

## Securosys 365 DKE

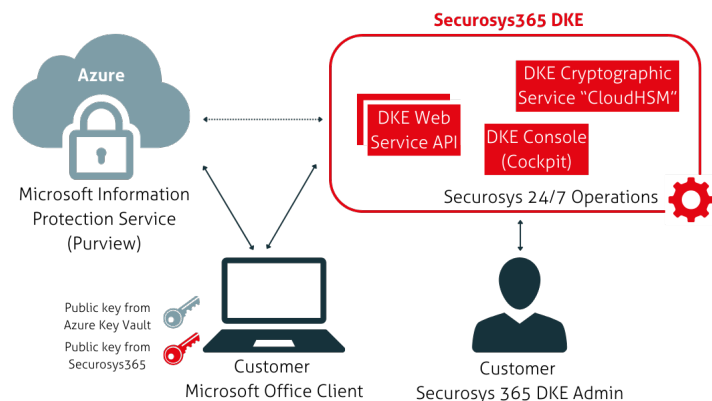
Enhance data privacy: Safeguarding Microsoft Office 365 data with your secure HSM keys

### Enhanced Security and Control

Securosys 365 DKE is a Swiss Cloud service designed to encrypt Microsoft Office application data in the Microsoft Azure Cloud using Double Key Encryption (DKE). Similarly to a Cloud Access Security Broker (CASB), it encrypts highly sensitive data on the client side before transferring it to the cloud, ensuring robust security and regulatory compliance with two encryption keys: one controlled by you and one stored in Azure.

### Key Benefits:

- Ready to start instantly
- Fully managed service
- User-friendly management panel
- Seamless integration with Microsoft Azure
- Key Storage on HSM
- Comprehensive security



### Innovative Enhancements:

Building on Microsoft's DKE sample code, Securosys 365 DKE has been significantly enhanced for increased functionality, robustness, and enterprise alignment. Leveraging Securosys CloudHSM technology, it provides the highest grade of customer key protection. The Securosys 365 DKE Console (Cockpit) facilitates the dynamic creation of DKE Web Service API apps, DKE keys, tenants and sub-tenants for specific domains (B2B), with a strong focus on Cross-Site-Request-Forgery (CSRF) protection.

- GetKey and Decrypt Endpoints: Respectively encrypts the document key using a public key retrieved from the Securosys HSM, and decrypts the document key using a private key that remains securely within our HSM.
- CRUD (Create, Read, Use, Delete) operations on keys.
- Management of DKE apps for specific domains.
- Protection against Cross-Site-Request-Forgery (CSRF).
- Comprehensive logging for cryptographic operations.
- Two-factor authentication (2FA) and support for any OpenID Connect identity provider.

### Seamless Integration and Deployment:

Implementing Double Key Encryption is straightforward with Microsoft Purview Information Protection sensitivity labels (i.e. «confidential», «secret»,...). The Securosys DKE module ensures dual protection of content encryption keys within file metadata. It integrates seamlessly with Azure, including auto-provisioning of the DKE Web Service API and Microsoft 365 Purview integration, requiring no customer engineering.

### Global Availability:

Operated from Switzerland, Securosys 365 DKE is globally accessible 24/7 as a cloud-based service. Its high-availability architecture allows for instant deployment within minutes, with on-premises options also available.

### Ultimate Data Protection:

Securosys 365 DKE provides ultimate data protection for Microsoft Office 365 data. Customer-controlled DKE keys are securely stored on FIPS 140-2 Level 3, Common Criteria EAL4+ validated Securosys HSMs. Comprehensive security measures, including two-factor authentication for the DKE Console and ISO/IEC 27001 certified service operation, ensure your sensitive information remains secure and under your control.

Components	Description
<b>DKE Cryptographic Service on HSM</b>	<b>Hardware Secured Cryptographic Keys for Microsoft 365 DKE Based on Securosys CloudHSM</b> <ul style="list-style-type: none"> <li>Geo-redundant HSM clusters co-located in datacenters in Switzerland (optional: Germany, US, and Singapore)</li> <li>Generation and storage of DKE service keys on Securosys Primus HSMs (FIPS 140-2 Level 3 and Common Criteria (CC) EAL4+)</li> <li>Unwrapping of document encryption keys: AES 256-bit, wrapped with RSA2048</li> </ul>
<b>DKE Web Service API</b>	<b>DKE Endpoint Provider</b> <ul style="list-style-type: none"> <li>Auto-provisioned, high-available, DoS protected and managed DKE service</li> <li>Fully integrated DKE service for Microsoft Purview Information Protection Sensitivity Labels with DKE keys backed by CloudHSM service</li> <li>GetKey and encrypt endpoints</li> <li>External double key encrypted document sharing beyond Microsoft Tenant borders (B2B)</li> </ul>
<b>DKE Console</b>	<b>Key Management System User Interface</b> <ul style="list-style-type: none"> <li>Securosys 365 DKE key lifecycle management console for customer administrators</li> <li>Generation of DKE RSA-keys on HSM</li> <li>Provisioning and configuration of DKE endpoint providers</li> <li>Audit and monitoring of DKE key usage</li> <li>User and policy management of console administrators</li> <li>Identity Access Management interface for integration with IAM solutions (optional)</li> </ul>
<b>Operations</b>	<b>DKE Managed Service</b> <ul style="list-style-type: none"> <li>Managed cloud service</li> <li>Operated by Securosys from Switzerland</li> <li>Cloud native design</li> <li>Zero-down-time architecture</li> <li>7x24 Monitoring and Support</li> <li>Securosys 365 DKE service is ISO/IEC 27001 certified</li> </ul>

### Prerequisites for Using Securosys 365 DKE Service

To use the Securosys 365 DKE service, subscribers must meet the following requirements:

- Office 365 E3 + Microsoft 365 E5/A5/F5/G5 Information Protection and Governance + EMS E3, or Microsoft 365 E5/A5/F5/G5 Compliance + Microsoft 365 F5 Security & Compliance, or Microsoft 365 E5/A5/F5/G5 Information Protection and Governance, or Office 365 E5 + EMS E3, or Microsoft 365 E5/A5/G5
- Microsoft 365 Office Apps (2307 or later)

With Securosys 365 DKE, your privacy is paramount.  
Experience ultimate data protection – let's start the conversation today!

**securosys** Microsoft Partner

Keys as a Service | Easy to use | Lean deployment | Made for Microsoft 365

**HEADQUARTERS**  
Securosys SA  
Max-Högger Strasse 2  
8048 Zürich  
SCHWEIZ  
+41 44 552 31 00  
info@securosys.com  
www.securosys.com

**GERMANY & EU**  
Securosys  
Deutschland GmbH  
Darrestrasse 9  
87600 Kaufbeuren  
DEUTSCHLAND  
+49 8341 438620  
info@securosys.de  
www.securosys.de

**APAC**  
Securosys  
Hong Kong Ltd.  
Unit 704B Sunbeam Centre  
27 Shing Yip Street  
Kwun Tong  
Hong Kong  
+852 8193 1646  
info-apac@securosys.com  
www.securosys.com