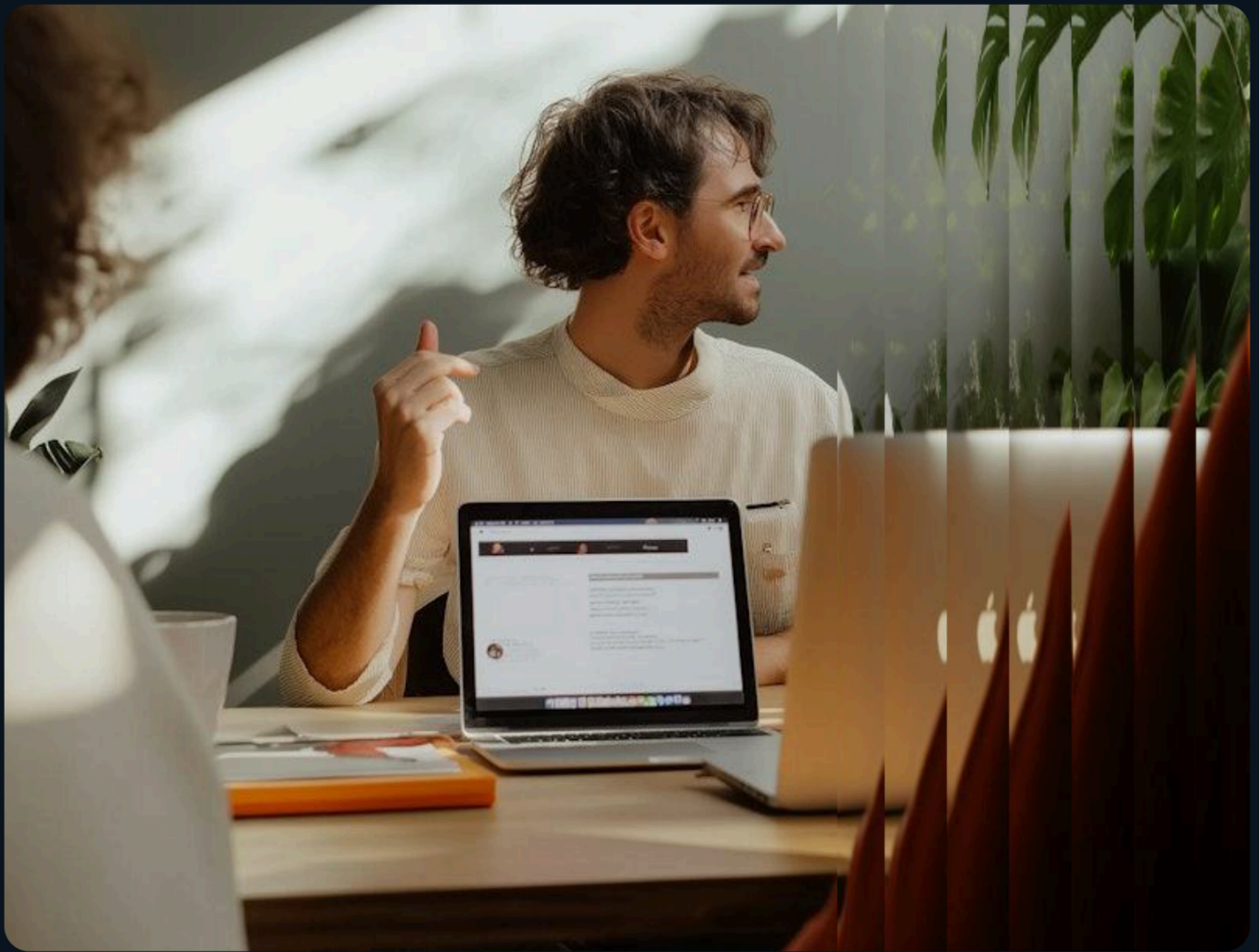




Technical & Security Whitepaper

2026

Uniqkey Security Whitepaper

Password and Access Management Platform

Version: 2.2.1 | Published: October 2026 | Classification: Public

📖 How to Read This Document

This whitepaper serves different audiences. We recommend focusing on the sections most relevant to your role:

🛡️ Security Teams

Sections 2, 6: Architecture & Security

⚙️ IT Administrators

Sections 4, 5, 8, 9: Discovery, Auth, Integration & Ops

⚖️ Compliance Officers

Sections 10, 11: Compliance & Use Cases

📜 Document History

Version	Date	Changes
2.2.1	October 2026	Documented one-time code (TOTP) generation: RFC 6238 with SHA-1, SHA-256 and SHA-512, 6 to 8 digits and configurable period, read from the otpauth profile
2.2.0	October 2026	Added Discovery as a dedicated chapter covering deployment, data collection and minimisation, enrolment, access control and privacy, with related threat model, FAQ and glossary updates
2.1.0	June 2026	Added the Single Sign-On (SSO) authentication model: new SSO section, expanded the authentication models comparison to four models, and documented SSO key protection and integration
2.0.0	March 2026	Major revision: Updated security architecture, added post-quantum roadmap, expanded authentication models, added comprehensive compliance section
1.0.0	October 2023	Initial public release

Table of Contents

	Executive Summary	1
1	Introduction	3
2	Architecture Overview	4
3	Credential Management & Sharing	6
4	Discovery	13
5	Authentication Models	17
6	Security Architecture	25
7	Technical Implementation	39
8	Integration Capabilities	41
9	Operations	43
10	Compliance & Governance	46
11	Use Cases	48
12	Conclusion	50
13	Frequently Asked Questions	52
	Appendix	56

Executive Summary

Why password security still fails

Credentials are involved in nearly 9 out of 10 web application breaches^[1]. Despite widespread adoption of password managers, most solutions still rely on distributed encryption keys, browser-resident secrets, human-dependent recovery processes, and legacy key derivation functions like PBKDF2 that are increasingly vulnerable to GPU-accelerated attacks.

These design choices leave organisations exposed to phishing, endpoint compromise, insider risk, and regulatory uncertainty.

What Uniqkey changes

Uniqkey is an enterprise password and access security platform designed around a single principle:

If attackers breach the server, the browser, or the vendor - credentials must still remain cryptographically unreachable.

To achieve this, Uniqkey enforces a mobile-anchored, zero-knowledge security architecture where encryption keys never exist on servers and are not persistently stored in browsers or desktops.

Security architecture at a glance

Zero-Knowledge by design: All encryption and decryption happens on user devices. Servers store ciphertext only and are cryptographically incapable of accessing credentials - even with full database or infrastructure access.

Mobile-Anchored Key Security: The primary encryption key (EKEK) is stored exclusively on the user's mobile device, protected by hardware-backed secure storage and biometric authentication. This removes browser extensions, desktops, and servers as key-holding attack surfaces.

Reduced attack surface: Even a fully compromised browser extension, desktop client, or Uniqkey backend cannot decrypt vault contents without access to the authenticated mobile device.

Defence in depth across asset classes: Uniqkey's security model protects both primary assets (credentials, encryption keys, master passwords) and secondary assets (identity state, personal data as defined by GDPR, organisation structure, audit logs, session tokens). Primary assets are shielded by end-to-end encryption and mobile-anchored key storage, ensuring they remain cryptographically inaccessible even during a server breach. Secondary assets are protected through access controls, audit logging, and retention policies, limiting exposure of operational metadata that could aid an attacker in mapping the organisation or escalating privileges.

Enterprise-grade recovery without breaking zero-knowledge: Uniqkey enables administrator-assisted recovery without data loss and without exposing credentials, eliminating the traditional trade-off between security and operational continuity.

Designed for real enterprise environments

Flexible authentication models: Mobile-first, Trusted Browser, and Phoneless modes support regulated, shared, and mobile-restricted environments without weakening cryptographic guarantees.

Clear separation of personal and corporate credentials: Private Keychain ensures employee privacy while maintaining organisational oversight and auditability of corporate credentials.

Built for governance, not workarounds: SCIM provisioning, audit logs, policy enforcement, and lifecycle controls are native - not layered on top of consumer security models.

Access management, not just password storage: Instant onboarding and offboarding, shared vaults with group permissions, and credential capture through the browser extension help organisations maintain control and reduce shadow IT risk.

Visibility with Discovery: Discovery maps the web services employees sign in to, how each login is protected, and where shared accounts and weak logins exist, using metadata only. Passwords and field values never leave the browser (see Section 4).

Cryptography you can trust

Uniqkey's cryptographic stack relies exclusively on open, peer-reviewed standards with proven track records:

- **AES-256:** The symmetric cipher trusted by governments and financial institutions worldwide, with no known practical attack after over two decades of cryptanalysis.
- **Curve25519 / X25519:** Designed by Daniel J. Bernstein, adopted by Signal, WireGuard, SSH, and TLS 1.3. Engineered to resist timing side-channels and implementation errors.
- **Argon2id:** Winner of the Password Hashing Competition (2015) and recommended by OWASP. Memory-hard by design, making GPU and ASIC-accelerated cracking orders of magnitude more expensive than PBKDF2, which most password managers still use as their default (see full comparison in Section 6).
- **SRP (Secure Remote Password):** A zero-knowledge protocol that authenticates users without ever transmitting or storing passwords on the server, even during login.

No proprietary cryptography. No security through obscurity. Every primitive is independently auditable.

EU-native security and compliance

Uniqkey is built, hosted, and operated exclusively in the EU, ensuring full GDPR alignment by design and guaranteed EU data residency. Our infrastructure providers are certified to ISO 27001 and BSI C5 standards.

Uniqkey holds **ISAE 3000 Type 2** and **ISAE 3402 Type 2** attestations. Our ISAE 3402 Type 2 is audited against all ISO 27001 control points, combining the depth of ISO 27001's security framework with the rigour of independent assurance that controls operate effectively over a sustained period. Uniqkey has been audited flawlessly for four consecutive years, achieving Type 2 certification in Q1 2026.



Audited by PricewaterhouseCoopers (PwC)

Uniqkey's ISAE attestations are conducted by PwC, one of the Big Four professional services firms and a globally recognised leader in assurance and cybersecurity advisory. Their independent verification provides enterprise customers with confidence in the design and operational effectiveness of Uniqkey's security controls.

As more vendors adopt "EU-hosted" marketing without meaningful legal separation from non-EU parent companies, organisations face growing risks from **sovereign washing**: the appearance of European sovereignty without protection from extraterritorial laws such as the U.S. CLOUD Act. Uniqkey's Danish ownership, EU-only operations, and zero-knowledge architecture ensure that sovereignty is technically enforced, not merely claimed (see Section 10.3).

How Uniqkey stands apart

Most enterprise password managers share a common architecture: keys on every device, US or Canadian corporate jurisdiction, and recovery flows that require user pre-configuration. Uniqkey takes a fundamentally different approach across each of these areas, resulting in a smaller attack surface, stronger regulatory positioning, and fewer operational dependencies. A detailed comparison is available in Section 12.

1. Introduction

1.1 Purpose & Audience

This whitepaper is intended for security professionals, IT administrators, and compliance officers evaluating enterprise password and access management solutions, including Discovery for visibility into the services employees use. It provides a technical examination of Uniqkey's security architecture, cryptographic implementation, and operational controls, enabling informed decisions about credential management infrastructure.

This whitepaper covers Uniqkey's security model, key hierarchy, authentication mechanisms, encryption standards, Discovery, and compliance posture. Infrastructure implementation details that could aid attackers are intentionally omitted.

1.2 Solution Overview

Uniqkey is a zero-knowledge password and access management platform designed for European enterprises requiring data sovereignty and strong security guarantees:

- **Mobile-Anchored Key Storage:** Encryption keys reside exclusively on the user's mobile device, eliminating server-side key exposure
- **Zero-Knowledge Vault:** All encryption occurs client-side; servers store only ciphertext
- **Flexible Authentication:** Mobile-first, Trusted Browser, and Phoneless modes for diverse enterprise requirements
- **Privacy Separation:** Private Keychain keeps personal credentials private - admins can assist with recovery but cannot access contents
- **Enterprise Controls:** SCIM 2.0 provisioning, policy enforcement, audit logging
- **Discovery:** Visibility into the services employees use and how their logins are protected, without credentials leaving the browser

1.3 How Uniqkey Differs

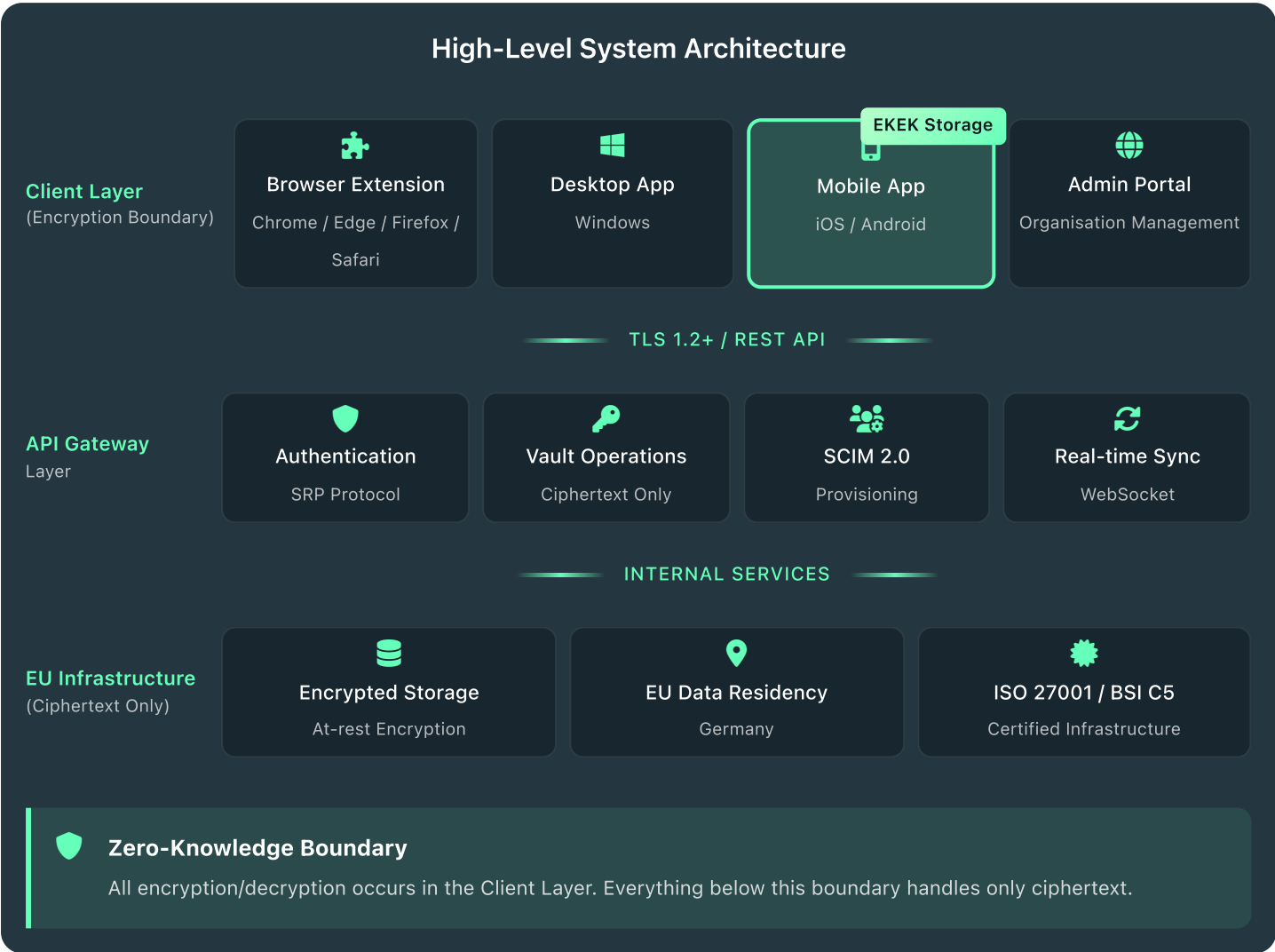
All other major password managers distribute encryption keys across browser extensions, desktop applications, and servers, each a potential attack vector. Uniqkey's mobile-first architecture (detailed in the Executive Summary) means that even if an attacker compromises the browser extension, desktop application, or Uniqkey's servers, they cannot decrypt vault contents without physical access to the user's authenticated mobile device.

For a detailed comparison of authentication models, see Section 5: Authentication Models.

2. Architecture Overview

2.1 System Architecture

Uniqkey's architecture is designed around security boundaries that enforce the zero-knowledge model. The critical security property: encryption keys never leave client devices, and servers only process ciphertext.



Security Boundaries

The **Client Layer** is where all cryptographic operations occur. Plaintext credentials never leave this boundary. The **API Layer** receives and transmits only encrypted data, with SRP (Secure Remote Password) authentication, a zero-knowledge protocol that verifies the user's password without ever transmitting it to the server. The **Infrastructure Layer** stores only ciphertext; even with full database access, vault contents cannot be decrypted.

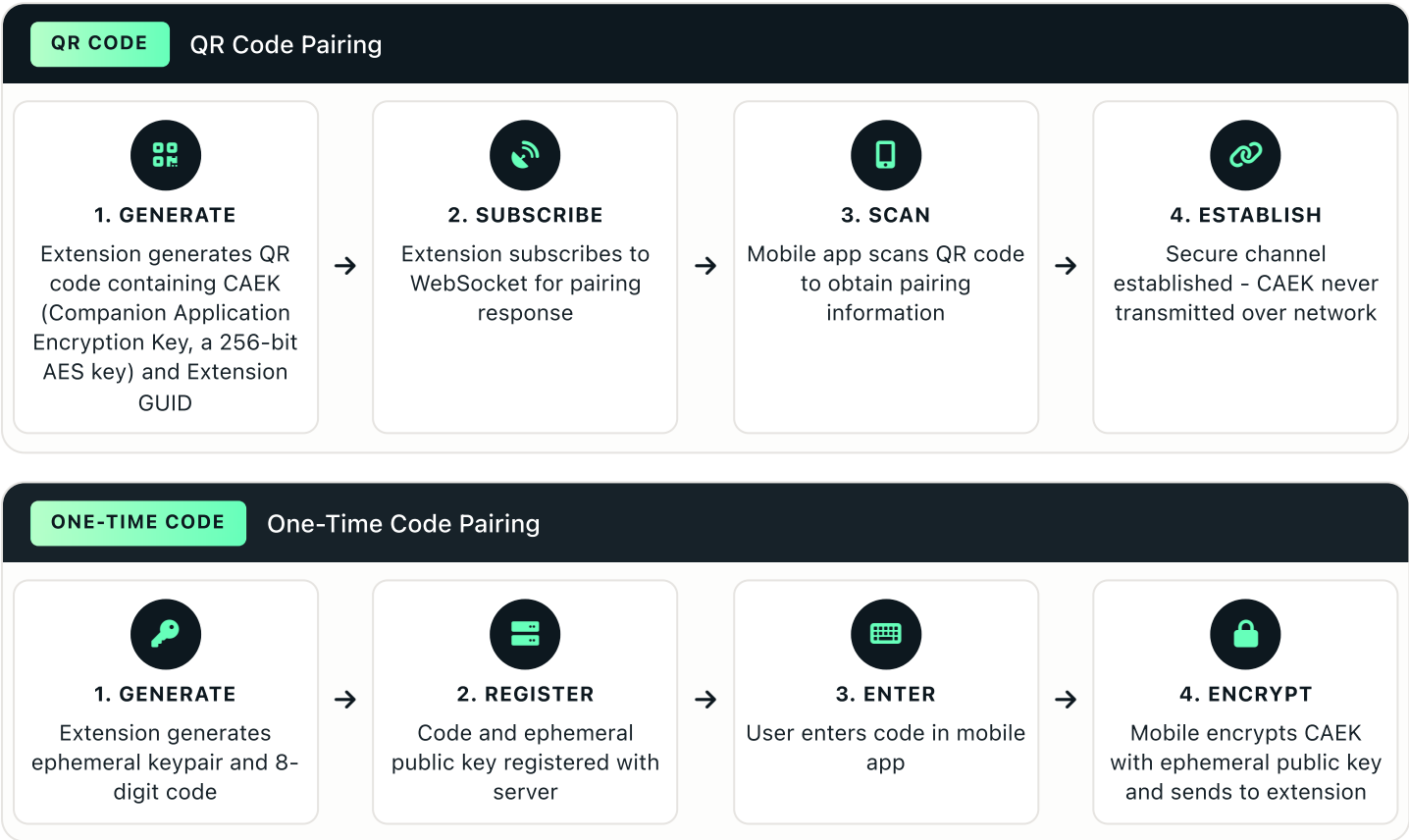
Client Applications

The **Mobile App** (iOS/Android) serves as the primary security anchor, storing the EKEK in hardware-backed secure storage. The **Browser Extension** (Chrome, Edge, Firefox, Safari) handles autofill and credential capture, while the **Desktop App** (Windows) provides native OS integration. Both require mobile pairing. The **Admin Portal** enables organisation management, policy configuration, and audit log access.

2.2 Client Pairing

Uniqkey ensures secure communication between browser extensions, desktop applications, and the mobile app through a cryptographic pairing process. Only paired clients can exchange sensitive data. Pairing is required when signing in to the browser extension, Admin Portal, or desktop app, during account activation, and when registering a secondary mobile device.

Pairing Methods



Secure Client Communication

After pairing, all communication between clients is encrypted with the shared CAEK using AES-256. Messages are encrypted before leaving the device and decrypted only by the paired client, providing true end-to-end encryption. The Uniqkey backend relays these encrypted messages but cannot read their contents. Communication is bi-directional, with both clients able to initiate secure requests and receive responses, supporting complex operations like vault creation and credential retrieval.

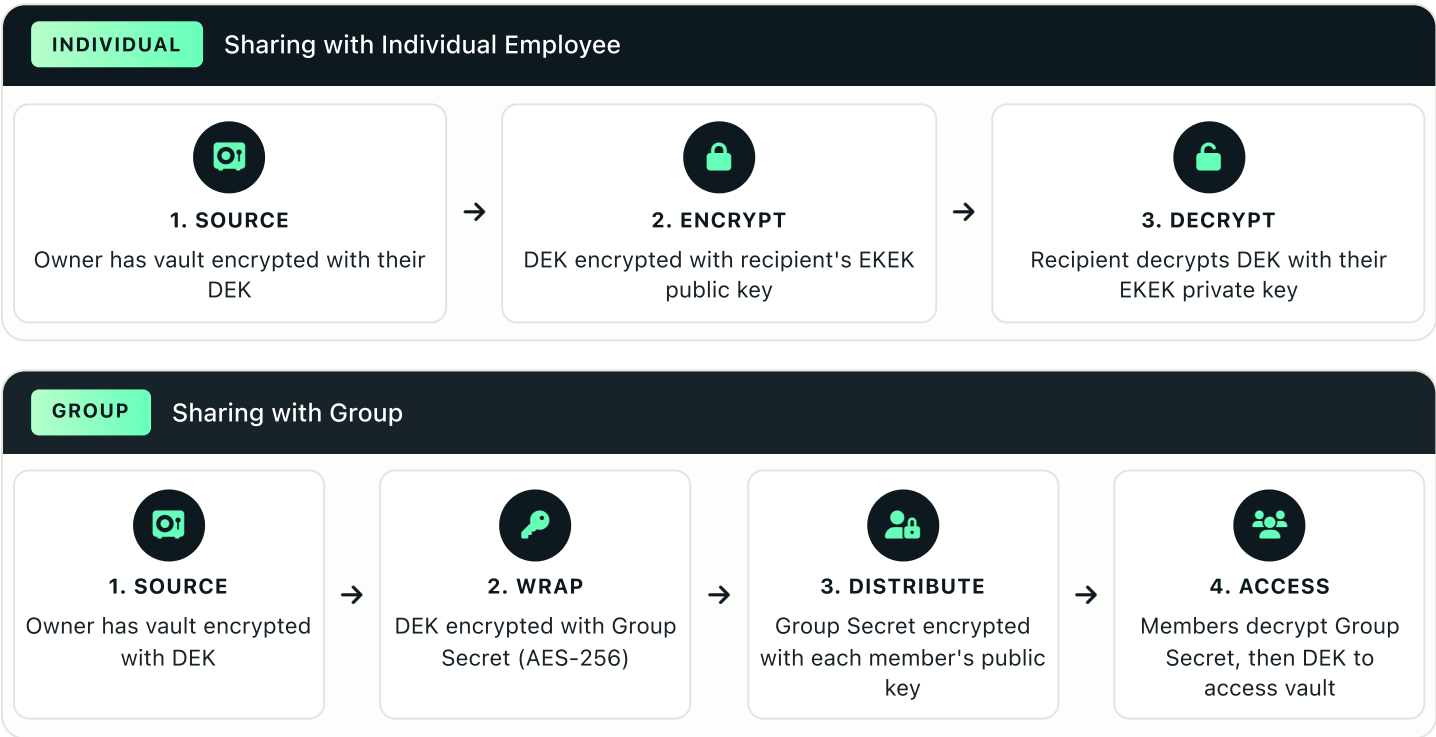
3. Credential Management & Sharing

This section covers credential management capabilities including secure sharing, password generation, breach detection, and organisational controls. Vault sharing, the private keychain, and organisation management all rely on the mobile-anchored key hierarchy described in Sections 1.3 and 2, where encryption keys reside exclusively on the user's mobile device in the default authentication mode. For user interface details and autofill behaviour, see the Uniqkey product documentation.

3.1 Vault Sharing

Uniqkey enables secure credential sharing without exposing plaintext to servers. All sharing operations use asymmetric encryption to transfer Data Encryption Keys (DEKs) between users.

Sharing Flows



Sharing Controls & Audit Trail

Administrators can disable peer-to-peer vault sharing at the organisation level, and control sharing behaviour per group through granular permissions (add, view, copy, edit, delete). Shared vaults can be given a time-based expiration, after which access is automatically revoked. Every sharing operation, including grants, revocations, moves between groups or employees, and expirations, is recorded in the audit log for compliance and forensic review.

3.2 Private Keychain

Uniqkey provides a Private Keychain feature that allows employees to store personal credentials separately from organisational credentials, maintaining a clear boundary between work and personal password management.

Key Differences from Organisation Keychain

 Organisation Keychain	 Private Keychain
<ul style="list-style-type: none">• Keys generated during employee onboarding• Administrator manages access• EKEK backup encrypted with OKEK• Org can recover via OKEK if employee leaves• Vaults accessible to admins for business continuity	<ul style="list-style-type: none">• Keys generated by user on mobile device• No administrator access to vault contents• EKEK backup encrypted with OKEK for recovery assistance• Admins can help recover access, but cannot view data• Vault contents never exposed to organisation administrators

Features

- **Personal Credential Storage:** Store personal passwords, logins, and sensitive data completely separate from organisation-managed credentials
- **Cryptographic Isolation:** Private Keychain vault contents are encrypted with the employee's EKEK. While a backup key exists (encrypted with OKEK) to allow admin-assisted recovery, administrators cannot decrypt or access the actual vault contents - only help restore access.
- **Vault Movement:** Move vaults between Private Keychain and organisational storage. Encryption is properly adjusted when moving between contexts.
- **Survives Offboarding:** When leaving an organisation, Private Keychain remains accessible. Personal credentials are never affected by employment status.
- **Unified Interface:** Both organisational and personal credentials accessible through the same Uniqkey interface - seamless user experience.

3.3 Passkeys & WebAuthn Support

Uniqkey provides comprehensive support for passkeys, the modern passwordless authentication standard built on FIDO2/WebAuthn. This enables organisations to store, manage, and use passkeys alongside traditional credentials.

What are Passkeys?

Passkeys replace passwords with cryptographic key pairs. Instead of remembering a password, users authenticate with biometrics or a device PIN. The private key never leaves the device, while websites verify a signed challenge.

Uniqkey's Passkey Advantage

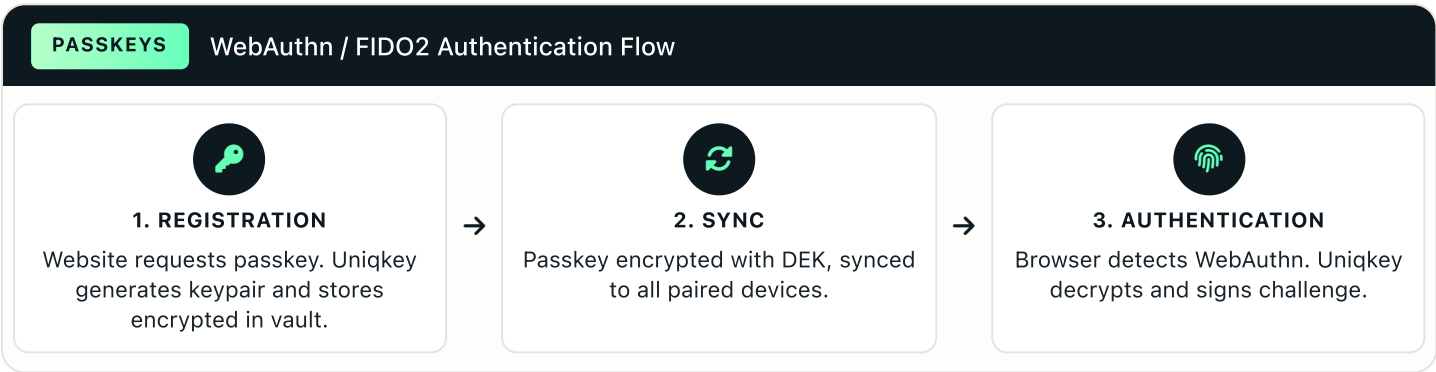
 **Traditional Passkeys Problem**

1. Device-bound: passkey only works on the device that created it
2. Lost devices = lost passkeys, tedious recovery
3. No cross-platform: iPhone passkey does not work on Windows
4. Enterprise management difficult

 **Uniqkey Solution**

1. Passkeys stored in encrypted vault, synced across all devices
2. Same zero-knowledge protection as passwords
3. Works on any platform: mobile, browser, desktop
4. Full organisational sharing and management

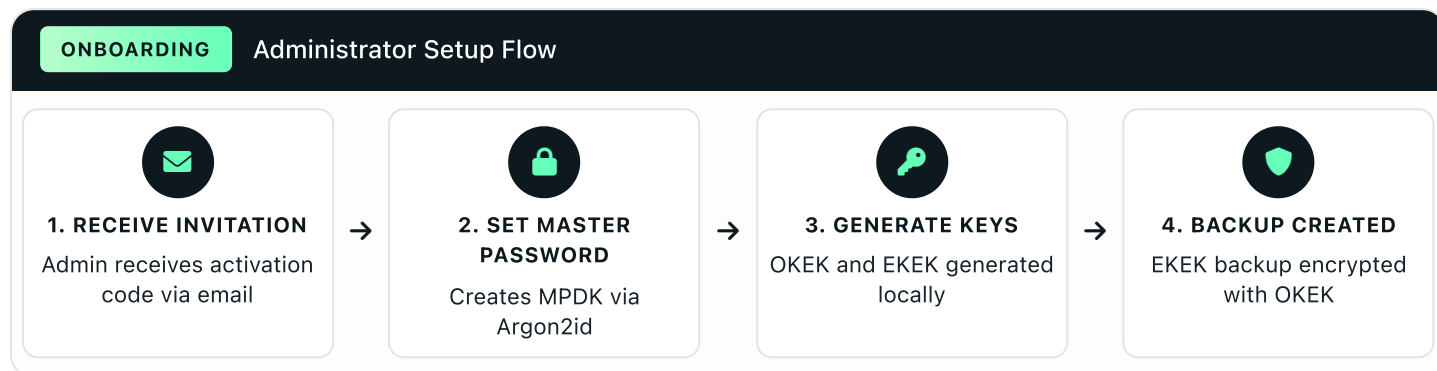
How Passkeys Work in Uniqkey



Group Management

Groups enable secure credential sharing among team members with cryptographic access control. Each group has a unique 256-bit **Group Secret (GS)** for encrypting shared vault DEKs. When adding a member, the GS is encrypted with their EKEK public key, granting access. Administrators can manage group membership without accessing vault contents, maintaining zero-knowledge principles. Removing a member immediately revokes access, and they lose the ability to decrypt the GS.

Administrator Onboarding



Employee Offboarding

When an employee is offboarded, setting their status to "Archived" instantly revokes all access to organisational credentials. The organisation retains access to work-related vaults via OKEK-encrypted copies, while the employee keeps access to their personal Private Keychain. All offboarding actions are logged for compliance.

3.5 Password Generation

Uniqkey includes a built-in password generator that creates high-entropy passwords with configurable length and character sets, helping users create strong, unique passwords for each account.

Random Number Generation

All password generation uses cryptographically secure random number generators (CSPRNGs) via crypto-js's `CryptoJS.lib.WordArray.random()`, which delegates to the browser's Web Crypto API (`crypto.getRandomValues()`). This ensures generated passwords are unpredictable and resistant to statistical analysis.

Why this matters: Standard random number generators (such as `Math.random()` in JavaScript) use deterministic algorithms that can be predicted if the internal state is known. The Web Crypto API's `crypto.getRandomValues()` sources entropy from the operating system's entropy pool (e.g., hardware events, interrupt timing), making output computationally indistinguishable from true randomness. This is essential for password generation, where predictability would allow attackers to reconstruct generated passwords.

Generation Parameters

 **Random Passwords**

- **Default length:** 20 characters
- **Configurable range:** 6-72 characters
- **Character sets:** Uppercase, lowercase, digits, symbols
- **Entropy:** ~130 bits for default configuration
- **Ambiguous characters:** Option to exclude (0, O, l, 1, etc.)

Security Properties

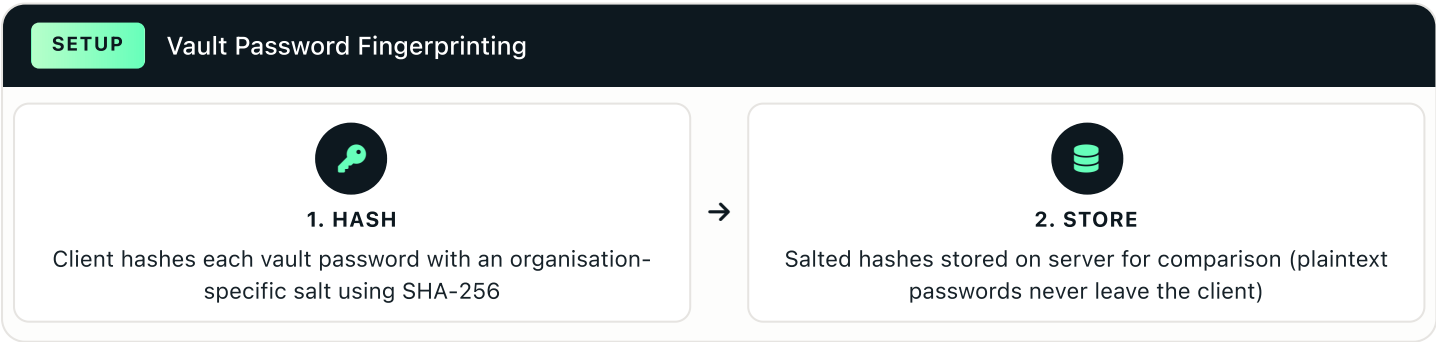
Password generation occurs entirely on the user's device. Generated passwords are never transmitted to or stored on Uniqkey's servers, ensuring that only the user has access to the plaintext password at the moment of creation.

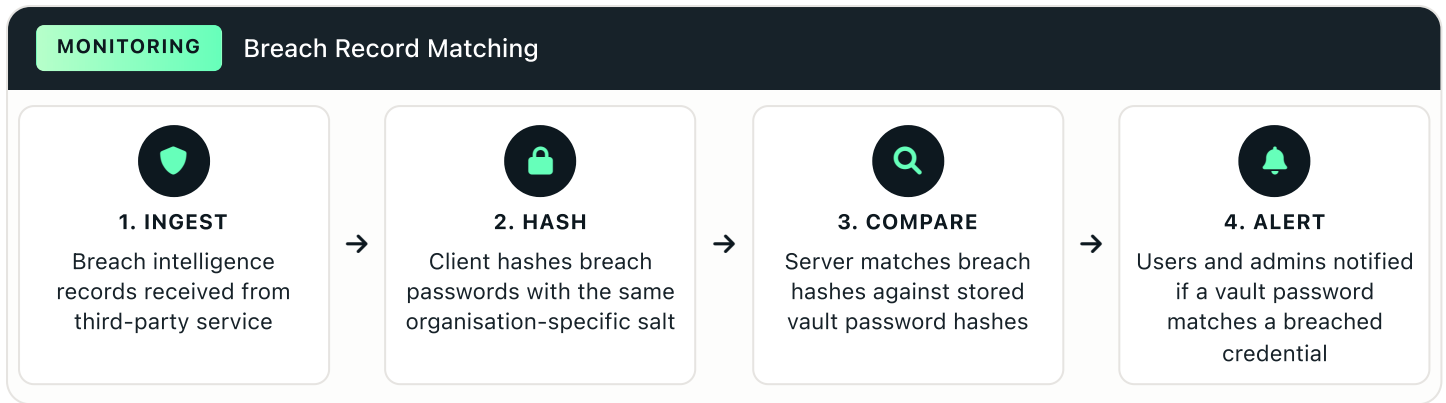
3.6 Breach Detection & Monitoring

Uniqkey proactively monitors credentials against known data breaches, alerting users and administrators when stored passwords appear in compromised databases.

How Breach Detection Works

Uniqkey integrates with an EU-based breach intelligence provider that continuously collects compromised credentials from known data breaches. Vault passwords are hashed on the user's device before being transmitted. Only salted hashes leave the device, never plaintext passwords. The server then compares these hashes against breach intelligence records using organisation-specific salts, ensuring that neither Uniqkey nor a database attacker can reverse the hashes without the organisation's private key.

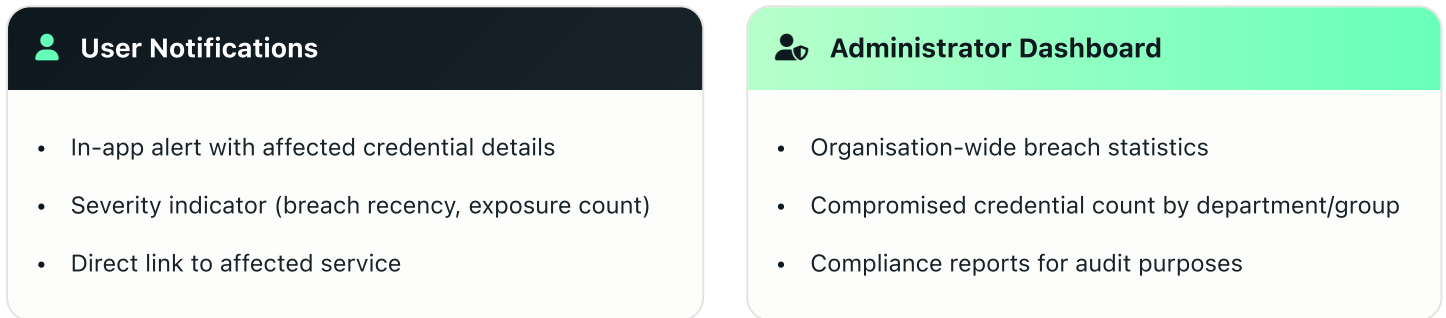




Detection Triggers

- **New Vault Creation:** Passwords checked automatically when saved
- **Periodic Background Checks:** Existing credentials re-checked against updated breach databases
- **Password Updates:** Changed passwords immediately verified against breach data

Alert & Response



Password Protection

Breach detection uses SHA-256 hashing with an organisation-specific salt derived from the organisation's private key. Plaintext passwords are never stored on or transmitted to the server - only salted one-way hashes are used for breach comparison. Because the salt is unique per organisation and only accessible to that organisation's clients, an attacker who compromises the database alone cannot reverse the hashes or correlate them across organisations.

3.7 Reused Password Detection

Password reuse is one of the most common security vulnerabilities in credential management. When users employ the same password across multiple accounts, a single breach can cascade into widespread compromise. Uniqkey automatically detects and flags reused passwords.

How Reused Password Detection Works

All reuse detection happens entirely on the user's device. Passwords are hashed locally using salted SHA-256, then compared against all other vault hashes to identify duplicates. Only boolean reuse flags are synchronised with the backend - actual passwords are never exposed.

Detection Types

- **User-Level Reuse:** Detects when a user has the same password across multiple vaults by comparing password hashes within their account. Affected credentials are flagged with a "reused" status.

- **Master Password Reuse:** Detects if the master password matches any vault password. This triggers a critical security alert, as the master password should always be unique.

Detection Triggers

- **New Vault Creation:** Password hash generated and compared against existing vault hashes
- **Password Updates:** Changed passwords trigger re-evaluation of all related reuse flags
- **Phoneless Mode Authentication:** Full reuse check performed after user authentication
- **Periodic Background Checks (Phoneless):** Vault state changes trigger throttled reuse detection (10-second intervals)
- **Bulk Processing:** Unprocessed passwords are hashed in batches for efficient analysis

Alert & Response

- **User Notifications:** Visual indicators on affected credentials, security score impact, and one-click password updates with the built-in secure generator
- **Administrator Dashboard:** Organisation-wide reuse statistics, user security posture overview, and compliance reporting - all without exposing individual passwords

Zero-Knowledge Preserved

All password comparison operations occur exclusively on the user's device. Only cryptographic hashes and boolean reuse flags are synchronised with the backend - actual passwords are never transmitted or stored in plaintext. The backend receives only vault identifiers to mark as reused.

4. Discovery

Most organisations cannot see which web services their employees actually sign in to, how those sign-ins are protected, or where shared accounts and weak logins are putting the organisation at risk. Discovery gives administrators that visibility, without credentials ever leaving the browser.

Discovery is available as a standalone product or alongside the Uniqkey password manager. It does not require employees to be onboarded to Uniqkey, and it runs on the same EU-hosted platform, under the same security practices, as the rest of Uniqkey.

Discovery at a Glance

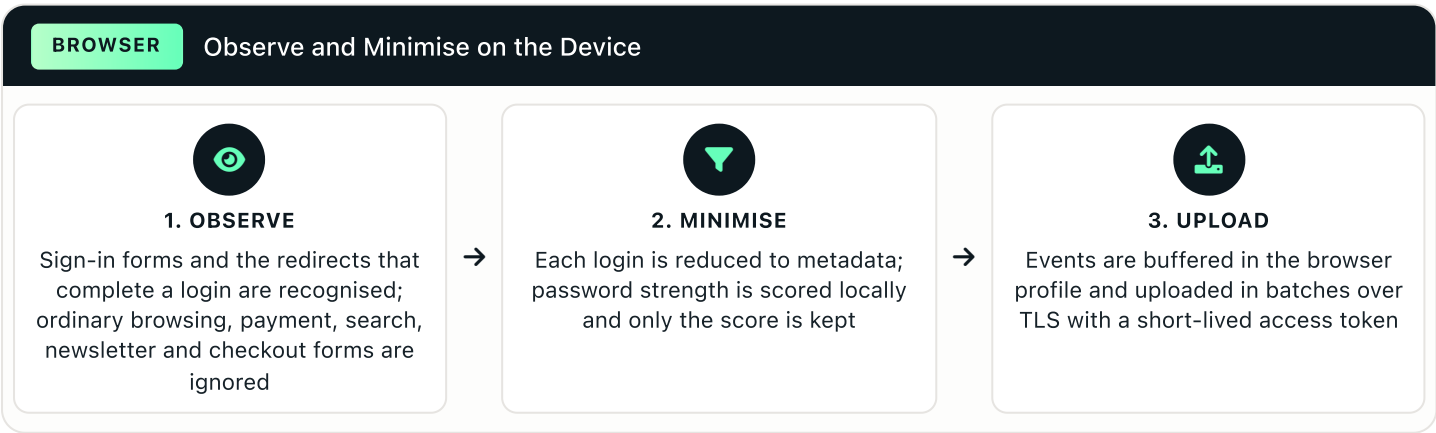
Discovery is **observe-only** and collects **metadata only**. Passwords, one-time codes and field values never leave the browser, sign-in identities are only reported for the organisation's verified domains, and Discovery is **disabled by default** and visible only to administrators.

4.1 Capabilities

- **Service Landscape:** A factual map of the corporate web services in use across the organisation, including newly discovered services, which exposes shadow IT.
- **Login Security Posture:** An organisation security score based on password strength, second-factor and passkey use, and the services with the weakest logins.
- **Shared Accounts:** Accounts used from more than one installation, which indicate shared credentials.
- **Access Adoption:** Second-factor and passkey coverage over time, and the services used without any form of multi-factor authentication.
- **Login Methods & Friction:** The mix of SSO, manual entry, password manager and browser autofill, and where employees experience the most login friction.

4.2 How Discovery Works

Discovery separates what happens on the employee's device from what happens on the platform. Data minimisation happens on the device, before anything is uploaded.





1. INGEST

Events are validated and stored for the installation's organisation only



2. ASSEMBLE

Events are grouped into login flows, detecting SSO redirects, second-factor steps and retries



3. REPORT

Insights are presented to the organisation's administrators in the Admin Portal

4.3 Requirements & Deployment

- **Supported Browsers:** Google Chrome and Microsoft Edge on Windows and macOS. Firefox and Safari are not supported for Discovery.
- **Managed Devices:** Discovery is installed through enterprise browser policy, so browsers must be centrally managed (for example domain-joined, MDM-managed or enrolled in Chrome Enterprise Core). The extension is distributed as a signed package and is not available in public extension stores.
- **Deployment Packages:** Uniqkey provides ADMX/ADML policy templates, PowerShell scripts for RMM tools and macOS configuration profiles. The enrolment token is delivered through the same policy.
- **No Employee Onboarding:** Employees do not need a Uniqkey account and are not asked to take any action.
- **Automatic Updates:** The signed extension package is updated automatically by the browser from Uniqkey's update service.
- **Combined with the Password Manager:** If an employee activates the Uniqkey password manager in a browser, that installation becomes the regular Uniqkey extension and stops reporting Discovery data.

4.4 Data Collection & Minimisation

Collected (metadata only)

- Website origin (scheme and host name only), including the hosts a login redirects through, such as an identity provider
- Form type (login, two-factor, sign-up, password reset or change)
- How each field was filled (typed, pasted, browser autofill or password manager), never its value
- Password strength score (0 to 100), calculated in the browser
- Whether a second factor or passkey was used
- Login duration, rounded to half a second
- The corporate sign-in identity, only when it is an email address on one of the organisation's verified domains

Never Collected

- Passwords or password hashes
- One-time codes and other second-factor values
- Passkey private keys or any other credential material
- Values entered into any form field
- Page paths, query strings or page content
- Sign-in identities outside the organisation's verified domains, which never leave the browser

4.5 Enrolment & Authentication

- **Enrolment Token:** Administrators generate an enrolment token in the Admin Portal and include it in the browser policy. The token is 256 bits of cryptographically secure randomness, is shown once, and only its SHA-256 hash is stored. Tokens can be given an expiry date and revoked at any time.
- **Installation Registration:** Each installation exchanges the enrolment token for a short-lived signed access token bound to the organisation and to that installation. An installation can belong to only one organisation.
- **Revocation:** Access tokens are short-lived, and every renewal verifies that the enrolment token is still valid and that Discovery is still enabled for the organisation. Revoking the token or disabling Discovery stops installations from obtaining new access tokens.

4.6 Access Control & Auditability

- **Disabled by Default:** Discovery must be explicitly enabled by an administrator for the organisation.
- **Administrator Only:** The Discovery dashboard and enrolment tokens are available only to administrators, and all data is scoped to the administrator's organisation.
- **Audit Logging:** Enabling or disabling Discovery, creating or deleting enrolment tokens and registering new installations are recorded in the audit log.

4.7 Privacy by Design & Zero-Knowledge Preserved

Discovery is built on data minimisation. Credentials and field values never leave the page, URLs are reduced to the host name, and a sign-in identity is only reported when it belongs to one of the organisation's own verified domains. Logins with personal identities are counted without any identity attached. Administrators can see corporate sign-in identities in Discovery, for example to identify shared accounts or accounts with repeated login problems. As Discovery observes employee sign-ins, organisations should inform employees about its use in line with their internal policies and GDPR obligations.

Discovery data is operational metadata, classified as a secondary asset in the threat model. It is stored separately from the vault and protected by access controls and audit logging. Discovery has no access to vault data or encryption keys, and it does not change any of the zero-knowledge guarantees described in this whitepaper.

4.8 Hosting, Security & Compliance

- **EU Hosting:** Discovery data is processed and stored on the same EU-hosted infrastructure, under the same operational controls, as the rest of the Uniqkey platform (see Section 9 and Section 10).
- **Encryption in Transit:** All communication between the extension and the Discovery ingestion service uses TLS.
- **Threat Model:** Discovery is included in Uniqkey's threat model and attack surface analysis (see Section 6.4).

5. Authentication Models

Uniqkey offers four distinct authentication models to accommodate different security requirements and use cases. Each model maintains zero-knowledge security principles while providing flexibility for various organisational needs.

Choosing the Right Model

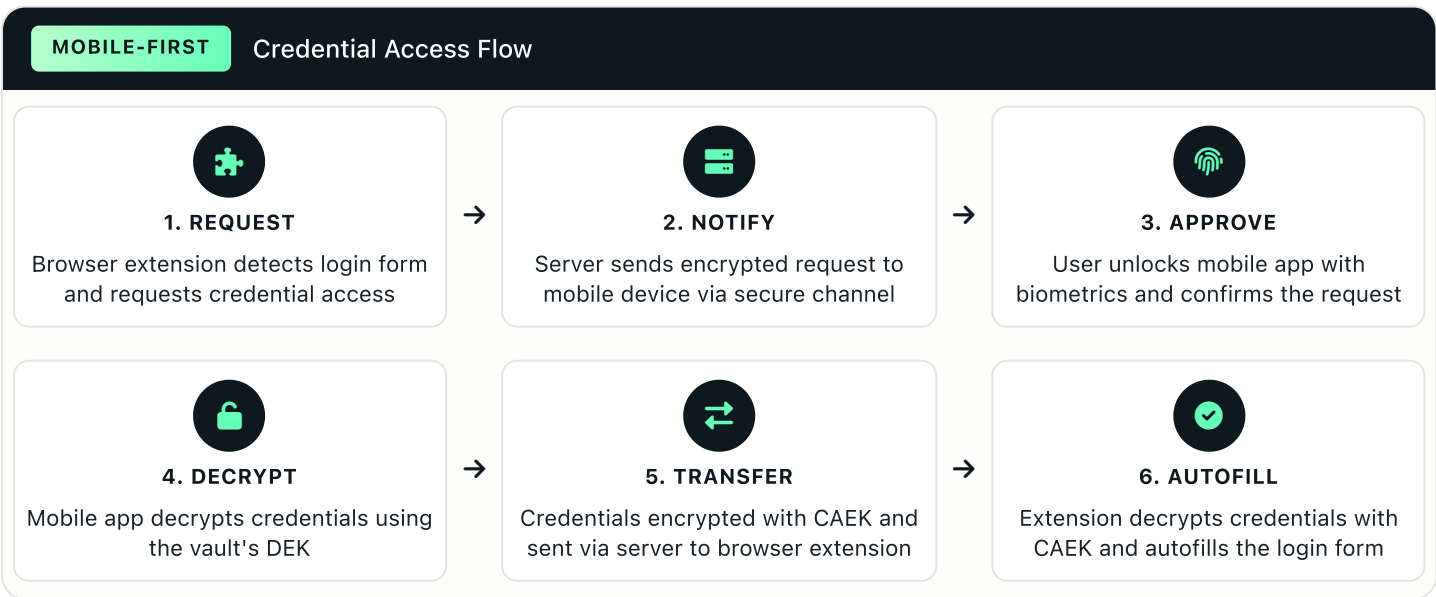
Mobile-First is recommended for maximum security and is the default for all users. **Trusted Browser** offers a balance between security and convenience for users on dedicated workstations. **Phoneless** provides accessibility options and backup access when mobile devices cannot be used. **SSO** lets employees sign in through the organisation's identity provider with no separate master password.

5.1 Mobile-First Authentication (Primary Model)

The mobile-first model is Uniqkey's **recommended** and most secure authentication approach. It provides the strongest security guarantees of all four models, and we encourage organisations to adopt it as their default wherever possible. In this model, the mobile application serves as the central authentication device and cryptographic key holder.

- **How It Works:** The mobile device stores cryptographic keys and encrypted vault data. Browser and desktop access requires mobile app authorisation, creating a two-device authentication flow.
- **Key Storage:** Private keys stored in native secure Keychain (iOS) or Keystore (Android), protected by hardware-backed encryption and biometric authentication.
- **Offline Access:** Complete encrypted vault cached on mobile, enabling credential access during internet outages or server unavailability.
- **Pairing:** Browser extensions and desktop apps pair via QR code or one-time code, establishing an encrypted CAEK communication channel (see Section 2.2).
- **Security:** Highest security model. Requires physical possession of the authenticated mobile device, protecting against remote attacks.

Mobile-First Authentication Flow

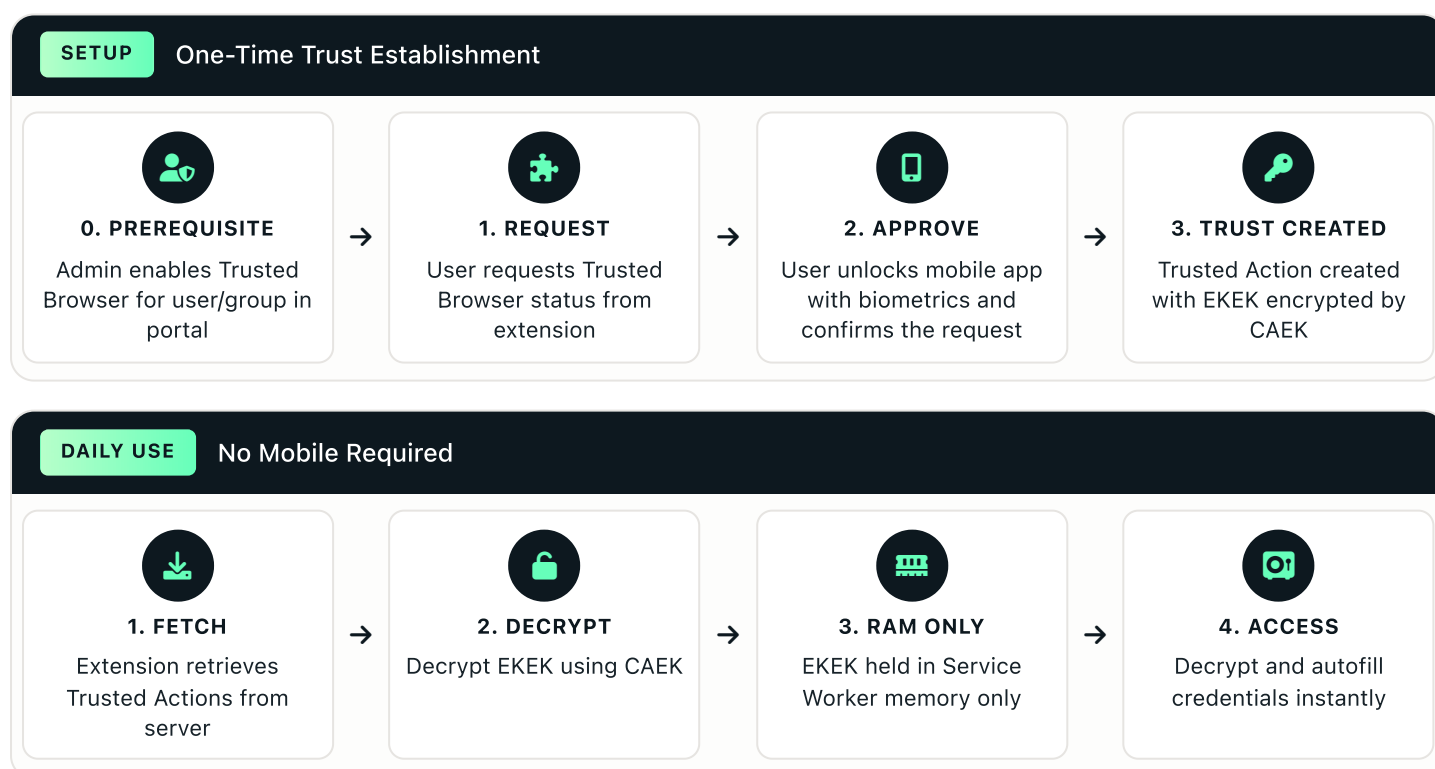


5.2 Trusted Browser

Trusted Browser mode allows users to access their credentials directly from the browser extension without requiring mobile app approval for each action, while maintaining security through controlled trust delegation. This is not Uniqkey's recommended authentication model; the mobile-first approach provides stronger security guarantees. Trusted Browser is designed for scenarios where constant mobile interaction is impractical, such as users working from a single secure workstation for extended periods or environments where mobile devices cannot be kept nearby.

- **Administrator Control:** Administrators enable Trusted Browser through an organisation-wide setting in the admin portal. When enabled, users gain the ability to activate the feature for themselves
- **User Activation:** Once enabled by the administrator, each user can activate Trusted Browser for a configurable duration. Users approve the activation through their mobile app with biometric authentication
- **Local Encryption:** Credentials accessed via Trusted Browser remain encrypted with the employee's asymmetric key pairs, which are derived from the master password on the mobile device and transferred encrypted to the browser. The master password itself never leaves the mobile device
- **Session Duration:** Users choose how long Trusted Browser remains active. When the session expires, mobile app approval is required again to re-activate
- **Use Cases:** Ideal for users who primarily work from a single, secure workstation and need quick access to credentials without constant mobile app interaction
- **Security Considerations:** While convenient, this mode delegates some security to the browser environment. Administrators maintain control over whether the feature is available to their organisation

Trusted Browser Setup & Usage Flow



Trusted Browser: How Keys Are Protected

Understanding how Uniqkey protects your credentials in Trusted Browser mode is essential for security-conscious organisations. Here's exactly what happens:

- **Master Password (Never Stored):** Your master password is **never written to disk** in the browser. It exists only in memory during authentication and is used to derive the MPDK.
- **Trusted Action (Server-Side):** When Trusted Browser is activated, the server creates a "Trusted Action" containing your encrypted EKEK. This payload is encrypted with the CAEK before transmission.
- **CAEK (Browser Storage):** A unique 256-bit symmetric key generated when the extension is first installed. Used to encrypt/decrypt trusted action payloads. Stored in the browser's extension storage API.
- **Session Keys (Memory Only):** During an active session, decrypted EKEK and vault keys exist only in memory. When the session expires or browser closes, these are cleared automatically.

Important: The CAEK is stored in the browser's extension storage which does not use OS-level encryption. This is why Trusted Browser mode requires administrator approval and should only be used on physically secure workstations.

Session Duration & Expiration:

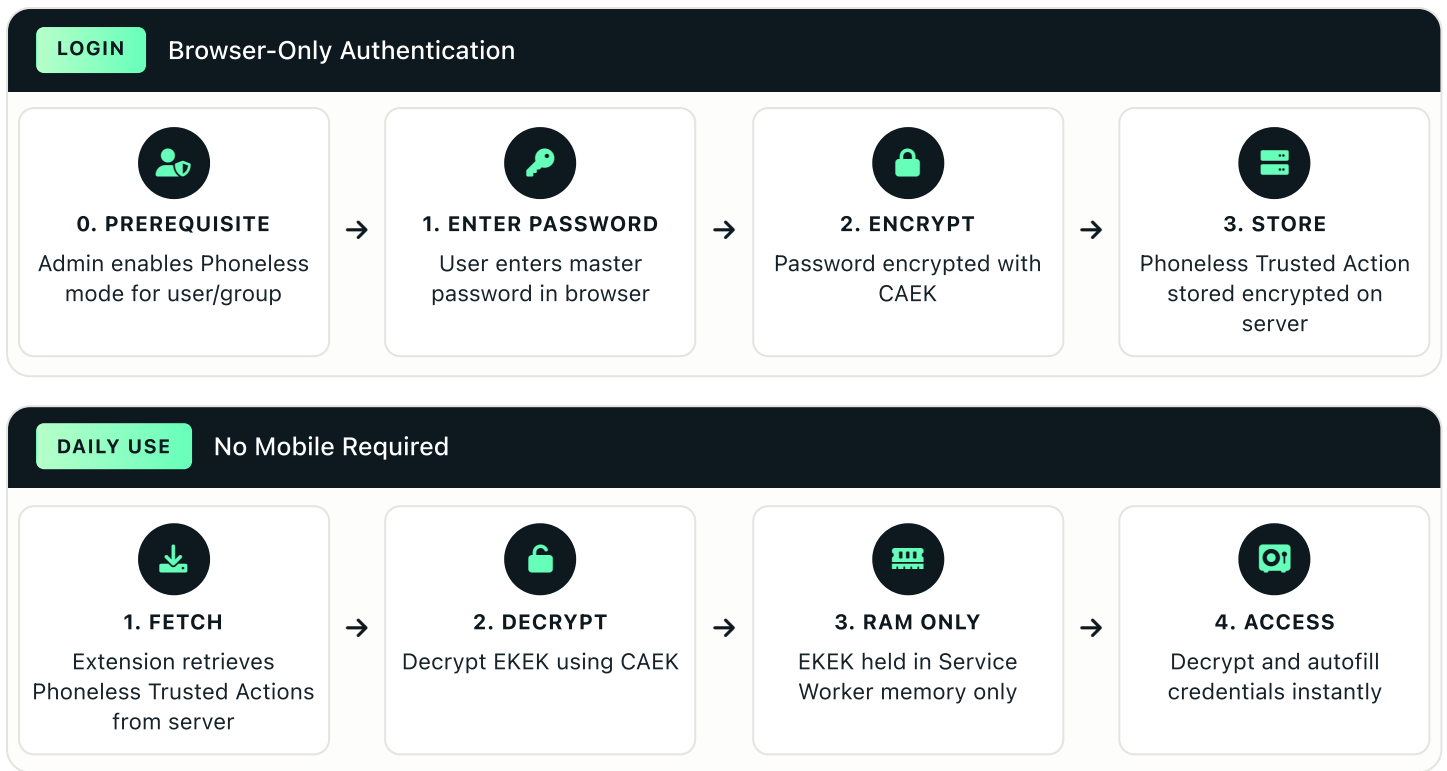
- **Configurable Duration:** Organisations can set trusted browser session length (default: 8 hours)
- **Automatic Expiration:** Sessions expire and require re-authentication
- **Remote Revocation:** Administrators can revoke trusted browser status at any time, immediately invalidating all sessions
- **Memory Cleanup:** All decrypted keys are cleared from memory on session end, logout, or browser close

5.3 Phoneless Authentication

Phoneless mode provides an alternative authentication path for users who cannot use the mobile application, ensuring accessibility while maintaining security through alternative verification methods.

- **How It Works:** Users authenticate using their master password combined with additional verification factors, without requiring the mobile app. The browser extension or desktop app handles all cryptographic operations independently
- **Key Derivation:** Cryptographic keys are derived directly from the master password using Argon2id, with the derived keys enabling vault decryption without mobile device involvement
- **Administrator Control:** Phoneless mode must be explicitly enabled by organisation administrators. Organisations can restrict which employees are permitted to use this mode
- **Additional Security:** When phoneless mode is enabled, organisations can require additional security measures such as IP restrictions, time-based access controls, or enhanced audit logging
- **Use Cases:** Suitable for environments where mobile devices are prohibited (e.g., secure facilities), for users without smartphones, or as a backup access method when mobile devices are unavailable
- **Recovery Scenarios:** Phoneless authentication can serve as a recovery mechanism when users lose access to their mobile device, ensuring continued access to critical credentials

Phoneless Authentication Flow



Phoneless Mode: How Keys Are Protected

Phoneless mode allows browser-only access without a mobile device. Here's how security is maintained:

- **Master Password (Server-Side Encrypted)**: In Phoneless mode, the master password is stored as an encrypted "Phoneless Trusted Action" on the server. It is encrypted with the CAEK, meaning only your specific browser installation can decrypt it.
- **CAEK (Browser Storage)**: A unique 256-bit AES key generated on first extension install. This key is required to decrypt the Phoneless Trusted Action from the server. Without this key, the encrypted master password cannot be recovered.
- **SRP Authentication (Zero-Knowledge)**: Authentication uses the Secure Remote Password (SRP) protocol. The server never receives your actual password, only a cryptographic proof that you know it.
- **Key Derivation (On Demand)**: The MPDK is derived from the master password using Argon2id with your employee account ID as salt. This derived key decrypts your EKEK, which in turn decrypts vault DEKs. All derivation happens in browser memory.

Defence in Depth: Even if an attacker gains access to the encrypted Phoneless Trusted Action on the server, they cannot decrypt it without the CAEK stored in your specific browser installation.

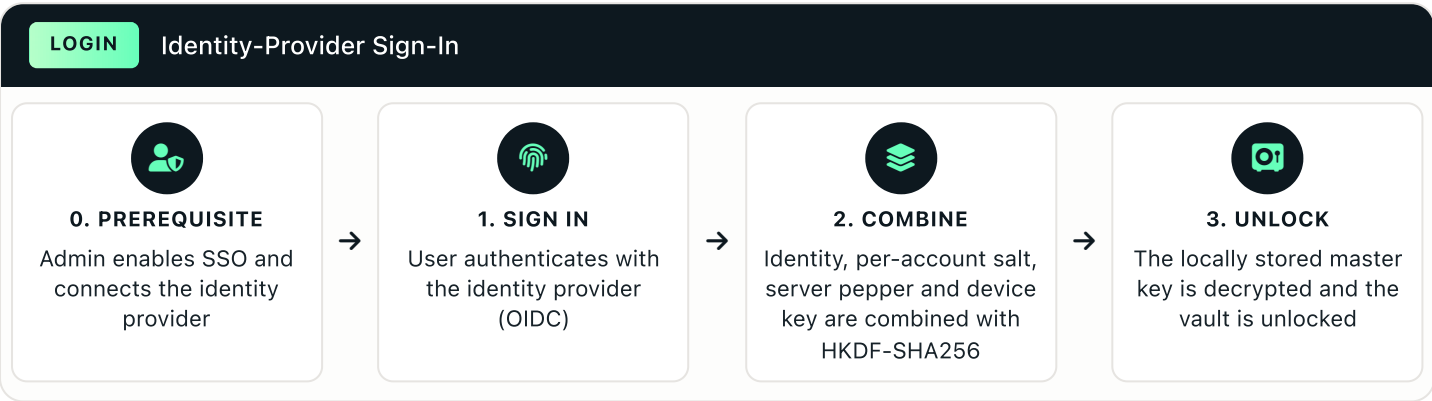
5.4 SSO Authentication

Single Sign-On (SSO) lets employees access their vault through the organisation's existing identity provider using the OpenID Connect (OIDC) standard. Single Sign-On is currently available with Microsoft Entra ID. There is no separate master password to create or remember, while the vault remains protected by Uniqkey's zero-knowledge, client-side cryptography.

- **How It Works:** Users authenticate with their identity provider. Once the provider confirms their identity, the browser extension reconstructs the key that protects the locally stored master key and unlocks the vault. All cryptographic operations happen on the user's device.

- **Master Key:** Rather than a human-chosen password, each SSO user is assigned a 256-bit master key produced by a cryptographically secure random generator. There is nothing to guess, phish or reuse.
- **Administrator Control:** SSO is enabled per organisation. Administrators choose their identity provider and which employees authenticate through it, and SCIM provisioning keeps accounts and group membership in sync (see Section 8.1).
- **Key Derivation:** Once the master key is recovered on the device, vault keys are derived from it using Argon2id, following the same key hierarchy as every other authentication model (see Section 6.2).
- **Use Cases:** Organisations standardised on an identity provider that want frictionless, password-free onboarding while retaining end-to-end encrypted vaults.

SSO Authentication Flow



	RECOMMENDED	BALANCED	ACCESSIBLE	IDENTITY-BASED
Master Password Storage	Mobile device secure Keychain/Keystore (hardware-backed)	Not stored	Stored as an encrypted Phoneless Trusted Action	Stored as an encrypted SSO Trusted Action, plus a device-local copy
Key Storage Location	Mobile device secure Keychain/Keystore (hardware-backed)	Browser extension storage + server-side encrypted payload	Browser extension storage + server-side encrypted payload	Browser extension storage + server-side encrypted payload
Mobile App Required	Yes Required for every authentication	Partial Initial setup and periodic re-approval only	None Mobile app is not required	None Authentication handled by the identity provider
Daily Authentication Flow	Browser requests → Mobile push → Biometric approval → Vault data sent	Auto-retrieve encrypted Trusted Action from server	Auto-retrieve encrypted Phoneless Trusted Action from server	Auto-retrieve encrypted SSO Trusted Action from server; identity-provider sign-in only when the session expires
Session Persistence	Per-request (most secure)	Time-limited (configurable by organisation)	Time-limited (configurable by organisation)	Time-limited (configurable by organisation)
Browser Reinstall Impact	Keys remain on mobile device. Requires re-pairing with the browser	Requires mobile app re-approval to re-establish trust	Enter master password again	Re-authenticate with the identity provider, then restore via a recovery code
Lost Mobile Device	Requires a new mobile device. Login via email and master password, or recover via admin	Can continue with existing trusted browsers. A new mobile device is needed to create new trusted browsers	Full access via browser without mobile	Not applicable; no mobile device is required

Offline Access	<div>Full offline access</div> Complete vault cached on mobile	<div>No offline access</div> Requires server connection	<div>No offline access</div> Requires server for encrypted password retrieval	<div>No offline access</div> Requires a server connection for each unlock
Security Level	<div>●●●</div> Highest Hardware-backed key storage + biometric + 2-device model	<div>●●○</div> High Password never stored, but relies on browser security	<div>●○○</div> Moderate Encrypted password on server, device-key protected	<div>●●○</div> High Identity-provider sign-in with multi-factor local key protection
Best For	<ul style="list-style-type: none"> Security-focused users Privileged accounts Remote workers Offline access 	<ul style="list-style-type: none"> Dedicated workstations High-frequency access Single trusted location Productivity-focused 	<ul style="list-style-type: none"> Backup access method Shared workstations Users without smartphones Accessibility needs 	<ul style="list-style-type: none"> Identity-provider organisations Password-free onboarding Frictionless daily access Centralised identity control

Security Summary

All four models maintain Uniqkey's **zero-knowledge architecture** (see Section 6.2). The key differences lie in *where* cryptographic keys are stored and *how* authentication is initiated:

Mobile-First	Master password and keys in hardware-secured mobile Keychain/Keystore
Trusted Browser	CAEK in browser storage, encrypted EKEK on server as Trusted Action
Phoneless	CAEK in browser storage, encrypted master password on server as Phoneless Trusted Action
SSO	Master key on the device, sealed by identity, per-account salt, server pepper and device key

6. Security Architecture

6.1 Encryption Standards

Each cryptographic algorithm is selected based on specific security requirements, performance characteristics, and resistance to known attack vectors. Below are Uniqkey's cryptographic choices and the rationale behind each.

AES-256	Symmetric Encryption
Why AES-256? AES (Advanced Encryption Standard) with 256-bit keys is the gold standard for symmetric encryption. It is NIST-approved ^[2] , extensively analysed for 20+ years, and considered quantum-resistant (Grover's algorithm reduces effective key size to 128-bit, still computationally infeasible). Hardware acceleration (AES-NI) ensures excellent performance across all platforms.	
Curve25519 / X25519	Asymmetric Key Exchange
Why Curve25519? Designed by Daniel Bernstein ^[3] , Curve25519 offers several advantages over traditional RSA or NIST curves: constant-time implementation prevents timing attacks, smaller key sizes (256-bit vs 2048-bit RSA) with equivalent security, and resistance to various implementation pitfalls. The curve has no known weaknesses and is not subject to NSA-related concerns that affect NIST P-curves.	
SRP-6a (Secure Remote Password)	Authentication Protocol
Why SRP? Unlike traditional authentication where password hashes are sent to the server, SRP uses zero-knowledge proof. The server verifies the user knows the password without ever receiving it. This means: (1) passwords cannot be intercepted in transit, (2) server compromise does not expose passwords, (3) mutual authentication prevents phishing, and (4) forward secrecy protects past sessions. Uniqkey uses SRP-6a with a 4096-bit prime group (per RFC 5054) and SHA-256 as the hash function.	
Argon2id	Password-Based Key Derivation
Why Argon2id? Winner of the 2015 Password Hashing Competition ^[4] , Argon2 is the modern successor to bcrypt and scrypt. Argon2id specifically combines resistance against both GPU-based (Argon2d) and side-channel (Argon2i) attacks. This memory-hard algorithm ensures that parallel cracking attempts require substantial memory per attempt, making large-scale brute-force attacks economically infeasible even with specialised hardware (ASICs/FPGAs).	
TOTP (RFC 6238)	One-Time Codes

Why RFC 6238? One-time codes stored alongside a login are generated on the client from the shared secret, following the Time-based One-Time Password standard^[8]. Uniqkey reads the full authenticator profile from the otpauth QR code or URI: HMAC-SHA1, SHA-256 or SHA-512, 6 to 8 digits, and the code period. Services with non-default settings therefore produce the same codes as a dedicated authenticator app. The secret is encrypted like any other vault field, and codes are only ever computed on the device that holds the decrypted secret.

Why Argon2id Beats PBKDF2

The majority of major password managers still rely on PBKDF2 for key derivation, often advertising high iteration counts (600,000 to 1,000,000) as a measure of security. PBKDF2 is purely CPU-bound, which means attackers can leverage GPUs and custom hardware to test billions of password guesses in parallel at relatively low cost. **Memory-hard algorithms like Argon2id provide fundamentally stronger protection** by requiring significant memory for every single attempt, making large-scale parallel attacks economically impractical regardless of iteration count.

Uniqkey's Parameters

MEMORY	ITERATIONS	SALT
16 MB	10	Unique
per derivation	opsLimit	per employee ID

Comparison

Factor	PBKDF2 (common alternative)	Argon2id (Uniqkey)
GPU Parallelisation	Highly parallelisable - cheap to attack	16MB per attempt blocks parallel attacks
ASIC/FPGA Resistance	Custom hardware attacks feasible	Memory requirements make ASICs impractical
Attack Economics	\$1M buys ~10 ¹⁵ PBKDF2 attempts	Same budget: orders of magnitude fewer Argon2 attempts (1,000x+ harder depending on memory configuration)
Modern Standard	NIST legacy (2000)	PHC winner (2015) ^[4] , OWASP recommended ^[5]

Bottom line: Argon2id's memory-hard design makes brute-force attacks orders of magnitude more expensive than PBKDF2, even at high iteration counts. The cost advantage grows with higher memory parameters.

Cryptographic Libraries

Uniqkey uses industry-standard cryptographic libraries selected for security, performance, and platform compatibility:

- **Libsodium/Sodium:** Used for key exchange (Curve25519), key derivation (Argon2id), and SRP authentication. Open-source, formally verified, and used by Signal, WhatsApp, and major cryptocurrency platforms.
- **CryptoJS:** Symmetric encryption uses AES-256 via CryptoJS across all platforms for consistent cross-platform cryptographic operations.

All cryptographic implementations use well-established, peer-reviewed algorithms with no custom or proprietary cryptography.

6.2 Key Management & Hierarchy

Uniqkey employs an envelope encryption model where data is protected by multiple layers of keys, each serving a specific purpose. This hierarchy enables secure sharing, organisational control, and recovery capabilities while maintaining zero-knowledge principles.

Key Hierarchy Overview

- **Master Password Derived Key (MPDK):** A 256-bit key derived from the user's master password using Argon2id. This key never leaves the user's device and is used to encrypt the user's private keys. The master password is stored securely in the hardware-secured mobile Keychain (iOS) or Keystore (Android).
- **Employee Key Encryption Key (EKEK):** A Curve25519 key pair unique to each employee. The private key is encrypted with the MPDK and stored securely. Used to encrypt vault keys for individual access and to receive shared credentials.
- **Organisation Key Encryption Key (OKEK):** A Curve25519 key pair for the organisation, accessible only to administrators. Enables organisational ownership of credentials. Administrators can recover employee vaults without knowing individual master passwords, ensuring business continuity when employees leave or forget credentials.
- **Data Encryption Key (DEK):** A unique AES-256 symmetric key generated for each vault. The DEK encrypts the actual vault contents and is itself encrypted with the appropriate key (EKEK for individual vaults, Group Secret for group vaults, OKEK for organisational backup).
- **Group Secret (GS):** A 256-bit symmetric key shared among group members. When a user is added to a group, they receive the Group Secret encrypted with their EKEK public key, enabling access to all vaults shared with that group.

Master Key Protection in SSO Mode

For users who authenticate through Single Sign-On (see Section 5.4), the master key is not held in a mobile Keychain. Instead it is held in encrypted form, both on the user's device and as a server-side payload (as in the Phoneless model). The device-local copy is sealed with a key derived via HKDF-SHA256 from four factors: the user's verified SSO identity, a per-account salt held server-side, a server-held secret (an HMAC-SHA256 "pepper") kept in a separate, hardened key store, and a device key (CAEK) that never leaves the device. Because the pepper lives outside the database, a database leak alone cannot derive the key. Once unlocked, the master key feeds the same MPDK and key hierarchy described above.

Key Hierarchy Diagram

This diagram shows how encryption keys derive from your master password and protect each other in layers, ensuring that compromising any single key cannot expose your vault data.

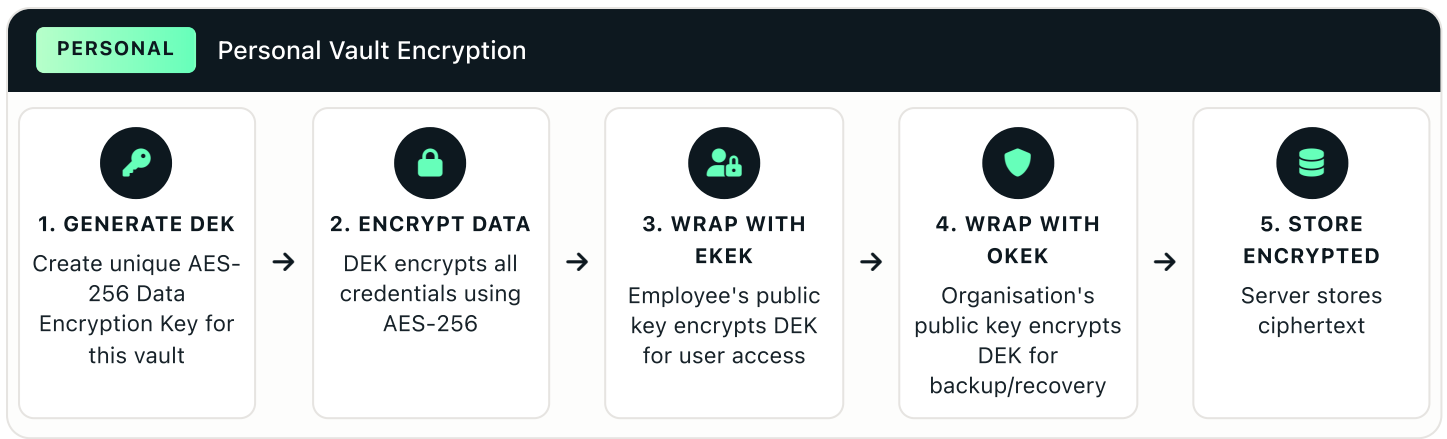
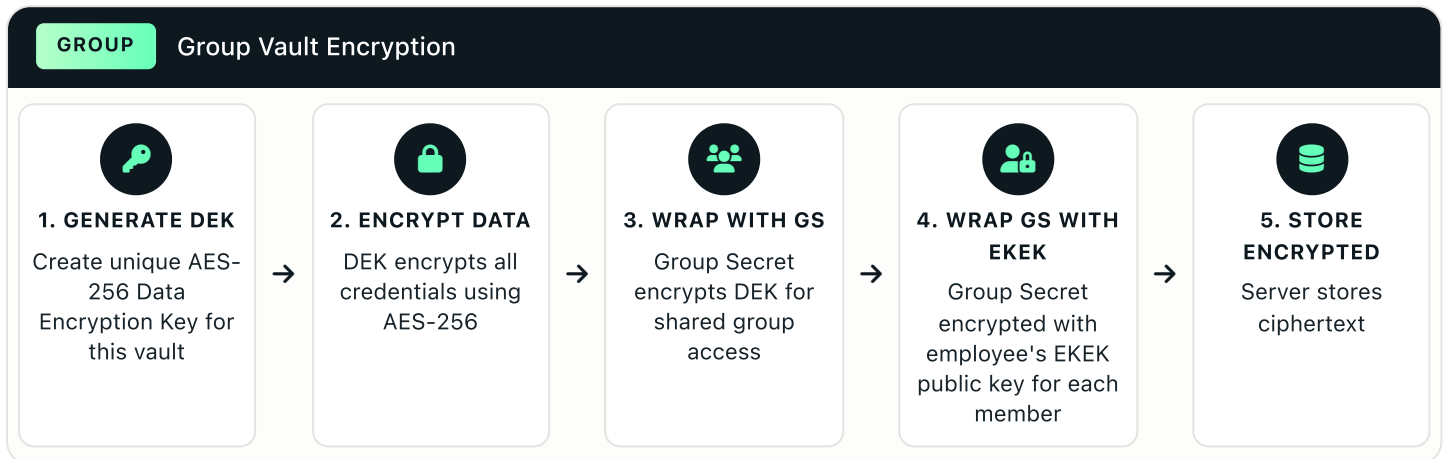


How It Works Together

When a vault is created, a unique DEK is generated and used to encrypt the vault data. The DEK is then encrypted multiple times: once with the employee's EKEK (for user access) and once with the OKEK (for organisational backup). This dual encryption ensures that users can access their own vaults while the organisation retains cryptographic access for recovery and compliance purposes, all without anyone being able to access plaintext credentials without the appropriate keys.

Vault Creation & Encryption Flow

When you save a new credential, this is the step-by-step process that encrypts it and ensures both you and your organisation can access it when needed.



6.3 Master Password Reset & Recovery

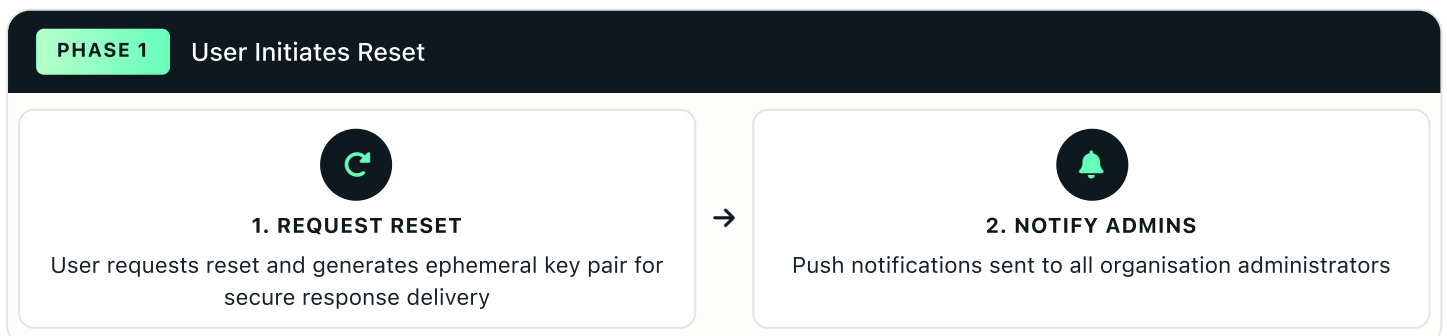
Uniqkey provides a secure master password reset mechanism that allows users to recover access to their vaults without losing any data. This process leverages the organisational key hierarchy to enable administrator-assisted recovery while maintaining zero-knowledge principles.

Why Reset is Possible

Unlike some password managers where forgetting the master password means permanent data loss, Uniqkey's architecture includes a secure backup mechanism. When a user's account is created, their MPDK is encrypted with their EKEK, which is itself encrypted with the organisation's public key (OKEK). Only organisation administrators, who hold the OKEK private key, can initiate the decryption chain needed for recovery.

Master Password Reset Flow

Forgot your master password? This flow shows how you can securely recover access with administrator approval, without anyone ever seeing your credentials.



PHASE 2 Admin Approval & Key Recovery



3. APPROVE

Admin approves and retrieves encrypted EKEK backup



4. DECRYPT EKEK BACKUP

Using OKEK private key (organisation's key)



5. RETRIEVE MPDK

Decrypt MPDK using EKEK private key



6. ENCRYPT MPDK

Encrypt MPDK using the user's ephemeral public key

PHASE 3 User Sets New Password



7. RECEIVE DATA

User receives and decrypts recovery data using ephemeral private key



8. NEW PASSWORD

User enters new master password; new MPDK derived via Argon2id



9. RE-ENCRYPT KEYS

Decrypt EKEK with backed-up MPDK, then re-encrypt using the new MPDK



10. ACCESS RESTORED

All vaults accessible with new master password

Security Safeguards

- **Last Admin Protection:** The system prevents reset requests that would lock out the last remaining administrator, ensuring organisational continuity
- **Ephemeral Encryption:** Recovery data is encrypted with a one-time ephemeral key, ensuring only the requesting device can decrypt the response
- **Audit Trail:** All reset requests and approvals are logged for compliance and security review

Zero-Knowledge Preserved

During the reset process, **vault contents are never decrypted**. Only the key encryption keys are re-wrapped with the new master password derivation. The actual vault data (passwords, notes, etc.) remains encrypted with their original DEKs throughout the entire process. Administrators facilitate the recovery but never gain access to the user's actual credentials.

How This Compares to the Industry

Master password recovery is one of the most security-critical operations in any password manager. Many approaches in the industry introduce trade-offs that weaken zero-knowledge guarantees or depend on user behaviour that frequently fails in practice. Uniqkey's approach avoids these pitfalls:

- **No pre-configuration required:** Many password managers require users to save a recovery phrase, opt into an admin recovery policy, or have logged in via a specific client before recovery becomes possible. If the user never took that step, a forgotten master password means permanent data loss. Uniqkey's OKEK-based backup is created automatically as part of the standard encryption architecture, ensuring every user is recoverable from day one with zero action required.
- **No temporary passwords or master password escrow:** Some enterprise password managers require the administrator to create a temporary master password and communicate it to the user out-of-band. This is a direct zero-knowledge violation: the admin knows a valid credential, and the communication channel may

be insecure. Uniqkey's recovery is fully cryptographic, with no human-mediated password exchange at any point.

- **Admin recovers access, not data:** In some solutions, administrator-assisted recovery involves transferring the user's vault to another account, giving the recipient full access to the original user's credentials. Uniqkey's administrators only re-wrap encryption keys using the OKEK. They facilitate recovery without ever being able to decrypt vault contents.
- **Structural resilience to key escrow attacks:** Recent academic research has identified vulnerabilities in the key escrow mechanisms used by several major password managers, where a compromised server could exploit the recovery process to access user data. Uniqkey's architecture separates the user's encryption keys (EKEK) from the organisational backup keys (OKEK) with distinct key hierarchies, providing a structural defence against this class of attack.

6.4 Threat Model & Attack Surface Analysis

Uniqkey's security architecture is built on a formal threat model that assumes breach attempts are inevitable. This section defines what we protect, who we protect against, and how our architecture mitigates each threat vector.

Protected Assets

These are the assets our security architecture is designed to protect, categorised by their sensitivity and impact if compromised.

Primary Assets

- User credentials (passwords, passkeys)
- TOTP secrets and secure notes
- Encryption keys (EKEK, DEK, Group Secrets)
- Master passwords

Secondary Assets

- User identity and authentication state
- Personal data as defined by GDPR (e.g. names, email addresses, device identifiers)
- Organisation structure and group memberships
- Audit logs and access patterns
- Session tokens and API credentials
- Discovery metadata (services used, login methods, corporate sign-in identities)

Threat Actors

We design our security assuming these adversaries will attempt to compromise the system, including ourselves.



External Attacker

Motivation: Credential theft, ransomware

Capabilities: Network attacks, phishing, malware

Mitigations: Zero-knowledge, E2E encryption, SRP



Malicious Insider

Motivation: Data exfiltration, sabotage

Capabilities: Authorised access to systems

Mitigations: Zero-knowledge (no plaintext access), audit logs



Compromised Employee

Motivation: Credential access post-termination

Capabilities: Knowledge of systems, cached credentials

Mitigations: Instant revocation, OKEK backup



Nation-State Actor

Motivation: Espionage, mass surveillance, hybrid warfare

Capabilities: Advanced persistent threats, legal pressure

Mitigations: Zero-knowledge (nothing to compel), EU jurisdiction



Uniqkey (as threat)

Motivation: N/A - architecture prevents access

Capabilities: Full infrastructure access

Mitigations: Zero-knowledge: even with database access, no decryption possible

Trust Boundaries

In security architecture, a **trust boundary** defines where data transitions between zones with different security properties. Uniqkey's zero-knowledge design deliberately places all decryption within the *Trusted Zone* (your devices), ensuring that our servers in the *Untrusted Zone* only ever handle encrypted ciphertext. This means even if our infrastructure were compromised, attackers would gain nothing but unreadable encrypted blobs. The *Transport Zone* represents the secure channels connecting these zones, protected by TLS encryption and additional measures like certificate pinning.



Trusted Zone

Devices with encryption keys



Mobile app (EKEK storage)



Browser extension (session)



Transport Zone

Encrypted channels only



TLS 1.2+ for all connections



SRP (no password transmission)



Untrusted Zone

Server sees ciphertext only



API servers



Database



Backup systems

Attack Surface

An **attack surface** represents all the points where an attacker could potentially interact with or exploit a system. The table below maps each component of Uniqkey's architecture, what data it exposes, the assessed risk level, and the security controls we've implemented to mitigate threats.

Even "Medium" risk surfaces are protected by multiple layers of defence. Our zero-knowledge design ensures that compromising any single component cannot expose plaintext credentials.

Surface	Exposure	Risk	Controls
Browser Extension	Session data, auto-fill	Low	No EKEK by default, mobile approval required
Database	Encrypted vault storage	Low	Zero-knowledge (ciphertext only), at-rest encryption
Mobile App	EKEK storage, biometric auth	Medium	Hardware keystore, biometric, app sandboxing
Public API	Authentication, encrypted data transfer	Medium	Tiered rate limiting, SRP auth, WAF, monitoring
Admin Portal	Organisation management	Medium	MFA required, audit logging, role-based access
Discovery Extension	Login metadata (no credentials)	Low	Observe-only, data minimised in the browser, hashed enrolment tokens, short-lived access tokens

Attack Scenarios & Mitigations

Uniqkey's architecture is designed with a "when, not if" breach mentality. Here's how each attack scenario is mitigated:

 Database Breach

Attacker gains access to backend database

Protection:
All vault data encrypted with keys that never exist on server. Attacker gets encrypted blobs with no way to decrypt.

 API Compromise

Attacker compromises API layer

Protection:
Cryptography layer beneath API. Even with full API access, decryption keys remain on user devices only.

Browser Extension Attack

Malicious extension or browser compromise

Protection:

EKEK stored only on mobile (default). Browser holds metadata only. Trusted Browser mode optional and admin-controlled.

Employee Offboarding

Former employee retains credential access

Protection:

Instant revocation via "Archived" status. OKEK-encrypted vault copies ensure org retains access.

Lost Phone

User loses device containing EKEK

Protection:

EKEK in biometric store requires authentication. Master Password Reset with admin approval enables recovery.

Compromised Mobile Device

Malware or root exploit gains access to the user's phone

Protection:

EKEK in hardware-backed Keychain/Keystore, gated by biometric authentication. App sandboxing prevents cross-process key extraction.

Man-in-the-Middle

Attacker intercepts network traffic

Protection:

SRP authentication (password never transmitted). Client-to-client encryption via CAEK. HTTPS throughout.

Rainbow Table Attack

Precomputed hash attack on passwords

Protection:

Argon2id with unique salts (Employee ID). Memory-hard algorithm defeats GPU/ASIC attacks.

Quantum Computing

Future quantum computer breaks encryption

Protection:

AES-256 is quantum-resistant. Grover's algorithm halves effective key size, but 128-bit equivalent remains secure.

Phishing Attack

User tricked into entering credentials on fake site

Protection:

Mobile-first requires phone approval. SRP prevents credential transmission to fake servers.

Brute Force Attack

Attacker attempts to guess master password

Protection:

Argon2id memory-hard derivation (resistant to GPU/ASIC). Per-IP rate limiting on authentication endpoints (see Section 8.3: API Access).

Supply Chain Attack

Compromised dependency or build pipeline

Protection:

Signed releases. Code review requirements. Minimal dependency footprint for cryptographic operations.

Social Engineering

Attacker impersonates support to gain access

Protection:

Uniqkey support cannot access vaults (zero-knowledge). Master Password Reset requires admin approval. No password reset via email/phone.

Leaked Discovery Enrolment Token

Attacker obtains the enrolment token from a deployment script or browser policy

Protection:

The token only allows submitting Discovery metadata and reading the organisation's list of verified domains; it grants no access to collected Discovery data, vaults or any other API. Only its hash is stored, new installations are audit-logged, and administrators can revoke and replace it at any time.

6.5 Post-Quantum Cryptography Readiness

As quantum computing advances, Uniqkey is committed to ensuring long-term cryptographic security. Our current architecture provides strong quantum resistance for symmetric encryption, and we are actively monitoring post-quantum asymmetric algorithm developments.

Current Quantum Resistance

Overview of Uniqkey's cryptographic algorithms and their resilience against quantum computing threats.

Algorithm	Usage	Quantum Impact	Status
AES-256	Vault encryption	Grover's algorithm reduces to 128-bit effective security	Quantum-Resistant
Argon2id	Key derivation	Memory-hard design unaffected by quantum algorithms	Quantum-Resistant
Curve25519	Key exchange (EKEK, OKEK)	Shor's algorithm can break ECC in polynomial time	Future Consideration
SRP	Authentication	Based on discrete log; vulnerable to Shor's algorithm	Future Consideration

For the two components marked *Future Consideration*: one alternative under evaluation for key exchange is a **hybrid model** combining classical Curve25519 with a post-quantum algorithm such as ML-KEM (formerly Kyber), the lattice-based key encapsulation mechanism standardised by NIST as FIPS 203. In a hybrid model, both algorithms protect each key exchange independently; if either one remains secure, the communication stays protected. This strategy is recommended by NIST, BSI, and ANSSI and has already been adopted by leading messaging protocols. For SRP authentication, post-quantum alternatives such as OPAQUE with a lattice-based key exchange are being explored by the wider cryptographic community, though no standard has been finalised yet.

Post-Quantum Migration Roadmap

Our approach to quantum-resistant cryptography ensures Uniqkey stays informed of emerging threats while maintaining stability.



Today

COMPLETE

Symmetric encryption (AES-256) and key derivation (Argon2id) already quantum-resistant

 AES-256 vault encryption

 Argon2id key derivation



Awareness

ONGOING

Following NIST PQC standardisation developments

 NIST standards finalised

 Monitoring industry adoption



Future

UNDER CONSIDERATION

Post-quantum alternatives as standards and tooling mature

 Hybrid Curve25519 + ML-KEM key exchange

 OPAQUE-based authentication to replace SRP

 Backward-compatible migration



Practical Timeline

Cryptographically relevant quantum computers (CRQC) capable of breaking current asymmetric encryption are estimated to arrive within **10 to 20 years**, with expert surveys indicating roughly a 25% probability by 2030 and 50% by 2035^[7]. Uniqkey's symmetric encryption (AES-256) protecting vault contents is already quantum-resistant. NIST released the first three PQC standards (FIPS 203, 204, 205) in 2024 and recommends organisations begin planning migration now. Uniqkey is actively evaluating these standards for our asymmetric components and will integrate NIST-approved post-quantum algorithms as enterprise tooling and library support matures.

6.6 Security Audits & Testing

Uniqkey maintains a rigorous security testing programme to identify and remediate vulnerabilities before they can be exploited. Our approach combines internal expertise with independent third-party validation.

Independent Audits & Certifications

Third-party validation of our security controls provides assurance that our claims are independently verified.



ISAE 3000 Type 2

Independent assurance report verifying security practices, data protection, and operational processes against recognised control frameworks.

- Covers security governance, data handling and operational controls
- Four consecutive years of flawless audits
- Report available to customers under NDA

35



ISAE 3402 Type 2

Independently audited against all ISO 27001 control points, ensuring maximum security and resilient infrastructure. Closely aligned with SOC reporting standards.

- Four consecutive years of flawless audits
- Type 2 certification achieved Q1 2026
- Covers access controls, encryption, change management and operational resilience
- Report available to customers under NDA

Cryptographic Library Transparency

Uniqkey uses a combination of **Libsodium** for key exchange and derivation, and **platform-native cryptographic APIs** for symmetric encryption. All libraries are open-source, extensively audited, and widely deployed. Our cryptographic implementations use well-established, peer-reviewed algorithms with no custom or proprietary cryptography.

Responsible Disclosure Programme

Uniqkey welcomes responsible disclosure of security vulnerabilities from security researchers and the broader community. We are committed to working with the security community to keep our users safe.



security@uniqkey.eu

Report security vulnerabilities directly to our security team.

- **Response time:** Acknowledgement within 48 hours
- **Scope:** All Uniqkey applications, APIs, and infrastructure
- **Safe harbour:** Good-faith researchers protected from legal action
- **Recognition:** Security researchers credited in our security advisories (with permission)

7. Technical Implementation

7.1 Technology Stack

Uniqkey is built on modern, enterprise-grade technologies chosen for security, performance, and reliability.



Backend

Modern .NET platform with secure data access patterns and encrypted storage



Frontend

React, React Native, TypeScript (cross-platform consistency)



Cryptography

See Section 6.1: Encryption Standards



Infrastructure

Containerised architecture on EU-based cloud infrastructure

7.2 Development & Security Practices

Uniqkey follows industry-leading security practices throughout the development lifecycle, ensuring code quality and security from design to deployment.

Secure Development Principles



Dual Approval

Dual approval required for all code changes before production merge.



Defence in Depth

Multiple security layers with Architecture team review for compliance.



Automated Analysis

Static code analysis in CI/CD blocks vulnerabilities from merging.

Development Governance

Uniqkey operates with a unified DevOps model: a flat organisational structure where development and operations function as a single integrated unit. Every team member owns both code quality and operational reliability. All changes require dual approval, ensuring collective oversight without hierarchical bottlenecks.

Environment Isolation

Development, testing, and production environments are strictly separated and fully isolated. Customer data is never used in non-production environments. Production access requires explicit approval and is time-limited.

External Review & Audit

In addition to internal practices, Uniqkey's security controls and development processes are externally reviewed and audited by PricewaterhouseCoopers (PwC), one of the Big Four professional services firms. This independent assurance validates that controls are not only well-designed but operate effectively over sustained periods, providing enterprise customers with a high degree of confidence in Uniqkey's security posture.

8. Integration Capabilities

Uniqkey integrates seamlessly with existing enterprise infrastructure, enabling organisations to deploy password and access management without disrupting current workflows or identity management systems.

8.1 Identity Provider Integration

SCIM 2.0 Provisioning

Uniqkey implements the SCIM 2.0 (System for Cross-domain Identity Management) standard for automated user lifecycle management.



Automated Provisioning

New employees automatically receive Uniqkey accounts when added to your IdP



Real-time Sync

Profile updates (name, email, department) sync immediately from directory



Auto Deprovisioning

Access revoked instantly when employees leave or are disabled in IdP



Group Mapping

IdP groups automatically map to Uniqkey groups for consistent access control

Supported Identity Providers

Uniqkey integrates with **Microsoft Entra ID (formerly Azure AD)**, **Okta**, and any other SCIM 2.0 compliant identity provider via Uniqkey's standard SCIM API with full attribute mapping. Setup guides are available for common identity providers.

Single Sign-On (SSO) Authentication

Beyond user provisioning, Uniqkey supports Single Sign-On so employees authenticate to their vault through the organisation's identity provider using OpenID Connect (OIDC). There is no separate master password to remember, and the vault remains protected by client-side, zero-knowledge cryptography (see Section 5.4 for the authentication flow and Section 6.2 for key protection). Single Sign-On is currently supported with Microsoft Entra ID. SCIM provisioning, above, supports a broader range of identity providers.



OIDC Sign-In

Users authenticate with their existing identity provider, with no extra password required



Zero-Knowledge Preserved

Vault keys are derived and used on the device; the server never sees them in readable form



Administrator Control

SSO is enabled per organisation, with control over which employees authenticate through it



Breach-Resilient Keys

A server-held pepper kept outside the database ensures a database leak alone cannot decrypt vaults

8.2 Browser Extension Integration

The Uniqkey browser extension provides seamless credential auto-fill without compromising security.

- **Supported Browsers:** Chrome, Edge, Firefox, Safari
- **Auto-fill:** Automatic credential detection and form filling
- **Save Prompts:** Intelligent detection of new credentials with save suggestions
- **Site Matching:** Secure URL matching to prevent phishing attacks
- **Mobile Authorisation:** All sensitive operations require mobile app approval (unless Trusted Browser enabled)
- **Discovery Mode:** An observe-only mode for managed Chrome and Edge browsers on Windows and macOS, deployed through enterprise browser policy (see Section 4: Discovery)

8.3 API Access

Uniqkey provides RESTful APIs for administrative automation and custom integrations.

- **Organisation API:** Manage employees, groups, and policies programmatically
- **Authentication:** JWT tokens via SRP protocol (no passwords over the wire)

Rate Limiting & Abuse Prevention

Uniqkey implements per-IP rate limiting at the infrastructure level to protect against brute-force attacks and ensure platform stability.

- **Authentication Endpoints:** Strict limits to protect against credential stuffing and brute-force attacks.
- **Password Reset Requests:** Throttled to prevent reset abuse and social engineering attacks.
- **2FA Endpoints:** Protected to secure two-factor authentication flows.
- **General API Traffic:** Default limits applied to all endpoints to ensure platform stability.

Rate limit responses include standard headers to help clients implement appropriate retry logic.

8.4 Real-time Synchronisation

Changes propagate instantly across all connected devices and clients.

- **WebSocket Communication:** Real-time bidirectional updates across all clients
- **Push Updates:** Vault changes appear immediately on all paired devices
- **Offline Support:** Mobile app maintains local encrypted cache for offline access
- **Conflict Resolution:** Automatic handling of concurrent edits

9. Operations

9.1 Datacenter & Hosting

Uniqkey infrastructure is hosted exclusively in EU-based datacenters selected for robust security infrastructure and commitment to European data sovereignty. Our infrastructure delivers enterprise-grade reliability with a 99.95% uptime guarantee, protected by DDoS mitigation, TLS encryption, and continuous security monitoring. All datacenters are powered by 100% renewable energy.

For compliance certifications and data sovereignty details, see Section 10: Compliance & Governance.

9.2 Backup & Disaster Recovery

Uniqkey maintains comprehensive backup and disaster recovery procedures to ensure business continuity and data protection in all scenarios.

≤ 30 min
Recovery Point Objective (RPO)
Maximum data loss window via continuous WAL archiving with 30-minute granularity

7 days
PITR Window
Continuous point-in-time recovery to any moment within the past 7 days

90 days
Backup Retention
Daily full backups, including encrypted immutable offsite copies, retained for 90 days

Backup Strategy

Uniqkey employs a two-tier backup strategy. The primary tier uses PostgreSQL Point-in-Time Recovery (PITR), which archives write-ahead log (WAL) segments every 30 minutes or 16 MB of data (whichever comes first), providing recovery to any point within the past 7 days. The secondary tier consists of daily full backups, encrypted at rest using AES-256 and stored as immutable offsite copies, retained for 90 days. In a worst-case disaster recovery scenario beyond the 7-day PITR window, the maximum data loss is up to 24 hours. Twice-yearly disaster recovery drills validate that both tiers work as expected.

Business Continuity

Uniqkey's architecture ensures credential availability even during infrastructure failures. The zero-knowledge design means that even complete server unavailability does not lock users out of their credentials.

Failure scenarios and recovery capabilities for Uniqkey's infrastructure.

**Service Outage**

Impact: Sync unavailable
Mitigation: Mobile app local cache provides offline access
Response: Users retain credential access via local encrypted cache

**Database Failure**

Impact: New vault operations paused
Mitigation: Real-time replication with automatic failover
Response: Standby node automatically promoted to primary

**Ransomware**

Impact: Data integrity at risk
Mitigation: Immutable offsite backups; point-in-time recovery
Response: Restore from PITR or immutable offsite backup

Offline Resilience

Unlike web-only password managers, Uniqkey's mobile-first architecture ensures credential access continues even during complete internet or service outages:

- **Local Encrypted Cache:** Mobile app maintains a fully encrypted local copy of vault data, accessible via biometric authentication for read-only viewing and copying
- **No Server Dependency:** Cached credentials can be viewed and copied without any network connectivity
- **Restriction Enforcement:** Credentials protected by access restrictions (e.g. geolocation, time-of-day) require server connectivity to validate, and are not accessible offline
- **Automatic Sync:** Vault data automatically synchronises when connectivity is restored

Incident Response & Communication

Uniqkey maintains documented incident response procedures to ensure rapid detection, containment, and transparent communication during security or availability events.

Customer Notification

- **Security Incidents:** Supervisory authorities notified within 72 hours of a confirmed breach per GDPR; affected customers notified without undue delay, with details on impact and remediation steps
- **Service Disruptions:** Real-time status updates via status page; post-incident reports for significant outages
- **Planned Maintenance:** Minimum 48-hour advance notice for scheduled maintenance windows

9.3 Availability & SLA

- **High Availability:** Multi-instance deployment with load balancing for optimal performance
- **Service Level Agreement:** Enterprise SLA with guaranteed uptime commitments
- **24/7 Monitoring:** Continuous infrastructure and application monitoring with automated alerting
- **Incident Response:** Defined incident response procedures for rapid issue resolution

9.4 Security Monitoring

Uniqkey employs defence-in-depth security monitoring to detect and respond to threats across all infrastructure layers.

- **Runtime Security:** Real-time detection of anomalous behaviour, container threats, and system call monitoring with continuous visibility into unexpected application behaviour and intrusion attempts
- **Endpoint Detection & Response:** Enterprise-grade EDR capabilities including advanced threat protection, automated investigation, and real-time threat intelligence
- **Centralised Logging:** Security events aggregated and correlated for comprehensive threat analysis and forensic investigation
- **Automated Alerting:** Real-time alerts for security anomalies with defined escalation procedures

9.5 Vulnerability Management

Uniqkey uses a comprehensive vulnerability management programme covering infrastructure, application code, and third-party dependencies.

- **Static Application Security Testing:** Continuous code analysis with release gating integrated into the development pipeline. All changes scanned for vulnerabilities, with deployments blocked if severity thresholds are exceeded

9.6 Change Management

Uniqkey's software development process provides full traceability from requirements to deployment, with segregation of duties and verifiable audit evidence.

- **Structured Workflow:** All work items tracked from Initiatives → Features → User Stories with documented acceptance criteria
- **Branch Protection:** Direct commits to main branches prohibited; CI pipeline must pass before merge is permitted
- **Mandatory Code Review:** At least one independent reviewer approval required for all changes, verifying code quality, security compliance, and acceptance criteria
- **Automated Testing:** Unit and integration tests executed in CI pipeline; defects logged and linked to parent features for traceability
- **Segregated Releases:** Developers cannot access production environments or manually deploy builds; releases executed through controlled CI/CD pipelines
- **Full Audit Trail:** All commits, pull requests, and deployments linked to work items with timestamps and user attribution

Detailed change management procedures and control evidence are available for compliance audits upon request.

10. Compliance & Governance

10.1 Certifications & Standards

Uniqkey maintains compliance with internationally recognised security standards:

Uniqkey Certifications

- **ISAE 3000 Type 2 Attested:** Independent assurance report verifying security practices, data protection, and operational processes. Four consecutive years of flawless audits.
- **ISAE 3402 Type 2 Attested:** Audited against all ISO 27001 control points, ensuring maximum security and resilient infrastructure. Type 2 certification achieved Q1 2026. Closely aligned with SOC reporting standards.
- **GDPR Compliant:** Full compliance with EU data protection requirements. All production services hosted in Germany with no cross-border transfers to non-EU countries.
- **NIS2 Supportive:** Uniqkey's zero-knowledge architecture, audit logging, access controls, and incident response procedures support organisations in meeting NIS2 Directive requirements for cybersecurity risk management and supply chain security.

Infrastructure Provider Certifications

- **ISO 27001 Certified:** Uniqkey's infrastructure provider maintains ISO 27001 certification, meeting international standards for Information Security Management Systems (ISMS).
- **BSI C5 Attested:** Infrastructure provider holds the German Cloud Computing Compliance Criteria Catalogue (C5) attestation from the Federal Office for Information Security (BSI), required for public sector and regulated industries in Germany.

Documentation: Certification reports and attestation documentation are available upon request for customers and prospective customers undergoing security evaluation. Contact your account representative or email security@uniqkey.eu.

10.2 Data Retention & Residency

- **Data Residency:** All data stored exclusively in EU datacenters with no cross-border transfers to non-EU countries
- **Organisation Data:** 90-day default retention period (administrator-configurable)
- **Archived Employees:** Configurable soft-deletion period for departed employee data
- **Unmanaged Vaults:** Configurable retention for orphaned vault data
- **Audit Logs:** Configurable audit log retention to meet compliance requirements

10.3 Digital Sovereignty

As European organisations increasingly adopt cloud-based security tools, a practice known as **sovereign washing** has emerged: vendors market solutions as "EU-hosted" or "sovereign" without providing meaningful legal or technical guarantees. In practice, the vendor retains ownership of the infrastructure, operations remain outside the EU, and foreign legislation, most notably the U.S. CLOUD Act, can compel data disclosure regardless of where the data is physically stored.

Encryption and data residency alone do not ensure sovereignty. If a non-EU parent company controls the management plane, telemetry, support escalation, or key management, the organisation remains exposed to

extraterritorial jurisdiction. True digital sovereignty requires that ownership, operations, and legal accountability all reside within the EU.

How to Evaluate Sovereignty Claims

Organisations should verify the following before trusting a vendor's sovereignty claims:



Ownership & Jurisdiction

Verify the vendor's corporate structure, executive residency, and governing law. A non-EU parent entity means non-EU jurisdiction applies.



Key Management

Demand customer-managed encryption keys or zero-knowledge architecture. If the vendor holds decryption capability, legal compulsion can unlock the data.



Contractual Guarantees

Require written commitments preventing non-EU data transfers, backed by third-party audits and transparency reports.

Uniqkey's Position

Uniqkey is a Danish company, wholly owned and operated within the EU. All infrastructure is hosted in Germany with EU-based providers. There is no non-EU parent entity, no foreign operations, and no exposure to extraterritorial data access laws such as the CLOUD Act. Combined with Uniqkey's zero-knowledge architecture, where encryption keys are generated and stored exclusively on user devices, even Uniqkey itself cannot access customer vault contents. This provides sovereignty that is technically enforced, not merely contractually promised.

For a deeper exploration of sovereign washing and how to identify it, see [Sovereign Washing: What It Is and Why It Matters](#) on the Uniqkey blog.

11. Use Cases

11.1 Password and Access Management

Centralised credential storage and management for organisations with secure sharing capabilities and policy enforcement.



Team Credential Sharing

Marketing team shares social media credentials. New hires automatically get access via group membership; departing members instantly lose access.



Infrastructure Credentials

DevOps team manages server passwords, API keys, and deployment credentials. Audit trail tracks who accessed what and when.



Executive Accounts

C-suite credentials with enhanced protection. Mobile-first authentication required; Trusted Browser disabled for maximum security.

11.2 IT Administration

User provisioning via SCIM, security monitoring, and compliance reporting for IT administrators.



Automated User Provisioning

Microsoft Entra ID integration via SCIM. Employees automatically provisioned when joining; access revoked when leaving the directory.



Security Compliance

Generate reports for auditors showing password policies, access logs, and encryption standards. ISAE Type 2 compliance documentation.



Breach Response

Receive alerts when credentials appear in breach databases. Quickly identify affected accounts and enforce password changes.



Shadow IT Discovery

Use Discovery to see which services employees sign in to, find shared accounts and logins without MFA, and prioritise which services to bring under central management.

11.3 Specialised Environments

Uniqkey adapts to unique organisational requirements through flexible authentication models.



Secure Facilities

Government or defence contractors where mobile phones are prohibited. Phoneless mode enables access with master password only.



Shared Workstations

Hospital or factory floor computers used by multiple shifts. Trusted Browser with schedule restrictions ensures access during work hours only.



Contractor Access

External contractors need limited credential access. Create restricted groups with specific vaults and automatic expiration dates.



Remote Workers

Distributed teams accessing credentials from home. Mobile-first ensures security regardless of network; IP restrictions for additional control.

11.4 End User Experience

Seamless autofill, cross-platform access, and mobile-first design for end users.



One-Click Login

Browser extension detects login forms and autofills credentials. Mobile approval takes seconds with biometric authentication.



Work-Life Separation

Private Keychain for personal passwords; organisation vault for work credentials. Both accessible in one interface, cryptographically separated.

12. Conclusion

Uniqkey provides a comprehensive, secure, and scalable platform for password and access management. Its robust architecture, strong security features, and integration capabilities make it an ideal solution for organisations seeking to improve their security posture while maintaining operational efficiency.

The zero-knowledge architecture ensures that your credentials remain protected even in worst-case scenarios. A complete server breach would yield only encrypted data that cannot be decrypted without keys that never leave your devices. Combined with EU-hosted infrastructure and ISAE 3000/3402 Type 2 attestations audited against ISO 27001 control points by PwC, Uniqkey delivers enterprise-grade security without compromising usability.

Key Differentiators



Business-First Approach

Designed for organisations, not individuals. Centralised management, SCIM provisioning, group sharing, and full audit logging from day one.



Shadow IT Visibility

Discovery shows IT teams which services employees sign in to and how those logins are protected, while credential capture through the browser extension brings unmanaged accounts under company control.



Zero-Knowledge Security

Encryption keys never leave user devices. Even a complete server breach yields only ciphertext that cannot be decrypted.



Access Management at Scale

Onboard and offboard employees instantly. Shared vaults, group permissions, and organisational recovery ensure credentials are always under company control.

How Uniqkey Compares

Architectural differences between Uniqkey and common password management approaches.

Capability	Common Approach	Uniqkey
Encryption Key Storage	Keys derived and present on every device (browser, desktop, mobile)	Mobile device only with hardware-backed security (default Mobile-First mode); alternative modes keep keys in memory only
Authentication Modes	Password-centric with optional MFA and biometric; some now offer dedicated passwordless modes	3 purpose-built flows (Mobile-First, Trusted Browser, Phoneless) optimised for different security scenarios
Key Derivation	Majority still default to PBKDF2; a few providers have adopted Argon2	Argon2id by default (memory-hard, ASIC-resistant, side-channel safe)
Personal Vault Privacy	Most offer personal vaults; admin access varies by provider	Private Keychain with separate key hierarchy; admin-assisted recovery restores access without exposing vault contents
Browser Compromise Impact	Keys present in browser memory during active session	No keys in browser by default ; mobile approval required for each session
Password Reset	Most offer admin-assisted recovery; zero-knowledge guarantees vary	Automatic OKEK-based recovery with zero data loss; no user pre-configuration required
Data Residency	Most major providers are US or Canadian companies; EU hosting available but subject to CLOUD Act jurisdiction	One of the few EU-native providers (Danish company, hosted in Germany); built and operated exclusively in the EU, outside CLOUD Act reach

By combining proven cryptographic standards (AES-256, Curve25519, Argon2id) with thoughtful user experience design, Uniqkey eliminates the traditional trade-off between security and usability. Organisations can deploy a solution that security teams trust and employees actually use, reducing shadow IT, reducing password reuse, and improving visibility into credential security.

For more information about Uniqkey or to schedule a demo, contact us at sales@uniqkey.eu or visit uniqkey.eu.

13. Frequently Asked Questions



Security & Architecture

What happens if Uniqkey's servers are compromised?

Due to our zero-knowledge architecture, a server compromise would only expose encrypted ciphertext. Attackers would gain access to encrypted vault data, but without the decryption keys (which never leave client devices), the data remains cryptographically secure. The EKEK stored on mobile devices and the MPDK derived from master passwords are required to decrypt any vault contents.

Can Uniqkey employees access our passwords?

No. Uniqkey operates on a zero-knowledge principle. All encryption and decryption happens on your devices. Our servers store only encrypted data, and we never have access to your master password or encryption keys. Even with full database access, Uniqkey staff cannot decrypt your credentials.

Why is the mobile app required for standard authentication?

The mobile app serves as the secure key storage for your Employee Key Encryption Key (EKEK). Unlike browsers or desktop apps which have larger attack surfaces, mobile devices provide hardware-level security through iOS Keychain and Android Keystore, biometric authentication, and app sandboxing. This single-point-of-security approach means even if your computer is compromised, attackers cannot access your encryption keys.



Usage & Features

What's the difference between Trusted Browser and Phoneless mode?

Trusted Browser requires a one-time mobile approval, after which the browser can auto-fill credentials without the phone. The EKEK is encrypted with your CAEK and stored on the server as a "Trusted Action."

Phoneless mode never requires a mobile device. During initial setup, you enter your master password in the browser, which is encrypted with the CAEK and stored on the server as a "Phoneless Trusted Action." For daily use, the extension automatically retrieves and decrypts this action using the CAEK, deriving the MPDK to decrypt your EKEK - no password entry needed each session.

Can I access my passwords if I lose my phone?

Yes. You have several options: (1) If you have Trusted Browser enabled, you can continue accessing credentials from that browser, (2) If Phoneless mode is enabled for your account, you can authenticate with your master password, (3) Organisation administrators can assist with account recovery using the OKEK backup mechanism.

What is the Private Keychain and who can access it?

The Private Keychain is a personal vault where contents are encrypted with your individual EKEK. An OKEK-encrypted backup exists solely for account recovery scenarios, for example, if you lose your phone and need to regain access. In such cases, an administrator can initiate the recovery process, but the decrypted vault contents are only ever revealed to you on your device, never to the administrator. This allows employees to store personal credentials alongside organisational ones, with recovery options available if needed, but without compromising privacy.

Can I access my passwords without an internet connection?

Yes, through the mobile app. The mobile app maintains a fully encrypted local cache of all vault data, accessible via biometric authentication even without an internet connection. Decryption happens entirely on your device, so no server connection is needed to view cached credentials. Changes made offline sync automatically when connectivity is restored. Note that Trusted Browser and Phoneless modes require a server connection and do not support offline access.

Enterprise & Administration

What happens when an employee leaves the organisation?

When an employee is archived, their access is immediately revoked. Organisation administrators can still access all organisation vault data using the OKEK, ensuring business continuity. Group Secrets are rotated to prevent the former employee from accessing shared credentials. Private Keychain data remains private; the OKEK-encrypted backup exists only for account recovery purposes and does not give administrators the ability to view the vault contents.

How does Uniqkey integrate with our existing identity provider?

Uniqkey supports SCIM 2.0 for automated user provisioning and deprovisioning. When integrated with identity providers, user accounts are automatically created, updated, and deactivated based on changes in your directory. Group memberships can also be synchronised to maintain consistent access controls.

Can we enforce password policies across the organisation?

Yes. Administrators can configure organisation-wide policies including: minimum password complexity requirements, master password requirements, mandatory 2FA, Trusted Browser restrictions, login frequency limits, and IP-based access controls. These policies are enforced at the platform level.

Can we import existing credentials or export our data?

Yes. Uniqkey supports importing credentials via CSV, which is compatible with exports from most password managers and browsers. For export, administrators can extract organisation vault data (passwords, secure notes, credit cards) in CSV format, with export permissions controlled at both organisation and group level. All imports and exports are handled client-side to ensure credentials are not exposed during the process.

How does Uniqkey handle passkeys differently than passwords?

Passkeys use public-key cryptography instead of shared secrets. When you create a passkey, Uniqkey generates a key pair, securely stores the private key in your vault (encrypted like passwords), and registers the public key with the service. Authentication uses cryptographic signatures rather than transmitting credentials, making passkeys phishing-resistant and more secure than passwords.

Can passkeys be shared between team members?

Yes. Uniqkey stores passkey private keys in encrypted vaults, so they can be shared with groups or individuals just like passwords. This enables teams to use passkeys for shared service accounts while maintaining the security benefits of passwordless authentication.

Are Uniqkey-managed passkeys compatible with all WebAuthn-enabled services?

Uniqkey supports the WebAuthn standard and can manage passkeys for any website or service that implements FIDO2/WebAuthn authentication. The browser extension acts as a virtual authenticator, intercepting WebAuthn requests and using the securely stored private keys from your vault to complete authentication. This means you get the phishing resistance of passkeys with the convenience of cross-device access through Uniqkey's encrypted sync.

Discovery

Can Discovery be used without the Uniqkey password manager?

Yes. Discovery is available as a standalone product. Administrators enable it and view results in the Admin Portal, while employees do not need a Uniqkey account and are not asked to take any action. It can also be used alongside the password manager.

Can Discovery see employees' passwords or browsing?

No. Discovery only observes sign-in activity (login forms, passkey prompts and the redirects that complete a login) and reduces each login to metadata in the browser: the host names involved, how the login was performed, a password strength score and whether a second factor or passkey was used. Ordinary browsing is not recorded, and passwords, one-time codes, field values, page paths and page content are never collected. A sign-in identity is only reported when it is an email address on one of the organisation's own verified domains. Discovery is disabled by default and is enabled and deployed by the organisation's administrators.

Which browsers and devices does Discovery support?

Discovery supports Google Chrome and Microsoft Edge on Windows and macOS, on centrally managed devices. It is deployed through enterprise browser policy using the templates, scripts and configuration profiles provided by Uniqkey.

How can Discovery be stopped?

Administrators can disable Discovery for the organisation or revoke the enrolment token in the Admin Portal, after which installations can no longer obtain access tokens. Removing the browser policy removes the extension from managed browsers.

Compliance & Data Privacy

Is Uniqkey compliant with GDPR and other data protection regulations?

Yes. Uniqkey's zero-knowledge architecture inherently supports data protection requirements by ensuring that personal credentials remain encrypted and inaccessible to anyone other than the user. We process only the minimum data necessary for the service to operate, and all encryption happens client-side. This design aligns with GDPR principles of data minimisation and privacy by design.

Where is Uniqkey data stored?

All data is stored exclusively in Germany, ensuring full EU data residency with no cross-border transfers to non-EU countries. Encrypted vault data, authentication tokens, and metadata are hosted on infrastructure that is ISO 27001 certified and BSI C5 attested. Because of our zero-knowledge architecture, even the hosted data cannot be read by anyone without the user's decryption keys.

Does Uniqkey hold any security certifications?

Uniqkey holds ISAE 3000 Type 2 and ISAE 3402 Type 2 attestations, audited by PwC. Our ISAE 3402 is audited against all ISO 27001 control points, and Uniqkey has been audited flawlessly for four consecutive years. Our infrastructure provider is ISO 27001 certified and BSI C5 attested. We also undergo regular independent security audits and penetration testing to validate our security posture.

Appendix

A. Glossary

For detailed explanation of the key hierarchy and how these keys work together, see Section 6.2: Key Management & Hierarchy.

Vault

Encrypted container for storing credentials and sensitive information

DEK (Data Encryption Key)

Unique AES-256 key that encrypts vault contents

EKEK (Employee Key Encryption Key)

Employee's Curve25519 key pair for personal vault access

OKEK (Organisation Key Encryption Key)

Organisation's key pair for admin recovery and backup

MPDK (Master Password Derived Key)

Key derived from master password via Argon2id

CAEK (Companion Application Encryption Key)

A unique 256-bit AES symmetric key generated when the browser extension is first installed. Used to encrypt communication between the browser extension and mobile app, and to encrypt Trusted Actions and Phoneless Trusted Actions stored on the server

Group Secret (GS)

Symmetric key shared among group members for shared vault access

SRP-6a (Secure Remote Password)

A cryptographic protocol (version 6a, RFC 5054) for secure authentication without transmitting passwords over the network. Uniqkey uses a 4096-bit prime group with SHA-256

SCIM

System for Cross-domain Identity Management - a standard protocol for automated user provisioning

TOTP

Time-based One-Time Password (RFC 6238) - a method of generating temporary authentication codes from a shared secret and the current time. Uniqkey honours the algorithm (SHA-1, SHA-256, SHA-512), digit count (6 to 8) and period declared in the otpauth profile

Zero-Knowledge Architecture

A security model where the server stores only encrypted data and has no ability to decrypt user information, even with full database access

Private Keychain

A personal credential storage area where vault contents are encrypted with the employee's EKEK. Includes an OKEK-encrypted backup for admin-assisted recovery, but administrators cannot access the actual vault contents. Allows employees to store personal passwords separately from organisational credentials while retaining recovery options

Passkey

A FIDO2/WebAuthn credential that enables passwordless authentication. Consists of a cryptographic key pair where the private key remains securely stored and the public key is registered with the service

WebAuthn

Web Authentication API - a W3C standard for passwordless authentication using public-key cryptography, forming the foundation of passkey technology

FIDO2

Fast IDentity Online 2 - an authentication standard comprising WebAuthn and CTAP protocols, enabling strong passwordless authentication

Discovery

A Uniqkey capability that gives administrators visibility into the web services employees sign in to and how those logins are protected, based on metadata collected by the browser extension in observe-only Discovery mode

Enrolment Token

A secret generated in the Admin Portal and distributed through browser policy, which enrolls Discovery installations into an organisation. Only its SHA-256 hash is stored

Verified Domain

An email domain the organisation registers as its own (for example company.com). Discovery only reports sign-in identities on these domains

B. API Overview

Uniqkey provides multiple API endpoints for different client types. All APIs use RESTful conventions with JSON payloads over HTTPS. Authentication uses JWT tokens obtained via SRP protocol.

- **Client APIs:** Mobile, Desktop, and Browser Extension endpoints for credential access
- **Organisation API:** Administrative operations (employee management, groups, policies)
- **SCIM API:** SCIM 2.0 compliant endpoints for identity provider integration

For detailed API documentation, contact your Uniqkey account representative.

C. References

[1] Verizon, "2025 Data Breach Investigations Report," 2025.

<https://www.verizon.com/business/resources/reports/dbir/>

[2] NIST, "FIPS 197: Advanced Encryption Standard (AES)," 2001.

<https://csrc.nist.gov/publications/detail/fips/197/final>

[3] D.J. Bernstein, "Curve25519: new Diffie-Hellman speed records," Public Key Cryptography, 2006.

<https://cr.yp.to/ecdh.html>

[4] Password Hashing Competition, "Argon2: the password hashing winner," 2015.

<https://www.password-hashing.net/>

[5] OWASP, "Password Storage Cheat Sheet," 2024.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

[6] NIST, "Post-Quantum Cryptography," 2024.

<https://csrc.nist.gov/projects/post-quantum-cryptography>

[7] Global Risk Institute, "2024 Quantum Threat Timeline Report," 2024.

<https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/>

[8] IETF, "RFC 6238: TOTP: Time-Based One-Time Password Algorithm," 2011.
<https://www.rfc-editor.org/rfc/rfc6238>