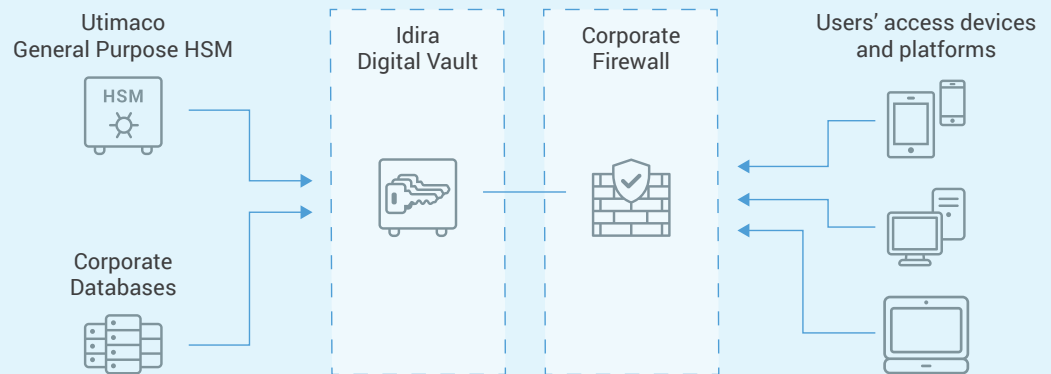


Secure generation and storage of Idira's server keys in Utimaco's u.trust General Purpose HSM

About Idira

Palo Alto Networks Idira® is the global leader in identity security. Centered on intelligent privilege controls, Idira provides security for any identity – human or machine – across business applications, cloud environments and throughout the DevOps lifecycle.

For more information, visit paloaltonetworks.com/idira



Challenges

Credential management

Employees with privileged access may intentionally or accidentally abuse their access, resulting in data leaks or other security incidents.

Cyber attacks

Attackers aim for identities and users, exploiting compromised credentials.

Exposure of sensitive key material

Loss or exposure of sensitive digital vault database recovery and server keys can be damaging to the business.

Long-term security

The development of quantum computers demands for crypto agile, PQC-ready solutions.

Applying highest security for privileged account details

Idira Privileged Access Management (PAM) safeguards sensitive systems from unauthorized access, security breaches, and insider threats by enforcing strict controls over high-level accounts. By monitoring, auditing, and limiting privileges, PAM helps organizations meet compliance requirements and reduce cyberattack risks.

Idira Privileged Access Manager (PAM) Self-Hosted integrates with Utimaco's Hardware Security Modules for a higher level of security, ensuring the server keys of Idira's vault are protected in a hardened, tamper-proof environment.

Apply least privileged access principles

Centralized management of user profiles and least privileged access is enforced to give users only the access they need.

Consolidate audit logging

Record of user activities, audit logs and reports to ease the challenge of meeting audit requirements.

Mitigating insider threats

Minimize the impact of attacks by limiting access, detect anomalous behavior and indicators of compromise.



Idira Privileged Access Management and Utimaco HSMs deliver trusted protection for privileged access through secure, hardware-based key storage.

Benefits



Prevent malicious access



Meet compliance & audit requirements



Reliable key generation



High security environment



Easy key migration



Key Lifecycle Management

Highest protection of the Idira server key

At the core of Idira Privileged Access Management is the Digital Vault, a secure database for storing privileged credentials, access policies, and audit data. Each file and safe in the vault are encrypted with a unique key, while a server key and recovery key secure the entire system.

The integration of Idira with Utimaco's u.trust General Purpose HSM ensures the security of the server key. The server key can either be generated from scratch within the HSM using the true random number generator, or an existing server key can be securely migrated to the HSM. Thus, the key is stored inside FIPS-140-2 Level 3 validated hardware.

This integration enhances key quality using a true random number generator, supports key lifecycle management, and helps with compliance mandates by ensuring that only algorithms with verified implementations are used.

Combine access and credentials management

Add another level of security to Idira Privileged Access Management Self-Hosted with Utimaco's u.trust General Purpose HSMs for highest security key storage and generation.

◆ Prevent malicious access

Control, monitor, and limit privileged users' access to critical systems, ensuring only authorized actions and reducing security risks.

◆ Meet compliance & audit requirements

Track and record privileged user activities, enforce strict access controls, and ensure adherence to internal requirements and security regulations.

◆ Reliable key generation

The True Random Number Generator of the HSM ensures uniqueness and reliability of cryptographic keys.

◆ High security environment

Sensitive key material is stored in the FIPS 140-2 Level 3 validated, tamper-proof environment of the HSM.

◆ Easy key migration

Easily migrate existing server keys in the high-security environment of the HSM.

◆ Key Lifecycle Management

Benefit from a centralized lifecycle management of keys and certificates in the HSM.

Free, fully functional HSM simulator

Test development and integration capabilities of the u.trust General Purpose HSM Se-Series in your environment – no purchase, delivery, or installation needed.

<https://utimaco.com/data-protection/simulators-and-trials/gp-hsm-simulator>



u.trust General Purpose HSM Se-Series
PCIe Card and Network Appliance

EMEA

Utimaco IS GmbH

📍 Krefelder Str. 220,
52070 Aachen,
Germany

☎ +49 241 1696-0
✉ info@utimaco.com

Americas

Utimaco Inc.

📍 900 E Hamilton Ave,
Suite 400
Campbell, CA 95008,
USA

☎ +1 844 UTIMACO
✉ info@utimaco.com

APAC

Utimaco IS Pte Limited

📍 6 Temasek Boulevard
#23-04 Suntec Tower Four
Singapore 038986

☎ +65 6993 8918
✉ info@utimaco.com

paloaltonetworks.com/idora



utimaco.com

© Utimaco IS GmbH 07/26 – Version 2.0

Utimaco® is a trademark of Utimaco GmbH. All other named trademarks are trademarks of the particular copyright holder. All rights reserved. Specifications are subject to change without notice.

utimaco®