

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

Contact

info@leverid.com
+372 656 5600
www.leverid.com

LeverID



LeverID is a Post-Quantum Capable Digital Identity and Signature Platform. In case individuals hold Government issued identification document (either passport or some sort of identity card), LeverID can be added on top of that, giving individuals a real Digital Identity with all the benefits and functionality. Since we also offer LeverID as White-Label solution, countries and organizations can customize (e.g. rename and rebrand) the platform according to their needs. In order to respond to the call of modern technology trends, LeverID was especially designed as mobile-first application making it usable wherever life takes you provided that there is internet connection.

What are the benefits of LeverID?

- 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

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 'Relaying 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 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. In the case of private digital identity, the accountability will lay on the LeverID certified infrastructure.