NIST Crypto Agility Workshop
April 17-18, 2025

Software-Defined Cryptography

Enabling Crypto Agility in Enterprise IT

Jihoon CHO

VP of Technology
Samsung SDS

https://www.linkedin.com/in/jihoon-cho-1566415/

Cryptographic Agility

- Cryptographic agility is a **Design Feature**
- Enabling updates to crypto modules **without** the need **to modify** or **replace IT infra**

MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

*"Central to this migration effort will be an emphasis on **cryptographic agility**, both to reduce the time required to transition and to allow for seamless updates for future cryptographic standards.*

...

*the term cryptographic agility means a **design feature** that **enables future updates** to cryptographic algorithms and standards **without the need to modify or replace** the surrounding infrastructure .. "*

+source: https://www.whitehouse.gov/briefing-room/statements-releases/

Three Pillars of Crypto Agility in Enterprise IT

01

Governance

Central management of crypto policies with Crypto Center of Excellence (CCoE)

02

Abstraction

Well-defined interfaces designed to enforce crypto policies without changing applications

03

Automation

Crypto policies should be automatically enforced for enterprise applications

Three Pillars of Crypto Agility in Enterprise IT

01

Governance

Central management of crypto policies with Crypto Center of Excellence (CCoE)

02

Abstraction

Well-defined interfaces designed to enforce crypto policies without changing applications

03

Automation

Crypto policies should be automatically enforced for enterprise applications

Governance with Cryptographic Center of Excellence (CCoE)

- Growing need for **centralized governance** for cryptography in enterprise IT.
- **CCOE** ensures **consistent crypto policy enforcement** and **oversight** across the entire organization, especially **during cryptographic transitions**.
- Strong governance with **CCoE** can be an essential **cybersecurity capability** in RMF and CDM.

Continuous Diagnostics and Mitigation (CDM) and Governance for Cryptography

Asset Management	Identity and Access Management	Network Security management	Data Security Management
What is connected? SW (crypto) vulnerabilities, Configurations (for crypto policies)	Who is using the network? IAM, Entitlement (authentication/authorization)	What is happening on the network? Zero Trust Networks	How is data protected? Data Encryption, KMS

Three Pillars of Crypto Agility in Enterprise IT

01

Governance

Central management of crypto policies with Crypto Center of Excellence (CCoE)

02

Abstraction

Well-defined interfaces designed to enforce crypto policies without changing applications

03

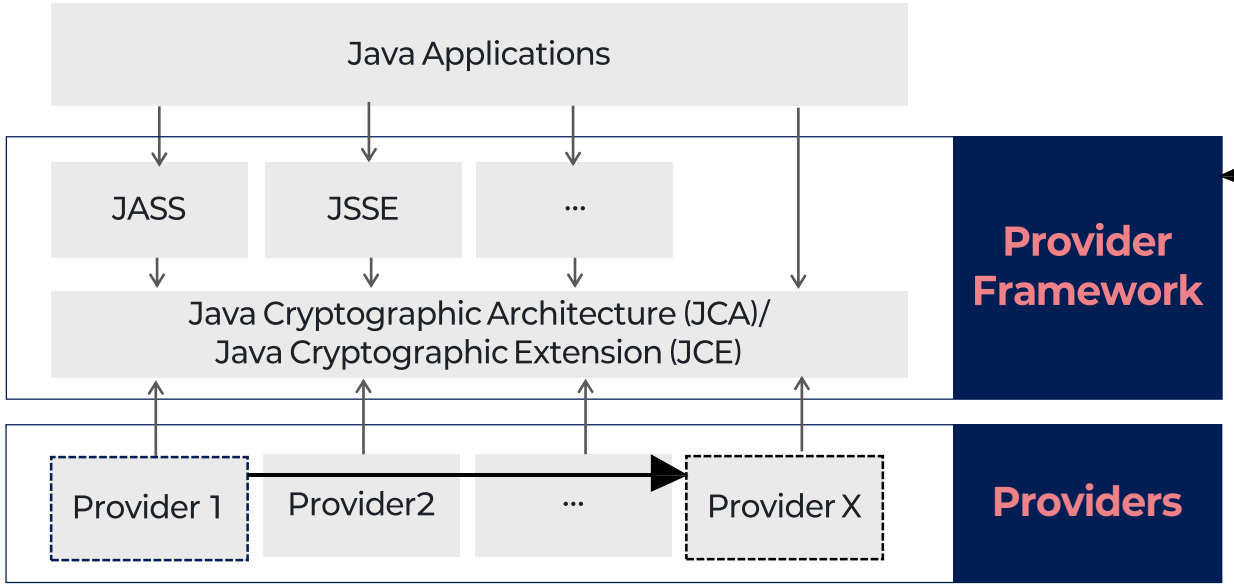
Automation

Crypto policies should be automatically enforced for enterprise applications

CASE STUDY

Abstraction:
Separating Cryptographic Configurations from Applications

Java Cryptographic Architecture (JCA) provides **abstraction** enabling to transition to other provides by **updating** the **configuration** file without modifying application



Crypto Policy Enforcement

By updating "java.security" file

AS-IS

security.provider.1 = Provider 1
security.provider.1 = Provider 2
security.provider.1 = Provider 3
...

TO-BE

security.provider.1 = Provider X
security.provider.1 = Provider 1
security.provider.1 = Provider 2
...

Application-Level Crypto Agility vs. **Service-Level** Crypto Agility

Three Pillars of Crypto Agility in Enterprise IT

01

Governance

Central management of crypto policies with Crypto Center of Excellence (CCoE)

02

Abstraction

Well-defined interfaces designed to enforce crypto policies without changing applications

03

Automation

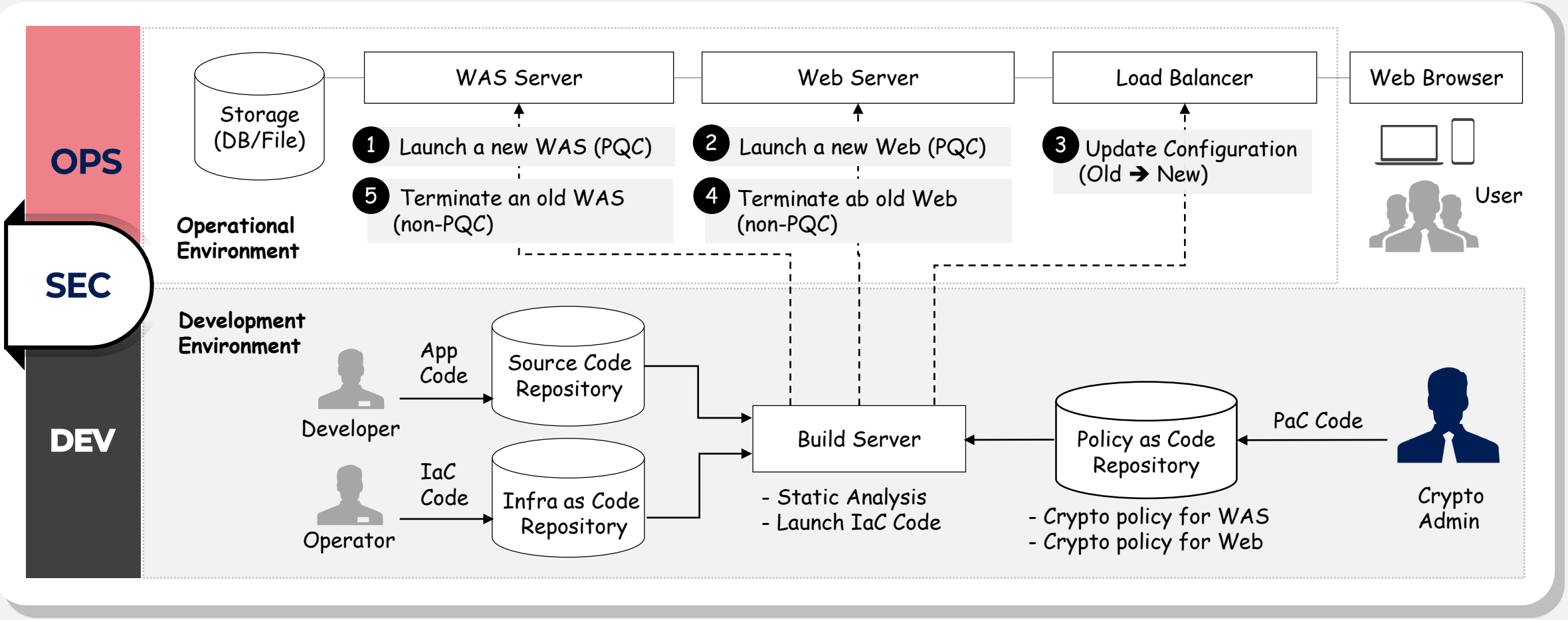
Crypto policies should be automatically enforced for enterprise applications

CASE STUDY

Automation:

Automate crypto policy enforcement with DevSecOps Tools

Cryptographic policies can be defined as codes (Policy as Code), and automatically enforced using codes (Infrastructure as Code)



Toward Software-Defined Cryptography

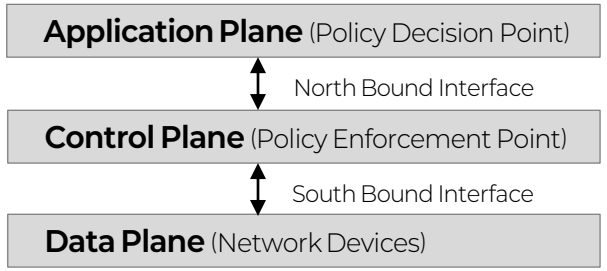
Enabling Crypto Agility in Enterprise IT

SW-Defined Network (SDN) emphasizes the role of **software** and **programmability** with the **three pillars**

Governance	Abstraction	Automation
Centrally managing the behaviors of network as a whole	Introducing an **abstraction** for the data plane, separating it from the control plane	**Automating** the configuration with programmable interface

Software-defined approach has been applied to storage and data center, and also to **SW-defined perimeter** and **Zero Trust Architecture**.

Simplified SDN Architecture



Three Pillar of Crypto Agility in Enterprise IT

Governance ⊕ Abstraction ⊕ Automation

It is the time for cryptography to embrace **SW-Defined Approach!**