Staying ahead of Counterfeiters when using OEM Generic Drives for Enterprise

Luis Freeman

August 8, 2024

FMS

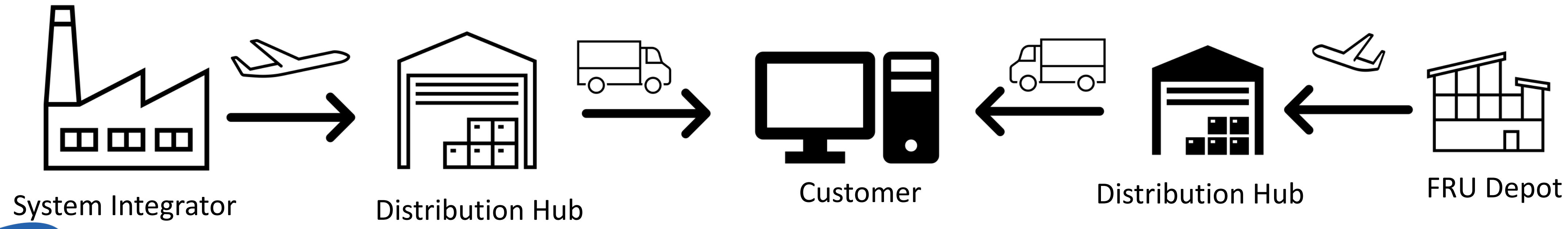
the **Future** *of* **Memory** *and* **Storage**

Why the move to OEM Generic drives for Enterprise

- Hyperscalers don’t focus on drive customization.
- Enterprise likes Custom Features on their drives for product differentiation.
- Today, Over 90% of drives are consumed by Hyperscalers.
- With only 10% or less of the volume, Enterprise is being forced to move to Generic drives or pay higher cost for Custom Firmware Drives.

⏰ No Customization = Easier Counterfeit

- Abundance of OEM Generic drives (refurbished, repaired, stollen, etc) on distribution is prime source for Counterfeit stock.
- Counterfeits can be introduced at several points across the Enterprise Supply Chain



System Integrator

Distribution Hub

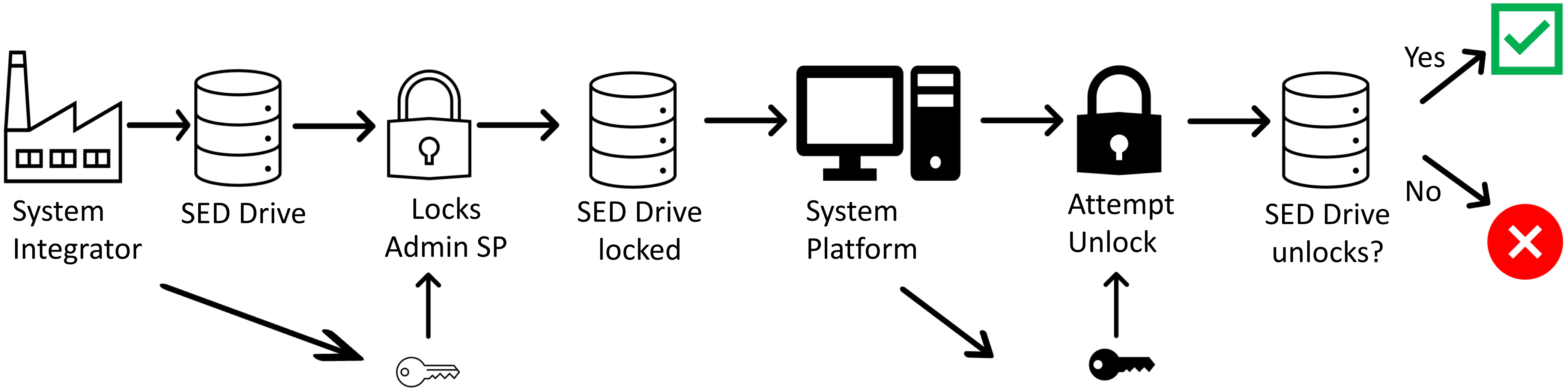
Customer

Distribution Hub

FRU Depot

Leveraging Drive SED capabilities for Authentication

SED drives make use of Credentials to Lock/Unlock the Admin Security Partition and User Data partition.



System Integrator → SED Drive → Locks Admin SP → SED Drive locked → System Platform → Attempt Unlock → SED Drive unlocks?

Yes → Drive is Authentic

No → Unknown Source – Potential Counterfeit

Sets SID credential to predetermined value

Retrieves SID credential from System TPM

How Authentication Works?

System Integrator sets the Secure ID (SID) credential to a predetermined value locking the Drive's Admin SP. The predetermined SID credential is also stored on the System's Trusted Platform Module during System integration.

CONCERN WITH THIS SOLUTION:
One credential value across all devices.
Once credential is known by Countefeiters, difficult to revoke and create new one.

SED Drive Authentication

Admin SP ➔ Admin Security Partition. Controls access to logical ports (FW Downloads, Diagnostics state, etc) using Secure ID (SID) Credential.

Locking SP ➔ Locking Security Partition. Controls access to user data

Security Module on System

Trusted Platform Module (TPM)
➔ Computer chip that can securely store artifacts to authenticate the platform.

What can we learn and leverage from Authentication on the World Wide Web?

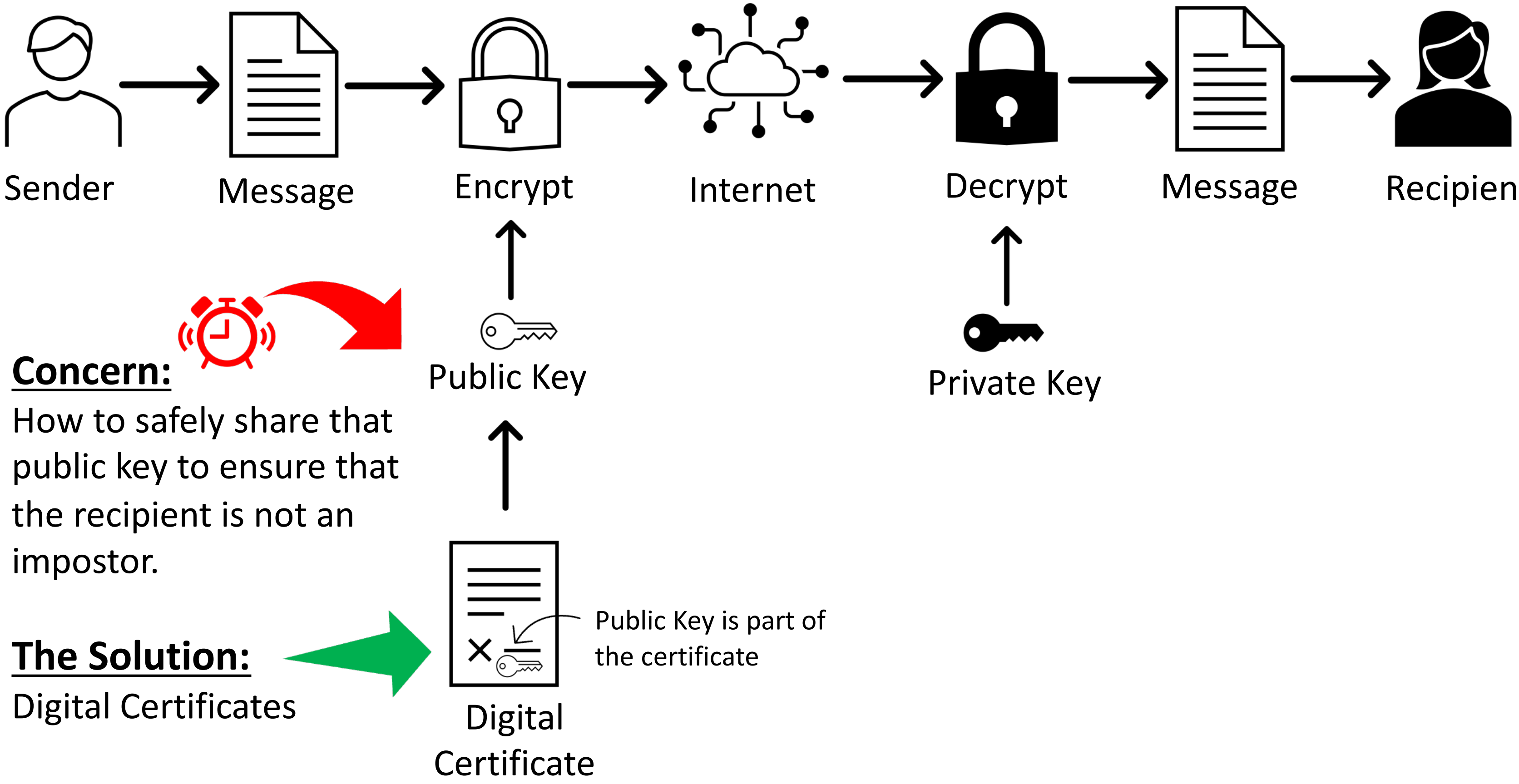
Asymmetric Encryption

Key pair, mathematically related to each other, generated from a large random number. What is encrypted with one key can only be decrypted with the other key. The key used to encrypt is called Public Key. The Key used to decrypt is called Private key.

How World Wide Web Communication works?

~~Recipient shares Public Key to Sender to encrypt message~~ and uses Private Key to decrypt the message.

Recipient shares Digital Certificate to Sender. The Digital Certificate authenticates the recipient. The public Key on the certificate is then used to encrypt the message.



Public Key is part of the certificate

<u>Concern:</u>

How to safely share that public key to ensure that the recipient is not an impostor.

<u>The Solution:</u>

Digital Certificates

Public Key Infrastructure (PKI)

Uses Chain of Trust to vouch for the authenticity of the owner's public key

Chain of Trust

A series of certificates that link back to the issuing Certificate Authority (CA)

How it works?

The offline Root CA certificate private's key signs the certificates of the issuing CA.

The issuing CA is responsible to issue Identity certificates signed by its private key.

This provides a layer of separation between the Root CA and the Identity Certificates, denoted by the dotted line

Certificate Authority (CA)

- Trusted Organization that verifies the entity issuing the **Digital Certificate.**

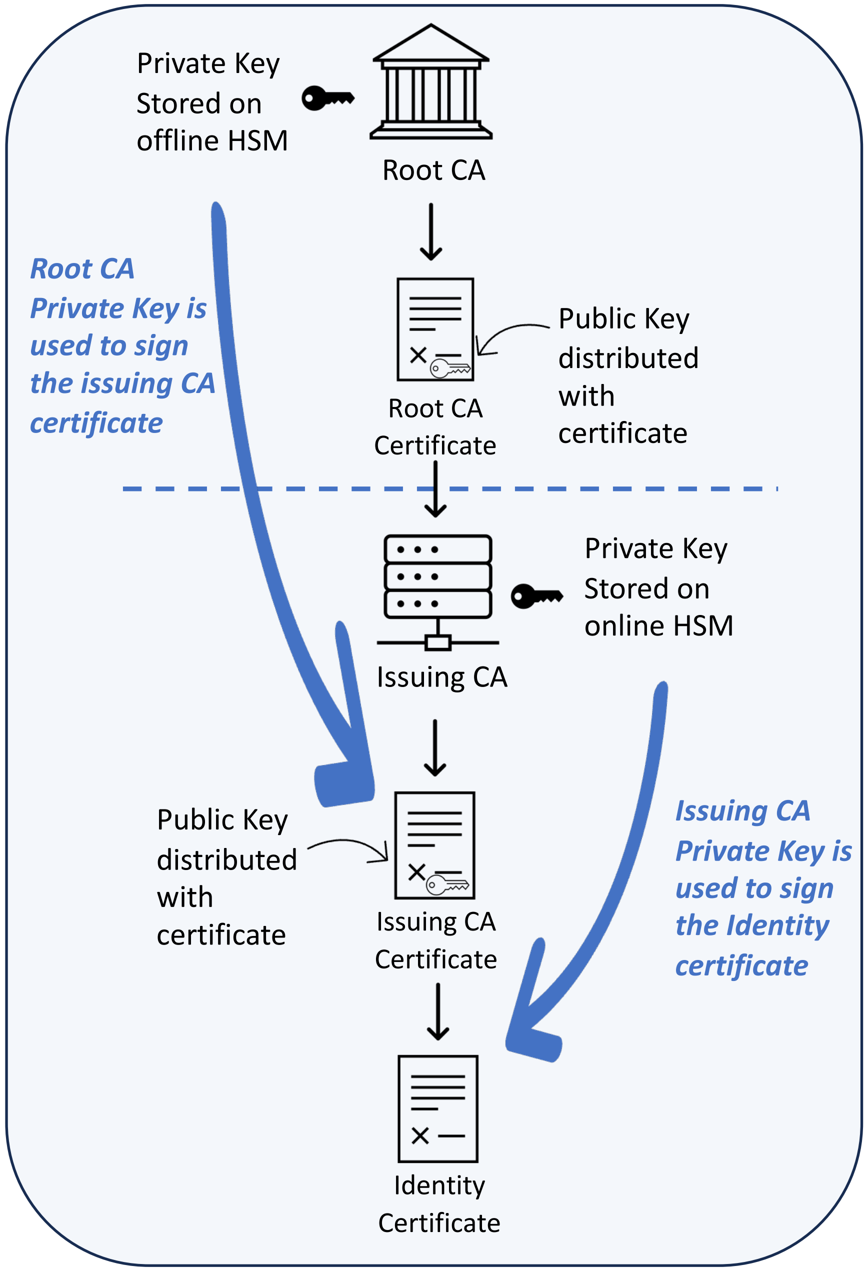
Digital Certificate

- Takes advantage of Asymmetric Encryption to Create the Certificate.
- Distributes the owner's public key.
- Establishes the identity of the owner of the certificate by **Digitally Signing** the certificate.

Digital Signature

- Secures the integrity of data.
- Makes use of hashes to generate a digest code or Fingerprint which is then encrypted to generate the Digital Signature

Chain of Trust



Private Key Stored on offline HSM

Root CA

Root CA Private Key is used to sign the issuing CA certificate

Root CA Certificate

Public Key distributed with certificate

Private Key Stored on online HSM

Issuing CA

Public Key distributed with certificate

Issuing CA Certificate

Issuing CA Private Key is used to sign the Identity certificate

Identity Certificate

Digital Signature

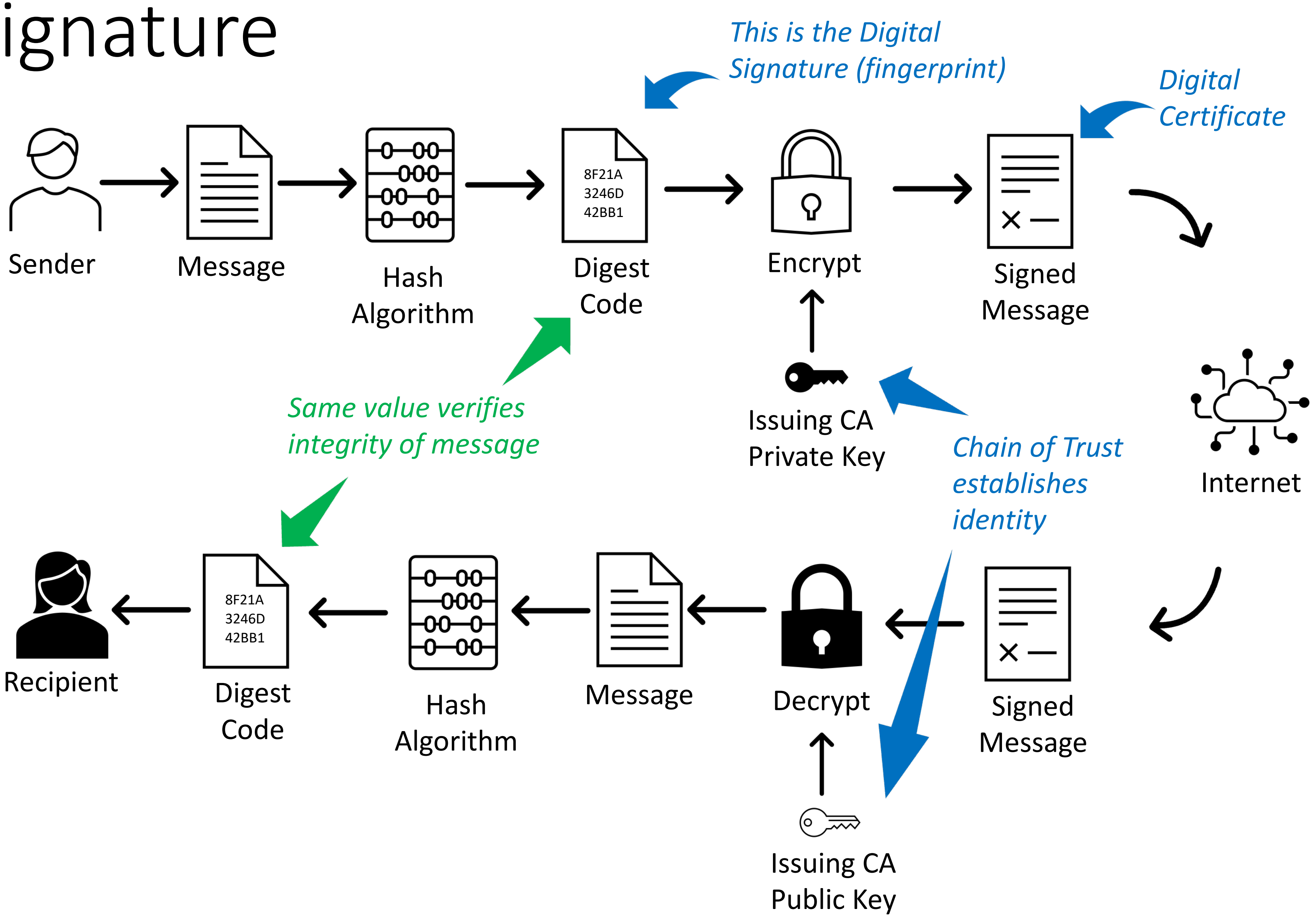
A Digital Signature ensures the integrity of the message by hashing a unique fingerprint of the message.

What is Hashing?

Process of converting data to a fixed length string using a Hashing Function (algorithm)

Hash properties:

- Deterministic
- Unique *
- Irreversible



This is the Digital Signature (fingerprint)

Digital Certificate

Sender

Message

Hash Algorithm

8F21A 3246D 42BB1

Digest Code

Encrypt

Signed Message

Issuing CA Private Key

Chain of Trust establishes identity

Internet

Same value verifies integrity of message

Recipient

8F21A 3246D 42BB1

Digest Code

Hash Algorithm

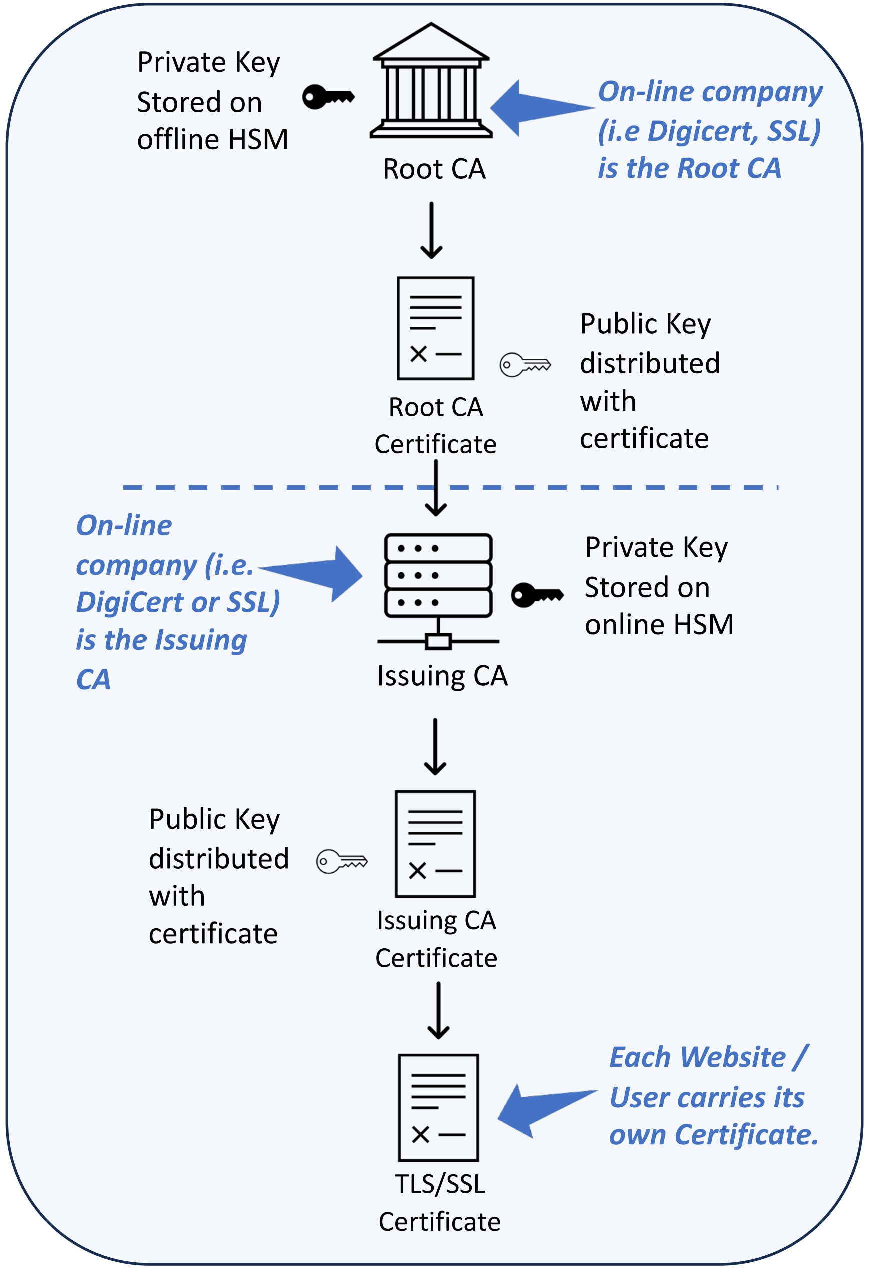
Message

Decrypt

Signed Message

Issuing CA Public Key

World Wide Web Chain of Trust



Private Key Stored on offline HSM

Root CA

On-line company (i.e Digicert, SSL) is the Root CA

Root CA Certificate

Public Key distributed with certificate

On-line company (i.e. DigiCert or SSL) is the Issuing CA

Issuing CA

Private Key Stored on online HSM

Public Key distributed with certificate

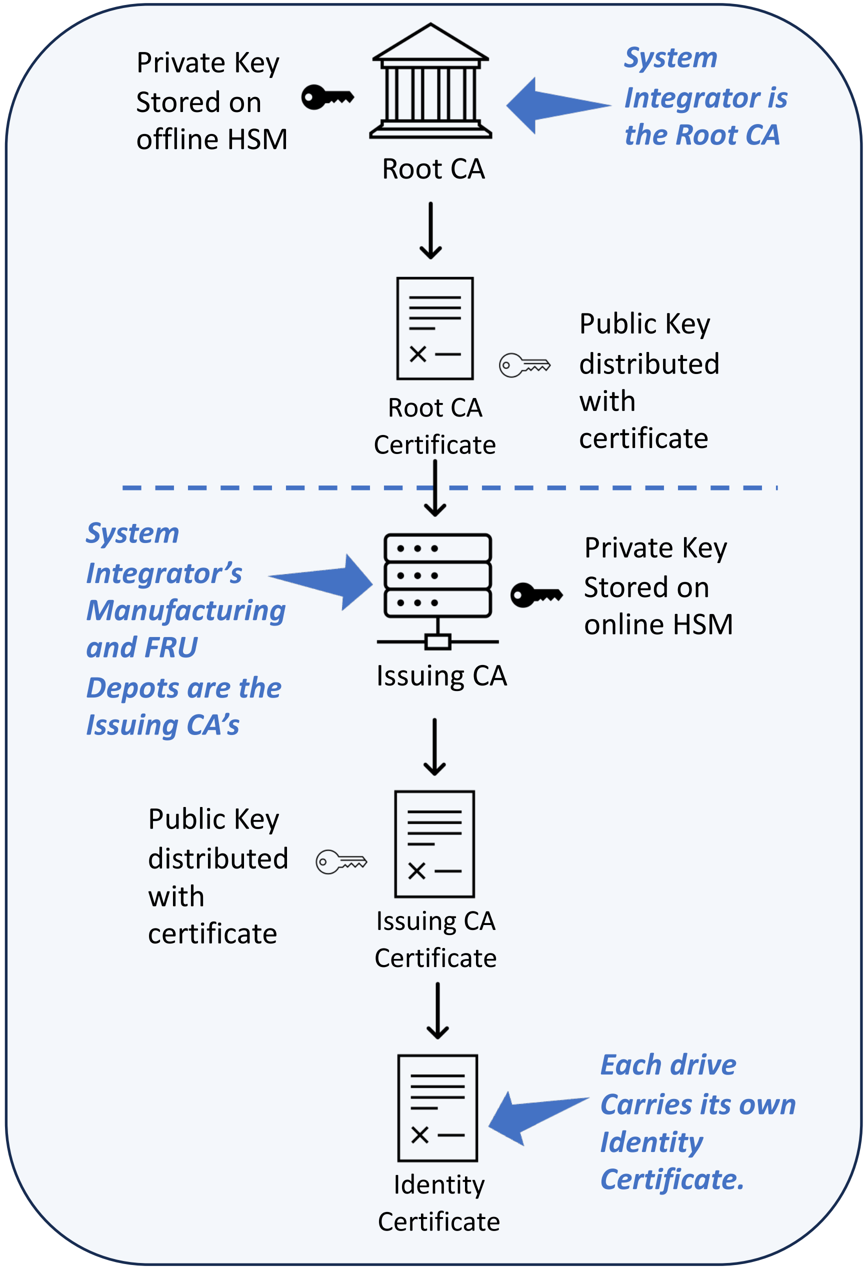
Issuing CA Certificate

TLS/SSL Certificate

Each Website / User carries its own Certificate.

Transfer concept to Drives

Drive Chain of Trust



Private Key Stored on offline HSM

Root CA

System Integrator is the Root CA

Root CA Certificate

Public Key distributed with certificate

System Integrator's Manufacturing and FRU Depots are the Issuing CA's

Issuing CA

Private Key Stored on online HSM

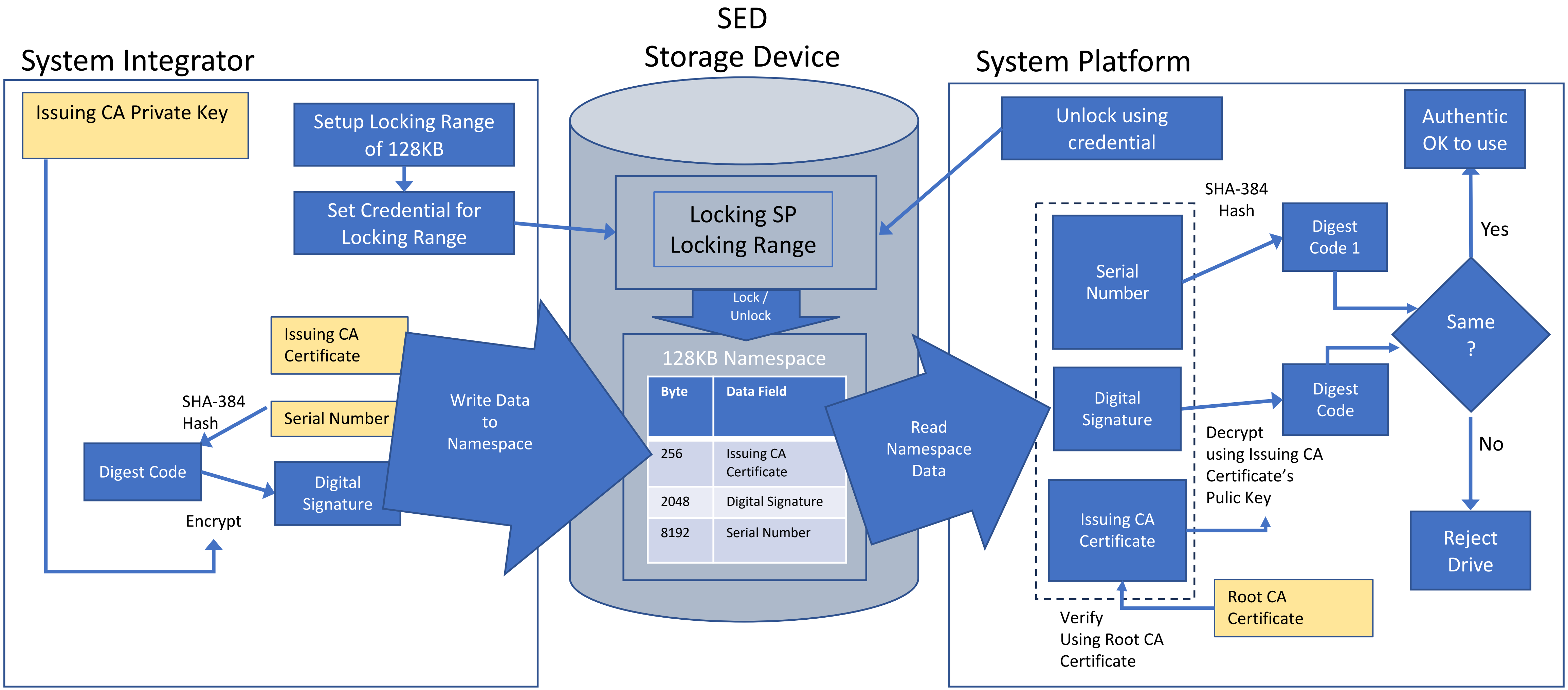
Public Key distributed with certificate

Issuing CA Certificate

Identity Certificate

Each drive Carries its own Identity Certificate.

SED Drive Authentication using PKI



Byte	Data Field
256	Issuing CA Certificate
2048	Digital Signature
8192	Serial Number

Security Protocol and Data Model (SPDM)

- Protocol that defines messages, data objects, and sequences for exchanging messages between devices over various physical and transport media.
- Used for Authentication, Attestation and protection of data in Flight.
- Can be enabled over a variety of media and can be referenced and leveraged by other standards organizations like NVM Express.
- For more information:
  - https://www.dmtf.org/standards/spdm