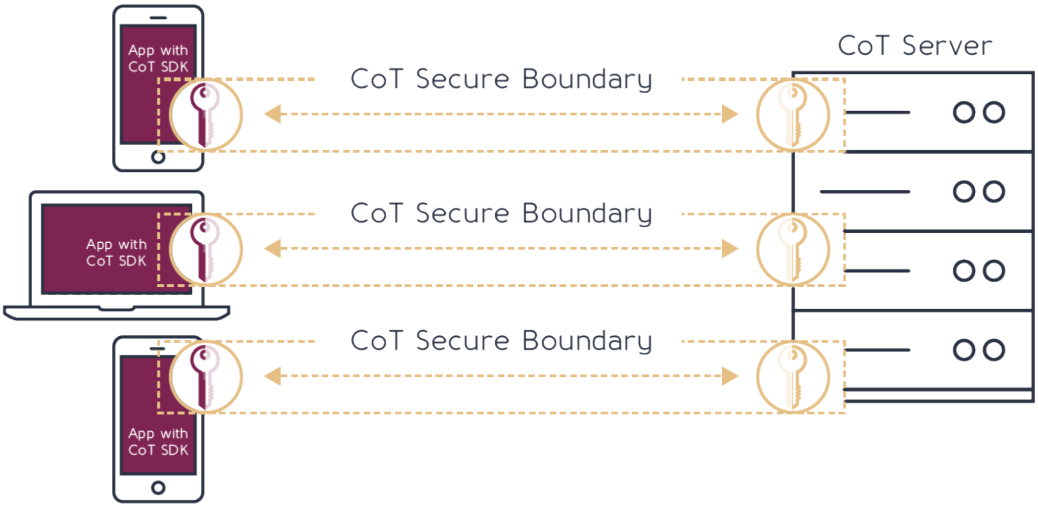
Use Cases

Unbound CoT supports large range of use cases including:

- Transaction authorization (signing)
- Wallets and payment applications
- Password replacement
- BYOD as a Smart Card / HW token (FIDO U2F)
- Security foundation for FIDO UAF (e.g. biometric authentication)
- PKI (e.g. document signing, eGovernment)
- M2M authentication
- Data protection
- Devices

Non-Continuous Secure Boundary:
Keys are Now Immune to Malware and Client-Side Attacks

Each Unbound CoT system is comprised of a central server (CoT server) that is installed and managed by the customer. Various endpoint devices that run CoT software (CoT library) connect to the CoT server, creating a series of pairs – where each pair consists of a single endpoint device and the CoT server. Each of the pair nodes hold one share of a key. Together, CoT software on the device and the CoT server form the secure boundary of Unbound CoT. Applications on the device use the CoT library API for consuming cryptographic service for the keys that are managed within the library, effectively creating a virtual secure enclave on the device. All connections between CoT devices to the CoT server are protected using server authentication (TLS).



The CoT limitless Secure Boundary adds a newly created dimension to security architectures. The inherent separation between and endpoint device and a remote server stretches the secure boundary far beyond the traditional physical casing of the device, ensuring that **keys on endpoint devices remain secure at all times, even in the presence of malware or malicious actor fully controlling the endpoint device**.

Securing Keys within the CoT Secure Boundary

- Each private key exists as two separate random shares, one share stored on the device and one on the CoT server.
- Key shares are never combined at any point in time.
- Key material never exists in the clear at any point in the key lifecycle
  - Not in memory, disk or over the network
  - Not even during key creation, in-use (e.g. for authentication, signing, decryption) or at-rest.
- Key shares are constantly refreshed, so in order to maliciously obtain key material an attacker must compromise **both** the device and the CoT server **simultaneously**.

Ultimate Security, Control and Audit

In addition to securing cryptographic keys and ensuring they cannot be compromised, cloned or tampered, Unbound CoT includes additional security layers that safeguard the usage of the key and provide unmatched levels of control and visibility.

Recovery	Instant, centrally controlled revocation
Malicious use of the key	Real time tamper proof audit trail
	Brute-force proof additional factors
Key theft, cloning	The key material never exists on the device

Brute-force Proof Authentication Factors

Unbound CoT provides two factor authentication that can optionally be used to authorize any usage of the cryptographic key. Various authentication factors are supported, including PIN code, password, fingerprint and face recognition. The authentication takes place using MPC algorithm between the endpoint and the vSE server[1], thus preventing brute force attacks on the endpoint side.

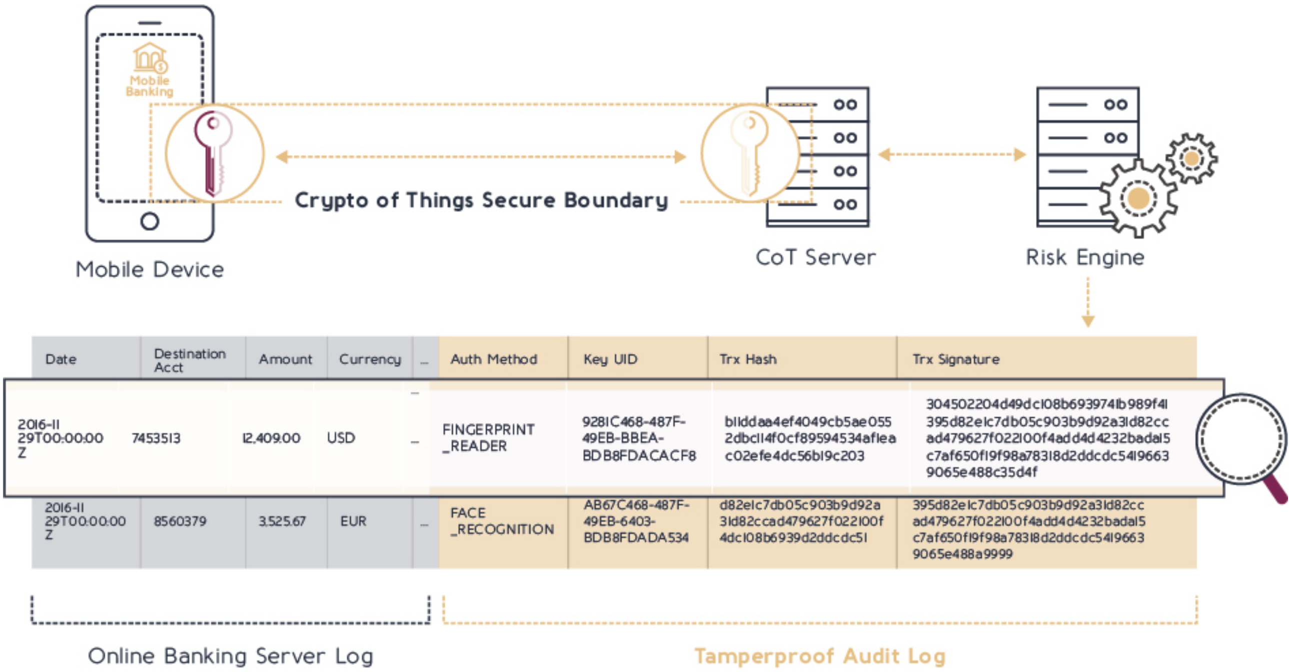
Central Management and Real Time Tamper Proof Audit Trail

Unbound CoT requires communication between the endpoint and the CoT server for performing any crypto operation. Thus, the CoT server includes real time tamper-proof audit log of any crypto operation performed on the endpoint (e.g. signing authentication token, signing a transaction, data decryption). The audit log data can be fed into a SIEM, UEBA or a risk engine, allowing detection of crypto key usage anomalies in real time.

Instant Revocation

When things go wrong and an endpoint is suspected as compromised, Unbound vSE allows ultimate control by ensuring instant revocation of any crypto key that is secured with vSE. Deletion of the relevant key share on the vSE server immediately renders the key useless, ensuring that any assets protected by this key are safe.

[1] Except for when using native biometric authentication on the device (if available). Such authentication is typically implemented locally on the device.

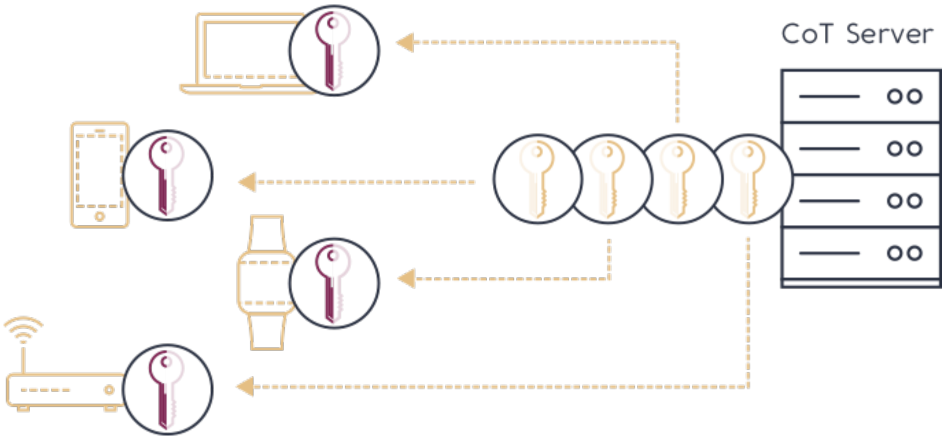


Date	Destination Acct	Amount	Currency	–	Auth Method	Key UID	Trx Hash	Trx Signature
2016-11 29T00:00:00 Z	7453513	12,409.00	USD	–	FINGERPRINT _READER	9281C468-487F-49EB-BBEA-BDB8FDACACF8	b11ddaa4ef4049cb5ae055 2dbc114f0cf89594534af1ea c02efe4dc56b19c203	304502204d49dc108b6939741b989f41 395d82e1c7db05c903b9d92a31d82cc ad479627f022100f4add4d4232bada15 c7af650f19f98a78318d2ddcdc5419663 9065e488c35d4f
2016-11 29T00:00:00 Z	8560379	3,525.67	EUR	–	FACE _RECOGNITION	AB67C468-487F-49EB-6403-BDB8FDADA534	d82e1c7db05c903b9d92a 31d82ccad479627f022100f 4dc108b6939d2ddcdc51	395d82e1c7db05c903b9d92a31d82cc ad479627f022100f4add4d4232bada15 c7af650f19f98a78318d2ddcdc5419663 9065e488a9999

Root of Trust for Any Endpoint Device

The proliferation of various endpoint types, models and platforms combined with the vulnerable nature of endpoint leads to a situation where cryptographic keys, despite being the foundation of the security architecture, are not secured by a root of trust: many devices lack a secure element (SE), Trusted Platform Module (TPM) or a Trusted Execution Environment (TEE) that allow secure storage of sensitive keys. Moreover, even when available, such hardware is typically not utilized by applications due to limited functionality (i.e. limited to specific algorithms and key sizes) and integration difficulties across large variety of endpoint platforms. This situation opens a broad attack surface that can be exploited, resulting in compromise of user / machine identity, data and authorization of sensitive activities such as transactions and document signing.

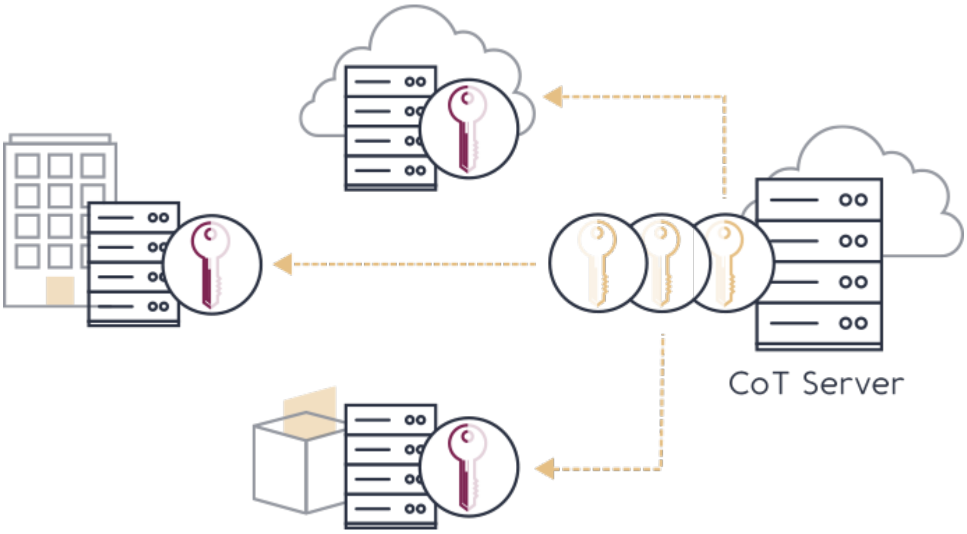
Unbound CoT completely abstracts the underlying hardware, effectively enhancing any endpoint device with a virtual root of trust that has a unified, single API used among all supported devices and platforms. In addition, CoT utilizes secure hardware if it exists on the device, to provide even higher level of security.



Root of Trust for Applications and Containers in the Cloud and Data Center

The rapid adoption of cloud services along with the emergence of data breaches make the data center a perimeter-less environment, effectively requiring end-to-end encryption and reliable identity of services and applications accessing the most sensitive data stores of the enterprise. Within cloud-native environments the challenges are even greater, where ephemeral micro-services and containers require access to vaults and secret stores. In parallel, adoption of distributed, hybrid IT and software defined architectures renders the reliance on secure hardware in the endpoint side limiting and challenging.

Unbound CoT completely abstracts the underlying hardware, effectively creating a virtual root of trust for any application, server or container in the cloud or data center. In addition, CoT utilizes secure hardware such as a TPM or Intel Software Guard Extensions (SGX), if it exists on the endpoint, to provide even higher level of security.



Embrace the Future: Centrally Managed, Platform Independent & Agile Cryptography

Unbound CoT is future-ready, so your cryptography infrastructure can be too.

- Without the need for dedicated hardware, Unbound CoT can be deployed on virtually any endpoint, from IoT and mobile to laptops and even application servers and containers in the cloud / data center.
- Expanding the secure boundary of endpoint devices to include a central server allows unparalleled level of real-time control and audit for any activity performed on the endpoint.
- With the emergence of quantum computing and blockchain on one hand and crypto vulnerabilities on the other, changes in crypto are faster than ever. Unbound CoT is a crypto-agile system that ensures you will be up and running the latest crypto, with update cycles measured in days to weeks, not months or years.

Technical Specifications

Operating Systems and Platform

Component	Device Type	Supported Operating Systems
CoT Endpoint	Mobile (smartphones, tablets, wearables)	Android, iOS
	Desktop/laptop	Windows , Mac, Linux
	Virtual/physical server, container	Linux, Windows
CoT Server	Virtual/physical server	Linux, Windows

API Support

- Mobile: Simple and easy to use SDK
- Desktop/laptop/server: PKCS#11, Java (JCE) Microsoft CNG, OpenSSL

Cryptography

- Full Suite B support
- Asymmetric: RSA (2048, 3072, 4096), Elliptic Curve Cryptography with P256 | P384 | P521 curves
- Symmetric: AES (128, 256)
- Hash/HMAC: SHA-256, SHA-384
- Proprietary algorithms: Secure password verification using PIN/Native biometrics, Post-Quantum Crypto (PQC)[2], Bitcoin and blockchain, generic secrets

Endpoint Additional Authentication

- Device-native fingerprint/Face Recognition[3]
- Face recognition
- SAML
- PIN, password

Leverage Secure Element (SE) and Trusted Execution Environment (TEE)[4]

- Mobile: iOS secure element, Android TEE
- Desktop/laptop/server: TPM, TXT, SGX

High Availability

- Active/Active and Active/Passive modes (with external load balancer)

Management & Administration

- Command Line Interface (CLI)
- Management REST API
- Full multi-tenancy support with cryptographically isolated domains

Performance Specifications

- Cryptographically isolated domains: up to 10,000
- Maximum total endpoints for all tenants commutatively: up to 250,000,000
- Keys: bound by disk space only
- Capacity in transactions per second (TPS)[5] for sample configurations:

[2] Asymmetric PQC decryption in hybrid mode for preserving session privacy. In accordance with NIST issued guidelines for PQC standardization (http://csrc.nist.gov/groups/ST/post-quantum-crypto/faq.html)

[3] Integrated with on-device hardware, where applicable

[4] On supported endpoint devices. Note that the secure hardware is leveraged as an additional and optional layer of protection, securing the key share residing on the endpoint. This key share is meaningless as it cannot be used alone to derive any information on the key material.

[5] Capacity was tested with 2.1GHz CPU cores; using a faster CPU would result in higher performance figures.