Introducing SAP® Data Custodian Key Management Service

Cloud-Ready Encryption and Key Management as a Service

THE BEST RUN SAP®

With the proliferation of new security threats and the rise of global data protection regulations, your organization needs to maintain confidentiality, integrity, and data authenticity now more than ever. And data loss prevention, encryption, and key management are top data security priorities. That means your enterprise requires a solution that can address data challenges including the inability to obtain total control of encryption keys and data, malicious insider attacks, and government compulsion.

To combat these challenges, organizations are increasingly leveraging multiple clouds for their applications. They are embracing new use cases such as multi-cloud encryption, enterprise-wide single key management policy, at-speed transport layer security termination, Internet-of-Things key management, distributed public key infrastructure systems, and secure manufacturing. Encryption can help protect data, but the challenge is how to secure the keys. Existing key management and hardware security module solutions using proprietary hardware and software are no longer effective in the modern era. To protect your data, you need an independent key management service that is segregated from the cloud providers hosting your data. The SAP® Data Custodian key management service can get you there.

Secure Key Management

The SAP Data Custodian key management service provides a secure key management service, which protects data in public, private, hybrid, or multi-cloud environments, simplifying provisioning and control of encryption keys. It provides cloud scalability and secure key storage, addressing performance as well as governance, risk, and compliance requirements at the digital edge, close to clouds and carriers.

With it, you can provision next-generation key management service functionality at the click of a button. Built using FIPS 140-2 level 3 certified hardware, it meets both compliance and security requirements with all the ease of software as a service.* The key management service offers first-of-its-kind central tamperproof logging and RESTful APIs.

UNMATCHED SECURITY

The key management service fulfills the segregation-of-duties security principle where keys are managed separately from the cloud provider hosting your data. Key access is restricted to authorized owners, protecting against insider attacks and exposure in a shared cloud infrastructure. Even if the host operating system is compromised and the root user is malicious, you keep cryptographic control of all your assets. That means it eliminates the risk of compromise in shared infrastructures, thanks to complete key confidentiality, even from the service providers.

This architecture protects you from unauthorized disclosure of your data, such as compliance with a subpoena without customer knowledge or approval.

Key access is restricted to authorized owners, **protecting against insider attacks** and exposure in a shared cloud infrastructure.

*FIPS validation pending

Why SAP Data Custodian Key Management Service

With the key management service, enterprises can protect data in public, private, hybrid, or multi-cloud environments and simplify provisioning and control of encryption keys while keeping keys at the digital edge – in close proximity to the data. You also receive multisite and hybrid cloud support, including support for a single, enterprise-wide key across your cloud and IT data center. And you can take advantage of private connectivity options for your public cloud deployments. With the key management service, you get centralized management capabilities with enterprise-level access controls and audit logging.

The key management service supports your compliance with global data protection and data localization legislation, including the General Data Protection Regulation, or GDPR, with key management capabilities that include regional isolation.

Try it now.

With the key management service, enterprises can **protect data** in public, private, hybrid, or multi-cloud environments.

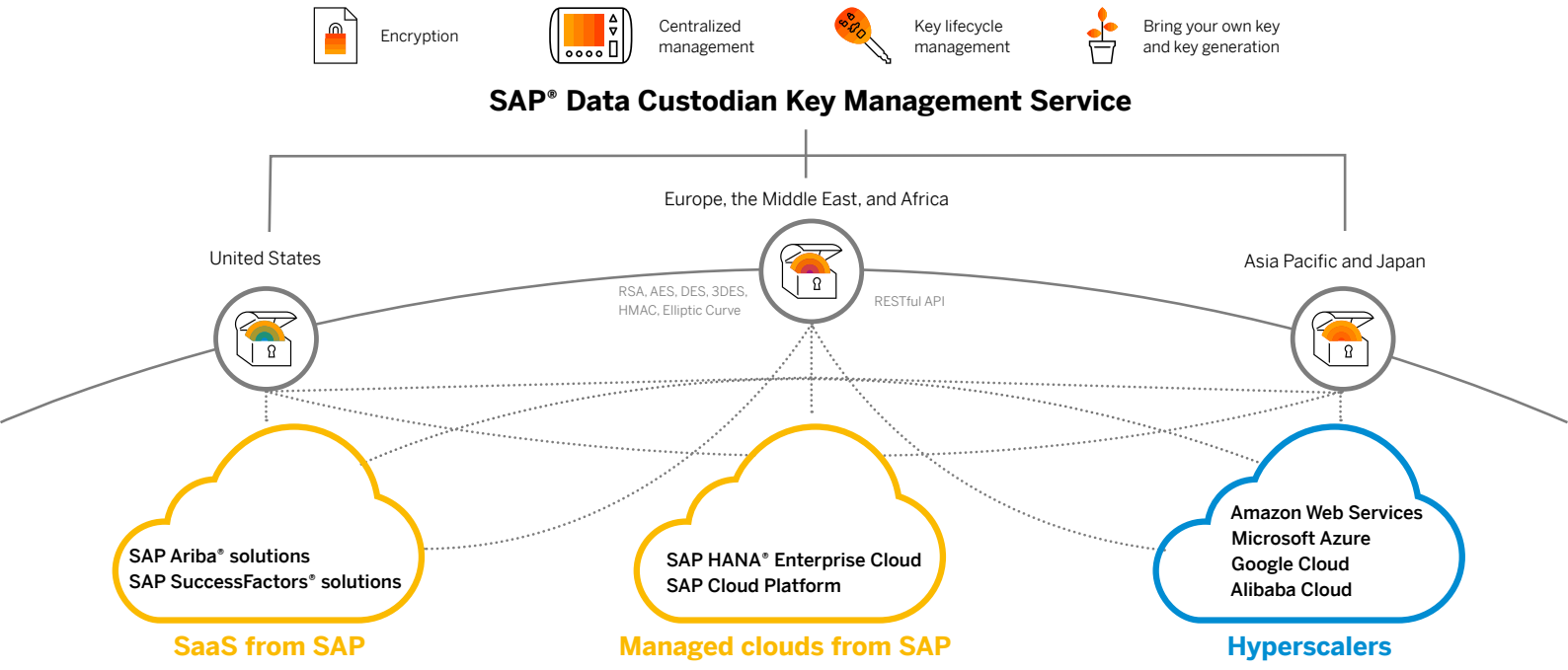
Why SAP Data Custodian

The SAP Data Custodian key management service is a feature of the SAP Data Custodian solution, which is designed to support organizations that wish to move to the public cloud or use cloud applications from SAP, but have concerns about data protection, legislative compliance, and handing control of their business data to third-party organizations. SAP Data Custodian is designed to give public cloud users similar transparency and control over their public cloud resources and applications that were previously available only in private cloud or on-premise configurations, as seen in the figure. The key management service extends the data protection capabilities of SAP Data Custodian to provide protection against inside and external data breaches and unauthorized access to data by third parties.

When used alongside the SAP Cloud portfolio, SAP Data Custodian can help mitigate security concerns and enable you to move to the cloud with confidence. SAP Data Custodian includes the following features:

- Public cloud data transparency
- Data placement, movement, and access controls
- Public cloud anomaly detection with alerts and notifications
- Public cloud inventory management
- Contextual cloud access controls
- Access controls to cloud offerings from SAP, including SAP S/4HANA® Cloud
- Independent key management service and encryption
- Incident management

Figure: Architecture of the SAP Data Custodian Key Management Service



AES – Advanced encryption standard
DES – Data encryption standard
3DES – Triple data encryption standard
HMAC – Hash-based message authentication code
SaaS – Software as a service

To find out more about the SAP Data Custodian key management service, visit us online.

Follow us

www.sap.com/contactsap

Studio SAP | 63759enUS (19/06)

THE BEST RUN SAP®