Crypto Valley

Trusted Key Ceremony Guidelines

Guidelines for Generating Digital Asset Secrets

Presented By CVA Cybersecurity Working Group

cybersecurity@cryptovalley.swiss

www.cryptovalley.swiss

@thecryptovalley

Table of Content

Trusted Key Ceremony Guidelines

Summary

Custodians and holders of digital assets need to know that the secrets and private keys stored in their wallet infrastructure cannot easily be guessed or seen by anybody.The initialization phase of the wallet infrastructure and private keys is critical to overall cybersecurity, and therefore should follow a strict protocol usually called "key ceremony".

This guideline brings together best practices from dozens of years of experience across Crypto Valley. It aims to improve awareness of protection of digital assets for everybody by helping practitioners at custodians and holders of digital crypto assets design or improve high security key ceremonies.

Introduction

In the realm of cryptocurrencies and digital assets, the keys to the kingdom are cryptographic secrets – seeds or private keys. If compromised, they can be used to steal your funds[1], and if lost, then the funds are lost as well. The risk is amplified when you are an organization managing millions or billions worth of assets with the involvement of various people, processes, and technical components. It is therefore critical to generate cryptographic secrets in a way that no unauthorized party can determine their values, and that they can be recovered by authorized parties in case of loss or disaster.

Organizations that want to securely manage digital assets therefore need a well-defined procedure to securely generate and backup secrets.

Such procedure is needed whether the underlying technology custody technology relies on

- Pure software (such as some hot wallets or multi-party computation-based methods);
- Software and dedicated hardware (such as hardware security modules);
- as well as whether secrets are generated
- directly as private keys, or
- as seeds from which keys are derived;
- in a centralized, or in a
- distributed manner;

In any case, the secrets must be generated securely, preventing unauthorized access, and be recoverable in case of loss. The associated processes and technology must be auditable for transparency towards customers, auditors, or regulators.

That is why, **a key ceremony is needed**.

[1] or to control the related assets

This report will not tell you how to carry out your key ceremony—which hardware to use, which randomness generator to use, and so on. The adequate level of security that needs to be implemented should be assessed based on the considered usage. There is no single correct way to perform a key ceremony, but there are many wrong ones, and our goal is to help you identify these through a Q&A format covering some of the most important points and preventing common shortcomings.

What Are the Goals of a Key Ceremony?

The main goals of a key ceremony are the following:

1. **Generate secrets securely**, such that nobody before or after the ceremony can determine all or part of the secrets.
2. **Perform backups in a secure way**, that is, such that recovery is guaranteed to work, and that access to the backups is adequately restricted, monitored, and logged.
3. **Be able to demonstrate**, to customers and other stakeholders, that 1. and 2. were carried out according to the documented procedure[1].

What Happens During A Key Ceremony?

A key ceremony is a procedure involving a number of operations carried out by participants with well-defined roles and responsibilities. For an example of such roles, please see the IANA's Key Ceremony Roles document[2]. Concretely, what happens during a key ceremony is typically the following:

- Several participants meet in-person or virtually in order to carry out the required steps.
- All actions and exceptions to the protocol are recorded and noted by an independent witness
- The hardware and/or software to be used is verified to be in a state suitable to generate secrets.
- Generation of secrets using a pseudo-random generator.

[1] and to assess in parallel on their own whether they consider the procedure up to the adequate level for the considered applications.

[2] https://www.iana.org/help/key-ceremony-role

- Creation of backups of the secrets, either by directly copying secrets to other media or devices, or by using some threshold secret-sharing scheme in order to distribute trust to multiple components and persons.

A key ceremony therefore requires people with assigned roles and responsibilities, pre-established processes, and reliable technology components (software and hardware).

Where Does the Concept Come From?

Key ceremonies existed before digital assets, and are a special case of ceremony protocol, as a concept studied in academic literature. For example, Ellison's seminal *Ceremony Design and Analysis*[3] proposes the following definition: "The concept of ceremony extends the concept of network protocol by including human beings as nodes in the network. Ceremonies include all network protocols as a degenerate case, but also all applications with user interfaces and all instances of workflow."

Key ceremonies are the process aiming to securely generate keys and are for example carried out by certificate authorities to generate root certificate keys, or during the coordination of internet resources. Other documented examples include the DNSSEC root signing ceremony[4], and in the blockchain world Zcash's ceremony[5]. Another common method to increase security by distributing trust is secret-sharing protocols[6].

[3] https://eprint.iacr.org/2007/399.pdf

[4] https://www.iana.org/dnssec/ceremonies

[5] https://electriccoin.co/blog/the-design-of-the-ceremony/

[6] https://cypherpunks.ca/~iang/pubs/mindgap-popets20.pdf

We Don't Do A Ceremony but Secure Key Generation Process, Is This Fine?

Key ceremonies differ depending on the organization performing them. What they have in common are some or all of the following elements: securely initializing the hardware and software used to store secrets, securely creating the secrets, and performing the steps required to protect against loss (that is, backups). As long as the key requirements of security, segregation of duties, ability to restore the keys, and auditability are given, we speak of a key ceremony.

What Should Be Prepared in Advance?

As with most things, preparation is key. Most of the work related to a key ceremony happens before the ceremony happens. This is to enable a smooth ceremony, and to have enough material to share with customers, auditors, and regulators, and provide security assurance about the process.

Preparation of a general key ceremony notably involves:

- Creation of a **ceremony storybook** template. Please see the next question for details.
- Evaluation and selection of **authorized software and hardware** components.
- **Ensure auditability**: Is there enough material to give a sufficient audit trail and evidence of all the steps carried out? Think of video footage, photos, signatures of participants, and other artifacts that may be of help.
- Creation of **software scripts and programs**, for example to automate operations in order to reduce the ceremony time, and to minimize the risk of human error.
- Consider performing a **security audit** of critical software and hardware.
- Mitigate the risk of supply-chain attacks or failures, for example make sure that pick-up and drop-off are securely performed and that access to storage facilities is restricted.

Preparation for a particular key ceremony:

- Make sure you have a **ceremony storybook template** suitable for the ceremony to be organized, in particular regarding the types of digital assets involved.
- **Select the personnel** involved in the ceremony, assign them roles, making note of their function in the organization, their skill set, and any conflicts of interest or segregation of duty issues this may give rise to.
- **Inventory the components** involved in the process and assess their trust level. List serial numbers of all devices used, if already available, and software versions.
- **Rehearse the ceremony**, including writing of detailed minutes.
- Make sure that the **ceremony room is clear** of disturbances (noise, electromagnetic, etc.) and of recording devices.
- **Acquire the hardware** needed for the ceremony (laptop, printer, etc.).
- Prepare **tamper-evident containers** (such as sealed bags) to store all smaller components for added security.
- If you include external suppliers, make sure to attach the **transport evidence** of pick-up and drop-off at the secure location.

What Are the Important Aspects of a Ceremony Storybook?

The ceremony storybook is the documentation of the process, technology, roles and responsibilities, and operations to be performed during the ceremony. It is the document that you will show to customers, partners, or auditors to demonstrate that your secrets are adequately protected from theft and loss. The exact content and structure of the storybook depends on your environment, but in any case, will likely include the following important points:

- Description of **roles and responsibilities**, with as typical roles: master of ceremony, operator, witness and auditor. Make sure that there is no segregation of duty issue with any of the people involved.
- **List of participants** and mapping to the roles, signed by participants.
- **Date and location**, description of secure facilities used.
- **Versions and serial numbers** of hardware used during the ceremony.
- Verifiable **checksums or authenticity certificates** of used software and scripts.
- **List of steps** to be performed. Non explicit or passive actions can be stated, such as “the auditor checks that serial number is correctly written down.”
- Placeholders for participants' **signatures and comments**, to confirm that the process was executed as specified.

Who Should Participate in a Key Ceremony?

Participants in a key ceremony can be technical or non-technical persons. Organization members, leading (executive / board members), technical experts, operational staff are all eligible, but make sure that the choice of the person can be justified. Think ahead whether the person's involvement in the key ceremony may cause segregation of duty problems later down the line during operations. You should also include at least one independent observer as a witness, for example an auditor or notary.

How to Make Sure That the Software and Hardware Used Are Secure?

There are several ways to reduce the risk related to vulnerabilities in hardware and software components. For software, best practices include:

- The use of **established components**, as opposed to, for example, recent code put on GitHub by anonymous persons, or old and unmaintained applications.
- **Update** of all software components to their latest versions.
- Minimizing the number of **third-party software** components and in particular the number of software dependencies.
- **Avoid pre-installed software**, including operating systems.
- Performing a **security audit** by an external, established firm.
- If possible, **avoid connecting** to untrusted networks, in particular to internet, prior to the ceremony.
- Verifying the **integrity and authenticity** of software components used, ideally leveraging a secure boot mechanism.

Note that there might be software components that must be trusted and can't be fully verified, such as operating systems, hypervisors, or build toolchains. For a summary of this problem, we refer to Thompson's famous lecture[7].

[7] https://www.cs.cmu.edu/~rdriley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf

As far as hardware is concerned, make sure that they are from a reputable vendor (include certificates and receipts in the documentation), prefer laptops with some security hardening (such as secure boot), prefer hardware security modules (HSMs) or similar secure components with meaningful security certifications.

How to Make Sure That People Can Be Trusted?

A ceremony should not rely on the trust in a single person, but instead distribute trust and include separation of duties and trust-but-verify processes. It makes sense to run background checks on all personnel involved in the ceremony. During a key generation process, the 4-eye principle should be ensured at all times: all participants present should be able to verify every step taken, and no operation should be performed by one unsupervised person alone. This includes transport to external locations and access to backups. If there is more than one ceremony, you should consider rotating the staff taking part.

Should Creation of the Backups Be Part of the Ceremony?

Backups, or more generally recovery values, must inevitably be created during a ceremony, as they involve secret values. The ceremony must also specify how said values are verified, how tamper evidence is guaranteed, and how transport to a secure location (such as a safe) is performed. Ideally, a chain of custody should be documented—i.e., who accessed or transported which backup at which time. Likewise, an access management process should specify adequate access control to backup values. Consider multiple signature requirements for access requests, as well as access logs. Finally, the recoverability of the backup should be tested before taking the solution into production.

It is crucial that your assets remain accessible at all times, including in disaster scenarios. Therefore, the recovery process should be fool proof. Make sure to consider aspects such as hardware failures or natural causes and mitigate these risks by creating backups on several different media, and in georedundant locations. For additional

security, you may want to devise a process where you test your backups every 6 months to make sure all devices work as planned, and your backup plans are still safe.

What Are Secure Ways to Generate Random Secrets?

Although randomness generation might be the easiest problem you'll have to solve when preparing a ceremony, it is of utmost importance, thus you must do it right and be capable of demonstrating the reliability of your key generation tools. There are essentially two aspects to worry about in a random generator:

- The **internal logic** of the cryptographic pseudo-random number generator (PRNG) used, which is a system that draws unpredictable bits from some analog sources and eventually returns a stream of pseudo-random bits that are uniformly distributed, and fulfill the security requirements of a cryptographic PRNG (namely, that it must be impossible to deduce unknown output bits from known output bits).
- The **sources of entropy**, or the analog sources of unpredictability used within the PRNG. On mainstream operating systems, it includes a combination of various sources such as clock, disk activity, system interrupts, as well as on-chip randomness sources if available. Entropy level is hard to quantify, but a heuristical lower bound is preferable.

These two components should be documented, auditable, and trustworthy enough. There is not one single best approach to this, and there are several standards to draw from. For example, an established open-source system, having undergone multiple security audits, and widely used for critical applications, would likely be acceptable. Likewise, a hardware cryptographic module including a random generator compliant with NIST SP 800-90 series and used via a secure interface would also be acceptable.

Furthermore, ensure that no one before or after the generation has access to info that could be used to recover the seeds by securely erasing any data used to generate seeds from any storage device before the end of the ceremony. This may take the form of wiping disks several times, or destroying materials used as a data source.

Are There Any Established Standards or Guidelines Available?

There is currently no standard regarding key ceremonies for cryptocurrencies. The most relevant reference is the recent Digital Assets Custody Standard (DACS) from CMTA[8], which includes comprehensive requirements and recommendations regarding key generation and recovery processes, aimed for financial organizations. The Cryptocurrency Security Standard[9] may also be a useful reference.

Authors

This document is an initiative from CVA's Cybersecurity Working Group, with contributors including security experts from leading organizations such as digital asset custody technology providers, auditing firms, blockchain organizations, and financial institutions. Several of us have designed, operated, and reviewed key ceremonies for regulated institutional firms.

[8] https://www.cmta.ch/

[9] https://cryptoconsortium.github.io/CCSS/Details/

Building the World's Leading
Blockchain Ecosystem
www.cryptovalley.swiss