netdocuments®

NetDocuments Encryption Key Management Datasheet

NetDocuments introduces its NetDocuments Encryption Key Management (EKM) technology to the base cloud service encrypting each object and offers advanced add-ons sold separately.

Top concerns the legal industry faces:

Concern 1: Secure information from intrusion and brute-force attacks.
Concern 2: Protect your clients, firm, and assets.
Concern 3: Protect against a silent subpoena.

Over the years, law firms have gained a reputation for taking inadequate security measures, while also having access to banking and financial information of clients. As a result, expert and skilled interceptors see law firms as easy targets to get to valuable client information.

The American Bar Association has warned lawyers to secure data, but the haphazard methods of implementation are not stringent enough. When encryption is applied, gaps can still lead hackers to the desired data. The need for a secure and tight encryption solution is greater than ever.

> "Law firms have an ethical and professional duty to make all reasonable efforts to protect the information they hold. Remaining the weakest link protecting clients' data is an unsustainable proposition. Not only does it expose firms to considerable liability, but it also threatens the ability to retain clients."[1]

Overview

The NetDocuments EKM technology offers three layers of encryption via three cryptography keys to secure a document and protect the key securing the document. The NetDocuments Trusted Cloud Platform includes the first two layers of the EKM technology. The third layer, an optional layer sold separately, provides dual jurisdiction and the control to apply encryption to the client or matter level. The EKM technology works as follows:

1. NetDocuments uploads a document and the first key, the **Object Encryption Key (OEK),** encrypts the document.
2. The second key, the **Master Encryption Key (MEK),** wraps the OEK.
3. The third key, the **Customer Managed Encryption Key (CMEK),** wraps the master-wrapped OEK.

A **Hardware Security Module (HSM)** provides a trusted and confined environment to create, manage, and store keys. You can use the keys to encrypt/decrypt data objects and wrap the cryptography key that protects the document.

To provide dual jurisdiction of the cryptography keys, the advanced add-ons offer two customer-owned key options with diverse security strategies to meet your needs:

- **CMEK Implementation**—where you can use, own, manage, and back up your customer-owned key—called the **Cloud CMEK** that the NetDocuments HSM creates.
- **Bring Your Own Key (BYOK) Implementation**—where you can create, use, own, store, manage, and back up your customer-owned key—called the **Private CMEK** that your privately-owned HSM creates.

The NetDocuments EKM technology is transparent and provides the following strengths:

Every document is encrypted. NetDocuments encrypts every document or object; in a brute-force attack, only one document has a chance for invasion at a time.

The base cloud service includes the EKM technology. Within the base cloud service, NetDocuments encrypts each document with a unique key; a second key encrypts the key protecting the document.

EKM uses AES-256 and QRNG. NetDocuments uses industry encryption standards and practices to create cryptography keys, including AES-256 and a key generation method, referred to Quantum Random Number Generator (QRNG)[2], which uses full entropy true quantum random encryption and a unique photon technology.

Advanced Add-ons achieve FIPS 140-2 Level 3 validation. With the use of the advanced add-ons, the encryption meets FIPS 140-2 Level 3 validation.

Advanced add-ons provide dual jurisdiction of keys. Dual jurisdiction of cryptography keys requires that you have both the NetDocuments-owned keys and your customer-owned key to access a document. Except for the customer-owned keys, NetDocuments owns and manages keys created with the NetDocuments HSM. Customer-owned keys give security teams full-control of keys and enable you to apply encryption via the matter, client, or to any other document attribute.

Purchase Customer-owned Keys and Privately-owned HSM. As a customer, you can choose to have the NetDocuments HSM or a privately-owned HSM to create your customer-owned keys. Choosing which HSM to use provides various security strategies to meet your needs. Available to purchase separately, you can buy a privately-owned HSM to create, manage, and store your customer-owned key.

To determine the advanced add-on security strategy that best meets your needs, contact NetDocuments Professional Services.

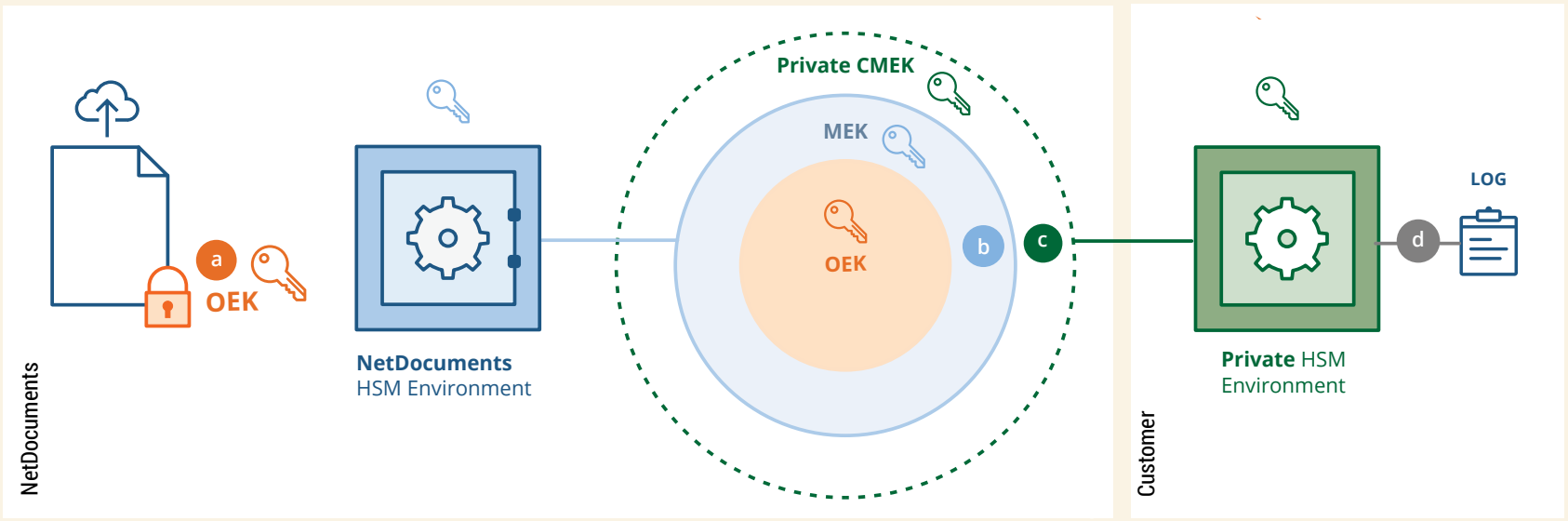
BYOK Implementation: Private CMEK using Private HSM

a **1ST CRYPTOGRAPHY KEY—OEK**
File uploads and the NetDocuments-owned OEK encrypts the document.

b **2ND CRYPTOGRAPHY KEY—MEK**
The NetDocuments HSM-owned MEK wraps the OEK.

c **3RD CRYPTOGRAPHY KEY—PRIVATE CMEK**
The customer-owned Private CMEK wraps the master-wrapped OEK.

d *The Private HSM provides encryption audit logs.*



References

1. Control Risks, contributor. "Is Cyber Risk An Existential Threat To The Legal Sector?" Forbes Business. July 13, 2016. https://www.forbes.com/sites/riskmap/2016/07/13/is-cyber-risk-an-existential-threat-to-the-legal-sector/#3af3c46a3c54. (Accessed June 19, 2017)

2. Jane Melia, Bruno Huttner, Richard Moulds, Nino Walenta, and Anthony Fuller, Quantum-Safe Working Group contributors. "Quantum Random Number Generators." https://cloudsecurityalliance.org/download/quantum-random-number-generators/. 2016. (Accessed June 19, 2017).