LeverID - A Post-Quantum Digital Identity and Signature Platform

LeverID is designed to provide a **single universal authentication and signing medium for government and business verticals.**

If individuals happed to hold a Government-issues identification document (either a passport or some sort of identity card), LeverID can be added on top of it, providing a true digital identity.

Since LeverID is offered as a white-label solution, countries nd organizations can customize (for example, rename and rebrand) the platform in rder to sut their needs.

Post-quantum cryptography problem

RSA-based encryption has been around since the late 70s, and a staggering 80% of the world's encryption is still reliant on it. But why exactly is it an issue?

RSA encryption works by choosing two distinct prime numbers and multiplying them. In 1994, a quantum algorithm that factors large trapdoor function numbers was discovered, leading the world one step closer to cracking RSA encryption.

In other words, it's easy to have two prime numbers, for example, 199 and 227, multiply them, and obtain 45173. However, calculating this in reverse is a much more troublesome endeavour.

Unfortunately, quantum computing algorithms are likely to be able to perform this in the very near future, essentially rendering RSA-based encryption useless.

The LeverID platform has been designed in a way that enables us to implement multiple cryptography standards. This will include post-quantum resilient cryptography standards once they've been established and agreed upon, internationally.

How does LeverID work

The **first phase** of the LeverID solution is for the individual user to **create a digital identity**. After the user's request to create a LeverID identity is made, LeverID will validate user eligibility, either through a third party 'Know your Customer' (KYC) provider, or a Government Registration Authority.

The **second phase** of LeverID begins when a user **initiates an authentication or a signing request** via LeverID via a 'Relying Party' (a service provider or vendor). Depending on the user's request, either an **authentication** certificate or a **signing** certificate is validated against the LeverID database.

If eligibility is met and confirmed, LeverID initiates the process of creating an authentication and signing certificate for the user.

Once this process is followed through, the **user obtains valid certificates in order to authenticate and sign digitally.**

The LeverID solution

The LeverID solution consists of **three principal components**:

- Server application and Hardware Security Module (HSM)
- Mobile device application
- Application Programming Interface (API) for Relaying Parties (RP)

For a higher level of security, both the user and server have **independent private keys**. The server and user's mobile device both sign the document or authentication challenge independently with their private keys. These signatures are then cryptographically combined into a standard verifiable digital signature that verifies against the user's public key certificate.

In addition, **two-factor authentication is used**. Both the user's mobile device and the server use independent mechanisms to authenticate the user.

CONTINUES

The critical components of LeverID

It is important to differentiate between **component responsibility** when talking about a **state/country or a private company** in terms of where the accountability of the components will lay.

The **critical components** of LeverID digital authentication and signing platform are:

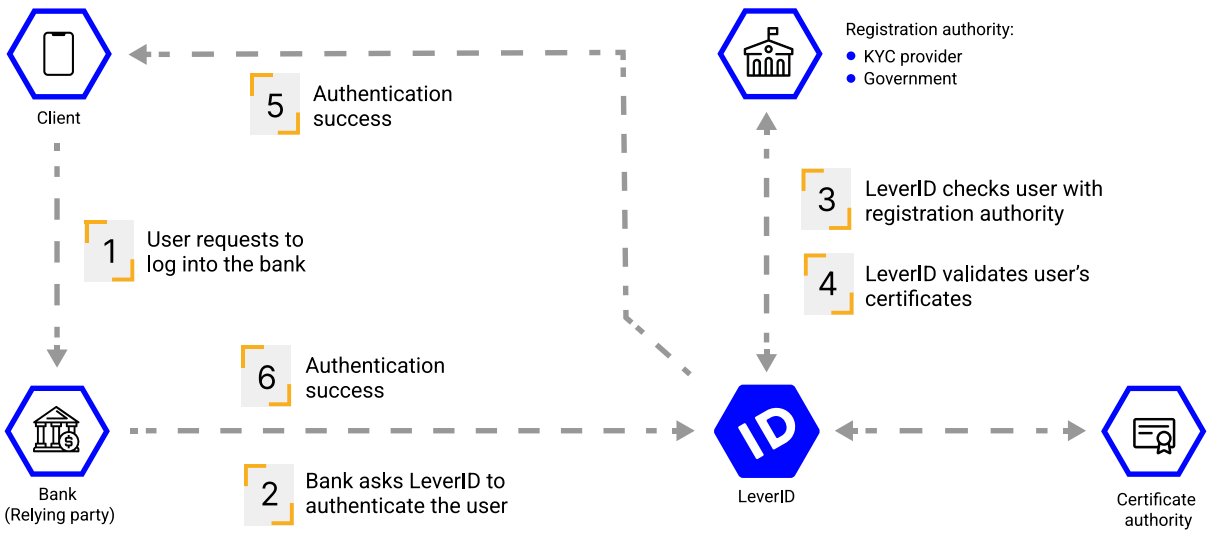
- Hardware Security Module and server application
- Mobile device application
- API for relaying parties
- Registration Authority (RA)
- Certificate Authority (CA)
- Verification Authority (VA)

In the case of state/country digital identity, all six components will be under the control of the state that is responsible for the identities.

The LeverID infrastructure will be configured and set up on-site and control can be handed over to responsible governmvent institutions.

In the case of private digital identity, the accountability will lay on the LeverID certified infrastructure. In order to provide LeverID with identities, the KYC service provider's information is used via an API. LeverID will continue to validate certificates for authentication and signing requests.

If certificates are proven to be valid, the user will be issued a challenge code through LeverID. If the challenge codes match, the user is prompted to enter their 4-digit authentication PIN or 5-digit signing PIN. If these PINs are then proven valid, authentication or signing can take place depending on the initial request.



What are the benefits of LeverID?

LeverID has several benefits both for governments and businesses. While some of them are universal, others are specific to each.

- Post-Quantum Capable Design
- Data Security & Ownership
- Ease of Integration
- Mobile-First Design
- Enhanced Employee Onboarding
- Fully Customizable Approach
- Scalability and Flexibility
- Fast Transaction Speed
- Attack-Tolerant and Reliable
- Universal Login