CRYPTOMATHIC

PrimeKey

Solution Brief

Agile Cryptography Management Platform For Secure IoT Manufacturing

Crypto Service Gateway with Secure Execution Environment Powered by Cryptomathic and PrimeKey

It all starts in the fabrication plant

In today's IoT world, device security starts in production. For example, provisioning certificates, key material for authentication and injecting birth certificates are the starting point for further lifecycle stages like code signing and secure OTA upgrades. Working with external production partners and running manufacturing in untrusted environments, requires advanced security concepts. Combining PrimeKey's SEE with Cryptomathic's CSG you can now implement a true end-to-end secure process and establish a chain of trust, which includes your own software required to inject data into your chipsets during wafer production. The integrated solution delivers an agile cryptographic platform which provides secure key generation and management for injecting unique identifiers into semiconductors during production, as well as secure code signing.

Certified crypto control center

Cryptomathic's Crypto Service Gateway (CSG) enables organizations to achieve the full potential of cost savings through shared hardware security modules (HSMs) and streamlined crypto operations. CSG is a central cryptographic infrastructure that simplifies application integration while ensuring the highest availability and utilization of HSMs. Acting as a crypto control center, CSG shares HSMs between applications, allowing central policy enforcement and key management.
PrimeKey's SEE supplies a seamless trustworthy platform for the CSG. PrimeKey's SEE is a FIPS 140-2 Level 3 certified rack-mounted server, which ensures that applications running in VMs are operated in an environment that fulfill the same FIPS 140-2 level 3 requirements as the HSM devices managed by CSG. With PrimeKey's SEE, a packaged solution is offered to the market where all the operational obligation and tasks to ensure trusted handling of cryptographic keys and runtime protection for applications is taken care of by the hardware.

Solution Benefits

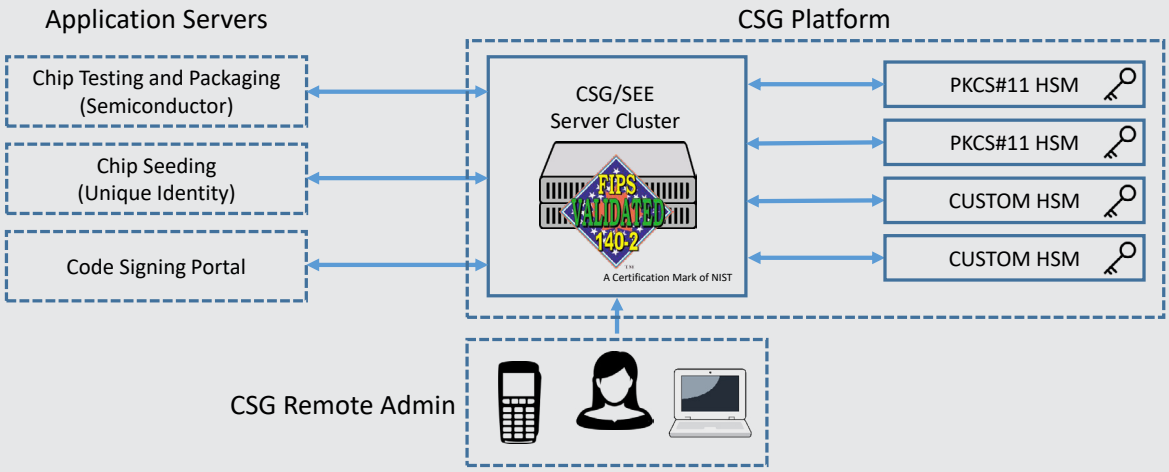
- ✓ **Reduce costs** through shared infrastructure
- ✓ **Centralize policy and control** over all keys and crypto operations; keeping crypto decisions in the hands of the security team
- ✓ **Enable complete central management** and monitoring over entire HSM real-estate
- ✓ **Provide easy to read audit** logs for proof of compliance
- ✓ **Simple-to-use API** delivers increased development velocity and reduced time to market
- ✓ **FIPS 140-2 Level 3** certified hardware
- ✓ **Highly-available and scalable** infrastructure for using HSM crypto services

For audits - "Just point to the rack"

With the traditional solution approach of using the Software Stack to manage HSMs, there are several obligations and demands on Data Center security, both physically and operational. Besides this, external audits often raise concerns about key handling and established processes and procedures. With the secure platform of SEE and CSG you take most of these concerns out of scope for the audits with a point to the Server Rack, where the SEE with the CSG is mounted. There is no doubt in the level of trust: With SEE FIPS 140-2 Level 3, secret keys are always processed in the secure environment and your applications are protected during runtime.

How the solution works

The complete solution incorporates Cryptomathic CSG and PrimeKey SEE to provide a comprehensive crypto control platform to our clients. The high-level architecture is illustrated below.



Cryptomathic CSG

Crypto Service Gateway (CSG) provides a highly-available and scalable infrastructure for using HSM crypto services. A CSG server cluster sits between HSMs and the applications, distributing load to the appropriate HSMs, enforcing crypto policy and centralized key management. CSG is managed using a dashboard allowing secure configuration, policy management and monitoring of the cluster. Administrators interact with CSG using two-factor smartcard authentication and calls to the API from applications are fully authenticated.

Application-specific crypto parameters are all managed centrally through an easy-to-read policy language. The policy simplifies internal and external compliance audits and empowers your security team with true crypto agility.

With CSG, a business can assert total control over its crypto estate, delivering increased efficiency, cost savings and confident compliance.

PrimeKey SEE

The PrimeKey Secure Execution Environment (SEE) is a full-size rack-mounted application server that comes with a patented FIPS protected execution environment for any operating system and application. It ensures that the server runtime environment can only be accessed by an authorized security administrator, making it impossible to access, to extract or to modify by an unauthorized party. By doing so it opens up a new world of possibilities where you can run each mission-critical application in any uncontrolled environment. With SEE, you can place your software wherever it benefits further advances of your business.

Prevent manipulation

If your software controls sensitive information or functionality, you know the consequences that an undetected malicious modification can have. Your IoT device might be hacked, your data compromised, or your machines stop working. With SEE you can sleep soundly, no one can access or modify your software and data.

CRYPTOMATHIC

Learn more at cryptomathic.com/CSG

PrimeKey

Learn more at primekey.com

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.

Contact us: sales_enquiry@cryptomathic.com

About PrimeKey

One of the world's leading companies for PKI solutions, PrimeKey Solutions AB has developed successful technologies such as EJBCA Enterprise, SignServer Enterprise and PrimeKey PKI Appliance. PrimeKey is a pioneer in open source security software that provides businesses and organisations around the world with the ability to implement security solutions such as e-ID, e-Passports, authentication, digital signatures, unified digital identities and validation.

Contact us: malin.ridelius@primekey.com