Enable Seamless Communication Between Issuers and mDL/mID/Wallet Providers

Scytáles Credential Service Provider (CSP) provides a unique and trusted service between the issuer's users and mDL/mID/Wallet providers, in practice, a direct contact between an External Registration Authority and a CSP

Scytáles CSP Features and Capabilities

Decentralised Issuers

There may be thousands of decentralised issuers. Each of these needs to collect and store their issued keys as part of a master list. The CSP helps to centralise these lists and provide a single source of trust.

Regional and Bilateral Agreements

Regional and bilateral agreements imply the manual exchange of verification data with another party. While this may be feasible for smaller parties, it is not feasible when dealing with thousands of issuers.

High Availability

The setup is database-driven, requiring three nodes to enable high availability. The setup uses a NoSQL database.

Security

- Implementation of data security at risk for the NoSQL database
- Two-factor authentication for login
- Proxy server to secure communication between endpoints
- Deployment of SSL endpoints
- Provision of a client to secure communication between the mDL/mID/Wallet repository and the client
- Load balancing solution to provide availability
- Storage of private keys within a FIPS-140-2 Level 3 secured device

SALES@SCYTALES.COM

WWW.SCYTALES.COM

Copyright © Scytáles AB 2023

Enhancing Trust and Connectivity

The core goal of the Credential Service Provider (CSP) is the establishment of TRUST between Issuing Authorities and Relying Parties. Just like the security features of a physical credential support its trustworthiness, a Relying Party requires the means to be assured of the authenticity and provenance of a digital identity document. The CSP will only maintain public keys for the issuing authorities. The current approach is for in-person (over the counter) and online (over the web) use cases where the credential needs to be verified.

How can the Scytáles CSP be delivered?

When it comes to delivering a versatile and powerful CSP, flexibility is critical. We understand that different organizations have varying requirements and approaches to implementing such solutions. That's why we offer multiple delivery options to cater to your unique needs.

Stand-Alone Project Development

If you're starting from scratch or need a dedicated CSP solution, our team can develop a whole new project specifically tailored to your objectives. This approach offers a clean slate for creating a customised solution that aligns perfectly with your requirements and branding.

Integration with Existing Solutions

We recognise the importance of seamless integration with your current systems. Whether it's an existing solution or a broader identity management platform, our CSP can be integrated as a complementary component. This ensures you can enhance your current offerings without needing a complete overhaul.

No matter which delivery option you choose, the Scytáles CSP is designed to meet the highest industry standards for security, usability, and performance. We're committed to providing you with a solution that not only fits your immediate requirements but also scales with your organization's growth. Plus, with our team of experts and comprehensive support, you'll have the guidance you need throughout the entire process.

Verifying a Digital Credential

- Obtain the original credential and the digital signature
- Verify the time of the issuance
- Verify the digital signature of the credential
- Verify the chain of issuance
- Verify that the credential has not been revoked in any way

Discover how our CSP can transform your digital identity management strategy by getting in touch with our team to help you select the delivery method that aligns best with your goals and infrastructure.

SALES@SCYTALES.COM

WWW.SCYTALES.COM

Copyright © Scytáles AB 2023