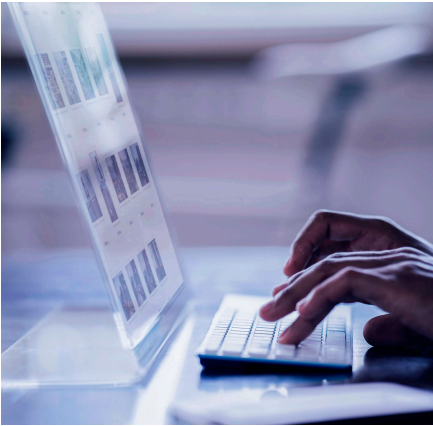


Trustway DataProtect KMS

Trustway DataProtect KMS is a centralized key management platform enhanced with data access control and monitoring features.



With its various standardized interface (JCE, KMIP, PKCS#11), it allows you to manage keys on every environment (cloud, virtual, on-premises), to ensure easy Information System (IS) audit and a meticulous access control.

Strong of our knowledge in our tamperproof infrastructure, we are providing you a key management appliance based on hardware infrastructure which meets the strictest international standards and brings the highest level of confidentiality.

Regardless of its location, be it stored in a database, file server, application, traditional or virtualized data center, or public cloud environment, your sensitive data is secure from compromise.

To guarantee you a full needs covering, Trustway DataProtect KMS is supporting a broad encryption ecosystem.

Trustway DataProtect KMS

Trustway DataProtect KMS offers customers a complete key management and data encryption platform providing the following advantages:

- Single, centralized platform for managing cryptographic content (keys and related data) and applications capable of running on-premises, in the cloud or hybrid environments.
- A server that includes support for the Trustway encryption connectors Trustway DataProtect App, Trustway DataProtect VM, Trustway DataProtect File, Trustway DataProtect DB, and Trustway DataProtect Token.
- Benefits of tamperproof appliance based on 100 % European certified HSM architecture to guarantee the security of your keys and data security.

Highlighted capabilities

Heterogeneous key management

Manage keys for a variety of encryption products including tokenization, and applications as well as self-encrypting drives, tape archives, Storage Area Networks, and a growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard.

Multiple key types

Centrally manage Symmetric and Asymmetric Keys, secret data, and X.509 certificates along with associated policies.

Full lifecycle key support and automated operations

Simplify the management of encryption keys across the entire lifecycle including

secure key generation, storage and backup, key distribution, deactivation and deletion. Automated, policy driven operations simplify key expiry and rotation tasks.

Centralized administration of granular access

Authorization controls and separation of duties. Unify key management operations across multiple encryption deployments and products, while ensuring administrators are restricted roles defined for their scope of responsibilities, from a centralized management console. Also, Trustway DataProtect KMS can utilize existing LDAP or AD directories to map administrative and key access for application and end users.

High-availability and intelligent key sharing

Deploy in flexible, high-availability configurations within an operations center and across geographically dispersed centers or service provider environments using an active-active mode of clustering.

Auditing and logging

Detailed logging and audit tracking of all key state changes, administrator access and policy changes. Audit trails are securely stored and signed for non-repudiation and can be consumed by leading 3rd party SIEM tools.

Next-generation storage and archive solution

Simplify secure storage and efficiently scale data centers while reducing costs and complexity, with Trustway DataProtect KMS and leading storage vendors such as NetApp, Dell, Nutanix, IBM, Hitachi, and HPE.

Trustway DataProtect KMS benefits

Single, centralized platform

To manage cryptographic content (keys and related data) and applications.

Use case expansion

Transform your key management appliance into a server that includes support for the Trustway encryption connectors, Trustway DataProtect App, Trustway DataProtect VM, Trustway DataProtect File, Trustway DataProtect DB, and Trustway DataProtect Token.

Lower administration costs

Lower the cost of key management and encryption with centralized administration and automated operations.

Simplify compliance

Efficiently audit key management practices, save staff time, and simplify attainment of compliance mandates with efficient, centralized auditing of key management practices such as GDPR, PCI- DSS, HIPAA...

Lower total cost of ownership

Leverage a continuously growing list of 3rd party technologies leveraging Trustway Encryption Connector family of products and the OASIS KMIP standard.

Security and compliance for cloud environments

Take advantage of the lower costs of virtualized and cloud environments with flexible deployment options and appliance models covering physical, and virtual environments (VMware and AWS Marketplace).

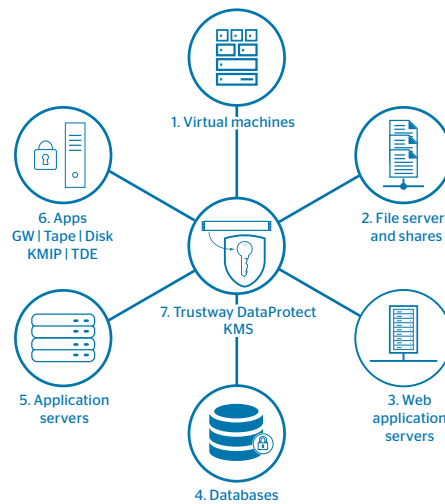
TurnKey encryption

In addition to its key management capabilities, the Trustway DataProtect KMS appliance offers customers the ability to perform high speed encryption/decryption operations as part of its capabilities. This allows customers to centralize encryption and crypto management operations regardless of its location.

Trustway DataProtect: a scalable solution

Trustway DataProtect offers a comprehensive data encryption solution to guarantee data security and the control on the data access.

This solution provides the customer with the tools to the capabilities to encrypt all the data format as Virtual Machine, Database, File system, Application and Tokenization. Trustway DataProtect is a complete solution for cloud, virtual and on-premises infrastructures and is compliant with the most restrictive data privacy regulations as GDPR, HIPAA or PCI DSS.



- 1. Trustway DataProtect VM**
Amazon Web Services VM
Azure | VMware
IBM SoftLayer
- 2. Trustway DataProtect File**
IBM DB2 | Oracle Database
Microsoft
SQL Server
Linux | Samba
Windows ServerNovell
Apache Hadoop
Cassandra
mongoDB | Docker
Microsoft SharePoint
Amazon EC2 & S3 | Chef
- 3. Trustway DataProtect App**
IBM
BEA Systems
Sun Microsystems
The Apache Software
Foundation
Oracle
Java
JBoss (by Red Hat)
- 4. Trustway DataProtect DB**
IBM DB2
Oracle Database
Microsoft SQL Server
- 5. Trustway DataProtect Token**
IBM | SAP Software Solution
BEA Systems
The Apache Software
Foundation | Sun Microsystems
Oracle | Java
JBoss (by Red Hat)
- 6. Ecosystem**
Multiple programming languages
SOAP and REST interfaces
KMIP interface | Tape Libraries
Storage | Cloud gateways
Databases | Applications
- 7. Trustway DataProtect KMS**
Key and crypto engine
Authentication and
authorization
Key lifecycle management
SNMP, NTP, SYSLOG

Technical specifications

Features	KMS
Max keys	1,000,000
Max concurrent clients per cluster	1,000
Redundant HDs & PSU	Yes
HSM Integration	Yes
Third-party integration	<p>Analytics: IBM Qradar, HPE ArcSight, Splunk, RSA Security Analytics, Above Security</p> <p>Application Servers: IBM WebSphere, Oracle Weblogic, Microsoft IIS, Apache Tomcat, Red Hat JBoss</p> <p>Backup Solutions: Commvault Simpana, Symantec NetBackup (via NetApp)</p> <p>Cloud Storage: Nutanix, Amazon Web Services S3, DropBox, Google Cloud Storage, Google Drive, NetApp Cloud ONTAP, NetApp AltaVault, Panzura Storage Controller</p> <p>Cloud Access Security Brokers: CipherCloud, SkyHigh Networks, Perspecsys (Blue Coat), Hitachi Sepaton VTL, CSC ServiceMesh, Netskope</p> <p>Databases: MS SQL Server (EKM), Oracle (TDE), IBM DB2, Oracle MySQL, Oracle Database, Teradata File and Disk Encryption: PKware, MongoDB</p> <p>Identity Management: Centrify Privilege Service</p> <p>Key Managers: Hadoop KMS, CloudEra Navigator Key Trustee Server</p> <p>Physical Storage: NetApp NSE, Dell Compellent (SC and XC), HPE MSL/ESL Tape Libraries, HPE 3Par StoreServ, HPE XP7, Hitachi VSP, Hitachi HUS, Hitachi RAID700, IBM XIV SED, Quantum Scalar Series(i6000, i500 & i40/80), Viasat, Brocade FS8-18</p>

More information:

atos.net/data-encryption-trustway-dataprotect

Contact us:

atos.net/en/solutions/cyber-security-products/contact-us-cybersecurity

Atos, the Atos logo, Atos|Syntel, and Unify are registered trademarks of the Atos group. September 2020. © 2020 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.