unbound security

Unbound CORE Crypto Asset Security

Frequently Asked Questions

Version 1.4
October 2021

Table of Contents

1. Revision History

The following table shows the changes for each revision of the document.

Version	Date	Description
1.4	October 2021	Rebranded and updated with Unbound CORE components.
1.3	May 2021	Updated links
1.2	July 2020	Updated the question Is there an integration with a NaaS provider? to include integration with the nodes of BRD using their Blockset product.
1.1	December 2019	Updated for CASP 1.0.1910.
1.0	February 2019	Initial version

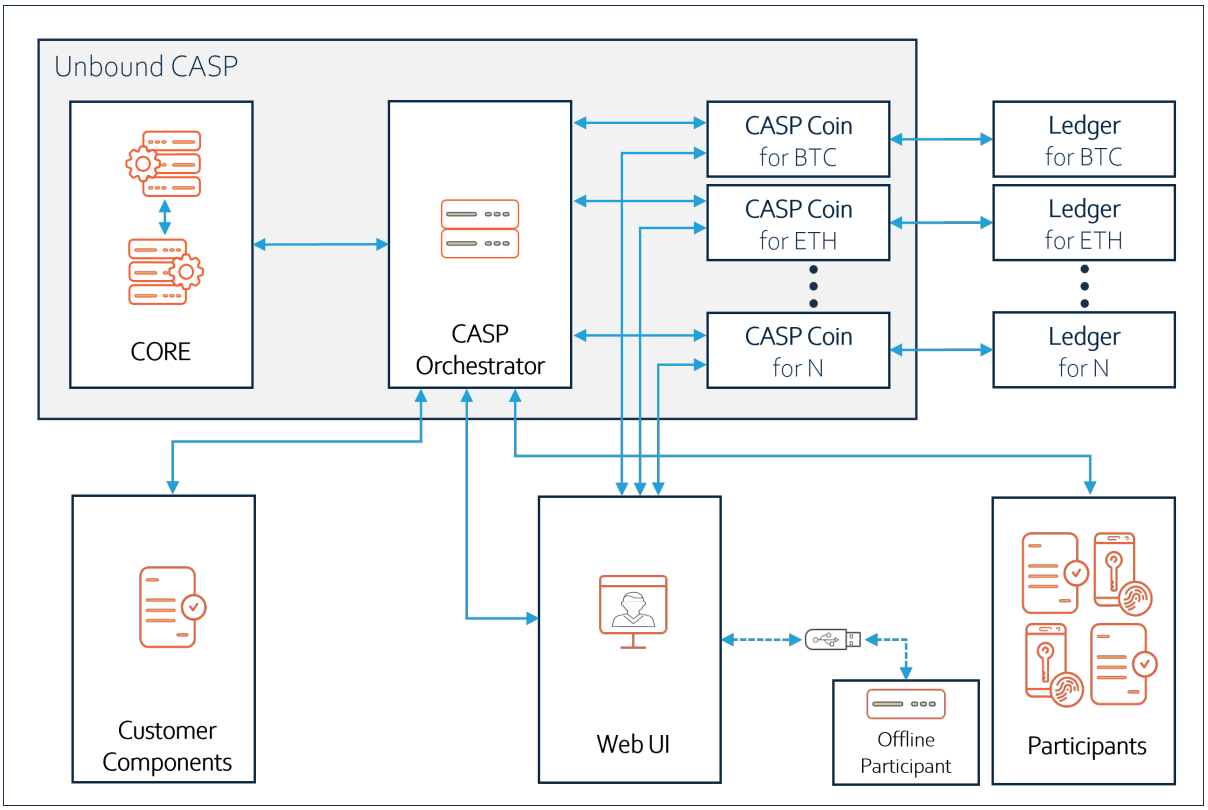
2. Frequently Asked Questions

The following sections contain answers to some of the frequently asked questions about CASP.

2.1. System

2.1.1. What are the components of the CASP platform?

CASP consists of the components shown in the following diagram:



The **CASP Orchestrator** is the heart of the CASP system. It communicates with all parts of the system, initiates creation of the key shares for the vault, manages the different distributed procedures, and acts as the external entry point for the relevant applications, such as the crypto asset applications.

The CASP Orchestrator is backed by the powerful key management capabilities of Unbound CORE Information Security (**CORE**). CORE works together with the **Participants** to provide the complete approval signature for transactions, where Participants can be mobile devices, desktops, servers, bots or offline participants. CASP creates an ECDSA key, EdDSA key, or a key with BIP derivation, which is used for all transactions.

CASP's open architecture enables communication with different types of crypto asset ledgers. For example, the BTC wallet enables communication with a Bitcoin ledger. It prepares a transaction from the available ledger data and sends it to CASP. CASP then signs the transaction and returns it, which then transmits the signed transaction to the ledger. CASP seamlessly works with many different types of ledgers.

2.1.2. Which wallets are currently supported?

All wallets that use ECDSA or EdDSA (Ed25519) algorithms to sign transactions can be supported by CASP using CASP API.

2.1.3. How does the CASP solution compare to other service provider solutions?

The CASP solution provides these additional capabilities above and beyond the other service providers:

- Strong MPC implementation for securing private keys.
- Flexibility and scalability.
- Cryptographically enforced key usage.
- Lower TCO.

2.1.4. How complicated is the deployment of CASP?

CASP can be deployed in many cases in a couple of days. Installation is facilitated by the following features:

1. The CASP server uses a standard RPM installer.
2. CASP can be install on many standard operating systems, such as iOS, Android, and Linux.
3. CASP can be installed anywhere.
4. A detailed online installation guide is provided that walks you through the prerequisites, CASP installation, and configuration.

2.1.5. Where can I deploy CASP?

CASP can be deployed in various locations:

1. On a private cloud.
2. On a public cloud (e.g. AWS, Azure, GCP).
3. On premise.
4. Hybrid deployment (On premise and public cloud).

2.2. Security

2.2.1. How does the CASP Multi-party signature differ from Multisig?

CASP MPC does not require any additional scripting as required for Multisig for the case of more complex quorums (such as 4 out of 6).

Multisig generates multiple signatures, whereas CASP MPC creates just a single signature. Therefore, CASP MPC needs to process less data, making it more efficient, which translates into better performance on the miner side.

CASP MPC has a more sophisticated quorum authentication scheme for the approvers. For example, you can have 4 out of 6 required to approve from an external group and 2 out of 4 required to approve from the internal group. This type of quorum is very hard to implement with multisig (which usually performs only 2 out 3 quorum authentication).

2.2.2. What is the different between Shamir's Secret Sharing and what Unbound does?

In general, Shamir's Secret Sharing provides a solution for sharing a key between many participants and enforcing some or all of them (quorum) to participate in key usage. Combining this technique with MPC, which is what Unbound does, allows using the key (for signing, encryption, etc), **without ever assembling the key**. This benefit is the result of MPC, which allows a set of parties to compute a function without revealing the secret data, which in this case are the Shamir Secret Shares. See the Unbound website for more information.

2.3. Wallets

2.3.1. Which ledgers are supported?

CASP supports two types of implementations for handling different types of ledgers. CASP provides built-in support for some types of ledgers, as described Built-in Coins.

CASP also provides the necessary APIs so that you can bring your own wallet (BYOW), meaning that you can use whatever ledger you have, and control the vault and key operations with CASP. Using BYOW, you can create an implementation that can handle any coin type, as well as any special operations that you use to communicate with your ledger and for ledger processing.

You may want to use BYOW when using one of the built-in chain adaptors, but need other features, such as using your own nodes and address caching. You may already have management in your application for one of the built-in chain adaptors and want to use CASP for key management and protection. BYOW provides the flexibility to be used with any blockchain application.

2.4. Integration/Operation

2.4.1. What are some common use cases for CASP?

CASP is a flexible platform that can be used in a variety of use case, including the following:

- Exchanges - Increase velocity and secure your internal vaults by applying MPC-based cryptographic enforcement to transactions' approval schemes.
- Custodians - Leverage a bank-grade crypto asset security platform to serve your retail and institutional customers, who are seeking crypto asset custodian and trading services.
- Trading Platforms – Secure transfers between counter-parties by applying MPC-based cryptographic approval policies.
- System Integrators - Leverage a mature SDK package to empower your customers to profit from emerging opportunities and market dynamics with the ultimate secure crypto asset security platform.

2.4.2. Does CASP support HD wallets?

Yes, CASP provides support for hierarchical deterministic (HD) wallets using the BIP32 and BIP44 HD wallet standards.

2.4.3. How do I connect AML and a customer ID?

It is recommended to use an AML and customer ID approver server/person as one of the participants in the approval process (within a separated group) as a bot approver. By doing so, the AML participant denies a transaction when a suspicious person is trying to transact money.

An additional benefit of this strategy is the ability to produce AML-based reports to a regulator, proving that each transaction went through an AML check.

2.4.4. How is backup approval handled?

The platform creates a secure backup of the key parts without ever bringing the parts together. The process is supported both for standard keys as well as BIP seeds. The key/seed is encrypted with an RSA key, which can be kept in cold backup, HSM, or any other secured component.

It is important to note that the platform provides a zero-knowledge proof that the content of the encrypted backup matches the public key. Meaning that when backing up the key, no party can cheat and cause key loss. The platform verifies backup content (without decrypting it, only using the RSA public key) and secured storage of it before the first deposit of money into the vault.

2.4.5. Is there an integration with a NaaS provider?

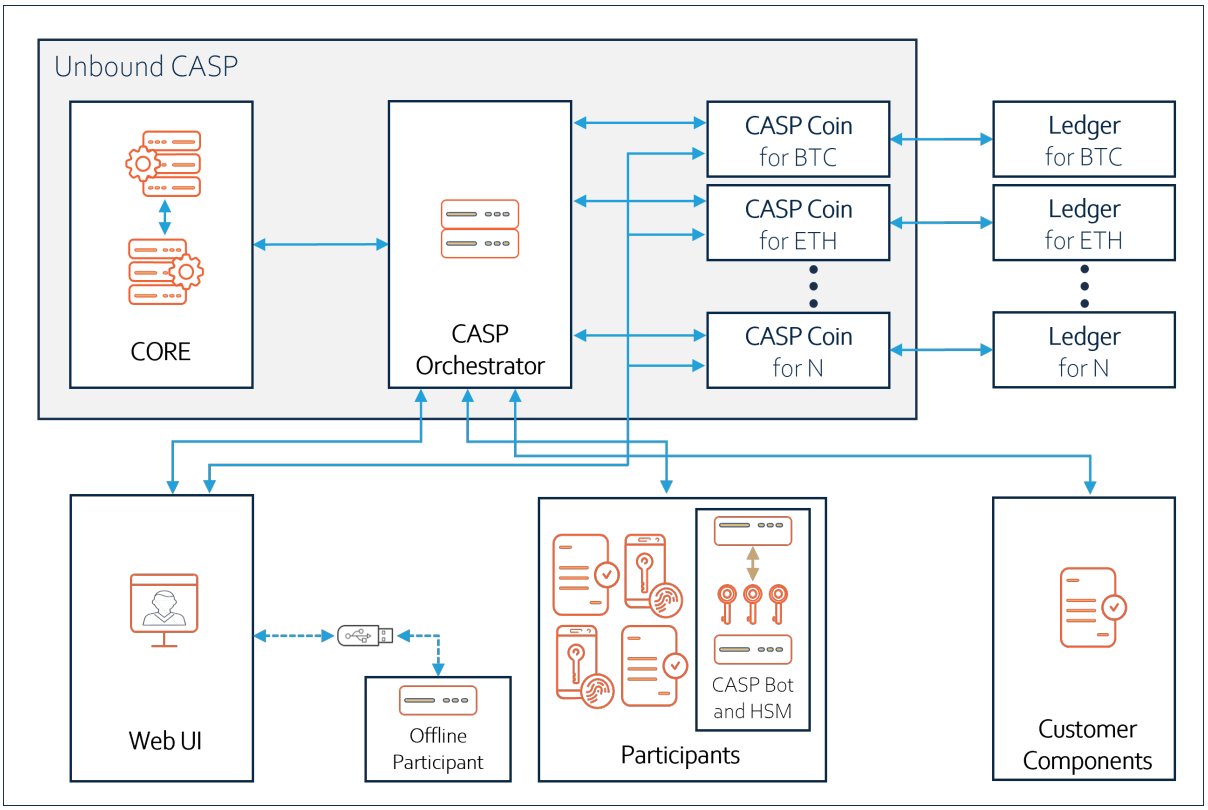
CASP provides integration with the nodes of BRD using their Blockset product. Blockset by BRD is designed for blockchain data with wallets, blockchain explorers, and data aggregators in mind - and (unlike raw full nodes) is designed to handle unlimited scale. Blockset by BRD handles the full nodes, pipes the data into a straightforward schema, and makes it publicly accessible via the blockset API.

2.4.6. Does CASP support completely offline participants?

Yes. CASP supports bots that do not have any network connection and only send and receive information by manually transferring the data using hard media, such as a USB drive. See Offline Bots for more information.

2.4.7. Does CASP integrate with HSM's and/or secured key stores?

The CASP bot can be integrated with an HSM. Integration is accomplished using the CASP Java SDK to extend the CASP bot capabilities, allowing it to store data and create keys in an HSM. The integration is shown in the following figure.



2.4.8. Is CASP easy to demo and test?

Yes. CASP can quickly be installed and used for demos, POCs, and development using CASP Express Deploy. This solution is a complete CASP system that is deployed and configured using Docker or Terraform.