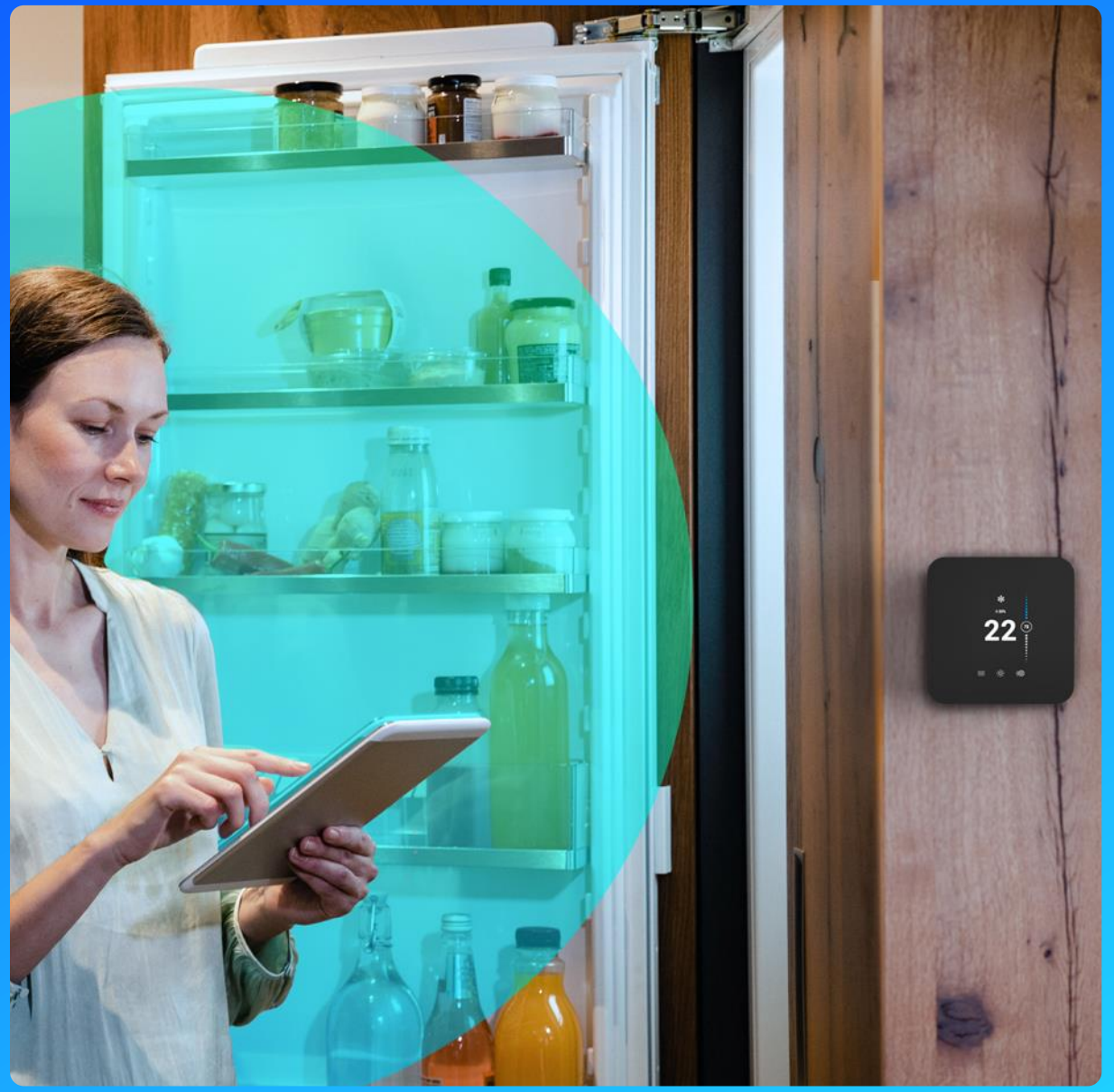
works with
BY SILICON LABS
VIRTUAL CONFERENCE

SILICON LABS

SEC-201: Applying Security to Verify Deployed Products are Authentic

Brent Wilson | September 2021

What do the Following Have in Common?



What do the Following Have in Common?

Hackers Can Steal a Tesla Model S in Seconds by Cloning Its Key Fob

Weak encryption in Tesla Model S key fobs allowed all-too-easy theft, but you can set a PIN code on your Tesla to protect it.

WIRED ANDY GREENBERG SECURITY 09.18.2018 01:00 PM

The researchers also believe their attack might work against cars sold by McLaren and Karma, and motorcycles sold by Triumph, which use keyless entry systems made by the same manufacturer. ETHAN MILLER/GETTY IMAGES

- **Security researchers from KU Leuven published this attack in October 2018**

What do the Following Have in Common?

Chamberlain 3-Button Garage Door Remote Control

$29.98

Garage Door Transmitter For 893MAX Function Digital LED Display

Alibaba.com

Ready to Ship

$2.99-$4.90

+$0.96 (Shipping)

50 Pieces (MOQ)

What do the Following Have in Common?

MOUSER ELECTRONICS

Mfr. #:	SI4463-B1B-FM
Mfr.:	Silicon Labs

Pricing (USD)

Qty.	Unit Price
1	$3.96
10	$3.74
25	$3.63

Alibaba.com

(All IC Chips) SI4463-C2A-GMR SI4463-C2A SI4463 Original in stock

Hot sale products

2 - 24 Pieces

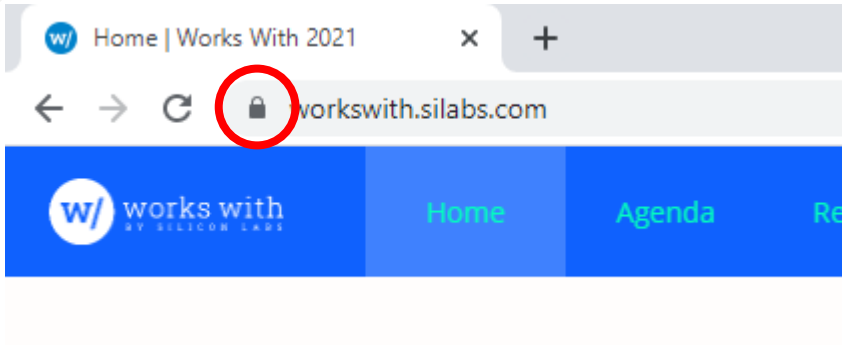
$10.35

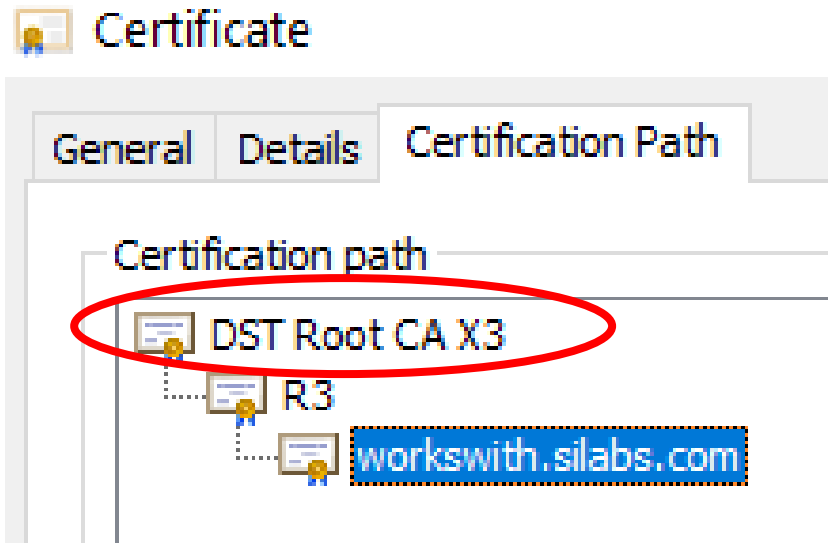
ANSWER

All are examples of weak or missing **Authentication**

Authentication = Trust

Certificate-Based Authentication





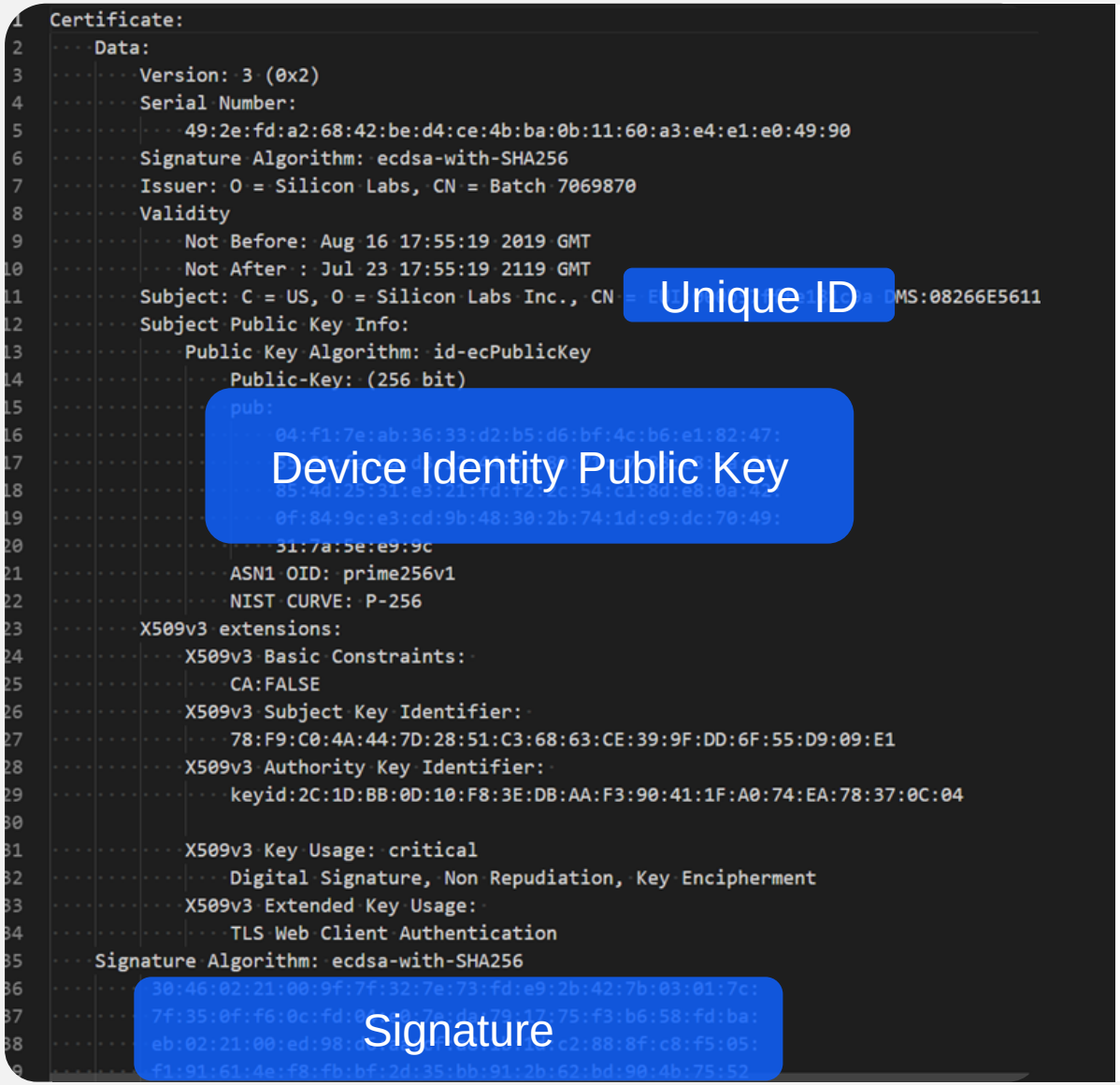
- HTTPS uses certificate-based authentication (“lock” icon in Google Chrome)
- Chrome trusts the root certificate in the workswith.silabs.com certificate chain

Emerging IoT Adoption of Certificate-Based Authentication

- Matter and Thread are actively exploring certificates
- Zigbee Smart Energy requires certificates
- Wi-SUN requires certificates
- Bluetooth Mesh v1.1 supports certificates
- ioXt is defining security certificates

Elements of a Secure Identity

Requirements for a Secure Identity



- **A Secure Identity should be:**
  - Unique for each instance of the product
  - Hard to fake
  - Hard to steal

What a Device Certificate Looks Like (1)

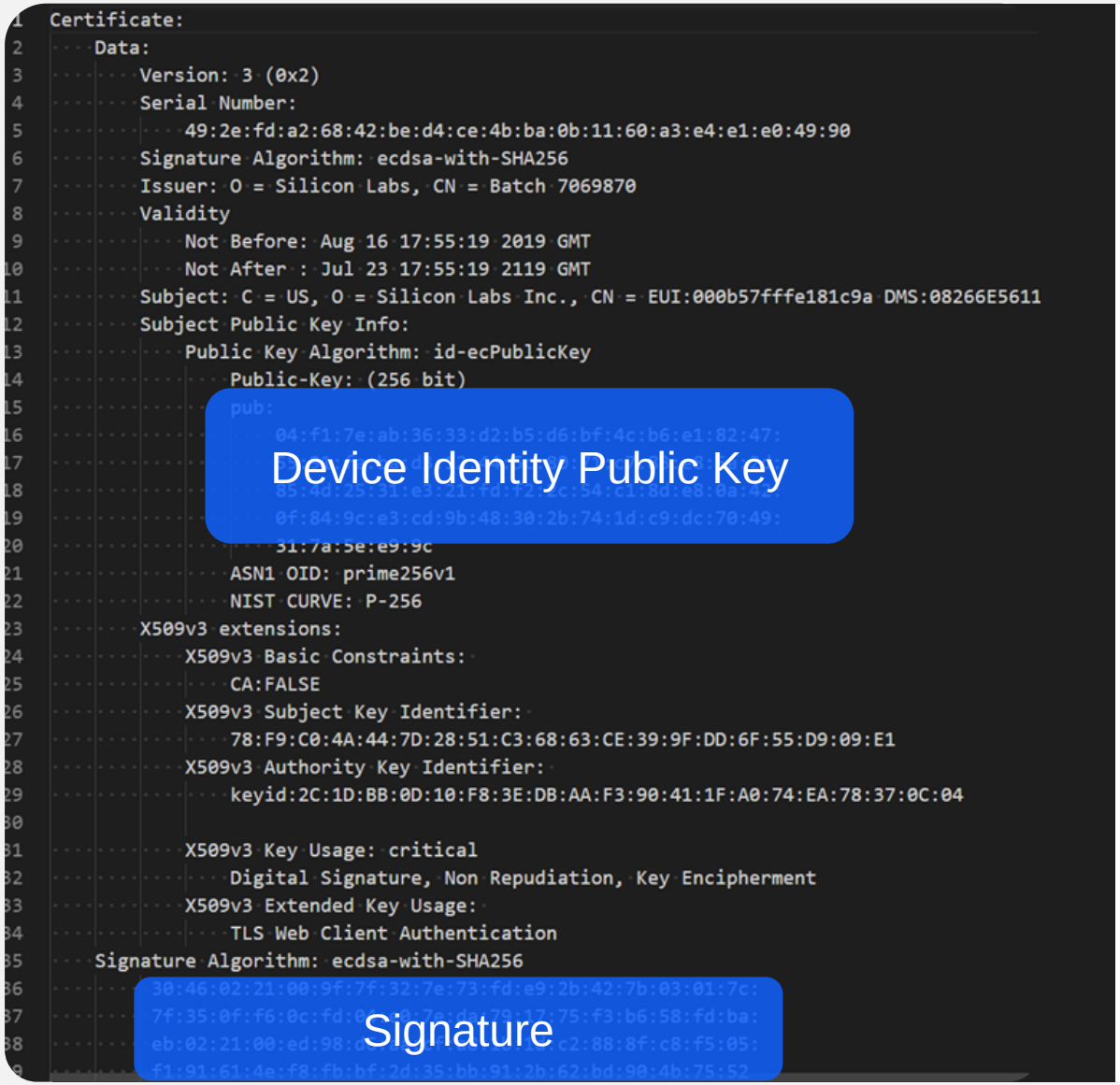
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            49:2e:fd:a2:68:42:be:d4:ce:4b:ba:0b:11:60:a3:e4:e1:e0:49:90
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: O = Silicon Labs, CN = Batch 7069870
        Validity
            Not Before: Aug 16 17:55:19 2019 GMT
            Not After : Jul 23 17:55:19 2119 GMT
        Subject: C = US, O = Silicon Labs Inc., CN = EUI:000b57fffe181c9a DMS:08266E5611
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:f1:7e:ab:36:33:d2:b5:d6:bf:4c:b6:e1:82:47:
                    55:91:fa:ba:d3:12:44:5c:80:71:c7:83:e8:5a:2d:
                    85:4d:25:31:e3:21:fd:f2:2c:54:c1:8d:e8:0a:42:
                    0f:84:9c:e3:cd:9b:48:30:2b:74:1d:c9:dc:70:49:
                    31:7a:5e:e9:9c
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                78:F9:C0:4A:44:7D:28:51:C3:68:63:CE:39:9F:DD:6F:55:D9:09:E1
            X509v3 Authority Key Identifier:
                keyid:2C:1D:BB:0D:10:F8:3E:DB:AA:F3:90:41:1F:A0:74:EA:78:37:0C:04

            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication
    Signature Algorithm: ecdsa-with-SHA256
        30:46:02:21:00:9f:7f:32:7e:73:fd:e9:2b:42:7b:03:01:7c:
        7f:35:0f:f6:0c:fd:0[illegible]:7e:da:79:17:75:f3:b6:58:fd:ba:
        eb:02:21:00:ed:98:c[illegible]:c2:88:8f:c8:f5:05:
        f1:91:61:4e:f8:fb:bf:2d:35:bb:91:2b:62:bd:90:4b:75:52
```

Signature

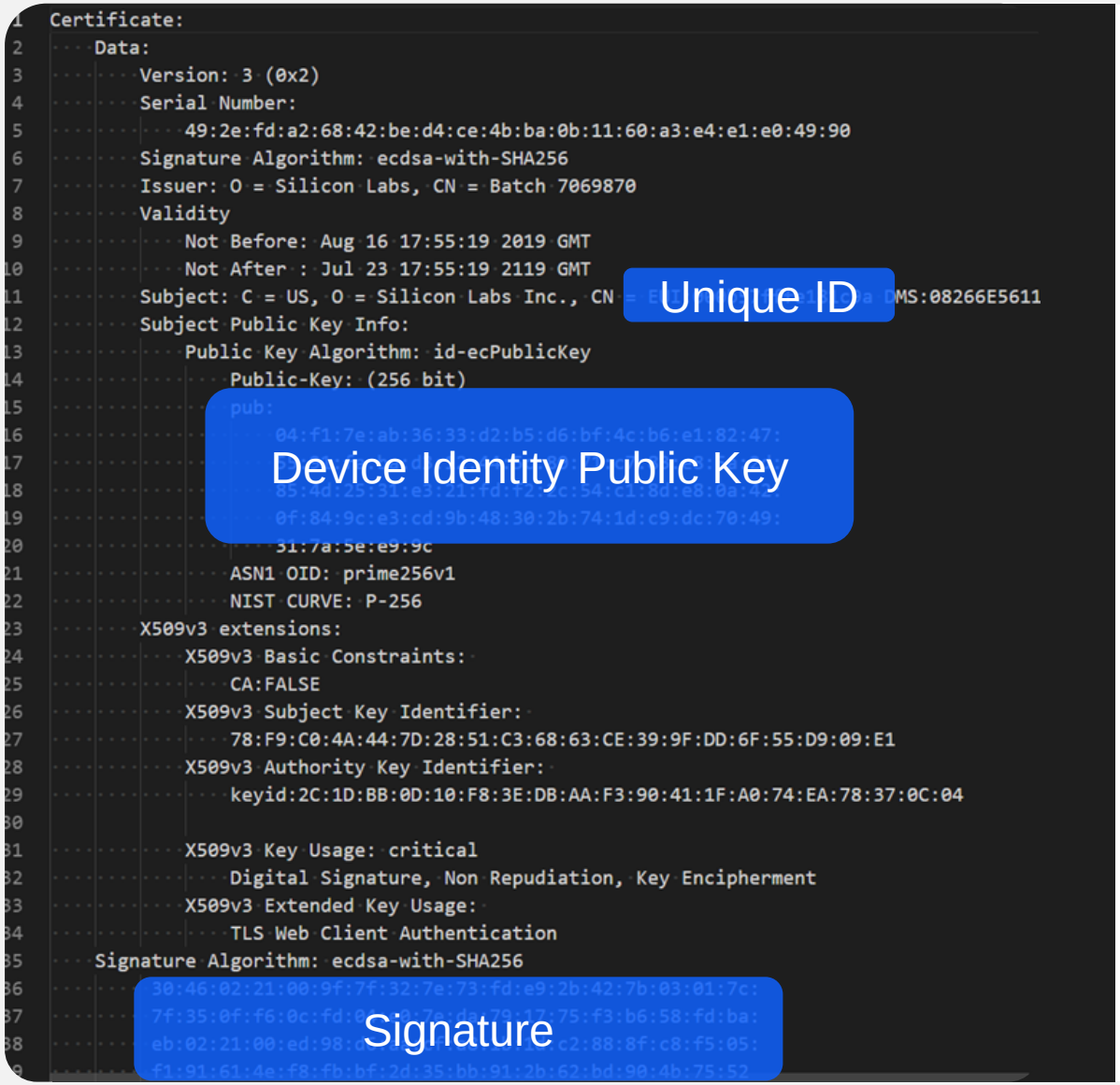
- **Common attributes of a Device Certificate**
  - **Signature** of the Device Certificate

What a Device Certificate Looks Like (2)



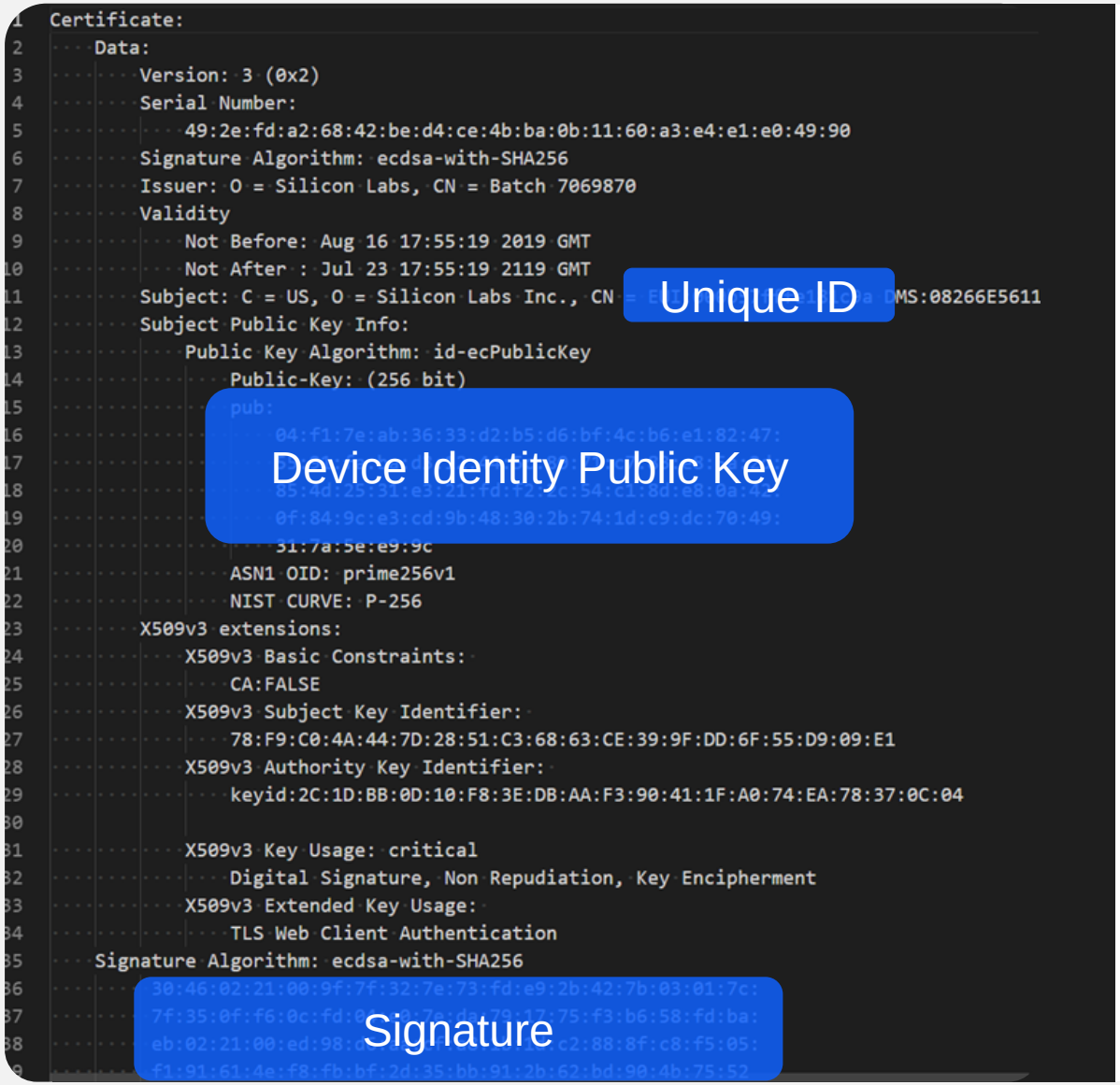
- **Common attributes of a Device Certificate**
  - **Signature** of the Device Certificate
  - **Device Identity Public Key**

What a Device Certificate Looks Like (3)



- **Common attributes of a Device Certificate**
  - **Signature** of the Device Certificate
  - **Device Identity Public Key**
  - **Unique ID**
  - (optional) Custom information

What a Device Certificate Looks Like (4)

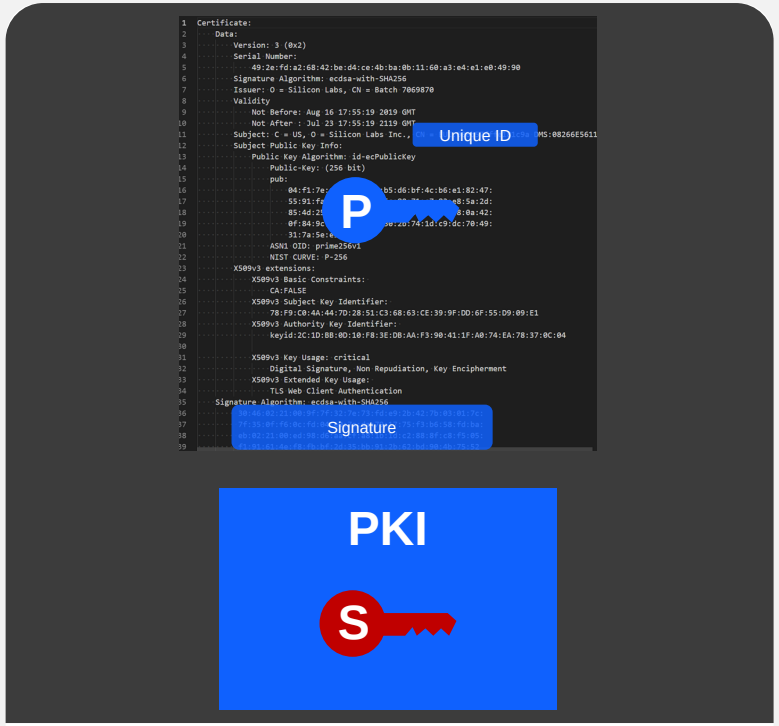


- **Note that the Device Identity Private key isn't in the Device Certificate**
  - The **Private** key is securely stored inside the device, ideally in secure key storage

How Secure Identities are Generated and Provisioned

DEVICE

1. Device generates a Device ID keypair and securely stores its **Private** key
2. Device sends its **Public** key to the PKI



PUBLIC KEY INFRASTRUCTURE (PKI)

3. PKI generates and signs the Device Certificate using a root **Private** key

PROVISIONED DEVICE

4. The signed Device Certificate is programmed into the device

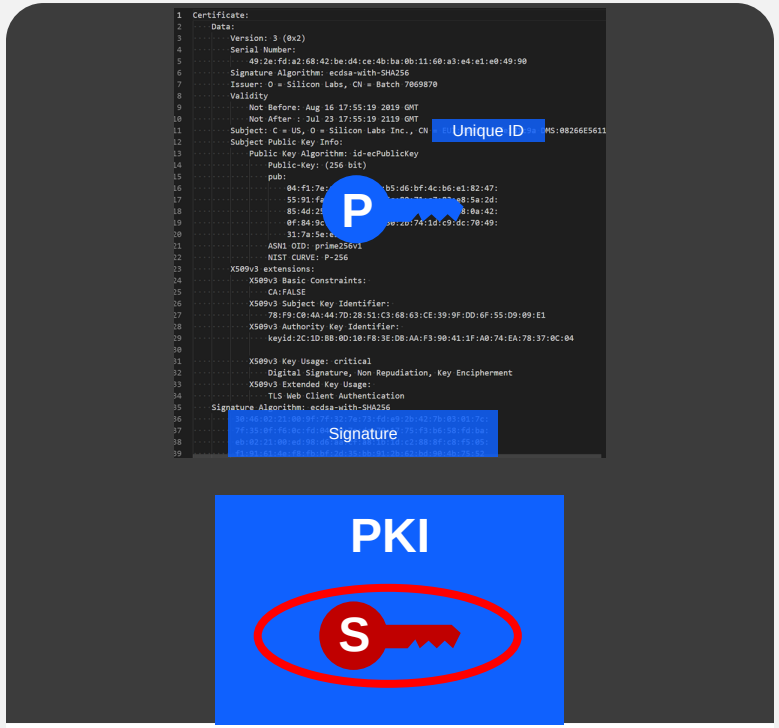
The Hard Problem to Solve – Protecting the Keys

PROTECTING KEYS ON THE DEVICE

Use Secure Key Storage

Use TrustZone

Use obfuscation techniques



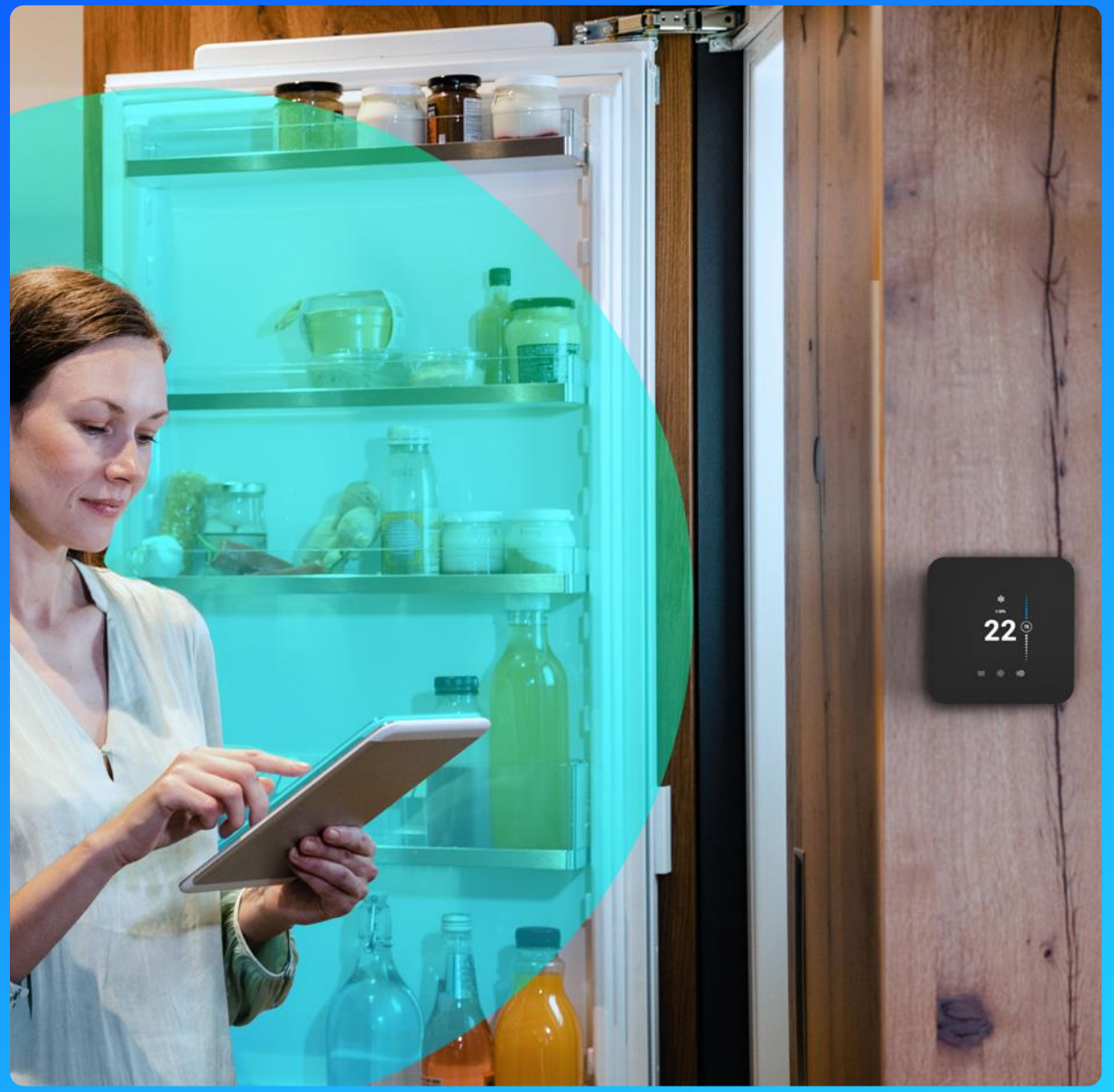
PROTECTING KEYS IN THE PKI

Use a Hardware Security Module

Physical security

Access controls and policies

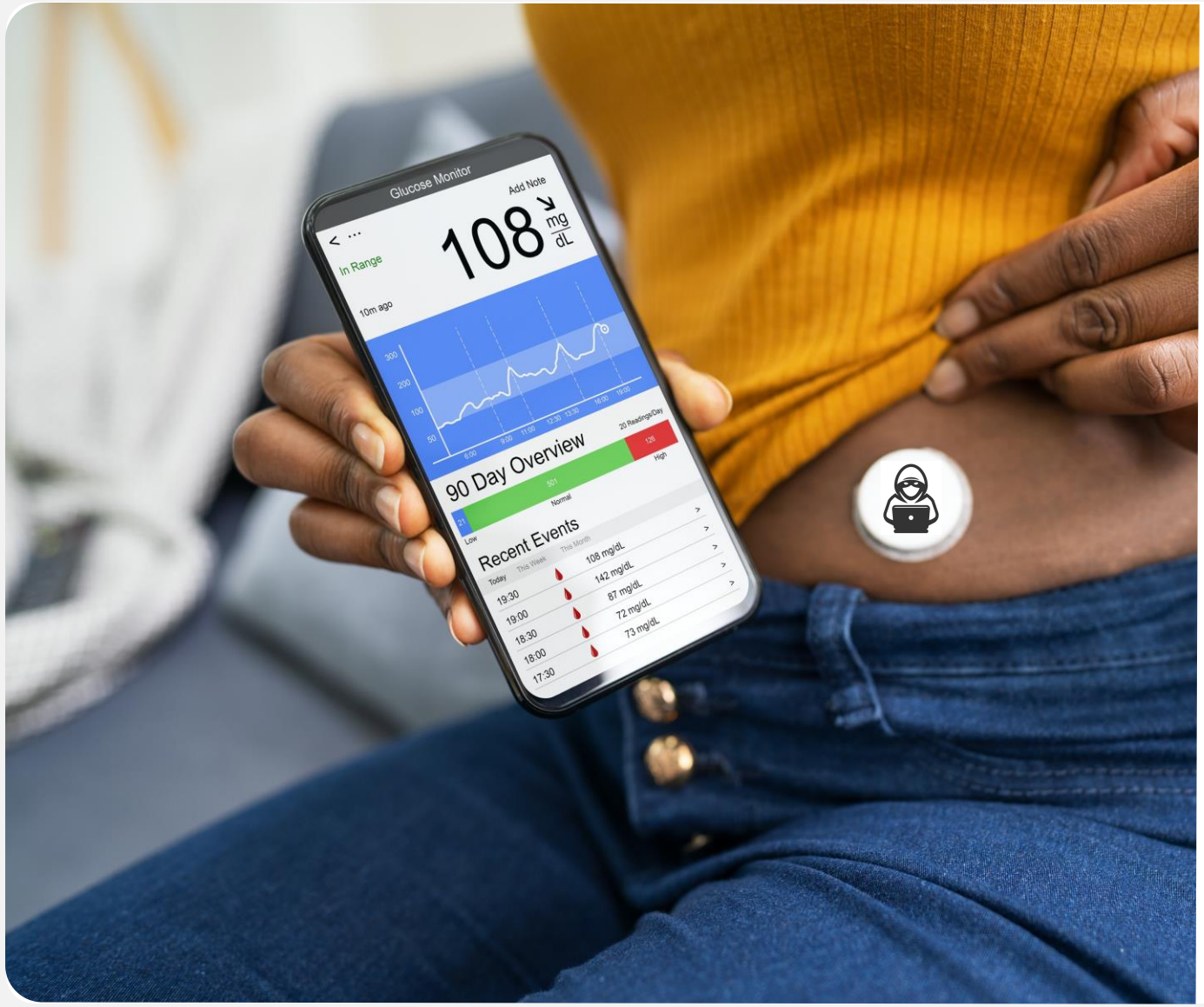
Authentication Example using Device Certificates



Use Case – Mutual Authentication Using Certificates

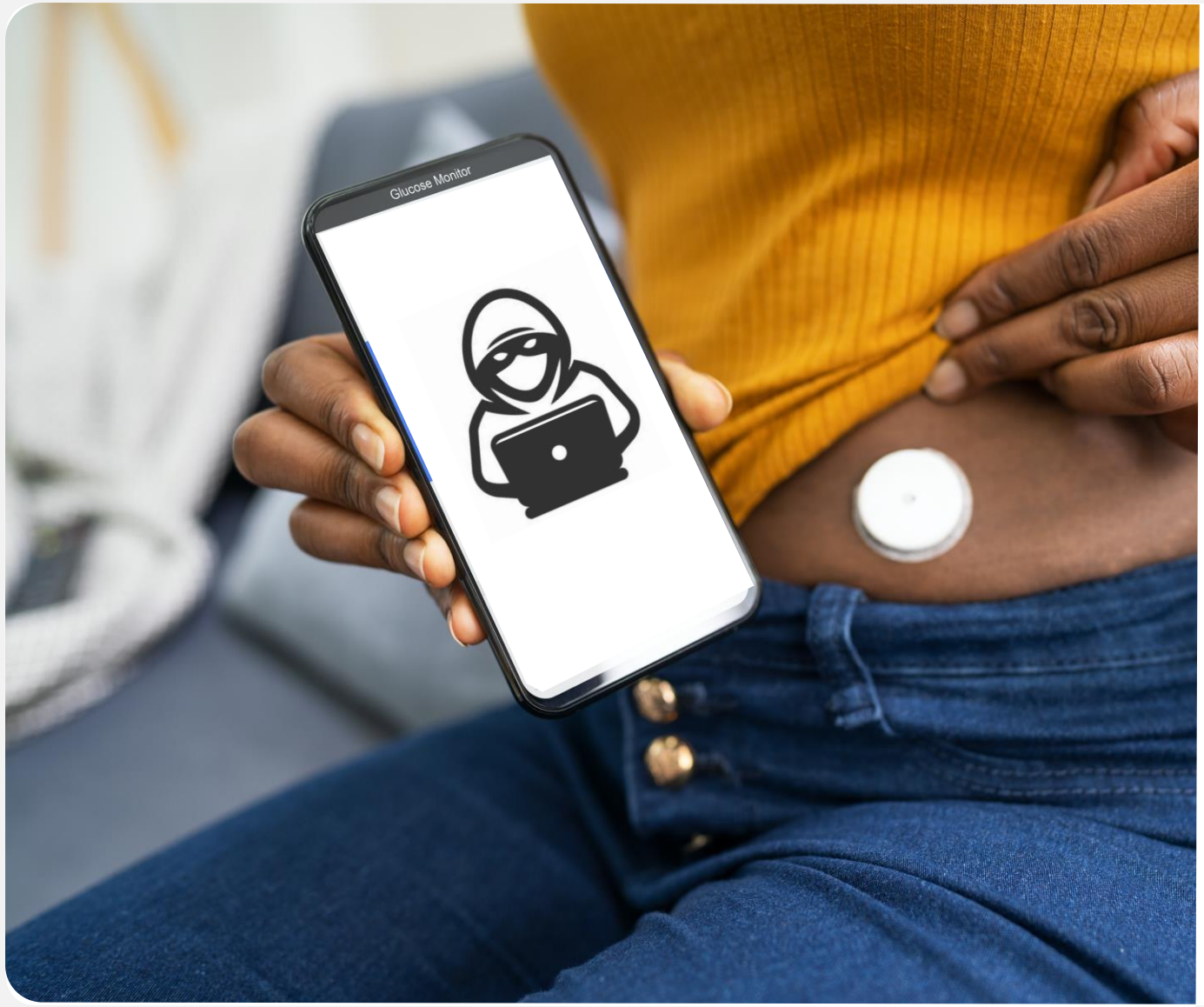
- Protects against counterfeit products and malicious apps or attackers
- Smartphone authenticates a Device
- Device authenticates a Smartphone application

Smartphone Authenticates a Device



- **Continuous Glucose Meter**
  - Ensure that the CGM is authentic (not counterfeit) and is not an attacker sending false readings to the Smartphone

Device Authenticates a Smartphone Application

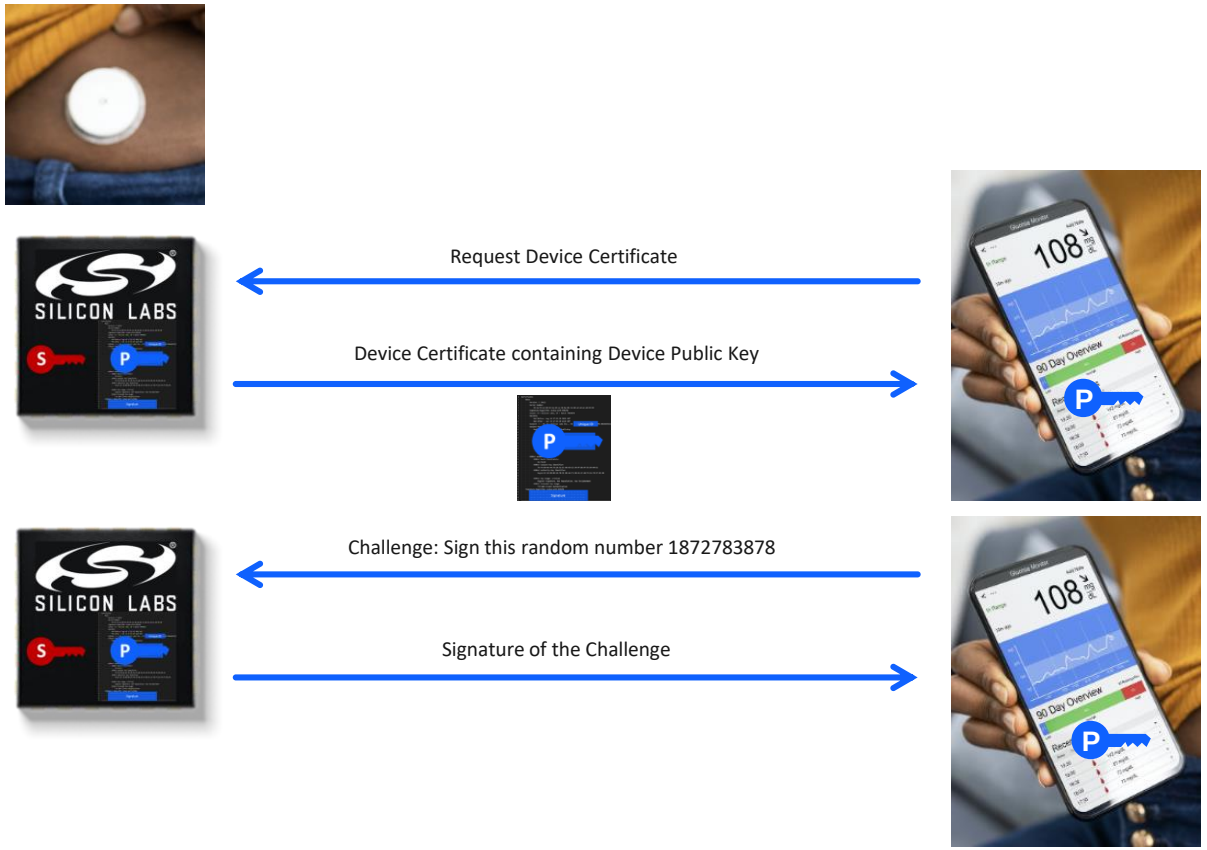


- **Insulin Delivery Device**
  - Ensure that Smartphone app and user are authentic and is not an attacker sending false commands to the insulin pump to harm the end user

Authentication Example Using a Passport

- **Give the official your passport**
  - Is the passport authentic?
  - Is the passport related to you?

Smart Phone Authenticating a Device



Is the certificate authentic?

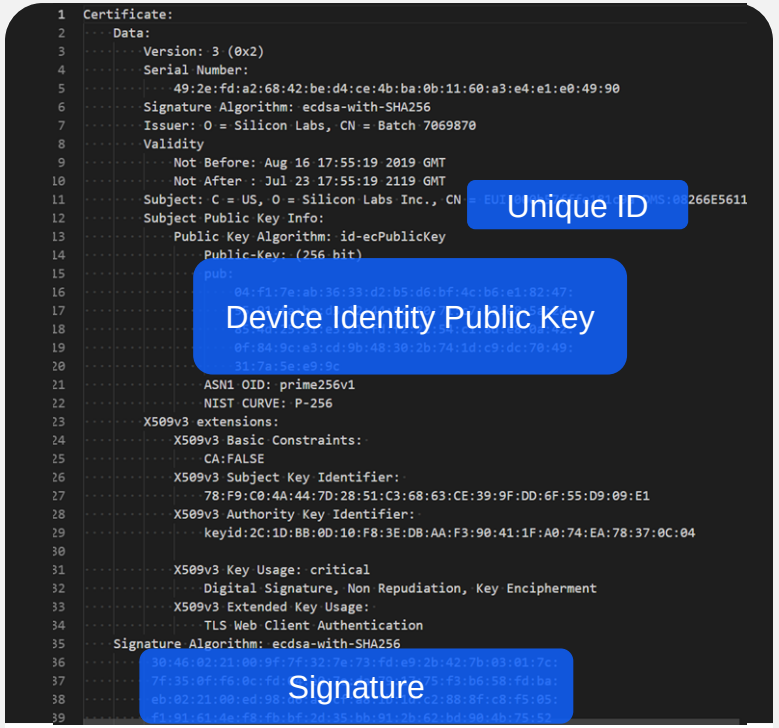
1. The App requests the Device Certificate
2. The App receives the Device Certificate and verifies its authenticity

Is the certificate related to this device?

1. The App sends a random challenge for the device to sign using the device's **Private** key
2. The App verifies the signature using the device's **Public** key from the Device Certificate

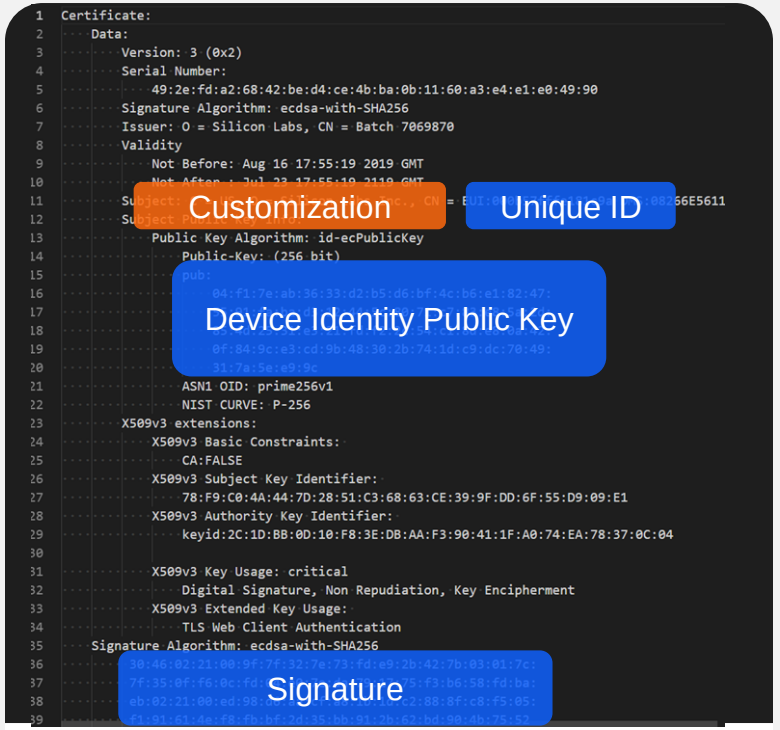
Customized Device Certificates

Use Cases for Standard and Customized Device Certificates



STANDARD DEVICE CERTIFICATES

Protects against counterfeit components



CUSTOMIZED DEVICE CERTIFICATES

Protects against counterfeit products

Protects against impersonation attacks

Supports streamlined commissioning

Resources

- SEC-301: Hands on with CPMS Security
- https://cpms.silabs.com
- AN1268: Authenticating Silicon Labs Devices Using Device Certificates
- https://www.silabs.com/security/secure-attestation
- https://www.silabs.com/support
- Brent.Wilson@silabs.com

works with
BY SILICON LABS

VIRTUAL CONFERENCE