Pantasign

A Licensed Certifying Authority

5th International Conference on

Public Key Infrastructure & Applications 2024

Building a Secure Foundation

Hardware Root of Trust, Attestation of Trust & PKI

by

Abhishek Ranjan

Why build a Security foundation?

Data

Security & Protection

→

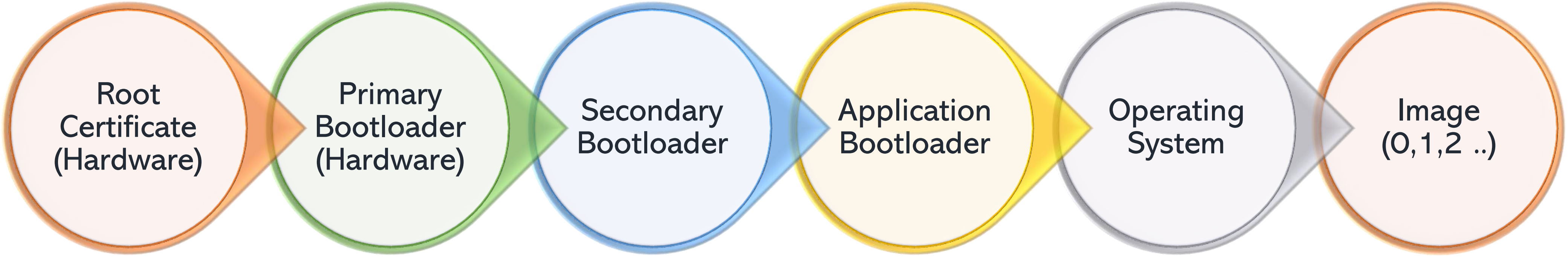
Future

Long-term Resilience

Prevention of Data & Information from unauthorized access & leakage

What is HW-RoT?

A **Hardware Root of Trust** is a security component that establishes trust between components of a computing system.



Immutability

HW-ROT is typically built into the silicon of the device, making it tamper-resistant and immutable

Cryptography

Cryptographic processor that performs secure operations, such as generating, storing, and managing cryptographic keys

Trust Anchor

All security protocols within the device depend on HW-ROT as the ultimate source of trust

HW-RoT Current Trends

HW-RoT is securing devices across various industries, from smartphones and IoT devices to servers and data centers, protecting sensitive data and preventing unauthorized access.

IoT Devices

integrated into IoT devices to secure connected devices, ensuring they operate securely within their ecosystems.

Critical Infrastructure

Industries such as energy, healthcare, and finance are adopting HW-ROT to protect critical infrastructure systems from sophisticated cyber attacks

Cloud & Edge Computing

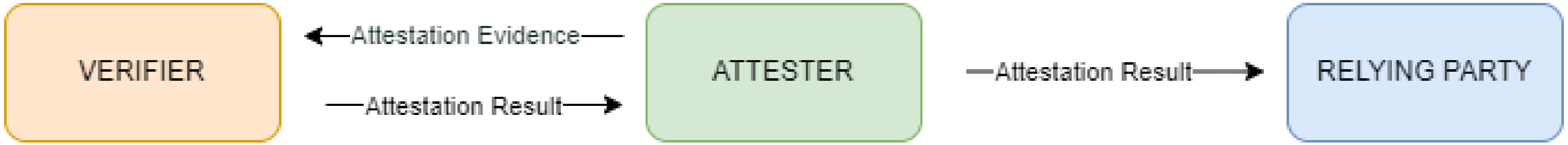
Secures cloud & edge computing environments, providing a trusted foundation for virtualized and distributed computing

AI & Machine Learning

Being leveraged to secure AI models and data processing environments, preventing tampering and ensuring trustworthy outcomes.

Attestation of Trust

Attestation of Trust is a security process that provides cryptographic proof of a device's integrity, ensuring that it has not been tampered with and is running authorized software



Security Assurance

Ensures devices operate in a trusted state

Trust Establishment

Protects against unauthorized access and tampering

Compliance & Integrity

Supports regulatory compliance and security auditing

Attestation in Real World

Google

Google Play Security

Google Play Security uses attestation to verify that apps are running on secure, unmodified devices.

Play Secure

Integrity checks on device and app before they are allowed to interact with Google services.

Apple

Apple Platform Security

Apple employs attestation as part of its broader security strategy, integrated within the Secure Enclave.

Secure Enclave

Apple devices use a unique, hardware-backed key-based for attestation to ensure the device is running genuine software

HW-RoT, Attestation & PKI

HW-ROT, Attestation of Trust, and PKI can collaborate to provide a comprehensive security framework, particularly in the context of evolving threats like quantum computing.

Enhanced Security

Combining HW-ROT, Attestation, and PKI offers a multi-layered defense, protecting devices and networks from a wide range of threats.

Trust & Compliance

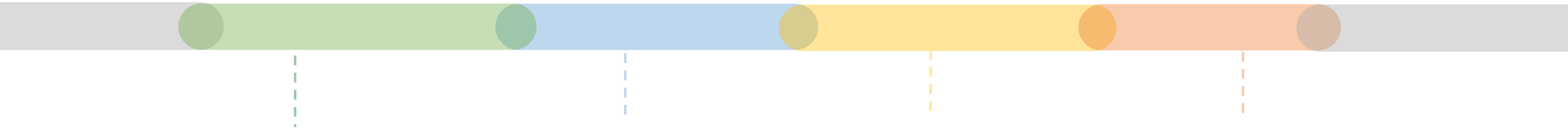
helps organizations meet stringent security standards and regulatory requirements by providing verifiable proof of device and data integrity.

Future Proofing

By integrating quantum-resistant solutions, organizations can prepare for the next generation of cybersecurity challenges, ensuring long-term protection.

Central Attestation Services

Central Attestation Service should be established to maintain a centralized record of controllers and manage attestation of trust requests from trusted devices operating within the country.



Central Registry

Placing controllers under Indian hardware root will enhance control over application deployment and accountability.

Enhanced Security

The registry will enhance national security by improving threat monitoring and response

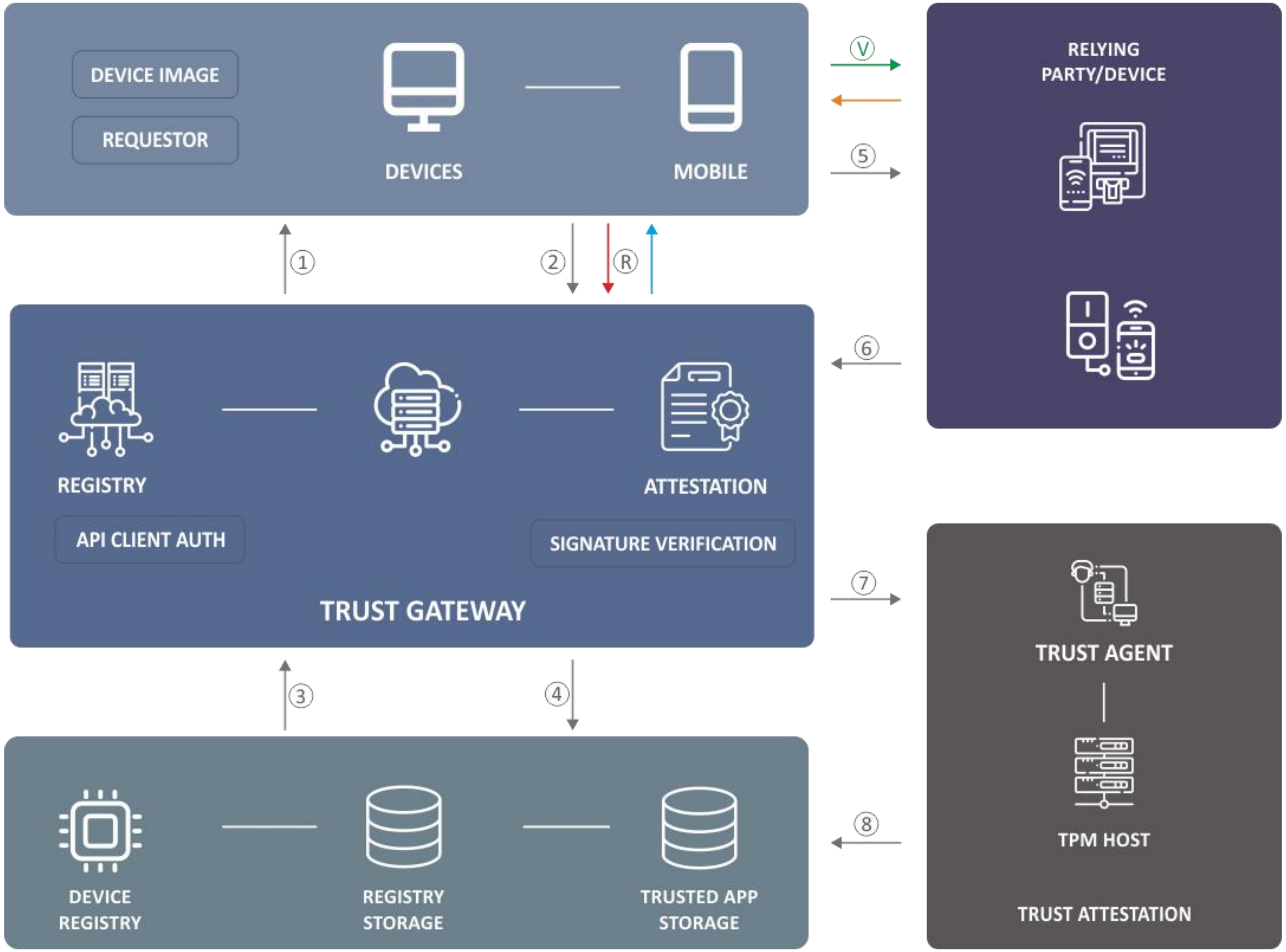
Threat Protection

The registry protects critical systems by preventing vulnerable devices from running insecure applications.

Non-Repudiable Trust

Embedding the CCA Root in the registry ensures non-repudiable, secure transactions

CAS Concept Architecture



Processing Flow

- Devices request attestation from CAS
- CAS validates the request against the Central Registry
- Attestation results are communicated securely
- Devices forwards the signed data to Relying party
- Relying party submits attestation request to CAS for verification on a different path
- PKI manages digital certificates for validated devices

Challenges

- Government Policy & Framework including necessary approvals
- OEM Co-Operation
- Timely Development

Advantages of CAS

Central Attestation Services (CAS) will enhance national security by ensuring only trusted devices and applications operate within the country.

CAS will ensure that applications run in a secure environment, protecting against threats like device takeover, impersonation, and unauthorized access.

Application Security

Quantum Ready

By embedding PKI, CAS enables a seamless transition to the Quantum Era, providing a future-proof security framework with ample time for adaptation.

- Robust Protection against threats
- Smooth transition to Quantum-Resistant Systems
- Ensures Compliance with Regulations

CAS will facilitate a smooth migration to quantum-resistant systems, reducing both the cost and time required for upgrading security protocols.

Seamless Migration

Robust Communication

Attestation process involves two-way communication with the central registry, where signature and verification messages travel through separate paths ensuring a high level of safety

Thank You!

in abhishekranjan