SECURITY PAPER

qredo.com

June 2021

Table of Contents

Design principles

Qredo is security conscious at every step of the software design lifecycle (SDLC).

Security ethos

- Security embedded into design, planning, architecture, and infrastructure.
- Balancing institutional grade security with application usability, speed, and convenience.
- Extra layer of security for Layer 1 asset ownership with multi-party computation.
- Proactive protection against known threats.
- Anticipation of future threats.

Usability

- Smooth adoption of security principles.
- Security protocols take human behavior into account.
- Customer-first configurable custodial policies and threshold signatory scheme hierarchies allows users to select the desired degree of oversight.

Privacy first

- Collect minimal data needed to run the services, as specified in our Privacy Policy.
- Limit access to essential customer data to those that need it.

24/7 support

- Qredo available at all times to help with customer issues.
- Support knowledge captured and relayed across our teams.
- Focus on continuous improvement.
- Advice users to operate latest version of OS for all apps.

Approach

Qredo adopts extensive processes and controls to ensure application security, from initial sign-up to every engagement with the Qredo Network. Assets on the Qredo Network are secured and protected by multiple layers of security.

Secure code development

- Qredo follows guidance from OWASP to secure against the Top 10 security risks.[1]
- Qredo engineers are familiar with common attack vectors and specific cryptographic and decentralized system attacks.

Framework security controls

- Qredo leverages modern and secure open-source frameworks that have built in security which reduce exposure to SQL Injection (SQLi), Cross Site Scripting (XSS), and Cross Site Request Forgery (CSRF), among others.
- Qredo implemented blockchain networks have inherent security.
- Cryptographic protocols such as MPC are orders-of-magnitude more secure than more common and widely-used Layer 1 transaction signing protocols.

Quality assurance

- Code and functionality are thoroughly reviewed and tested.
- A dedicated application security team identifies, tests, and triages security vulnerabilities in code.

Separate environments

- Testing and staging environments are logically separated from the production environment.
- No service data is used in our development or test environments.

[1] https://owasp.org/www-project-top-ten/

Staff security

- Training.
- Role-based access for secure environments.
- Rolling out BitWarden password manager for use with Qredo systems.
- Advise staff use latest OS.

Bug bounty program

- Report bugs to Qredo to qualify for a bug bounty.

User applications

Qredo protects its applications with multiple layers of security. User authentication takes place on devices against an incomplete software token in a web browser or mobile application. Qredo applications are secure against database breaches and man-in-the-middle intercept attacks because no credentials are exchanged between clients and servers in whole form.

- On initial sign up, users receive a One Time Password (OTP) to their emails.
- On authentication, users download the mobile signing application.
- The signing application secures access to the web application with Multi-factor Authentication (MFA).[2]

The web application

- The Qredo web application is a single user interface for managing multiple digital asset types.
- From this interface, individuals and organizations can access and manage portfolios and assets.
- The web application supports the following features:
    - Funds and wallet creation.
    - Custody policy management.
    - Address whitelisting.
    - Account auditing facilities.
- Fund managers and administrators of Qredo web application accounts are responsible for:
    - Defining custodial policies on funds which may include multiple signatories.
    - Defining the minimum threshold of signatories to authorize the movement of assets.
    - Account management.

The signing application

The Qredo Signing App for Android and iOS allows network participants to securely sign transactions through a combination of biometric and a master seed protected on the secure enclave.

[2] https://en.wikipedia.org/wiki/Multi-factor_authentication

- The signing application generates a cryptographic seed for securing user accounts on the network via mobile devices.
- Network transactions are protected with private/public key pairs generated by this single master seed.
- Qredo uses the BIP 39 standard[3] to generate a mnemonic sequence of 24 words which is used to recover the account in the event of a lost, stolen or damaged mobile device.
- The 24-word mnemonic is derived from a word list of 2048 words from the BIP 39 English Wordlist.[4]
- Users must write down/remember their seed phrase and keep it safe they only see it once**.**
- See the Qredo guidance on securing seed phrases.[5]

Governance of asset ownership

The flexibility of multi-signing means that no one person need control all the assets of an organization, eliminating single-point-of-failure attack possibility at the application layer.

- The Qredo Network allows account administrators to assign multiple roles and privileges to accounts.
- This network supports the appointment of custodians with governance responsibilities to authorize the management and transfer of assets.
- Transactions can only be approved according to user or organization defined custody policies.
- An administrator can appoint multiple custodians to sign and authorize transaction types.
- An organization can appoint multiple custodians, as well as multiple clients, to automate signing via sophisticated rule sets.
- This feature enables the provision of custody policies for every anticipated scenario. For example, a custody policy can be created to permit access to access assets in the event of a death.

[3] https://en.bitcoin.it/wiki/Seed_phrase
[4] https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt
[5] https://support.qredo.com/docs/seed-phrase

Mobile hardware security

Mobile devices have important security features that secure master seeds. Keys are generated and contained within the secure enclave of your mobile device by BLS cryptography. The public BLS key is used to register and authenticate the device on the Qredo Network.

No user-specific security information is stored on Qredo servers.

Android

- The Android keystore system[6] has its own storage space and processor that is separated from the primary storage of the device.
- The Android key store provides encryption.
- Some Androids have TrustZone technology implemented in their hardware (ARM processor).[7]
- The TrustZone technology implements Trusted Execution Environment (TEE) which binds the keys to secure hardware and isolates it from the Android OS. This means that it is protected against loopholes where other systems may have exposed internal storage in the device.
- Even with internal storage access, keys cannot be extracted from the device.
- Android has a screen protection mechanism preventing it from appearing in screenshots or from being viewed on non-secure displays. This minimizes the risk of adversaries collecting user data, credentials, or other sensitive information.

iOS

- The iOS secure enclave is a secure co-processor that includes a hardware-based key manager isolated from the main processor.[8] It guarantees encryption and security across the device.

[6] https://developer.android.com/training/articles/keystore

[7] https://developer.arm.com/ip-products/security-ip/trustzone

[8] https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/storing_keys_in_the_secure_enclave

Frontend security

The Qredo frontend infrastructure relies on a number of industry-standard security protocols for proactive protection.

The web application and iOS application were pen tested in September 2020 for OWASP top 10 threats.

Our internal security expert has given the frontend web application an excellent rating in June 2021, by implementing the following secure protocols and threat protection:

- The web application very simple and secure. Due to MFA signing app, there is no way an unknown attacker can inject any malicious code as every activity and transaction must be confirmed by the MFA signing app.
- MFA (multifactor authentication) does not rely on external services, like Google or Microsoft Authenticator, FreeOTP, or DUO Mobile for example. Qredo has its own mobile signing application with which any operation (swaps, transfers, authentication) must be confirmed. Users must make additional confirmations by entering a PIN code (at least 6 chars long), authenticating on Mobile Kernel Authenticator, and confirming all operations. All MFA activity is logged.
- Web application uses HTTP version 2 which reduces reduce load latency by using techniques such as compression, multiplexing, and prioritization.
- HTTP/2 is 14x faster than HTTP/1 by using a binary framing layer, as opposed to HTTP/1.1 which keeps all requests and responses in plain text format. Binary is more efficient, requires a single channel for parallelism, and is prone to fewer errors.
- HTTP/2 uses the binary framing layer to encapsulate all messages in binary format, while still maintaining HTTP semantics, methods, and headers.
- Multiplexing in HTTP/2 means there is less noise on network, and fewer fingerprints throughout the network.
- All known HTTP/2 attacks failed on the Qredo web application.
- More info on HTTP/2.[9]
- Qredo uses AWS CloudFlare Argo tunnel which isolates the web application.[10] Argo tunnel hides the origin server, the real IP address completely hidden to the outside world. Argo tunnel provides remote access to development environments by creating secure outbound-only connections to Cloudflare's edge network from a resource exposing it to the Internet. Argo tunnel sits in front of the hostname and checks for identity on every request.
- Web application is fully protected against Cross-Site Scripting (XSS), SSRF, CSRF, XXE, injecting headers, etc. All these operations are forbidden and protected against by WAF.

[9] https://http2.github.io/faq/

[10] https://www.cloudflare.com/products/tunnel/

- The application stores user geographical coordinates of the users to notifying them about previous operations, activity.
- Web application uses JWT session tokens which could be expensive as a token is created for every session.
- However, JWT has strong security. The HS256 algorithm for JWT token (HMAC + SHA256) is an algorithm that combines a certain payload with a secret using a cryptographic hash function like SHA-256. The result is a code that can be used to verify a message only if both the generating and verifying parties know the secret.
- Developers use UBI keys.
- AWS key management service[11] for client keys.
- AWS manages all logging and monitoring.

[11] https://aws.amazon.com/kms/

Backend security

The Qredo Network backend consists of two separate systems:

- The backend Qredo blockchain which stores an immutable data record of asset ownership.
- An MPC cluster which secures all transactions against Layer 1 blockchains.

The Qredo blockchain and MPC systems work in sync. They are cryptographically linked and provide privacy and non-repudiation.

The Qredo backend technology stack uses the Qredo-managed, open source Apache Milagro core security infrastructure libraries for decentralized networks and distributed systems.[12] These robust encryption libraries offer an alternative to centralized trust providers and solve common implementation issues, such as scaling for example.

Equinix data centers

The following table details the data center specifications.[13]

NODE LOCATION	UPS SYSTEM REDUNDANCY	COOLING REDUNDANCY	CERTIFICATIONS
TOKYO	N+1	N+20%	SOC 1 Type II SOC 2 Type II ISO 27001 PCI DSS FISC
HONG KONG	2N	N+1 Chillers N+20% CRAC units	SOC 1 Type II SOC 2 Type II ISO 27001 PCI DSS TVRA

[12] http://milagro.apache.org/docs/milagro-intro/
[13] https://www.equinix.com/data-centers

LONDON	N+1	N+1	SOC 1 Type II SOC 2 Type II ISO 27001 PCI DSS OHSAS 18001 ISO 9001: 2015 ISO 22301 ISO 14001: 1015 ISO 50001
NEW YORK	N+1	N+1	SOC 1 Type II SOC 2 Type II ISO 27001 NIST 800-53 / FI PCI DSS HIPAA
CHICAGO	N+2	N+2	SOC 1 Type II SOC 2 Type II ISO 27001 NIST 800-53 / FI PCI DSS HIPAA
SINGAPORE	N+1	N+1 Chillers N+25% CRAC units	SOC 1 Type II SOC 2 Type II ISO 27001 PCI DSS SS 564 TVRA OSPAR

Qredo blockchain

The Qredo Layer 2 blockchain runs on six validator nodes built on Tendermint. Tendermint is built on a DLS solution to the Byzantine Generals' Problem[14] which operates using energy efficient Proof of Authority and does not require proof of work mining protocols.[15] Each node will continue to process transactions if up to 1/3 of machines fail in arbitrary ways. Consensus is subject to more than 2/3 of validator nodes (subject to voting weight) verifying and authorizing each new block. This removes single points of failure and ensures the integrity of transactions on the network.

Tendermint provides defenses against common blockchain attack scenarios[16] such as flip-flopping, phantom validators, and on-chain attacks. Tendermint implements strict security protocols and runs its own bug bounty program.[17]

Qredo has implemented its own custom library over the Tendermint protocol that implements transaction and transfer types. This library will be open sourced on the release of the Qredo client code.

Each Tendermint node is secured on HSM[18] hardware devices hosted in six Tier 4 secure data centers located across the world.

Qredo blockchain transactions are secured with BLS signatures.[19] Any transaction against Layer 1 digital assets such as BTC, ETH, etc., are secured with an external multi-party computation cluster for enhanced security.

Proof of reserve (PoR)

The Qredo blockchain manages assets on underlying chains.

Exchanges have been hacked in the past without customers knowing if the exchange had sufficient funds to pay out. The insolvency only became evident when customers attempted to withdraw all their funds.

Qredo secure protocols allow anybody to determine the solvency of Qredo and ensures that Qredo is not acting as a fractional reserve.

- The Qredo ledger is transparent.
- Total assets held by Qredo can be viewed at any point in time.

[14] https://arxiv.org/abs/1809.09858
[15] https://tendermint.com/static/docs/tendermint.pdf
[16] https://docs.tendermint.com/master/spec/light-client/accountability/
[17] https://tendermint.com/security/
[18] https://en.wikipedia.org/wiki/Hardware_security_module
[19] https://en.wikipedia.org/wiki/BLS_digital_signature

- The mapping between Qredo funds (Layer 2) and the underlying cryptocurrencies (Layer 1) backing them is always publicly available via a visible demonstration that sum (layer 1) = sum (layer 2)

Multi-party computation (MPC)

BLS signatures enforce Qredo Layer 2 transaction security, as mentioned, and an MPC cluster provides an industrial-scale wallet functionality to the whole of the Qredo network by securing all transactions on underlying Layer 1, hard-asset blockchains.

The MPC uses a threshold signature scheme with a trustless key generation setup. Each MPC node manages a share of the cryptographic secrets so an attacker would have to successfully breach more than the threshold of nodes and gather sufficient key shares to enact a successful attack on the system.

- MPC is based on the Threshold Signature Scheme (TSS).[20,21,22]
- MPC provides keys and ECDSA signatures to an authorizing Qredo blockchain node for Layer 1 transactions.[23]
- MPC enables multi-party signature functionality for Layer 2 account wallets.
- Removing single-point-of-failure concerns around users having to protect their own hard-asset wallet private keys, MPC safeguards the generation and storage of private key shares across the Qredo ecosystem.
- It provides trustless secrecy, transaction correctness, and customer privacy.
- The MPC cluster generates private key shares, signs transactions, and guarantees that an attack will only succeed if a bad actor gets access to more than the signing threshold of secret shares.
- The signing threshold is around two thirds of the total shares that make up a private key. Private key share generation and storage is managed by nodes.
- Proactive security controls rotate keys around nodes at regular intervals.
- The MPC code is written in C for speed, efficiency, and security.
- A Python wrapper enables application development against the C code; for example, by supporting communication over a point-to-point protocol.
- MPC cluster nodes communicate point-to-point over HTTPS.
- Qredo has secured its MPC clusters in tamper-proof Raspberry Pi 4s residing in six Equinix hardware boxes across the globe.
- A Zymbit HSM[24] stores a key that encrypts the hardware. If pressure triggers the sensors, the system destroys the key, the device powers down, and it cannot restart.

[20] https://eprint.iacr.org/2019/114.pdf
[21] https://en.wikipedia.org/wiki/Threshold_cryptosystem
[22] https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing
[23] https://www.qredo.com/blog/mpc-over-ecdsa-signatures
[24] https://www.zymbit.com/

Platform threats

Denial of service (DDoS/DoS)

- HashiCorp Vault encrypt secrets and sensitive data at rest and in transit over the data centers.[25]
- Adversaries may perform Network Denial of Service (DDoS) attacks to degrade or block the availability of targeted resources to users.
- Network DoS can be performed by exhausting the network bandwidth services rely on.
- Qredo monitors resources to ensure that we provide sufficient bandwidth for demand. We also take the following steps:
  - Monitor traffic to detect for DDoS attacks.
  - Detect and stop malicious users by recognizing and filtering traffic such as that are originating from known attack addresses, known bot agents or from locations that are known to be the major source of attacks.
  - Detect and stop malicious application layer requests by recognizing and filtering excessive numbers of requests from a single source or user session, known application signatures and traffic that does not conform to known HTTP protocols.

Phishing

- Qredo client administrators may define policies and a minimum threshold of signatories to authorize the movement of assets, and all other actions to a fund e.g. changing an account email address.
- Policies can involve as many signatories as desired.
- This system reduces the risk of successful phishing attempts as multiple signatories would need to be compromised for a successful phishing attack.
- Whitelisting safe addresses.

[25] https://docs.equinix.com/en-us/Content/Edge-Services/SmartKey/kb/SK-hashi-vault.htm

Credentials access

- Qredo promotes the adoption of secure practices for storage of the seed recovery phrase.
- The Qredo signing application enables secure access to accounts and secure signing of transactions through a combination of biometric and a master seed protected on the secure enclave**.**
- MPC nodes store parts of the private keys so an attacker would need to access a number of nodes and access more than the threshold of cryptographic secrets.
- Qredo has measures in place to ensure that the Qredo Network can return users their deposits. The tasks can be performed even if the Qredo blockchain is completely unreachable.

Infrastructure

- Qredo's infrastructure of nodes in multiple geographical locations removes any single point of failure and ensures the integrity of transactions on the network.
- Via a series of steps, customers can have their deposits restored to a recovery wallet.
- The Qredo Security Architecture provides back up connectivity, failover and resilience in the event of an attack.

Code dependency attack

- Our code is audited regularly and we proactively monitor for new security developments.
- We have continuous integration, unit testing and different engineers in charge of different parts of the platform.
- We expect constant changes in the security landscape, as new bugs and security risks are discovered.
- We have multi-year commitments signed with the leading security audit firm TrailofBits.

Auditors

- Zokyo performed a pen test of the web application and iOS application in September 2020.[26]
- NCC Group reviewed the Apache Milagro MPC library in July 2020.[27]
- Quantstamp reviewed the Ethereum Solidity contracts in May 2021.[28]
- Marsh McLennan are going to review operational security of the platform in July/August 2021.[29]
- Trail of Bits are going to review the platform in September 2021.[30]

[26] https://www.zokyo.io
[27] https://research.nccgroup.com/wp-content/uploads/2020/07/NCC_Group_Qredo_Apache_Milagro_MPC_Cryptographic_Review_2020-07-16_v1.3.pdf
[28] https://quantstamp.com
[29] https://www.marsh.com/us/services/marsh-risk-consulting.html
[30] https://www.trailofbits.com

Compliance

Qredo supports the implementation of best practice protection controls based on industry standards.

Qredo is planning for ISO 27001 and SOC2 certifications.

Privacy and data protection

For information on Qredo's privacy and data protection policies, please visit Privacy Policy.

Legal resources

For information on Qredo's terms of service, please visit Qredo Terms of Service.