

HSM Reimagined: Cloud Ready Encryption, Key Management and Tokenization as a Service

With the proliferation of new security threats and the rise of global data protection regulations, the need for organizations to maintain confidentiality, integrity and authenticity of their data is more critical than ever.

According to research, IT executives expect 60% of workloads to run in the cloud by 2018.¹ This expected growth will present increased security challenges, including:

- Inability to obtain total control of encryption keys and data
- Malicious insider attacks
- Government compulsion

Furthermore, organizations are increasingly leveraging multiple clouds for their applications and embracing new use cases such as multicloud encryption, enterprise-wide single key management policy, at-speed TLS termination, IoT key management, distributed PKI systems and secure manufacturing. Encryption can help protect the data, but the challenge is how to secure the keys. Existing key management and hardware security module (HSM) solutions using proprietary hardware and software are no longer effective for the modern era.

Solution

Equinix SmartKey™ powered by Fortanix is a HSM as a Service that provides secure key management and cryptography service which protects data in public, private, hybrid or multicloud environments, simplifying provisioning and control of encryption keys. Accessible on Platform Equinix®, it provides cloud scalability, secure key storage, encryption and tokenization services; addressing performance and government, risk and compliance (GRC) requirements at the digital edge, close to clouds and carriers.

With SmartKey you can provision next-generation HSM functionality at the click of a button. Built using FIPS 140-2 Level 3 compliant hardware², it meets both compliance and security requirements with all the ease of a SaaS. SmartKey offers first of its kind central tamper-proof logging, RESTful APIs, and a variety of standard interfaces such as PKCS#11, KMIP, JCE, and CNG.

Unmatched Security

Key access is restricted to authorized owners, protecting against insider attacks and exposure in shared cloud infrastructure. Even if the host operating system is compromised and root user is malicious, customers keep cryptographic control of all their assets.

SmartKey is designed for security and compliance and all the core functionalities have been implemented inside Intel SGX enclaves to protect against man-in-the-middle attacks. All access control, key generation, cryptographic operations, user and application authentication, and logging are done in a protected environment implemented inside Intel SGX enclaves.

Features

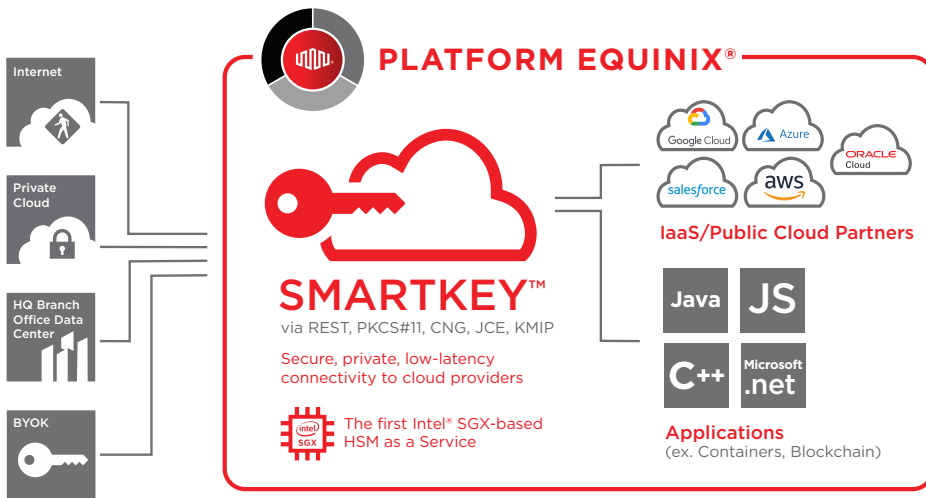
- Cryptographic opacity into customer keys—only authorized users can access
- Multi-site and hybrid-cloud support, including support for single enterprise-wide key across cloud and IT data center
- Built-in encryption, key management and tokenization with support for a variety of interfaces (RESTful APIs, PKCS#11, CNG, JCE, KMIP)
- Centralized management with enterprise-level access controls and audit logging
- Private connectivity options for public cloud deployments

Benefits

- Eliminate risk of key compromise in shared infrastructure with complete key confidentiality even from service providers and governments/state threat actors
- Achieve compliance & data sovereignty with General Data Protection Regulation (GDPR)—key management with regional isolation
- Gain predictable consumption with HSM-grade security in an easy-to-use cloud service
- Obtain rapid and easy integration of new or existing applications
- Enhance performance by storing keys at the digital edge—close to critical applications whether in cloud or on-premises

1. 451 Research Blog *Enterprise IT Executives expect 60% of workloads will run in the cloud by 2018*, September 1, 2016

2. FIPS validation pending



Why SmartKey

With SmartKey, enterprises can protect data in public, private, hybrid or multicloud environments and simplify provisioning and control of encryption keys while keeping keys at the digital edge—in close proximity to the data. Enterprises can also securely integrate with clouds and digital business services by strategically applying an Interconnection Oriented Architecture™ (IOA™) approach on Platform Equinix.

Try it now: <https://www.equinix.com/smartkey>

Why Equinix?

Interconnection solutions: Equinix delivers 330,000+ cross connects to allow you to connect directly to the clouds, people and places that matter to you.

Business ecosystems: Equinix has 9,800+ companies populating its diverse ecosystem, providing access to the right partners to re-architect IT and compete as a digital business.

Global reach: Equinix expands your market reach with 200 data centers in 52 major metro areas across 24 countries.

Network and service provider density: Equinix hosts 1,800+ network and 2,900+ cloud and IT service providers.

Proven expertise: Equinix has a 99.9999% uptime record to prepare you for tomorrow, today so you're always up and running.

About Equinix

Equinix, Inc. (Nasdaq: EQIX) connects the world's leading businesses to their customers, employees and partners inside the most-interconnected data centers. On this global platform for digital business, companies come together across more than 50 markets on five continents to reach everywhere, interconnect everyone and integrate everything they need to create their digital futures.

Learn more at [Equinix.com](https://www.equinix.com)

Equinix Americas

Main: +1.650.598.6000
Email: info@equinix.com

Equinix EMEA

Main: +31.20.754.0305
Email: info@eu.equinix.com

Equinix Asia-Pacific

Main: +852.2970.7788
Email: info@ap.equinix.com