rusty_auth

Distributed, Master-Slave encrypted store to generate, access and distribute dynamic secrets using modern encryption technologies and an encrypted file system.

Keep authentication tokens, passphrasses, certificates and encryption keys in a simple, easy to access encrypted key-value store.

Access from CLI, web-broswer and GUI

Technologies to use

1. Secstr - for in-memory encryption
2. CHACHA20-POLY1305 AEAD for authentication and encrypted tokens
3. Support for SHA256, KECCAK, HMAC etc
4. SRP & TLS-SRP
5. Rotating keys default-hourly and maintain connected until connection closed
6. Support TLS
7. Support email DMARC authentication
8. Support HTTP1/1 , HTTP/2 and QUIC, MLES, CoAP and Webscokets
9. Support some streaming protocols
10. Support TOTP, QR-CODE auth, email reset, Hardware Auth, SSO-Single Sign On, One-Click Account Suspension, re-assignment and Deletion, passhrase generation.
11. Raft Consensus Algorithm for Multi-DataCentre distributed systems
12. File timed-access
13. Secret Sharing & support for hardware based authenticated secret sharing
14. Two-factor auth
15. Access levels & access Rights with logging and notifications
16. Backend Public FIle Access from server
17. Firewall & De-militarized zones
18. Key-Value Store to protect other secrets
19. Shared-Secret passphrase reset.