

Technical Data Sheet

Keymaster

High security keyserver

Keymaster is a central keyserver that enables powerful and flexible management of private asymmetric keys. It offers a secure, flexible and integrated solution for managing and storing cryptographic keys for companies and public authorities.

Functions

- **Generation of key pairs:** Keymaster enables the secure generation of key pairs consisting of a public and a private key. The generation is based on proven cryptographic algorithms and standards.
- **Storage and protection of private keys:** Private keys used to decrypt encrypted data or for digital signing are securely stored by Keymaster. Keymaster offers numerous protection mechanisms to prevent unauthorized access to key material.
- **Support for numerous cryptographic algorithms and standards:** Keymaster uses standardized cryptography wherever possible. This increases both security and interoperability.
- **Highly flexible solution:** Keymaster, in combination with additional management modules/applications, allows for keys to be used for both group mailboxes as well as deputy arrangements. This covers a variety of scenarios, including vacation replacements, front office solutions and employee departures. This not only increases flexibility but also creates transparency and ensures efficient key management.
- **Integration into other systems:** Keymaster can be seamlessly integrated into existing IT environments. The product offers APIs and interfaces that enable easy connection to other security and communication systems. For example, cryptographic keys and certificates can be used for email encryption, digital signatures, VPNs (virtual private networks) and other applications.

Technical Data Sheet - Keymaster

Features	• Secure storage: Keymaster is a comprehensive solution for highly secure key management. The product enables the central storage of cryptographic keys in a hardware security module (HSM) that meets the highest security requirements and is also physically protected. • Key recovery: A special feature of Keymaster is the ability to provide controlled access to replacement keys (key recovery). Users can manage duplicate keys or copies of original keys and access them as needed. This ensures flexibility and security when managing keys, especially when a quick replacement is required after a loss. • Four-eyes principle: With Keymaster in combination with additional management modules/ applications, almost any security concept can be implemented reliably and audit-proof. Keymaster fulfills compliance guidelines and enables adherence to regulations on the separation of functions and tasks (dual control principle). Authentication takes place without transmitting secret keys to the end devices • Remote access: Keymaster enables the shared use of keys by several users, even beyond the boundaries of one location. In this way, for example, group and proxy solutions can be operated in which the use of keys for different users must be ensured. This application option solves various challenges regarding collaboration within an organization. • Powerful solution: Overall, Keymaster is a powerful keyserver solution that enables highly secure key management. With its numerous functions, Keymaster contributes to more security and efficiency in companies and authorities.
Scope of supply	• Keymaster Software • Keymaster Manual • Keymaster Release notes
Protocols	• OIDC • LDAP • TLS 1.3 • REST • PKCS#11
Supported HSMs	• AWS Cloud HSM5 • Thales Luna 7 • Utimaco • Trustway Protezione

Technical Data Sheet - Keymaster

Supported platforms	• Red Hat Enterprise Linux 9 (x86_64) • Oracle Linux R9 (x86_64) • Docker
Supported algorithms	• RSA (up to 16384 bit) • ECC (up to 571 bit) Note: depends on the capabilities of the HSMs
System requirements	• Redhat 9 / CentOS 9 • Intel Xeon CPU (minimum 2 Cores at 2.4Ghz) • 16GB RAM for 64bit CPU • 100 GB hard disk space LDAP-capable user directory service



Eviden Digital Identity
cv cryptovision GmbH
Munscheidstr. 14
D 45886 Gelsenkirchen

T: +49 209 16724-50
F: +49 209 16724-61

www.eviden.com