Vereign SEAL

vereign.com/seal

Verifiable Data Credentials for data spaces & more - Overview

Vereign SEAL

SEAL verifiable data credentials offer a unique combination of

- decentralized application available over the web, as integrated into browser and mobile app;
- blockchain secured data transport and archival;

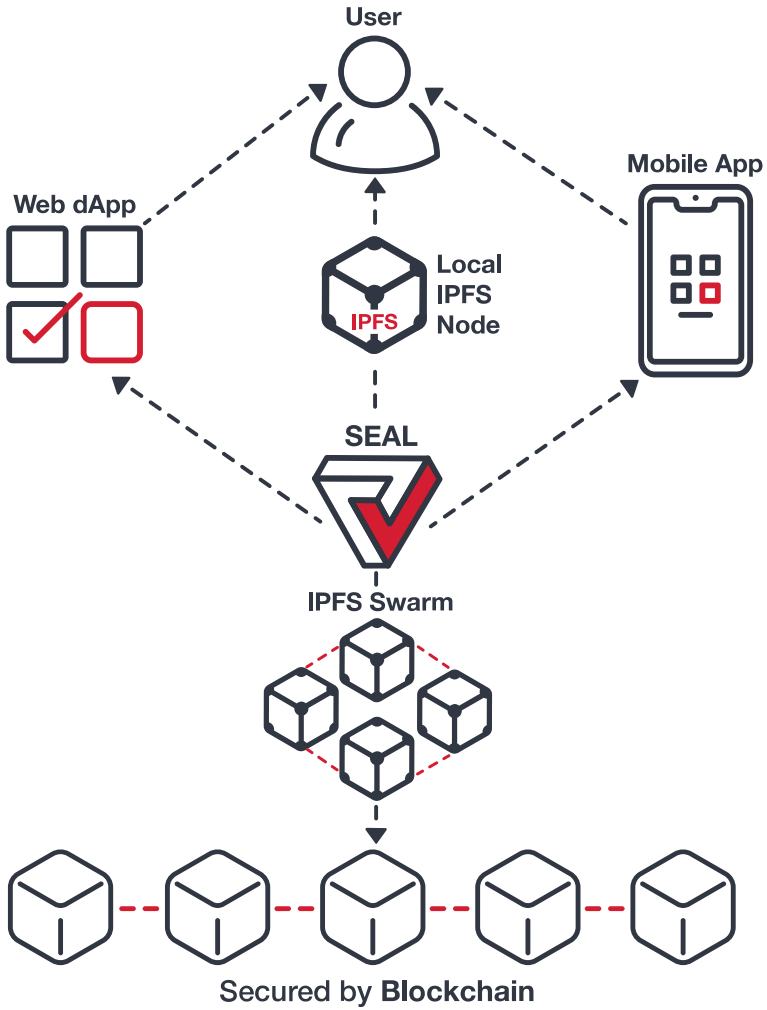
into one comprehensive solution that is usable for a variety of data space scenarios. It is readily available for **email** and **documents** today, but can be readily adapted in any scenario where compliant and secure user sharing and interaction are central, such as decentralized customer portals.

Professionally Supported

Vereign SEAL is available as fully supported product including guaranteed security updates, assured response and resolution times.

Vereign also offers the whole range of professional services, including integration, consultancy, development, and training.

Contact **sales@vereign.com** or call **+41 41 541 50 63** to let us know how our SSI experts can support you.



Vereign SEAL

vereign.com/seal

Verifiable Data Credentials - Technology

Verifiable data credentials offer multiple benefits over legacy native & web applications and data delivery:

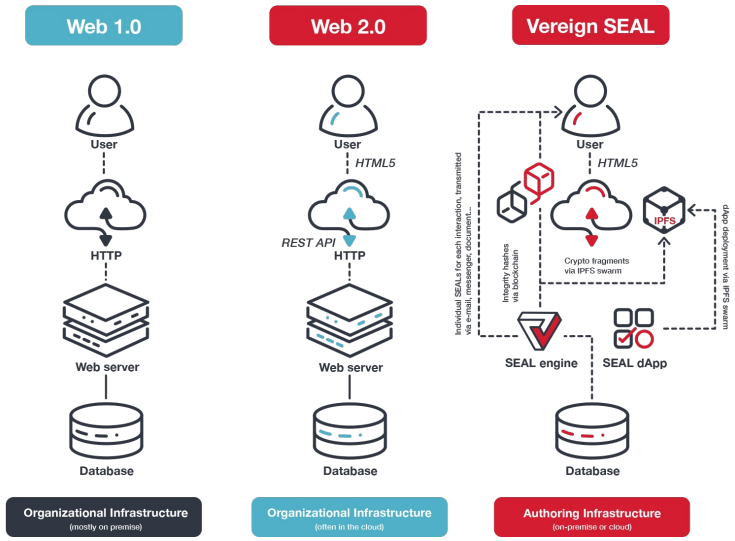
Usable on any device
- Decentralized application requiring zero user installation
- Application integrity secured by cryptographic hashing
- Easily provided as mobile and browser apps for even higher security, convenience and persistent device storage

Decentralized data storage
- IPFS swarm data storage using peer to peer transmission
- Persistent pinning on participant nodes

Serverless scaling at the edge
- Memory and compute exclusively on local user device
- Local data persistence in IPFS swarm for low latency

Authentic and revision secure
- All data secured against blockchain
- Highest level of proof for virtually any use case

Security & Compliance
- Data scarce, privacy by design, GDPR compliant
- No more internet connected databases to breach



SEALing in action

1. Each SEAL is generated in the SEALing engine where data is encoded into the correct sematic format
2. Afterward it is compressed, encrypted and its hash is anchored against the blockchain.
3. The encrypted container itself is split into fragments, which are stored into IPFS.
4. Key material and some data fragments are combined with the correct application URL and encoded into a link.
5. The link can be transported in any form over any medium, by default the SEALing engine encodes it into a small QR code.