2016

CONCLAVE SECURITY

AN OVERVIEW OF THE SECURITY ELEMENTS OF THE CONCLAVE SYSTEM

A letter to the reader:

Conclave is for anyone. Anyone that wants to restore trust in our cyber world. Conclave was built so that cyber security and privacy are not privileges, or something that requires a specialized degree to understand. Conclave is bringing cyber security to everyone, on all their devices.

This document serves to provide Conclave users with insight into the Conclave system's security in all areas of the architecture, development, and organization. Included are details about system architecture, specific implementations of security and cryptography, and details about internal processes that ensure that we are safeguarding our user's data, and more importantly, their online and offline identity. Trusting a third party to securely store and maintain your privacy begins with transparency. If after reading this document you have outstanding questions about how we operate, our technology or why you can trust us, please contact us at contact@Conclave and will happily answer your questions.

Never compromise,

The Conclave Team

SECURITY in the Organization

The identity of Conclave is defined by a commitment to never compromise the security and privacy for our customers. This whitepaper is intended to provide the information necessary for anyone to understand how serious Conclave takes security. Being security and privacy conscious is encouraged, and this paper serves to provide additional information to those who seek it.

The security architecture of the Conclave system is founded on the security principles outlined in the Federal Government's Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.

This document includes details about the foundational elements of Conclave security programs and technical implementations in the areas of: Personnel Security, Application Security, Infrastructure Security, Logging and Continuous Monitoring, Incident Response, Physical Security, Third Party Security, and Compliance.

Security is a priority for every member of the Conclave team at all levels of the organization. Questions regarding security or any of the content contained in this document can be directed to the attention of contact@Conclave.

SECURITY for the People

Background Checks and Personnel Management

Conclave LLC enforces FedRAMP Moderate compliant personnel screening and personnel-based action enforcements on Conclave operational information systems. All Conclave employees are required to be US Citizens and are screened, including background checks, prior to hiring. Conclave deactivates all user accesses upon termination or transfer from the organization.

Training

Once yearly, all Conclave employees receive a security briefing from a Conclave security representative to be made aware of applicable policies, standards, and procedures related to the security of Conclave systems. This briefing also serves to provide insider threat awareness and response procedures. Employees of Conclave will be trained for respective positions and made aware of applicable security risks. Conclave security briefing(s) can be made available upon request.

SECURITY in Development

Configuration Management

All Conclave employees implement and maintain Configuration and Change Management processes for the change and deployment of Conclave updates. Configuration management consists of the following sub processes:

- Establishment of baseline(s)

- Data management
- Configuration Identification
- Interface Management
- Configuration Control

Change management consists of the following sub processes:

- Track system changes
- Communicate system changes
- Make effective risk-based decisions to maintain the Conclave system's mission capability, security posture with minimized risk
- Implement changes, which consist of the following steps:
    - Plan
    - Notify
    - Develop
    - Test
    - Deploy

Code Review

All deployable builds are first fully regression tested and validated prior to any deployment activity being performed. Conclave downloads new protection mechanisms (signature databases, others) as recommended by the tool providers to remain abreast of current threat vectors and vulnerabilities. The Conclave continuous monitoring plan includes regular security scans of all conclave operational systems, including code. File transfers from external sources are scanned on transfer. The continuous monitoring plan additionally dictates the frequency and reporting of scanning of the Conclave system. Code is additionally peer reviewed for unexpected changes as part of the development process.

Development Testing

As part of the software update process, Conclave has a development environment which supports evaluation of updated virtual machines prior to operational deployment. Conclave developers install and review changes in the development environment and evaluate impacts to the operational Conclave software. Only upon approval are updates deployed into operations.

Developer Identification and Authorization

All Conclave information systems require that users uniquely identify and authenticate into Conclave systems. Authentication of Conclave personnel is achieved with passwords, tokens, multi-factor authentication, or a combination of these methods. Methods to resist replay attacks are used for all key exchanges for logging into Conclave systems.

To gain access to any Conclave information system, regardless of content, authenticators and passwords for personnel and devices adhere to the following guidance:

- A minimum and maximum lifetime restriction and reuse conditions for passwords
- Password integrity, strength, and length enforcement at the interface level
- Guidance for safeguarding keys, tokens, password, or any authenticator

Conclave guidance and procedures for initial authenticator distribution, for lost/compromised or damaged authenticators or passwords, and for revoking authenticators are all enforced by Conclave systems. Authenticators are generated for each individual uniquely for access to any Conclave information system, regardless of content. Passwords that are used in addition to any authenticator are limited in temporal use at the interface level by Conclave information systems. All Conclave systems obscure feedback of all login credentials for all information systems including encrypting keys and not displaying passwords or response phrases.

Developer/Administrator Access Management

Conclave system access is limited to only authorized personnel with specific access privileges and need-to-know/need-to-access. Access is permitted to Conclave information systems to the minimum level required for each authorized user with system access to separate duties and prevent malevolent activities without collusion (insider threat training discusses collusion and access). This least privilege approach allows only authorized access for users which are necessary to accomplish tasks in accordance with job descriptions and Conclave business functions.

Access requests to a Conclave information system are handled in accordance with the Conclave information system access procedures. Only screened individuals are permitted to access information systems. Access is revoked in the event of termination or transfer. Account usage is evaluated and stagnated accounts are deactivated periodically not to be less than once annually.

All information flows within the Conclave information system are treated and handled as if they contain controlled unclassified information (CUI). All information is encrypted and transferred through known elements of the Conclave system as depicted in the system architecture documentation.

In accordance with the Conclave Identity and Access Management Policy, unsuccessful login attempts are limited at the interface level for each Conclave system. Session locks are enabled on all Conclave systems. All access sessions to Conclave operational systems have a rule that they will terminate after four (4) hours of inactivity.

All interfaces to Conclave computing assets require cryptographic protections of information in transit. Conclave requires all approved mobile devices that are authorized into a conclave organization to have full encryption enabled.

SECURITY in the Application

Conclave is an application that runs on Web browsers and Android and iOS mobile devices. Conclave users can use the Conclave application across these devices using their account. This section provides an overview of the security and privacy aspects of the system that are intrinsic to the application itself, including what data the Conclave organization can potentially access, how cryptography is implemented, and the processes that are involved with user interactions with the system.

Information and Data Access

Conclave is a security and privacy centered application and is committed to being a trusted steward of user information. While the conclave system is designed to safeguard all user data, some user data is not encrypted, though it is protected. The information that is not encrypted with a user's private keys is

provided, in addition to how it is utilized within the conclave system. This data is protected by the secure infrastructure Conclave has built and Conclave's adherence to data protection compliance.

User Name

Purpose	Usernames are used to login to the conclave system. Additionally, users can search for contacts by username.

First Name and Last Name

Purpose	Conclave stores users first and last names unencrypted to allow users to search for contacts by name and to allow them to see the names of other users.

Email Address

Purpose	Conclave uses the user's email address to contact them for verification during certain system processes, and to send special offers, alerts, and updates using Mail Chimp. The user can opt-out of these non-critical emails.

User-links and Status

Purpose	Conclave stores the "contact" relationships between users to allow user's contact lists to be synchronized between devices and to perform server-side searches of contacts by username, first name, or last name.

File Directory Structure

Purpose	To allow users to organize and manage their files in a familiar way, Conclave provides a file directory feature ("folders"). The names of these directories are stored in plain text to provide support for server-side sorting and paging.

File Names

Purpose	In support of the file directory structure feature, Conclave stores file names in plain text to provide support for server-side sorting and paging.

Event Metadata

Purpose	To provide the user with persistent notifications of events involving them in the system, Conclave stores this data so that it is available when requested by the web app to provide a "Notifications" interface.

Conversation Metadata

Purpose	Conclave allows users to conduct conversations between fixed groups of users with persistent histories that are available on all of a user's devices. While the content of each of the messages in the conversation are end-to-end encrypted, Conclave must store the participants involved in each conversation as well as the time each message was sent.

File/Folder Share Metadata

Purpose	To allow users to send and share files and folders to one-another, the Conclave system must know which file or folder is to be shared or sent with which user(s). In the case of sharing, a list of the users who have access to the file/folder must be maintained so that the server knows which users it may serve the encrypted file or folder data to and so that it can store the encrypted key for that file/folder for each shared user.

Support Tickets

Purpose	When you contact Conclave to provide feedback or request support, we keep a record of this communication to help solve any issues. We may use this information for internal or external reporting, or to inform you of changes being made to the system to resolve your submission.

Mobile Code

Within the Conclave development environment, developers use approved devices for development and testing of mobile code within the conclave system. All Conclave external interface applications (such as web browsers) are configured to require users to permit specific transfers of mobile code from approved locations.

Algorithms

The following cryptographic algorithms and primitive lengths are used to implement the end-to-end encryption that Conclave provides in its client applications.

Name	Value
Encryption cipher	AES256-GCM
Message digest (MD)	SHA512
Password key derivation function (PKDF)	PBKDF2 using 10,000 rounds of SHA512
Symmetric encryption key length	1280 bits: 256 bits for encryption, 1024 bits for message authentication
Initialization vector length	128 bits
Password salt length	256 bits (Same as key length for encryption cipher)
Authentication tag length	128 bits

Components included in the HMAC	length of cipher name, cipher name, length of curve name, curve name, length of digest name, digest name, initialization vector length, initialization vector, salt length (optional), salt (optional), authentication tag length, authentication tag, cipher text length, cipher text

Server

All requests made from a user's device to Conclave use HTTPS with TLS 1.2 employing one of the following cipher suites.

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Employing HTTPS allows communication between the user's device and Conclave to be protected from eavesdropping. These specific cipher suites have been chosen because they are recognized by the security community to be the strongest widely supported cipher suites.

When the user visits Conclave, Conclave provides the user with a digital certificate (X.509) that asserts Conclave's identity. This digital certificate is digitally signed by the certificate authority (CA) Entrust using an elliptic curve certificate.

Conclave employs FIPS 140-2 validated endpoints on the server side. Clients can be configured to use FIPS 140-2 validated end points.

SECURITY in the Infrastructure

Administrative Access and Control

System administrators are screened and governed by the principles of least privilege as described in the Developer/Administrator Access Management section. System administrators can access any of the data detailed in the Information and Data Access section of this document. System administrator access to the Conclave system is detailed in the Developer/Administrator Access Management section.

Boundary Protection

The Conclave infrastructure implements a secure boundary layer between the application servers that provide services to customers and the public internet. The Conclave boundary is implemented through a combination of AWS provisioning and platforms designed to provide boundary protections such as firewall services and network address translation. The boundary is monitored through both the AWS portal for virtual machine status and audit monitoring, which is provided to Conclave administrators. The Conclave public servers include a firewall service that implements a "deny all, permit by exception" policy. This is true for all communications to the Conclave service. The Conclave system architecture includes an externally facing set of servers (demilitarized zone [DMZ]), which provides network-level separation between the public servers and back-end (private) servers.

Logging and Continuous Monitoring

Audit Logging and Reporting

All User access and User transactions for all Conclave information systems are capable of being logged and retained. Information that is captured and logged will be made available in the event of an internal or external audit upon request. All Conclave systems are configured to log and indefinitely store information that has been deemed as an adequate sample set for the purposes of an audit event. The minimum set of information required for an individual audit event consists of:

- Type of auditable event
- When the event occurred
- Where in the architecture the event occurred
- The source of the event
- The outcome (success or failure)
- The identity of the user/subject associated with the event

All Conclave systems alert appropriate Conclave personnel in the event of an audit logging malfunction or service disruption. All auditable events that are logged are recorded and monitored automatically for values exceeding Conclave determined thresholds and appropriate personnel are notified of incidents. Appropriate personnel are accountable for responding and reporting such situations within the Conclave team for resolution or escalation. If credible intelligence suggests the presence of a known threat or questionable activity has been observed, the frequency, persistence, and threshold sensitivities can be adjusted by Conclave personnel with appropriate permissions.

Audit reports are available at any time upon request, and are periodically requested for internal review. Internal system clocks are all aligned in accordance with the Conclave system architecture for the temporal alignment of audit events. All Conclave system's audit logging is held under the same data protection standards as CUI and can only be accessed in accordance with Identification and Authentication policies for qualified Conclave personnel with appropriate permission s or a need-to-know status in emergency situations.

System Flaw Monitoring

Conclave addresses information system flaw monitoring in two ways. Regarding operating systems and third party products, Conclave monitors national databases (Common Weakness Enumeration) to identify patches for remediation. For the conclave system, Conclave uses a continuous monitoring process that includes regular vulnerability scans to determine flaws in the system. Identification, reporting and remediation are all included in the process.

Threat Monitoring

The Conclave continuous monitoring plan includes regular security scans of all conclave operational systems. File transfers from external sources are scanned on transfer.

Conclave monitors national databases for security alerts and notifications. If any operational software is affected, Conclave follows all approved recommendations for timely remediation. Conclave downloads new protection mechanisms (signature databases, others) as recommended by the tool providers

Network Monitoring

The Conclave operational system provides real-time monitoring of network packet traffic, and uses thresholds and other notifications to receive indications and warnings of potential attacks. These mechanisms run constantly, and Conclave administrators receive email notifications when thresholds are exceeded.

Unauthorized Reuse

The Conclave audit collection system provides indicators of potential unauthorized use. Conclave administrators regularly review audit log information as part of the overall audit process.

Incident Response

All employees, contributors, and managers of Conclave must complete incident response training annually. Conclave incident response training is comprised of industry best practices. As part of the annual training, a simulated "blue flag" scenario is conducted to ensure the appropriate response, resolution, and handling of common and uncommon hypothetical incident scenarios.

Incidents are addressed in accordance with the Conclave incident management plan. Incident Response procedures begin immediately upon detection by Conclave administrators with current annual incident response training. Conclave incident management plans include the preparation, detection and analysis, containment, eradication, and recovery about an incident. All information is logged in an individual incident report that is then filed. All incidents are reported to appropriate personnel and escalated in accordance with the annual training.

Incident monitoring is tuned to the needs of Conclave such that thresholds for monitoring are set in alignment with expected threat vectors and predicted areas of incident. These thresholds can be changed at the discretion of Conclave system administrators and security specialists. Changes to monitoring parameters are logged as part of the configuration description of the Conclave architecture.

Physical SECURITY

All conclave physical infrastructure (computers, hard drivers, network gear, cables, power) physically resides at AWS GovCloud data center locations. This means that conclave inherits all data center physical protections from AWS. The only physical computers used in the Conclave organization are individual workstations used to access conclave systems on AWS. None of those workstations are part of the actual Conclave system.

SECURITY of Third Parties

As much as is prudent, Conclave attempts to avoid the use of third party applications within the conclave system. When necessary, third party applications are selected upon completion of a strict analysis of alternatives to determine the best solution for our requirements. When a third-party application is selected,

security implications are always considered. The considerations relating to the selection of the listed third party applications are provided in this section.

Amazon Web Services

Conclave is built on Amazon Web Services. Conclave is committed to not "owning" any data, and along with the advantages of cloud computing, AWS enables conclave to be truly separated from user data both in physical and electronic access. Additionally, the advantages of cloud computing are passed onto Conclave's users both in convenience, security, robustness, and cost savings.

Supply data to Conclave?	Yes	AWS provides data to Conclave in the form of virtual machine images, software package updates, and information on usage of AWS services.
Receive data from Conclave?	Yes	Conclave uses its infrastructure built on AWS to collect and store both customer data and operational data. For this reason, any information that Conclave has access to could potentially be accessed by AWS.
Process application data?	Yes	AWS provides the services, such as EC2, S3, and VPC that are used to transmit, store, and process the data in the Conclave system.
Provided security	Yes	Data on AWS is protected according to the AWS Customer Agreement

Apple App Store

Conclave relies on the Apple App Store to distribute the iOS Conclave application to Apple mobile devices. Apple provides very strict rules governing the code that is deployed to an iOS device. While Apple can modify application code prior to distribution, resulting in the deployment of an unauthentic version of the Conclave application, Apple's terms of service indicate that this will not happen intentionally, and provides safeguards and tools for monitoring and safeguarding application code.

Supply data to Conclave?	Yes	The App Store provides crash reports including iOS version, phone version, and stack trace to Conclave developers to assist in resolving defects in the app. The App Store also provides anonymized app download metrics.
Receive data from Conclave?	Yes	Conclave provides builds of its iOS App to the App Store for distribution to users.
Process application data?	No	N/A
Provided security	Yes	App builds are signed using Conclave's development keys

		which can be used to verify that the app distributed to users is the same as what was provided to the App Store.

Google Play Store

Conclave relies on the Google Play Store to distribute the Android Conclave application to Android mobile devices. Google Play provides very strict rules governing the code that is deployed to an Android device. While Google Play can modify application code prior to distribution, resulting in the deployment of an unauthentic version of the Conclave application, Google Play's terms of service indicate that this will not happen intentionally, and provides safeguards and tools for monitoring and safeguarding application code.

Supply data to Conclave?	Yes	The App Store provides crash reports including Android version, phone architecture, and stack trace to Conclave developers to assist in resolving defects in the app. The Play Store also provides anonymized app download metrics.
Receive data from Conclave?	Yes	Conclave provides builds of its Android App to the Play Store for distribution to users.
Process application data?	No	N/A
Provided security	Yes	App builds are signed using Conclave's development keys which can be used to verify that the app distributed to users is the same as what was provided to the Play Store.

Entrust Certificate Authority

Entrust Certificate Authority provides Conclave with TLS certificates. These are used to ensure that web traffic being sent and received to and from Conclave is authentic and arrives at its destination untampered.

Supply data to Conclave?	Yes	Entrust provides Conclave with the TLS certificates used to secure communications between the Conclave service and Conclave applications.
Receive data from Conclave?	Yes	Entrust only receives information from Conclave necessary to validate Conclave's identity and to issue TLS certificates.
Process application data?	No	N/A
Provided security	Yes	Conclave's relationship with Entrust is governed by Entrust's Certificate Services Subscription Agreement

Mail Chimp

The Conclave system leverages Mail Chimp for email list management. Conclave will periodically send information to users that elect to receive them. Information regarding application updates, alerts, and promotions may be sent to a user's email address.

Supply data to Conclave?	No	MailChimp does not supply data to the conclave system.
Receive data from Conclave?	Yes	User emails, first names, and last names from Conclave are provided to the MailChimp system to create mailing lists.
Process application data?	No	N/A
Provided security	Yes	Customer information provided by Conclave to MailChimp is governed by MailChimp's Privacy Policy, specifically section 12: "Your Distribution Lists"

Apple Push Notification Service

Apple Push Notification (APNs) Service is a service created and provided by Apple that allows badge, sound, or custom text alert notifications to be distributed to Apple devices from third party applications (in this case, Conclave).

Supply data to Conclave?	Yes	APNs delivers push notifications to the Conclave iOS application as requested by Conclave services.
Receive data from Conclave?	Yes	Conclave is designed to use APNs for delivery of notifications about events that occur in the system. These notifications include a description of the event that occurred (encrypted with a key not available to APNs), counts of various classes of events that have occurred, and an identifier for the APNs subscriber to deliver the notification to. This information is sent to APNs using a TLS connection.
Process application data?	No	N/A
Provided security	Yes	APNs security is implemented as described in the APNs Documentation

Google Cloud Messaging

Google Cloud Messaging (GCM) is a mobile service developed by Google that enables developers to send notifications from developer-run servers to applications on Android devices.

Supply data to Conclave?	Yes	GCM delivers push notifications to the Conclave Android application as requested by Conclave services.

Receive data from Conclave?	Yes	Conclave is designed to use GCM for delivery of notifications about events that occur in the system. These notifications include a description of the event that occurred (encrypted with a key not available to GCM), counts of various classes of events that have occurred, and an identifier for the GCM subscriber to deliver the notification to. This information is sent to GCM using a TLS connection.
Process application data?	No	N/A
Provided security	Yes	Conclave's connection to GCM is secured as described in the GCM Documentation

Stripe

Stripe is a US-based company providing payment capabilities to online and mobile applications. Within Conclave, Stripe is used to manage credit card transactions when a Conclave user elects to upgrade their personal account or add an individual to an organization. Stripe provides PCI-DSS compliance for all payments. With Stripe, each transaction is token based, therefore obfuscating any financial data to would-be attackers. Additionally, no sensitive payment information or data is sent or received by the Conclave system.

Supply data to Conclave?	No	N/A
Receive data from Conclave?	Yes	Interactions with Stripe are presented within the Conclave application, therefore a user input credit card information within the Conclave application. This information is NOT transferred to any Conclave assets and remains within the Stripe system.
Process application data?	No	N/A
Provided security	Yes	All information is protected with Stripe's compliance with Payment Card Industry Data Security Standards.

Compliance

From its inception Conclave has been designed to make compliance easier for small organizations that have compliance requirements imposed upon them, however, security and privacy is not just for organizations with compliance requirements. No one should ever have to compromise convenience, compliance, or cost for privacy and security. Conclave ensures that compliant security and privacy on the web is not a privilege. This section details the compliance aspects of the Conclave system.

DFARS 252.204-7012 and NIST SP 800-171

DFARS 252.204-7012 states:

If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

Conclave implements security controls equivalent to FedRAMP Moderate baseline and complies with the requirements in paragraphs (c) through (g) of 252.204-7012 for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment. Upon request, Conclave will provide its plan of actions and milestones (POAM) – required as part of FedRAMP Moderate.

Additionally, as designed, the Conclave system is structured to not violate NIST SP 800-171 compliance on behalf of the user for any data contained within Conclave. A user may still violate compliance by performing non-compliant activities within the system, but these activities are outside of the control of Conclave. A user may also violate compliance by performing non-compliant behaviors external to the Conclave system.

Export Control and International Traffic in Arms (ITAR)

The Conclave system is designed to not violate ITAR compliance on behalf of the user for any data contained within Conclave. A user may still violate compliance by performing non-compliant activities within the system, but these activities are outside of the control of Conclave. A user may also violate compliance by performing non-compliant behaviors external to the Conclave system.

Recommendations for Internet Behavior

Conclave is only one aspect of operating securely and privately on the Internet. Not all problems can be solved by Conclave, as only data that a user elects to put in Conclave can be safeguarded by the security outlined in this document. The following are recommendations for the diligent, secure use of the Internet for all activities that a user does not perform within Conclave:

1. Don't login to critical web applications from a public computer.
2. Don't cache your username and password in the workstation.
3. Remember to logoff at the end of a session.
4. Use different sets of logins and passwords for different web applications and services.
5. Regularly change your passwords used in critical web applications if a one-time password is not supported.
6. Report abnormal behavior to the service provider immediately.

7. Ensure that the operating system and system components like Internet Explorer (browser) are fully patched and up to date.
8. Install a personal firewall as well as anti-virus software with latest virus signatures. Any anti-virus software should be good enough to detect malware such as key loggers.
9. Don't download software or plug-ins from unknown sources.

Appendix

User Key Bundle

The Conclave applications generate key bundles for users. These key bundles are the basis of the end-to-end encryption and security that Conclave provides. A single key bundle contains multiple keys, each with unique and well-defined roles. The keys within the key bundle are ultimately secured by a user provided password.

Abbrev.	Name	Encrypted with key	Purpose
RK / RC	Root identity private key / certificate (one per user)	PPK	User identity proof, root of trust
SK / SC	Signing private key / certificate (one per user)	PPK	User (privileged) authentication, chain root trust to DC & MC
DK / DC	Device private key / certificate (one per device)	NPK	Device authentication
MK / MC	Media private key / certificate (one per user)	NPK	Media / message encryption / decryption
PPK	Privileged password key	Password	Secure privileged keys (RK, SK)
NPK	Normal password key	Password	Secure normal keys (DK, MK)

User Registration

This is the process to establish a new user account on Conclave.

1. User provides username and password twice
2. App validates that password entries match
3. App posts username to server to check validity & availability
4. If username is valid & available, server generates and replies with a user id, a device id, and unique identifiers for each key-pair to be generated
5. App generates four elliptic curve key-pairs for the RK, SK, DK, MK and two symmetric AES keys for NPK and PPK
6. App generates RC and self-signs with RK
7. App generates SC and signs with RK
8. App generates DC and signs with SK
9. App generates MC and signs with SK
10. App posts RC, SC, DC, MC, username, and a device ID (DID) to server

11. Server checks that each cert has appropriate information and that the signing chain is valid
12. Server replies with challenges for each private key (server generates random string)
13. App signs each of the challenges with the corresponding private keys and sends the signatures to the server
14. Server validates the challenge signatures
15. App uses PPK to encrypt RK and SK, and NPK to encrypt DK, MK
16. App uses keys derived from the password and unique salts to encrypt PPK and NPK
17. User is then prompted if they want to make a local backup of their key bundle (All encrypted public keys, encrypted symmetric keys, and certificates generated in the preceding process.

Login / Authentication

This is the process to authenticate devices with Conclave.

1. App prompts user for username and password
2. App uses password to decrypt the NPK and, NPK to decrypt DK.
3. App posts its username and the device identifier to the Conclave service
4. Server then generates and replies with a challenge
5. App signs the challenge with DK and posts signature to server
6. Server looks up DC based on identifier and username
7. Server validates signature, if valid, creates new session for the device

Privileged Authentication

This is the process to authenticate users with Conclave for privileged actions.

1. App attempts to perform privileged action on server
2. Server responds with a challenge for privileged authentication
3. App sees challenge and prompts user for password
4. App uses password to decrypt the PPK and, PPK to decrypt SK.
5. App signs the challenge with SK and re-attempts privileged action on server with signature
6. Server looks up SC based on user
7. Server uses SC to validate signature, if valid, performs privileged action

Device Registration

If the user wishes to add a new device to access their account, the following procedure is used.

1. Using App on new device, User enters their username and password.
2. App on new device notifies user they must add the device to their account or restore a key bundle backup.
3. User chooses to add the device
4. Using Authenticated App, User selects “add new device”
5. Authenticated App prompts user for password –to verify the identity of user
6. Authenticated App displays the side channel secret (hash of RK + random PIN), and optionally a QR code containing username and side channel secret
7. Authenticated App posts notification to server that new device will be logging on soon with the random PIN
8. Using App on new device, user enters the side channel secret from the Authenticated App (Alternatively user could capture the QR code from the Authenticated App)

9. App on new device posts username and random PIN from the side channel secret to the server
10. Server checks if the random PIN is valid for the username
11. Server replies with RC, SC, MC, user information, a new device id and creates a temporary session for the new device
12. App on new device hashes the server provided RK and verifies that its hash matches hash from the side channel secret
13. App on new device generates key pair DK2, a corresponding certificate signing request DREQ, and encrypts that signing request with RC.
14. App on new device sends encrypted DREQ to server
15. Authenticated App gets encrypted DREQ from server and decrypts using RK
16. Authenticated App generates DC2 from DREQ and signs using SK
17. Authenticated App encrypts RK, SK, and MK with DC2
18. Authenticated App posts DC2, and encrypted RK, SK, and MK to server
19. App on new device gets DC2, and encrypted RK, SK, and MK from server
20. App on new device generates PPK2, NPK2, decrypts RK, SK, and MK with DK2 and re-encrypts RK and SK with PPK2, and DK2 and MK with NPK2
21. App on new device validates its certificate bundle (RC, SC, DC2, MC)
22. App on new device gets challenges for each of its private keys from the server
23. App signs each of the challenges with the corresponding private keys and sends the signatures to the server
24. Server validates the challenge signatures & if successful, marks device as added

Symmetric Cryptography

Encryption Process

1. Generate a new random symmetric encryption key -OR- Generate a new random salt value and use the password key derivation function (PKDF) with the salt and provided password to generate the symmetric encryption key.
2. Generate a new random initialization vector (IV).
3. Initialize the selected encryption cipher using the initialization vector (IV), and the portion of the symmetric encryption key reserved for encryption.
4. Enter (optional) additional authenticated data (AAD) into encryption cipher.
5. Get cipher text by encrypting the plain text using the encryption cipher.
6. Get the counter mode (CM) cipher authentication tag (AT).
7. Calculate hashed message authentication code (HMAC) of the specified components using the selected message digest (MD) and the portion of the symmetric encryption key reserved for HMAC.

Decryption Process

1. Calculate hashed message authentication code (HMAC) of the specified components using the selected message digest (MD) and the portion of the symmetric encryption key reserved for HMAC.
2. Ensure that the calculated HMAC matches the stored HMAC.
3. Initialize the selected encryption cipher using the initialization vector (IV), and portion of the symmetric encryption key reserved for encryption.
4. Enter (optional) additional authenticated data (AAD) into encryption cipher

5. Get plain text by decrypting the cipher text using the encryption cipher.
6. Set the counter mode (CM) cipher authentication tag (AT).
7. Check that the authentication tag (AT) is correct.

Messaging

Conversation Start

1. User chooses to converse with a set of other users (participants)
2. App checks the server to see if this conversation already exists
3. If the conversation already exists
    a. Server replies with the user's encrypted key for the conversation
    b. App decrypts the conversation key with MK
4. If the conversation does not exist
    a. App retrieves the participants' MC from the server
    b. App generates a new random key for the conversation
    c. App encrypts the conversation key with each participant's MC (including their own)
    d. App sends the encrypted conversation keys to the server

Message Encryption Process

1. User enters a message and selects send
2. App encrypts the message using the conversation key
3. App sends the encrypted message using the message delivery protocol

Message Decryption Process

1. Message arrives from the message delivery system -or- conversation history retrieved from the server
2. App decrypts the message using the conversation key and displays to the user

Media Sharing

Media Encryption Process

1. User chooses to upload file to upload
2. App generates a new random key for the media: "media key"
3. App encrypts the media key with MC
4. App sends the metadata of the media and encrypted media key to the server to prepare for upload
5. Server replies with a "chunk size" for the media to be broken up into
6. App reads "chunk size" of the media to be uploaded and encrypts using the media key
7. App uploads the encrypted media chunk to the server
8. Steps 5-6 repeat until the entire media has been encrypted and uploaded
9. The server detects that all media chunks have been uploaded and makes the media available for download

Media Decryption Process

1. User chooses to download media
2. App gets the metadata and encrypted media key of the media from the server
3. App decrypts media key's using MK
4. App downloads an encrypted chunk of the media from the server
5. App decrypts the media chunk using the media key
6. Steps 4-5 repeat until the entire media has been downloaded and decrypted

Media Sharing Process

1. User chooses to share media with another user (recipient)
2. App gets the metadata and encrypted media key of the media from the server
3. App gets the MC of the user to share with from the server
4. App decrypts the media key with the user's MK and re-encrypts it with the recipient's MC
5. App instructs the server to share the media with the recipient using the re-encrypted media key

Folder Sharing

Initialization Process

1. User chooses to convert a folder to a shared folder
2. App generates new random key for the folder
3. App requests media keys of all media within the folder recursively
4. App decrypts each media key using MK and re-encrypts using the folder key
5. App posts the re-encrypted media keys to the server
6. Server ensures that all media keys have a folder key encrypted media key and then marks the folder as shareable.

Sharing process

1. User chooses to add another user (recipient) to the shared folder
2. App gets the shared folder's encrypted key and the recipient's MC from the server
3. App decrypts the folder key with the user's MK and re-encrypts using the recipient's MC
4. App posts the re-encrypted folder key and recipient's identifier to the server
5. Server allows the recipient to access the shared folder