CRYPTOMATHIC

Bring Your Own Key for Cloud Banking Applications

Exploring business considerations, IT implications and key management challenges of moving security-critical applications to the cloud

A Cryptomathic Business Guide

Executive Summary

The cloud offers banking and financial institutions various advantages, lowers barriers to entry, and introduces various challenges too. Banks need to harness the advantages and opportunities offered by the cloud as well as incorporate new digital business models to stay competitive. Such changes have a direct impact on the legacy security architecture and security measures that are proven to work to protect their sensitive data.

For many business-critical financial applications, security concerns are the largest barrier-to-adoption for cloud computing. The aggregation of sensitive data, critical business processes, and other corporate IP on a publicly accessible platform may open flanks to cybercriminals as well as inadvertent exposure of critical data to third parties. Banking-grade design, industry compliance and management of data security is vital. There are stringent requirements for the secure use of cryptography and the management of the cryptographic keys within the banking and payment sector - compliance can be enforced from regulatory and industry security standards bodies.

Bring Your Own Key (BYOK) is a popular term devised for addressing some of the security concerns around cloud encryption and the ownership of encryption keys that are used by cloud applications. BYOK cloud solutions, which enable businesses using cloud services to generate, back up, deliver and manage their own cryptographic keys, have quickly gained traction among businesses that require a high level of control over their data security in the cloud. Banks are under pressure to exploit the benefits of public cloud services while still retaining control of essential security; BYOK services are en route to this but have been hampered by proprietary standards. Cryptomathic has been an early supporter of BYOK for the hybrid cloud and the first to support it with a comprehensive HSM-agnostic banking grade-key management system, CKMS. By enabling users to control and manage the entire lifecycle of their own, unique portfolio of keys, Cryptomathic is answering the call for a new level of end-user security control in cloud services.

Table of Contents

The Advantages and Challenges of Moving to the Cloud

Moving to the Cloud - the Rationale and Challenges

The Rationale

In a process of digital transformation and the platformization of service offers, banks and financial institutions are increasingly migrating IT services from on-premise, self-managed data centers to public cloud services.

With the promise of lower capital costs to improve bottom lines, there are definitely significant advantages to embracing the native elasticity and resilience that cloud computing can bring to the banking and financial sector. These advantages align well with modern goals for rapid and agile development and delivery of products and services, to differentiate banks and others from their competition.

However, for many business-critical financial applications, security concerns are the largest barrier-to-adoption for cloud computing. The aggregation of sensitive data, critical business processes, and other corporate IP on a publicly accessible platform may open flanks to cybercriminals as well as inadvertent exposure design and management of data security is vital.

Challenges

Cryptography is the security foundation for any significant application - to protect data and communication and to authenticate processes and people.

Most organizations strongly rely on cryptography for their digital business, however, banks and financial institutions have a specific interest in high-assurance cryptographic processes, as any compromise can lead to fraud that can directly divert funds into attackers' accounts. For many banking applications, their core value is actually delivered through cryptography:

- Electronic banking and financial transactions are ultimately composed of cryptographic functions.
- Ownership of a set of cryptographic keys completely defines a bank's online existence.

Data Security and Privacy

With the decision of placing sensitive data in the Cloud, the data security and privacy assurances depend, to a certain extent, on the hosting company.

Conclusion: CKMS And Secure Banking-Grade BYOK

Summary of Key Management Challenges for the Cloud

Today's financial institutions face conflicting requirements to efficiently manage and control a key's lifecycle but also deliver it to an external environment for use.

At the same time, they might want to maintain the freedom to change provider without having to re-architect their entire key management ecosystem, or to 'dual source' cloud services for resilience and business continuity.

Another related challenge is to securely migrate high-value keys between on-prem and cloud application instances. Meanwhile proof of compliance and streamlined audits are just as essential.

CKMS for Cloud-Agnostic Key Management

Cryptomathic's Crypto Key Management System (CKMS) directly addresses these challenges through the following:

- A centralized, on-premise KMS enables multi-cloud key management and on-prem-to-cloud migration.
- Cryptographic keys are managed for all the regions of the different cloud providers, e.g., one key can be used in multiple regions in multiple clouds and can also be shared between on-prem and cloud applications.
- Keys are securely backed up on-premise and rotated when required.
- CKMS' Hold Your Own Key capability enables users to generate, store, deploy, retrieve, backup, revoke and retire keys regardless of cloud model (public, private or hybrid) and cloud provider.
- Keys can be distributed manually or automatically to the key vault of a cloud provider under a policy dictated by the business.
- Proof of compliance is enabled through centralized generation of strong keys, dual control for critical operations, and provision of operational insights on usage with signed logs, reports and administration dashboards.

Banking-Grade Key Management for Multi-Cloud Environments with an Automated HSM-Agnostic BYOK Process

CKMS integrates securely with FIPS140-2 level 3 approved HSMs. All cryptographic operations are executed inside the secure boundary of the HSM.

CKMS supports multiple ways to import and export keys in a variety of formats such as TR-31 key block, Atalla Key block, PKCS#8 cryptograms and others. BYOK wrapping methods used by the cloud providers, including PKCS#1 v1.5, OAEP SHA1 and OAEP SHA256 are supported.

Automated key distribution is ensured via the different REST APIs made available by the cloud-providers.

CKMS supports multiple HSM brands at its core, putting the choice of HSM vendor in the hand of the customer. This HSM-agnostic approach allows banks and organizations a wide range of support for their applications in the cloud and in their on-premise data centers, underpinned by their preferred HSM brand.

With more than 3 decades of experience, Cryptomathic offers leading key management services for the banking industry and lessens the burdens of digital transformation across the hybrid cloud.

References

Microsoft Digital Defense Report 2021 (October 2021), by the Microsoft Corporation

Microsoft Azure (retrieved November 2021), by the Microsoft Corporation

AWS (retrieved November 2021), by Amazon.com, Inc

Google Cloud (retrieved November 2021), by Google LLC

McKinsey on Payments (January 2020), by McKinsey Company, Volume 12, Issue 30

Cloud Threat Report 2020 (2020), by Oracle Corporation & KPMG International Limited

FINAL REPORT (EBA/GL/2019/04 - EBA Guidelines on ICT and security risk management (29 November 2019), by the European Banking Authority EBA

Global Retail Banking 2019 - The Race for Relevance and Scale (October 2019), by Thorsten Brackert, Chaojung Chen, Jorge Colado, Laurent Desmangles, Muriel Dupas, Pierre Roussel, Holger Sachse, Sam Stewart, and Monica Wegner at Boston Consulting Group

Encryption in Microsoft Dynamics 365 (retrieved May 2020), by Microsoft Corporation

How Value Creation Is Reshaping the Payments Industry (2017) by McKinsey Company

Platform-based Innovation Management: Directing External Innovational Efforts in Platform Ecosystems (2011), by Simone Scholten & Ulrich Scholten

Composite Solutions for Consumer-Driven Supply Chains (2010), by Simone Scholten, Ulrich Scholten and Robin Fischer. In: Bogaschewsky R., Eßig M., Lasch R., Stölzle W. (eds) Supply Management Research. Gabler

Banking-as-a-Service - what you need to know (2016), by Ulrich Scholten

Winning in a world of ecosystems (2019), by McKinsey Company

Global Banking Practice - The ecosystem playbook: Winning in a world of ecosystems (2019), by McKinsey Company

The power of many: Corporate banking in an ecosystem world (2019), by McKinsey Company

Microsoft Dynamics 365 Banking Accelerator is now generally available (2019). James Galvin Principal Program Manager, Dynamics 365, Microsoft Corporation

How banks can take their customer engagement to new levels (2019), Janet Lewis, Vice President, Global Financial Services, Microsoft Corporation

Dynamics 365 Financial Services Accelerator (2019), by Microsoft Corporation

10 reasons why you should use the Microsoft Dynamics 365 Banking Accelerator (2019), by Wim Geukens, Managing Director, VeriPark Europe, VeriPark

Resources and Next Steps

See more Cryptomathic resources on delivering banking-grade key management and agile cryptography for the the hybrid cloud.

White papers:
https://www.cryptomathic.com/resources/white-papers

Case studies:
https://www.cryptomathic.com/customers/case-studies

Products:
https://www.cryptomathic.com/products/key-management

Contact your Cryptomathic representative or email us on enquiry@cryptomathic.com for more details.

Disclaimer

This document is protected by copyright. No part of the document may be reproduced in any form by any means without prior written authorization of Cryptomathic. Information described in this document may be protected by a pending patent application. This document is provided “as is” without warranty of any kind. Cryptomathic may make improvements and/or changes in the product described in this document at any time. The document is not part of the documentation for a specific version or release of the product, but will be updated periodically.

Note: This material has been prepared for general informational purposes only.

About Cryptomathic

Cryptomathic is a global provider of secure server solutions to businesses across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile. With over 30 years' experience, we provide systems for Authentication & Signing, EMV and Crypto & Key Management through best-of-breed security solutions and services.
We pride ourselves on strong technical expertise and unique market knowledge, with 2/3 of employees working in R&D, including an international team of security experts and a number of world renowned cryptographers. At the leading edge of security provision within its key markets, Cryptomathic closely supports its global customer base with many multinationals as long-standing clients.