USING COMPOSITE CRYPTO IN BROADBAND NETWORKS

LONG-TERM STRATEGIES FOR ADDRESSING PUBLIC KEY CRYPTO FAILURES

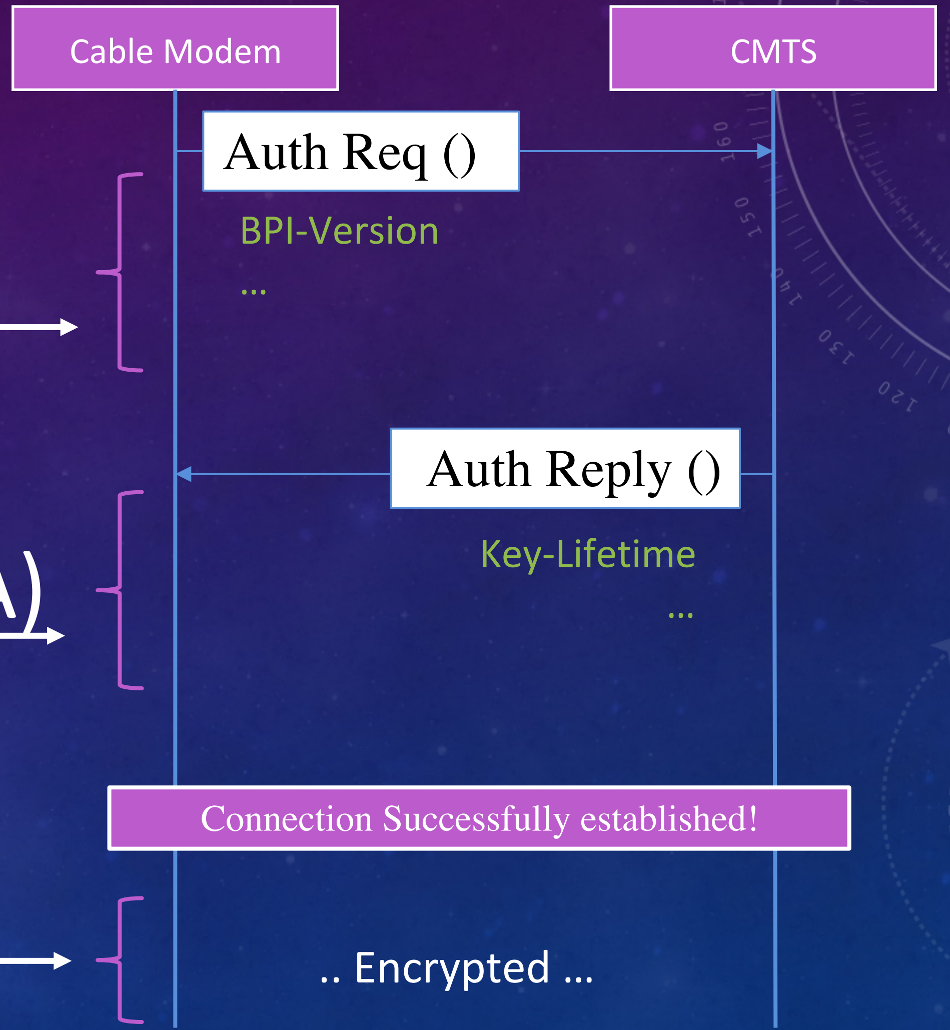
Massimiliano Pala, Ph.D. | PKI Architectures, Director
Security and Privacy Technologies, **Cable**Labs

DOCSIS® SPEC CRYPTO

Client Authentication (RSA)
(DOCSIS Specs 1.1-4.0)

Network Authentication (RSA)
(DOCSIS Spec 4.0 only)

Encryption (AES)
(DOCSIS Spec 1.1-4.0



Cable Modem

CMTS

Auth Req ()

BPI-Version
…

Auth Reply ()

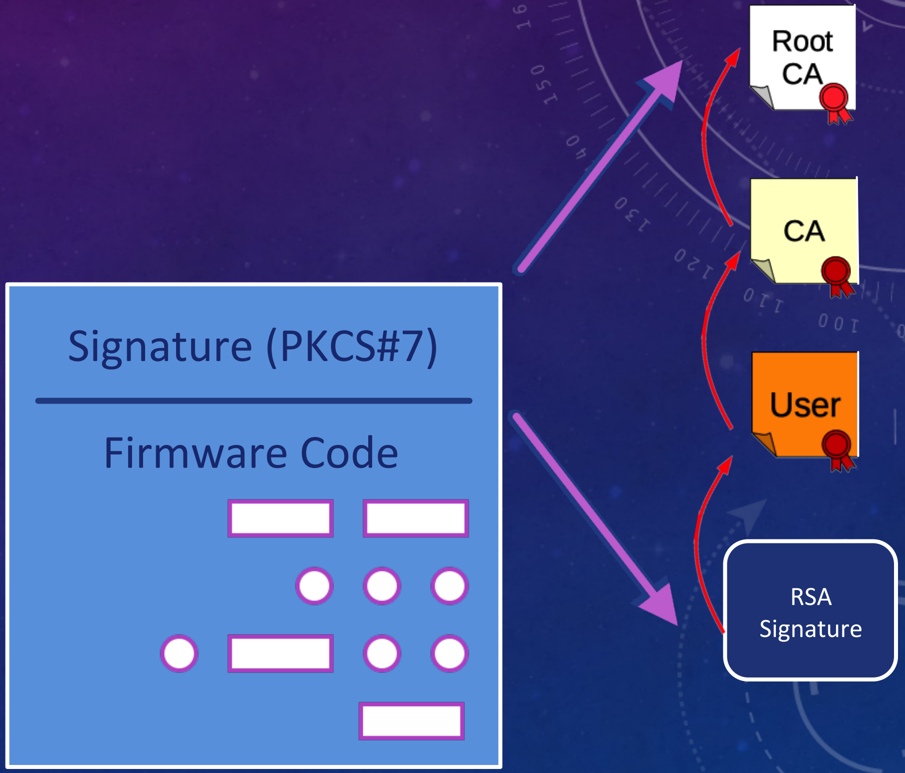
Key-Lifetime
…

Connection Successfully established!

.. Encrypted …

DOCSIS CRYPTO & CVC

- Firmware Upgrades Rely on CVC certificates and Public-Key Algorithms (RSA)
- The PKCS#7 format is used to sign and validate the Firmware Images
  - After installation, devices use internal processes (e.g., symmetric keys or hashes) to validate the next step in the boot process
- New post-quantum (or hybrid) CVC will be used to support new algorithms
  - What about existing/classic only firmware?



Firmware Code File

Technology Selection

- **How to live in a mixed environment**

Deployment Model Considerations

- **Single Certificate vs. Multiple PKIs**

Domain-Specific Requirements

- **Device Lifetime Expectations**

DEPLOYMENT MODEL

Multiple Infrastructures

- Two Certificates
- Two Separate PKIs
- Deployment Costs
- Protocol Changes

One Certificate Solution

- Single Certificate
- Multiple Algorithms
- Use Existing Identities
- No Protocol Changes for certificate selection

DEVICE CAPABILITY COMPARISON

← Device Types →

↑ Ops ↓

	Classic Only	Validation Capable	Quantum-Safe
Signing With Classic	**Yes**	**Yes**	**No**
Signing With Quantum-Safe	**No**	**No**	Yes
Verifying With Classic	Yes	Yes	Yes
Verifying With Quantum-Safe	**No**	Yes	Yes

SOLUTIONS COMPARISON

← Device Types →

↑ Ops ↓

	Classic Only	Validation Capable	Quantum-Safe
Signing With Classic	Yes	Yes	No
Signing With Quantum-Safe	No	No	Yes
Verifying With Classic	Yes	Yes	Yes
Verifying With Quantum-Safe	No	Yes	Yes

We Need Something to Allow non-Quantum-Safe devices to securely authenticate on our networks

SOLUTIONS COMPARISON

← Device Types →

↑ Ops ↓

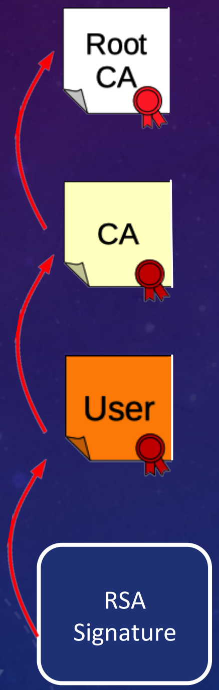
	Classic Only	Validation Capable	Quantum-Safe
Signing With Classic	**Yes**	**Yes**	No
Signing With Quantum-Safe	**No**	**No**	Yes
Verifying With Classic	Yes	Yes	Yes
Verifying With Quantum-Safe	No	Yes	Yes

We Need A Mechanism to Allow classic only devices to securely validate other devices on the network (classic and quantum-safe)

TWO CERTIFICATES VS. COMPOSITE CRYPTO

Feature	Two Certs	Composite Crypto
Changes to PKI	Not Needed	Requires Changes (New Algos Bolted On)
Certificate Size	Smaller Size (if only one cert is used)	Bigger Size for “classic” authentications
Certificate Validation	Requires both certs for interoperability	Chains can be validated with both algos
New PKI Deployment	Required	Not Required (*)
Auth Protocol Changes (Cert Agility)	Required	Not Required (1 cert)
Offline / Indirect Authentications	Requires Both Certs Usage	No Changes (1 signature)
PKI Management and Audit Costs	Double (2 infrastructures)	No Changes (1 infrastructure)
PKI Deployment Costs	Increased (2 separate certs and chains)	No Changes (1 cert)
Code Development	More Complex Logic (2 certs)	No Changes (1 cert)

MIXED ENVIRONMENT AUTHENTICATIONS

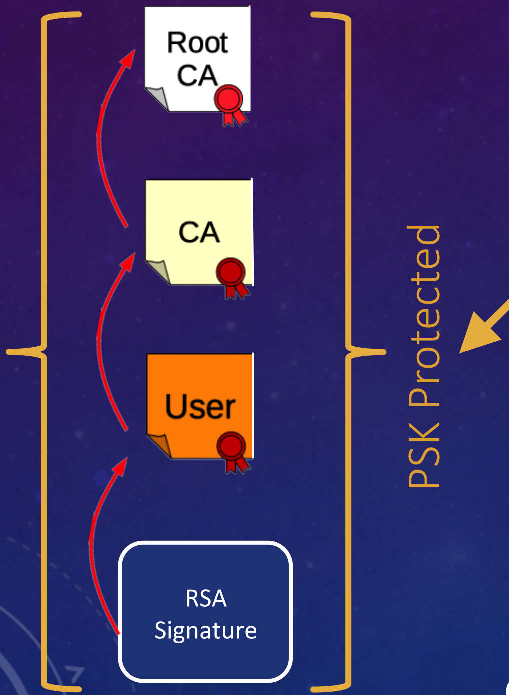


The Device Generates the authentication trace as usual by using its device private key

Classic Device

Quantum-Safe Device

MIXED ENVIRONMENT AUTHENTICATIONS



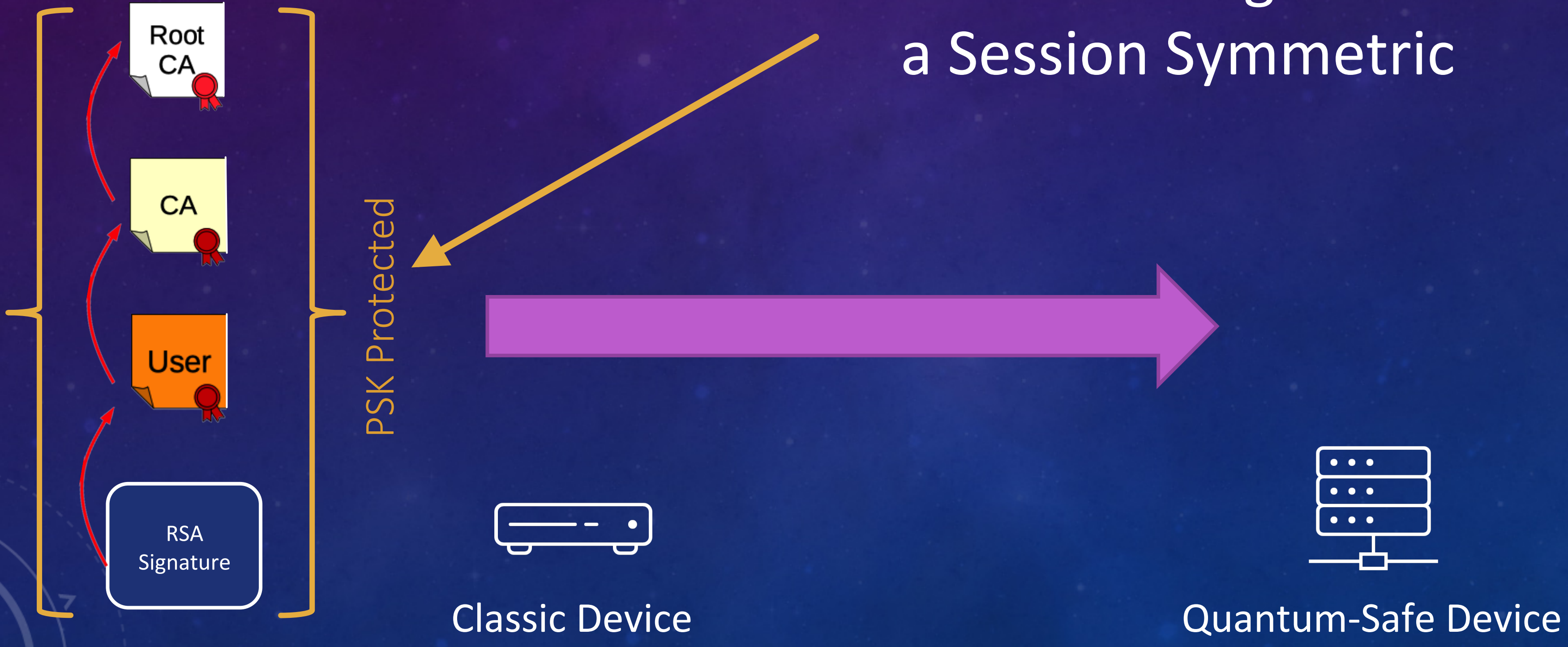
The Device can use the Session's Symmetric Key to protect the authentication

Classic Device

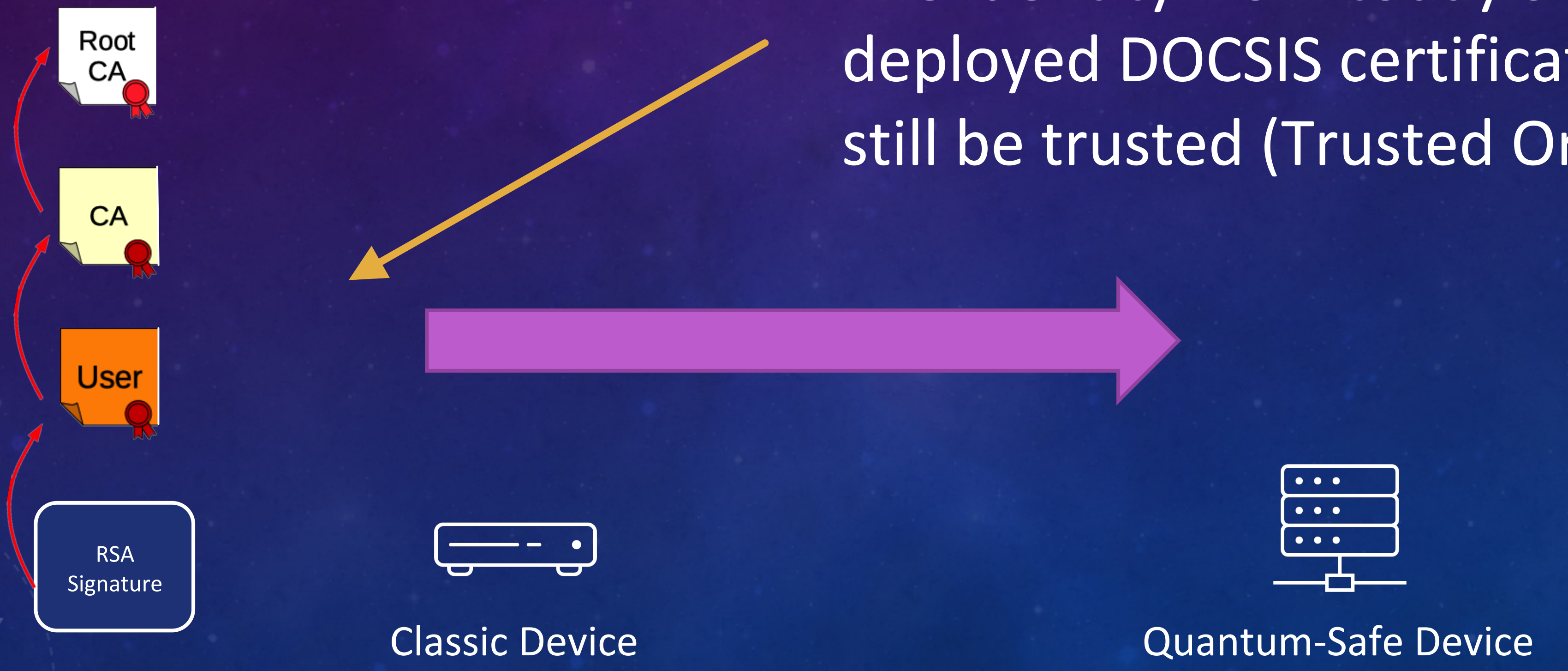
Quantum-Safe Device

MIXED ENVIRONMENT AUTHENTICATIONS

The Receiving Device First uses a Session Symmetric



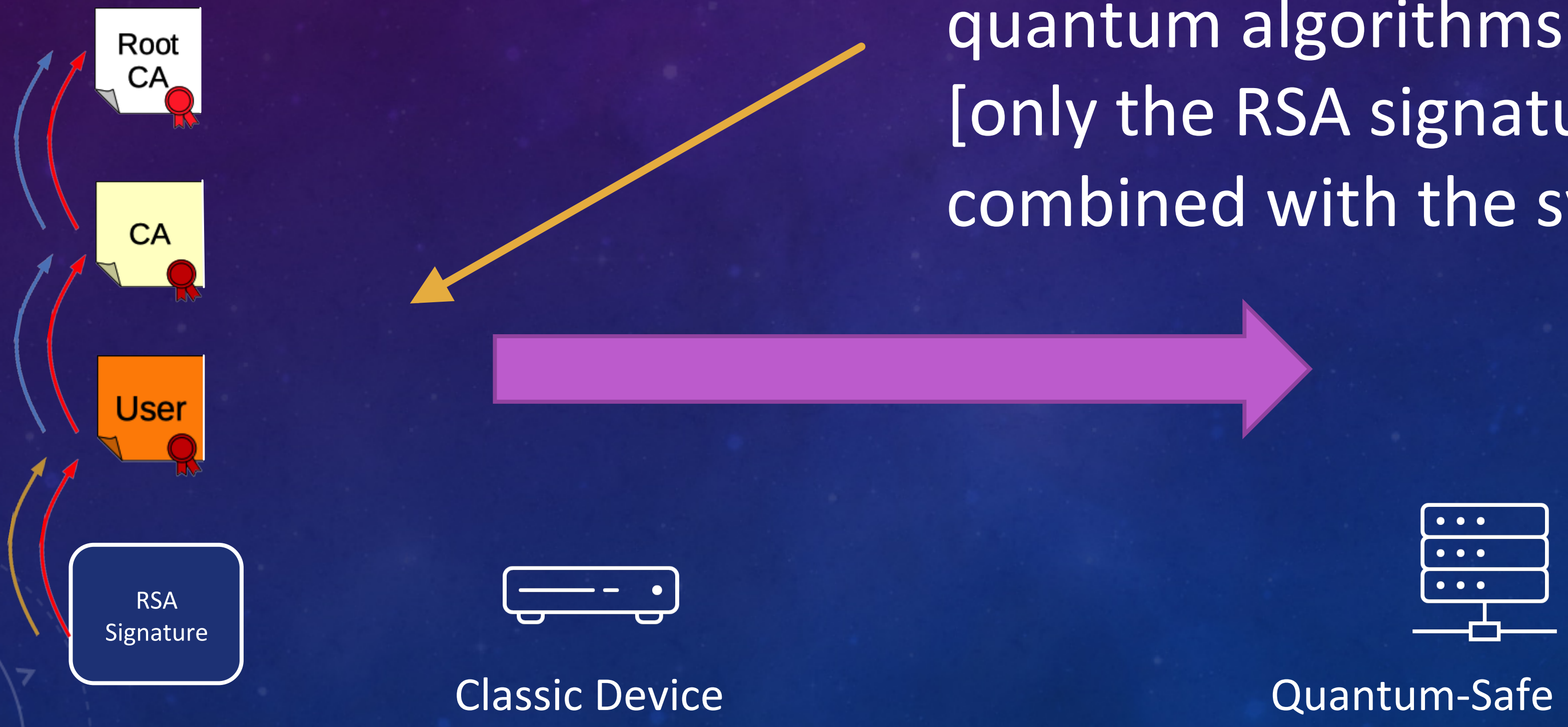
MIXED ENVIRONMENT AUTHENTICATIONS



The identity from today’s deployed DOCSIS certificates can still be trusted (Trusted Origin)

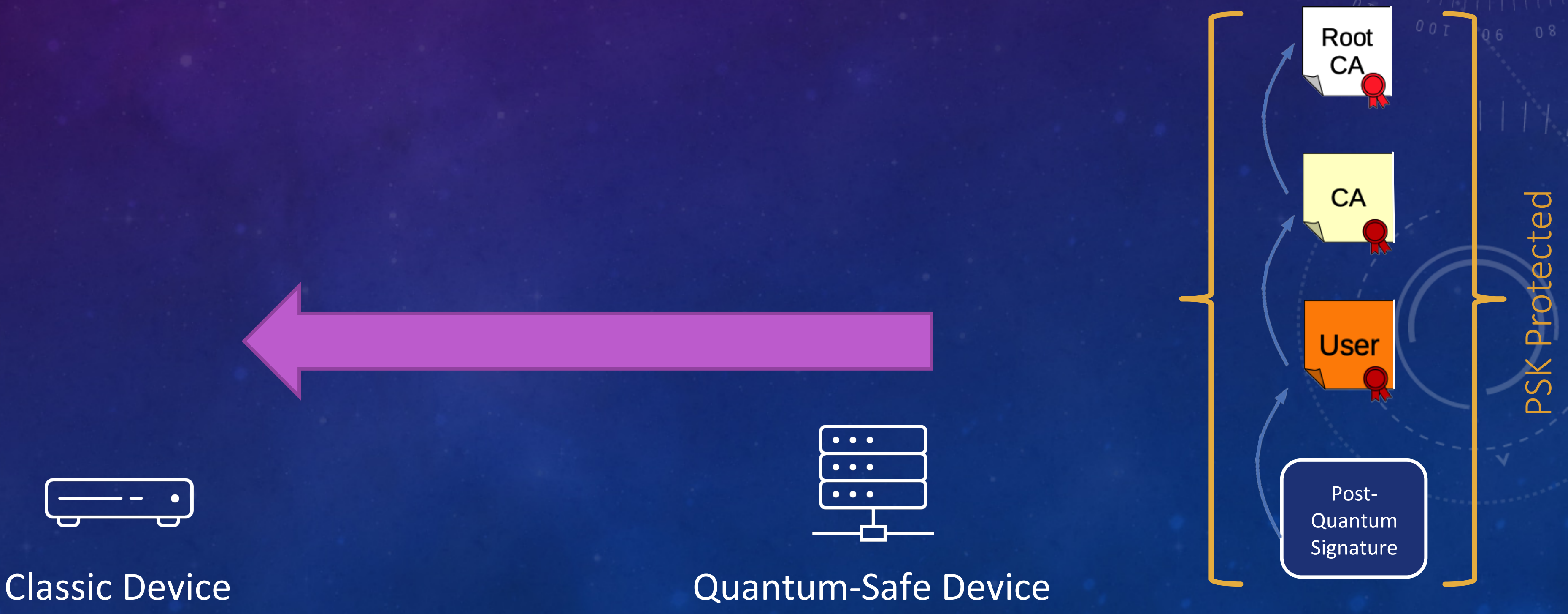
MIXED ENVIRONMENT AUTHENTICATIONS

When Composite-Crypto is used, the chain can be verified via post-quantum algorithms (if supported) [only the RSA signature must be combined with the symmetric key]



© Cable Television Laboratories, Inc. 2021.

MIXED ENVIRONMENT AUTHENTICATIONS



Root CA

CA

User

Post-Quantum Signature

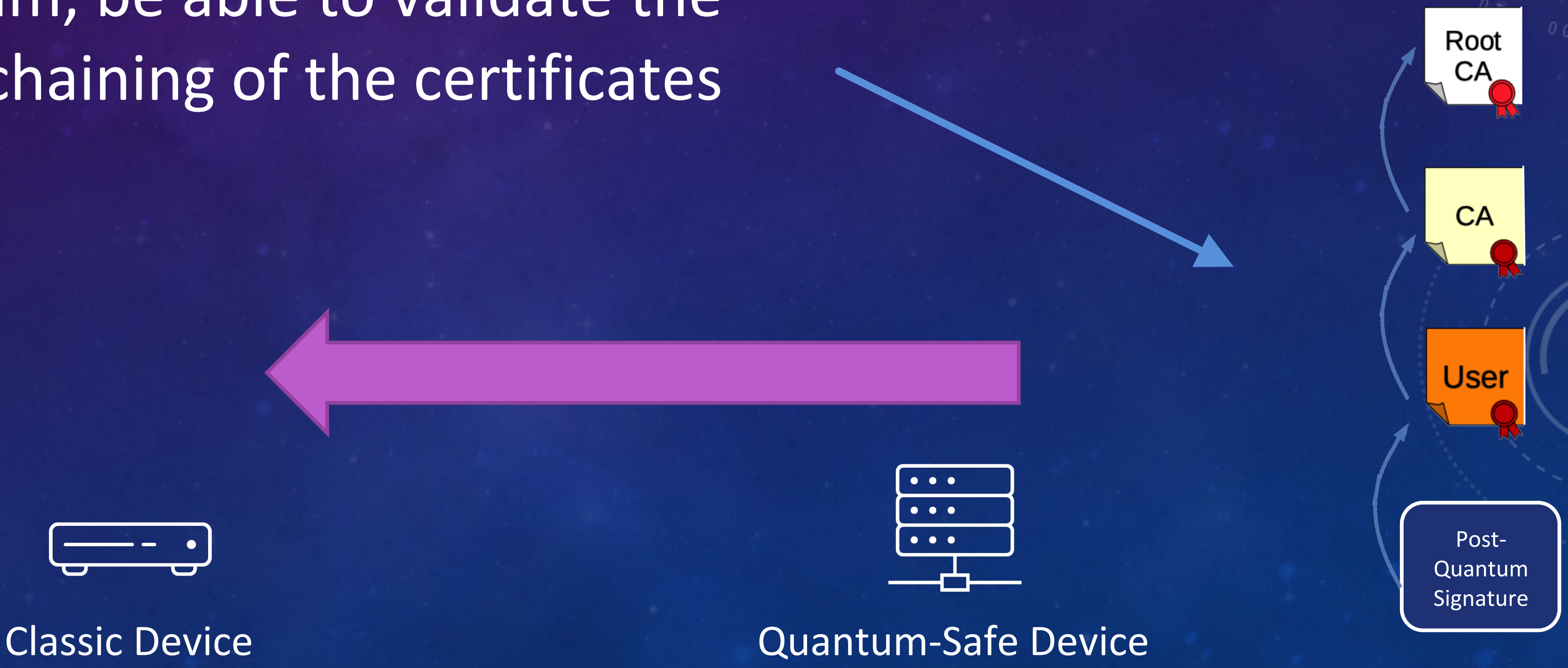
PSK Protected

Classic Device

Quantum-Safe Device

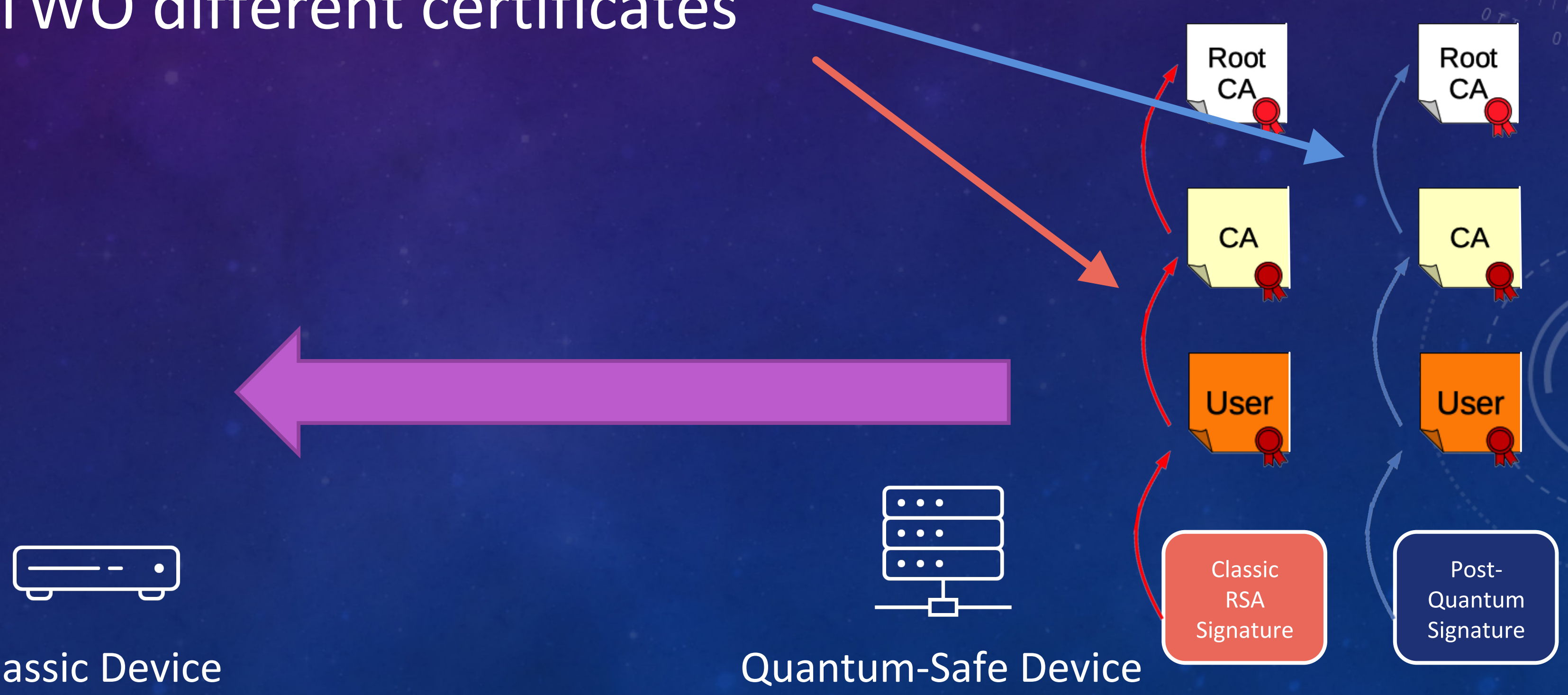
MIXED ENVIRONMENT AUTHENTICATIONS

The classic device MUST, at minimum, be able to validate the correct chaining of the certificates



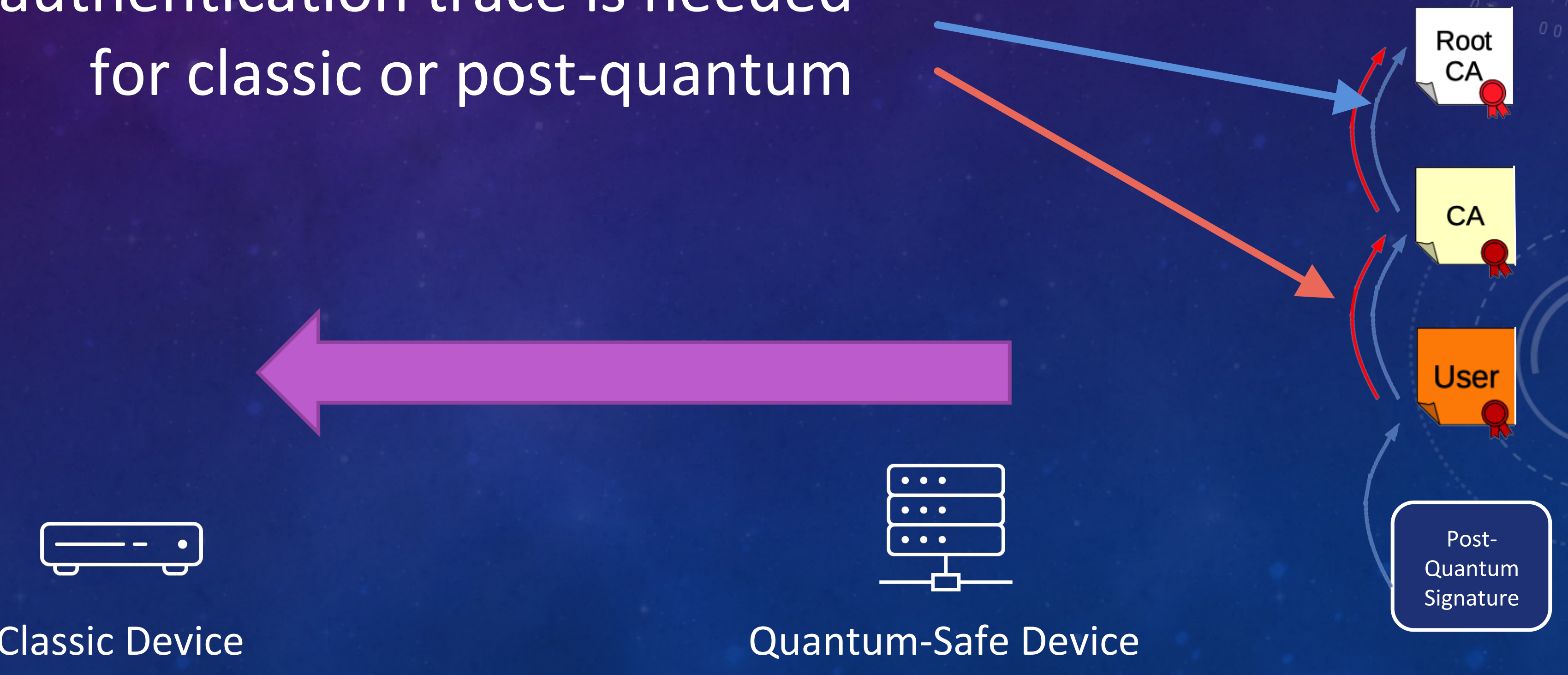
MIXED ENVIRONMENT AUTHENTICATIONS

When using the TWO certificates solution, devices might need TWO different certificates



MIXED ENVIRONMENT AUTHENTICATIONS

When using Composite Crypto, only one authentication trace is needed for classic or post-quantum



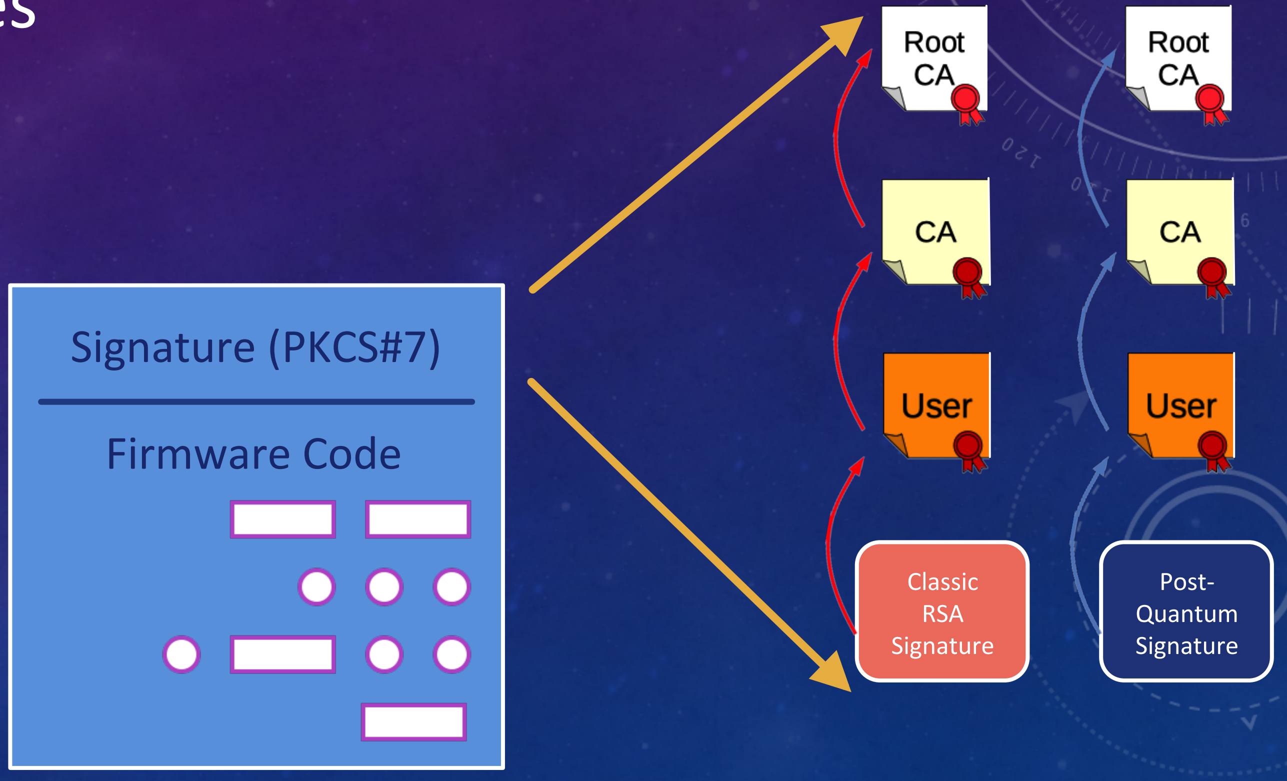
© Cable Television Laboratories, Inc. 2021.

MIXED ENVIRONMENT AUTHENTICATIONS

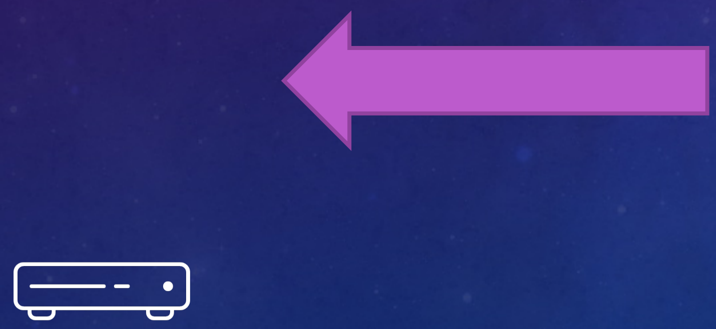
In a mixed environment, the use of Composite Crypto can help indirect (or proxied) authentications like in the case of OCSP, Firmware Upgrades, Secure Time Delivery, etc.

FIRMWARE UPGRADES

When single-algorithm certificates are used, multiple signatures and certificates must be used by the manufacturer (and/or co-signer)



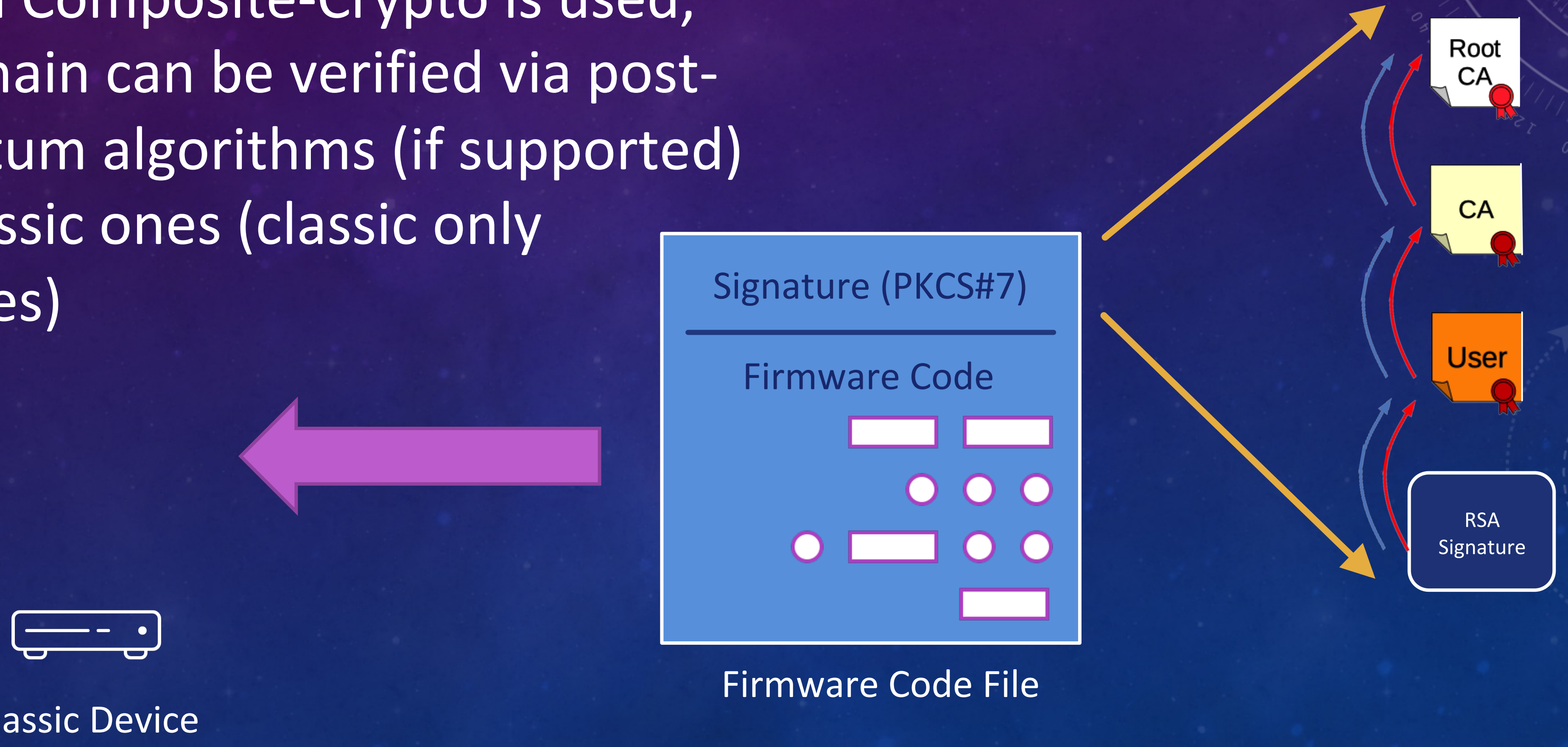
Firmware Code File



Classic Device

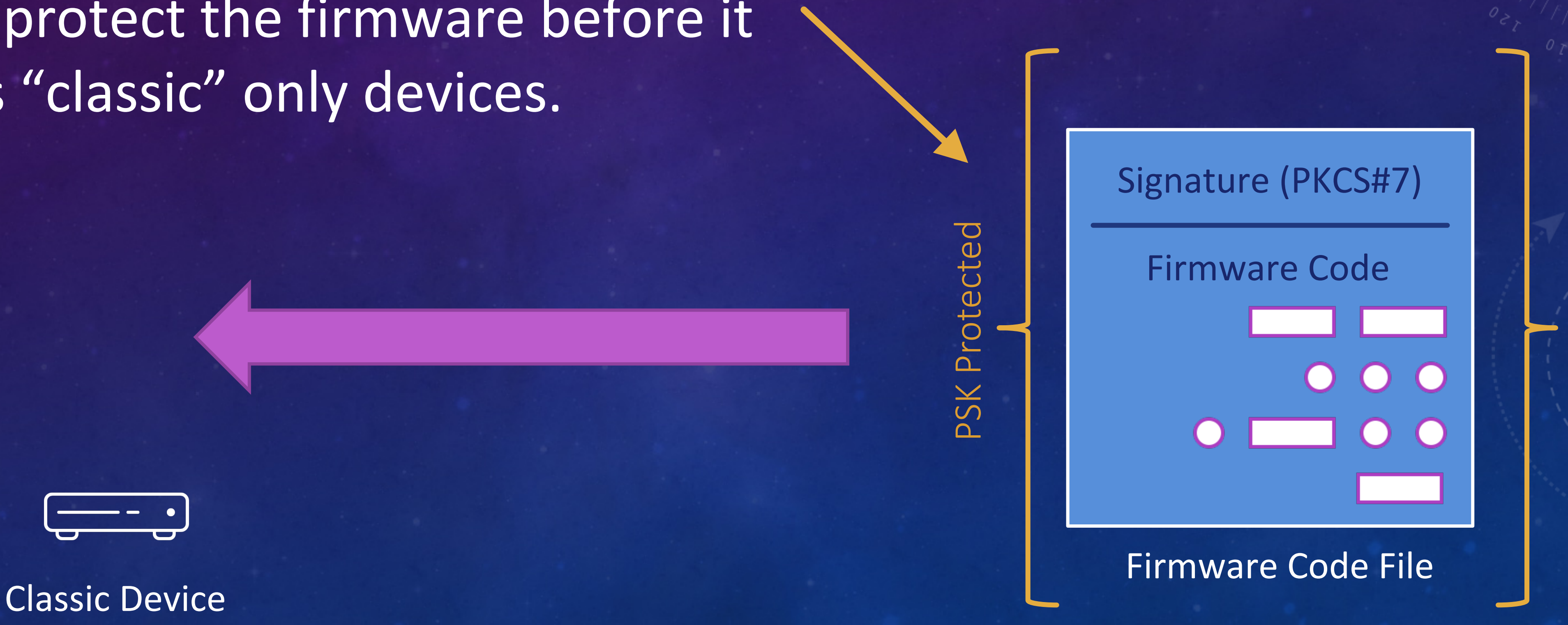
FIRMWARE UPGRADES

When Composite-Crypto is used, the chain can be verified via post-quantum algorithms (if supported) or classic ones (classic only devices)



FIRMWARE UPGRADES

Similar approaches can be used to further protect the firmware before it reaches “classic” only devices.



PROTECTING ROOT AND INTERMEDIATES…

- Composite Crypto can provide protection for the higher levels in the PKI hierarchy
- Factoring the Root RSA key (or an Intermediate CA key) is not sufficient to compromise the entire infrastructure (unless all keys are compromised)
- The two-certificate approach does not provide a mechanism to extend the protection from the new algorithm to the "old" infrastructure/identities easily

DOCSIS 4.0 NETWORK SECURITY & QUANTUM

CONSIDERATIONS ON QUANTUM-SAFE TECHNOLOGIES AND DOCSIS® NETWORKS

Security & Privacy Technologies

Massimiliano ("Max") Pala <m.pala@cablelabs.com>
Director, PKI Architectures