Password StoredSafe

Most organizations are faced with the challenge of storing of critical passwords and encryption keys securely. The necessity to share the password for certain accounts within an organization and the challenge to provide full audit trails are in conflict with basic compliance requirements and common security practices. As the threat environment has changed, more organizations and regulators have further tightened the requirements for the storage and administration of passwords for critical accounts and encryption keys. Common solutions such as storage of passwords in protected Microsoft documents or individual password applications need to be replaced with a secure enterprise solution.

Password StoredSafe
The primary objective of Password StoredSafe is to securely store and share passwords as well as other critical information related to your passwords on a "real" need to know basis with a full audit trail. Our solution ensures that even the Password StoredSafe system administrators do not have access to the critical information. The information owner maintains the master encryption key and is the person who remains in control!

Passwords StoredSafe is used to share passwords in a secure way. This functionality includes: full traceability of who has seen what, when passwords were accessed, an unlimited number of password policies, two factor authentication, regulatory compliance, role based access, assignment of privileges by the information owner, audit reports, and strong encryption.
This product is especially strong for protecting critical passwords against the risk of unauthorizedor unintentional access, hacking attacks, vendors and disgruntled employees. In addition, this solution can be used when there is a need to store passwords at other physical locations such as a hot site for disaster recovery, outsourcing, etc.

Our solution easily integrates with your current IT infrastructure without any major redesigns.

Examples of common uses of Password Storedsafe:

- Passwords for privileged accounts (root, sa, etc.)
- Password for service accounts
- Encryption keys
- PIN codes (alarms, safe combinations) Passphrases

The Key Benefits of Password StoredSafe:

- **Information Owner in Control** – Only information owner can authorize access.
- **Protection of Highly Critical Passwords** - all high-risk information is protected by an additional authentication factor, strong encryption and authorized access to all users.
- **Regulatory Compliance** – Several regulatory and common security standards require secure storage and traceability for privileged accounts.
- **Convenient and Easy to Use** – Easy maintenance and full traceability to ensure passwords are updated and maintained on a needed basis based on defined requirements.

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.

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.	✓