

Key Management for Cloud Document Security

A case study on how we delivered an enterprise key management solution with integrated true random key generation, for one of the global leaders in cloud-based document and email management.

Business Situation

Headquartered in the US, NetDocuments is a leader in cloud-based document and email management, with hundreds of thousands of users around the globe. They operate an expanding network of datacenters in the US, Europe and Asia-Pacific to service this worldwide customer base and meet growing customer demand. Their guiding strategic principle and differentiator is to provide the highest level of protection to the digital assets, addressing all potential risks. All data is encrypted to the highest standards, with one or more levels of encryption delivered at a customer level.

Challenge

NetDocuments needed to expand its databases to meet steep customer growth while continuing to enhance the protection provided; a vital component of the client's brand and image. As part of this effort, it wanted to implement best-in-class key management to generate and secure the master and document encryption keys for all its customers.

The NetDocuments team was generally satisfied with its existing solutions, but wanted to assess new options to maintain the company's leadership position, grow its customer base, and deploy an additional encryption layer for an even higher level of security. There were several high-priority considerations in choosing a solution:

- Unbeatable security: The best foundation for strong encryption that would deliver security, plus compliance to regulatory

requirements and ultimately peace of mind to customers.

- Interoperability and flexibility: The solution needed to integrate seamlessly with existing infrastructure to deliver a high performing, cost-effective implementation.
- Scalability and speed: The solution needed to handle substantial amounts of data without performance degradation, and allow flexible expansion as the customer base continued to grow.

The above requirements needed to be met in a cost competitive manner.

The solution is centrally managed, highly available, fully interoperable and delivers best-in-class key management functionalities.

Solution

The QuintessenceLabs solution is made up of multiple, redundant, and replicating qCrypt™ appliances deployed in NetDocuments data centers around the world. These are implemented in a multi-master configuration providing highly available key generation, storage, and lifecycle management from all active nodes.

NetDocuments application servers provide the user interface and business logic for the service. Customer documents are encrypted with unique keys generated by qCrypt. Document keys are wrapped using master keys to ensure isolation between customers, and to provide very high scalability – supporting hundreds of millions of uniquely encrypted individual documents.

Dual control for document access is supported as an option by using two layers of key wrapping with one set of wrapping keys managed by the customer, and a second set of wrapping keys managed by the NetDocuments application.

For the highest security, the qCrypt appliance incorporates a quantum-based high speed true random number generator ensuring that all keys have full entropy, removing reliance on deterministic random numbers and delivering output that is totally independent for each key and each user. The 1 Gbit/s output of the random number generator provides sufficient throughput to meet the master key needs for each data center with room for expansion.

The solution is centrally managed, highly available, fully interoperable and delivers best-in-class key management functionalities such as full key life-cycle management, object and usage policy management, fine grained policy control and logging.

Benefits

QuintessenceLabs' key management solution is allowing NetDocuments to:

- Continue the growth of their data centers and customer base without sacrificing quality or security and meeting the compliance needs of their customers.
- Reinforce their brand as the leader in terms of data security by using the highest-quality keys with full replication.
- Manage multiple layers of encryption keys for their customers.
- Integrate seamlessly and flexibly with existing and planned infrastructure through vendor-neutral interfaces.

This unique blend of capabilities provided a clear demonstration to our client's end users that the security of their digital information is in the best possible hands, reinforcing NetDocuments' position and helping grow their market share.

Since this deployment, NetDocuments and QuintessenceLabs have worked together to deliver an enhanced layer of security for customers looking for the highest level of control over their documents. Customers can now gain even higher security and control by deploying our Private TSF hardware on their premises or in their data center to further control the access within their NetDocuments' solution.



AUSTRALIA
Unit 1, Lower Ground
15 Denison St
Deakin, ACT 2600
+61 2 6260 4922

UNITED STATES
175 Bernal Road
Suite 220
San Jose CA 95119
+1 650 870 9920

www.quintessencelabs.com
Document ID: 1668