Certificate StoredSafe

Most organizations today rely on several different PKI components and vendors to achieve and secure inter-system data transfer, cross organizational communication, client logon and system access. Manage the certificates related to these solutions is a key component that the organization needs to manage to ensure a PKI installation.

Certification Management Made Easy

Solution–Certificate StoredSafe
Certificate StoredSafe enables the organization to securely store, ensure and prove that certificates and related information are known to and restricted to only authorized personnel.

Furthermore it provides critical information such as who has seen what certificate key passphrase, certificate last changed, certificate expirations, etc.

Certificate StoredSafe will reduce your risk significantly as well as improving your incident response capability by raising your control level, helping you monitor, alert and respond to operational risks posed by any certificate in you environment without vendor specific limitations.

Example of usage of your one stop shop for certificate information:

- Store and administrate your private keys and passphrases
- Store and administrate your public keys
- Store and administrate certificate meta data (inception date, expiration date, usage, etc.)
- Dynamic triggering and alerts for upcoming expiration dates and hosts needing renewed certificates.

This product is the one storing certificate signing requests, certificates, certificate key files and confidential information related to your PKI-Infrastructure.

STOREDSAFE

Secured Storage and Sharing of Highly Confidential Information

StoredSafe is a premium security appliance company utilized by organizations who have strong business security requirements related to critical data that needs to be shared with internal/external parties over time and in an auditable way.

Contact | Telephone: US +1 (717) 444 1010 | Telephone: Europe +46-8-5000 2140 | E-mail:sales@storedsafe.com | https://storedsafe.com

Technical Specifications

StoredSafe Secure Platform
All our products utilize the StoredSafe Secure Platform. Our unique architecture puts the information owner in control of the information on a scalable platform and enables an organization to choose between our products, based on their needs as well as adding functionality over time.

StoredSafe Audit Engine
All events in StoredSafe Secure Platform are logged and traceable in our easy to use audit engine.

2-factor Tokens
Our preferred, recommended solutions are Yubico's YubiKeys as client-side hardware token and Google Authenticator in addition to a strong passphrase.

Hardware Security Module (HSM)
To further improve security, YubiHSM (Hardware Security Module) is incorporated in the platform to store cryptographic keys for all YubiKey hardware tokens. This provides an excellent YubiKeys and Google Authenticator server and enables our customers to be independent of Internet connectivity.

StoredSafe Overview
Strong Encryption
To assure confidentiality over time all StoredSafe products can easily change encryption algorithms and modes (OFB, GCM, etc.) as needed without putting current data at risk.

Data at Rest
StoredSafe utilizes 4096 bit RSA Keys for asymmetric encryption and AES-128 in OFB mode for symmetric operations.

Data in Transit
StoredSafe uses TLS for protection of data in transit.

Role Based Access Control System
StoredSafe utilizes a Role Based Access Control System (RBAC) to supply a fine grained control of user capabilities and vault permissions.

Defining requirements, procure and implement a secure password management solution could be a challenging task. Below are some of the key factors an organization should consider for a secure password management solution.

Desired Outcome	Factors to Consider	Password StoredSafe	
Owner of information should be in control of the information.	Can only the information owner grant access to the information?	Password StoredSafe has no master key. Not even a system administrator can access information, unless the information owner has provided access.	✓
Access on a business need to know basis.	Does the solution support relevant business roles and responsibilities?	Password StoredSafe has a comprehensive and flexible RBAC system which is easy to administer.	✓
Full traceability.	Will the solution provide a full audit trail on all important events?	StoredSafe Audit Engine provides a full audit trail.	✓
Cost efficient setup for external information sharing	Does the solution facilitate information sharing with outside organizations?	Password StoredSafe supports different password policies per vault. Password StoredSafe also warns users when a stored password fails compliance.	✓
Cost efficiency	Total Cost of Ownership (TCO)	StoredSafe has a low TCO, a low cost for implementation and low annual operational cost.	✓
Scalability	Growth in number of users	StoredSafe can grow to thousands of users and additional StoredSafe functionality by adding modules as needed.	✓