Handling Millions Securely: WSO2 for High-Scale Digital Signature Services

Rifky Izdihar Haidi – Senior System Engineer

Steven Yohanes Tambunan – Senior System Engineer

Balai Besar Sertifikasi Elektronik

Empowering Secure Digital Services at National Scale

About BSrE:

- Government Institution under National Cyber and Crypto Agency
- Mostly known as Government Certification Authority

Our Core Responsibilities:

- Provides secure digital signature and verification services
- Provides Timestamping services
- Provides Electronic Seal
- Provides Digital ID

Our Scale

Number of Transaction

+ 1 Million Transactions/day

Number of Active Users

+ 1 Million Users

Number of Digital Certificate Issued

+ 1 Million Digital Certificates

Total Transactions

+ 2 Billion (Transactions)

Number of Clients

+ 800 Institutional Clients

Why It’s Challenging?

HIGH CONCURRENCY AND THROUGHPUT

IT MUST BE AVAILABLE **24/7, WITHOUT EXCEPTION**

SUPPORTS **CRITICAL SERVICES OF OTHER NATIONAL INSTITUTIONS**

REAL-TIME RESPONSIVENESS IS EXPECTED BY END USERS

COMPLIANCE REQUIREMENTS CONTINUE TO EVOLVE

What the System Must Deliver

Scalability

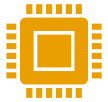
Must handle millions of transactions daily

Designed for horizontal scaling to meet demand

Security & Trust

Ensure cryptographic integrity

Ensure secure key management (HSM Integration)



High Availability

Designed for 24/7 uptime with active-active redundancy

Disaster recovery and failover built in

Performance

Process request in real time

Maintain throughput in peak load condition

Maintainability

Modular architecture to support upgrade and patches

Easy onboarding for new institutions or services

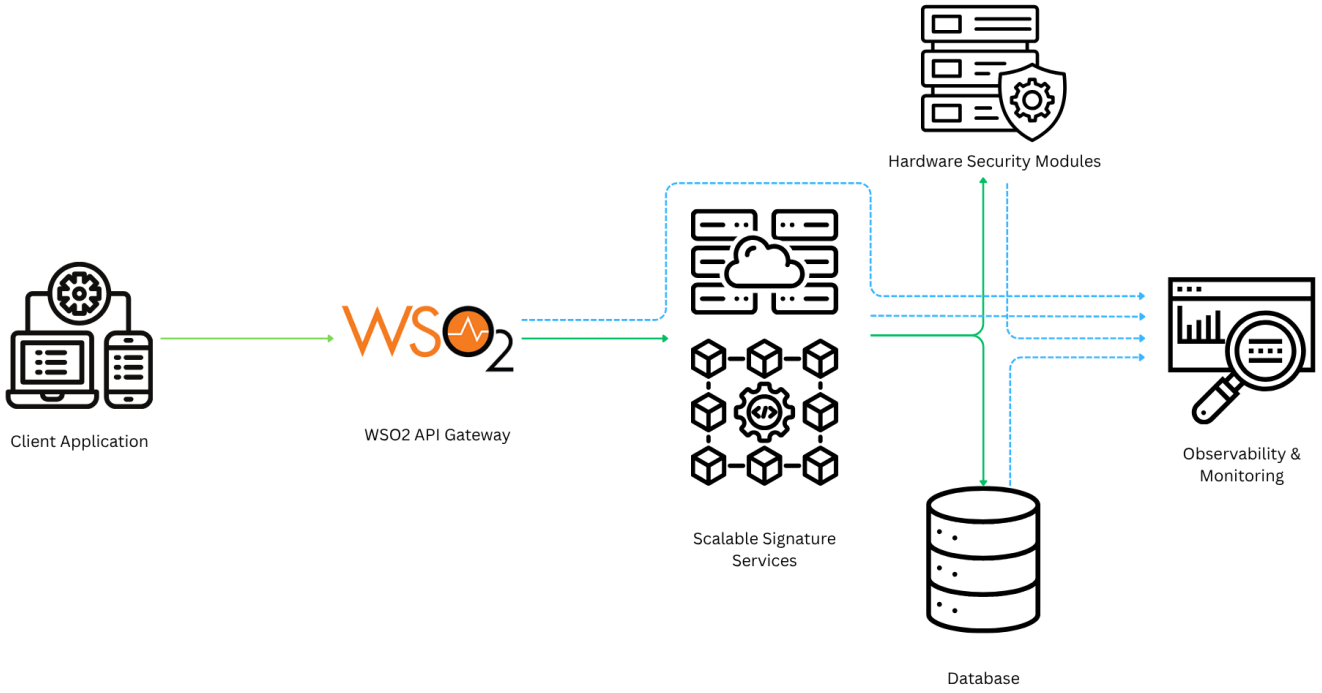
Compliance & Auditability

Comply to Local CA Regulation and International CA Compliance (WebTrust)

Security Architecture

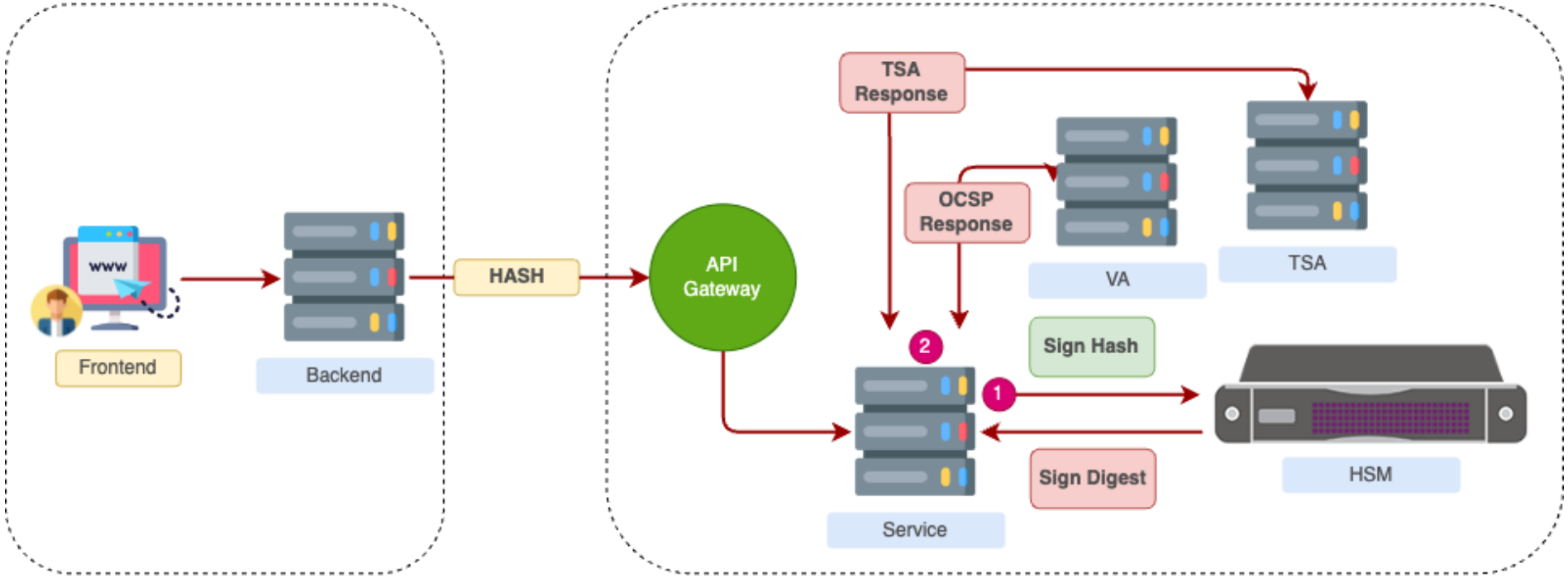
HSM-based Key Management	All private keys are securely stored and used within certified **Hardware Security Modules**
API access via Gateway	All requests pass through the **WSO2 API Gateway** with enforced **authentication and rate limiting**. No direct access to backend services.
DevSecOps-Driven Security	Security is integrated early and continuously through SAST, Container Scanning, and Dependency Vulnerability Scanning
Comprehensive Audit Trails	Every signature operation is **logged and signed** All **user and system activity** is traceable for compliance

High Level System Architecture Overview

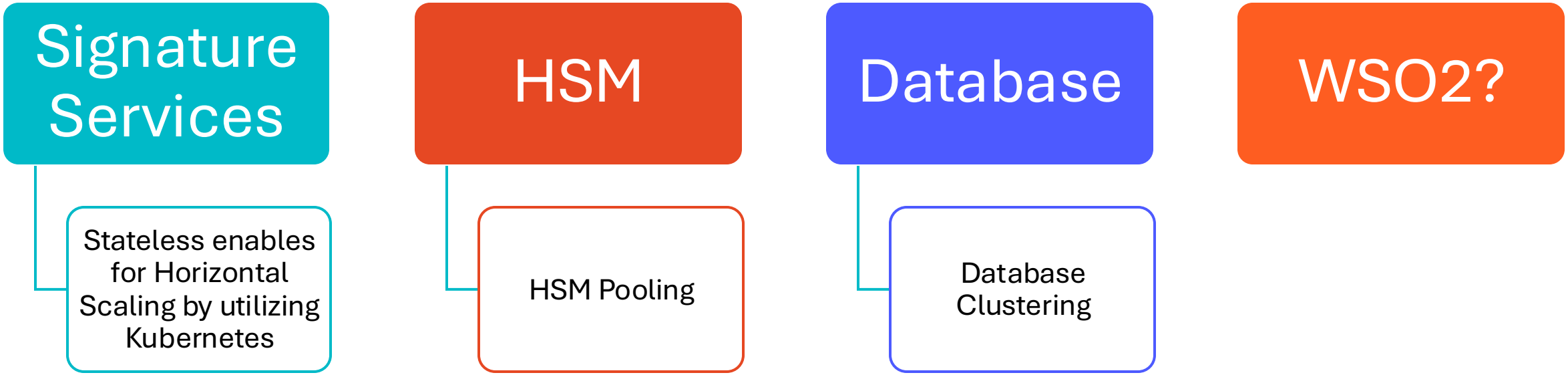


1. Client Applications
   - Communicate via REST API over HTTPS
2. WSO2 API Gateway
   - Authentication
   - Token Issuance & Validation
3. Signature Services
   - Stateless signature microservices
   - Integration with HSM
   - Database Cluster
4. Observability & Monitoring
   - Logging
   - Metric Monitoring

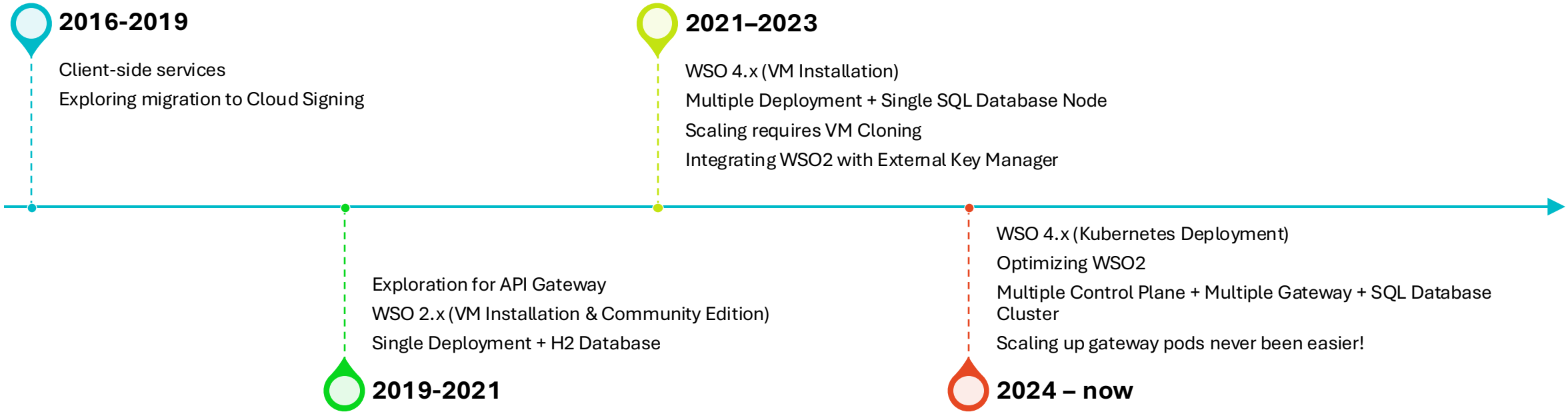
Digital Signature Creation Workflow



Scalability Design



Our Journey with WSO2 API Gateway and API Management



Optimizing WSO2

01

Tuning JVM to allocate more memory

02

Update kubernetes resource allocation

03

Update deployment.toml for cache.jwks_cache timeout and [oauth.jwt.renew_token_without_revoking_existing]

Key Takeaways

Secure at Scale:
Our digital signature service handles **millions of transactions** with **24/7 availability** and **strong security controls**.

WSO2 Powers the Core:
API Gateway and Identity Server enable **secure, auditable, and manageable** API access.

Built for Integration:
Designed to support **critical systems across institutions**, ensuring **interoperability** and **compliance**.

DevSecOps-Driven:
We embed security early in development and maintain full visibility through **observability and audit trails**.

Resilient Architecture:
Built on a **scalable, containerized, and cloud-native infrastructure** — ready to grow with demand.

“Handling millions securely isn’t just a goal — it’s a continuous commitment, and WSO2 helps us deliver on that promise.”

Thank You!