KYRIO™

CBRS Public Key Infrastructure and Certificate Authorities All You Need to Know

Wireless Innovation Forum Webinar
February 7, 2019

Your Speaker

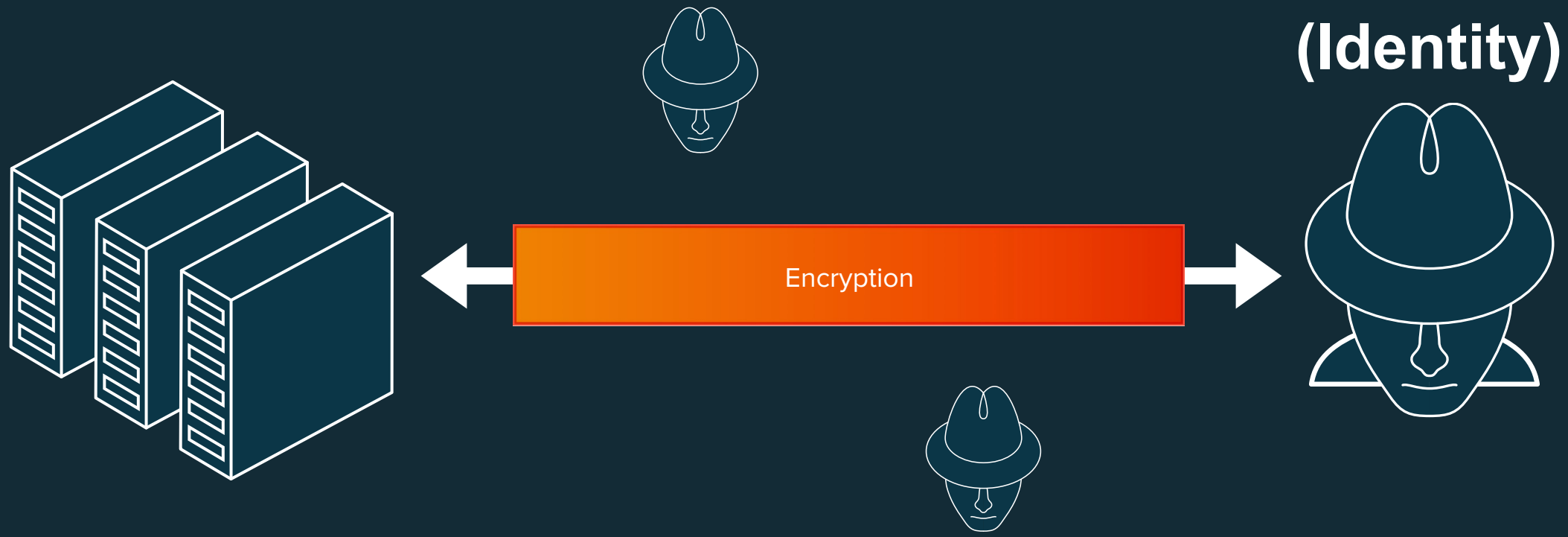
Ronald Ih
Dir. Business Development
Kyrio Security Solutions
r.ih@kyrio.com

Agenda

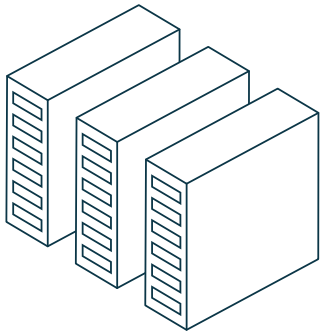
- PKI Overview
- Why PKI?
- How do I get started?
- Timeline for production certs
- How to get support

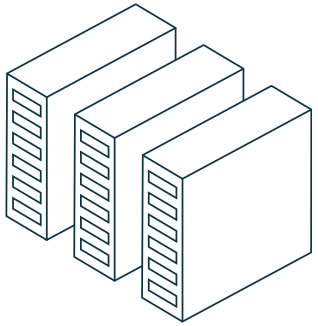
What Constitutes *SECURITY* ?

Authentication
(Identity)

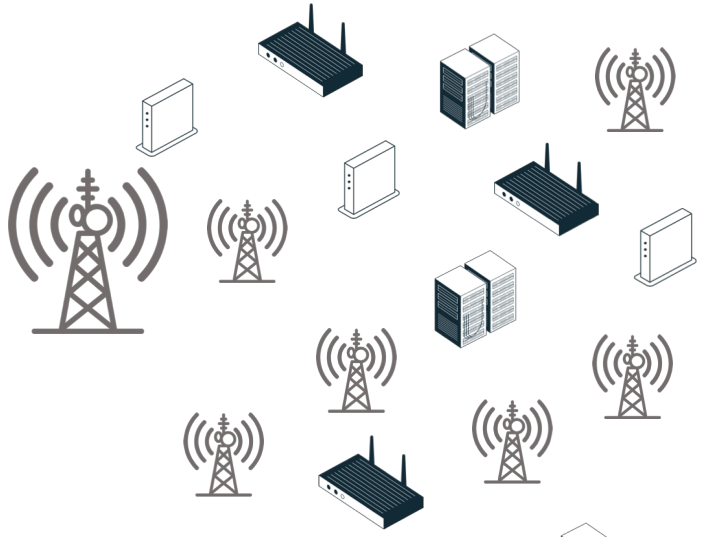


How do you give a device an identity?



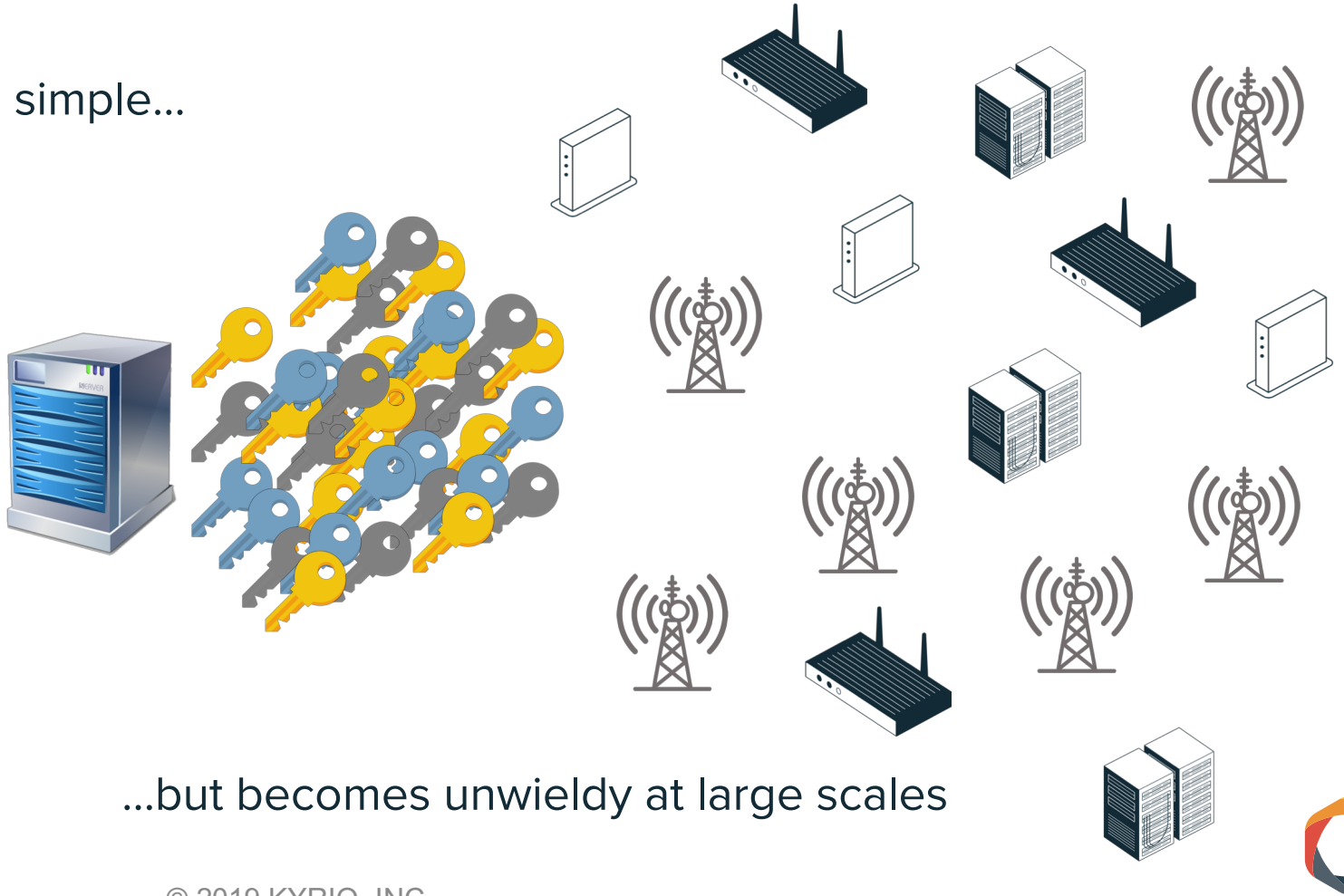


Username: user1
Password: ********



How do you give a device an identity?

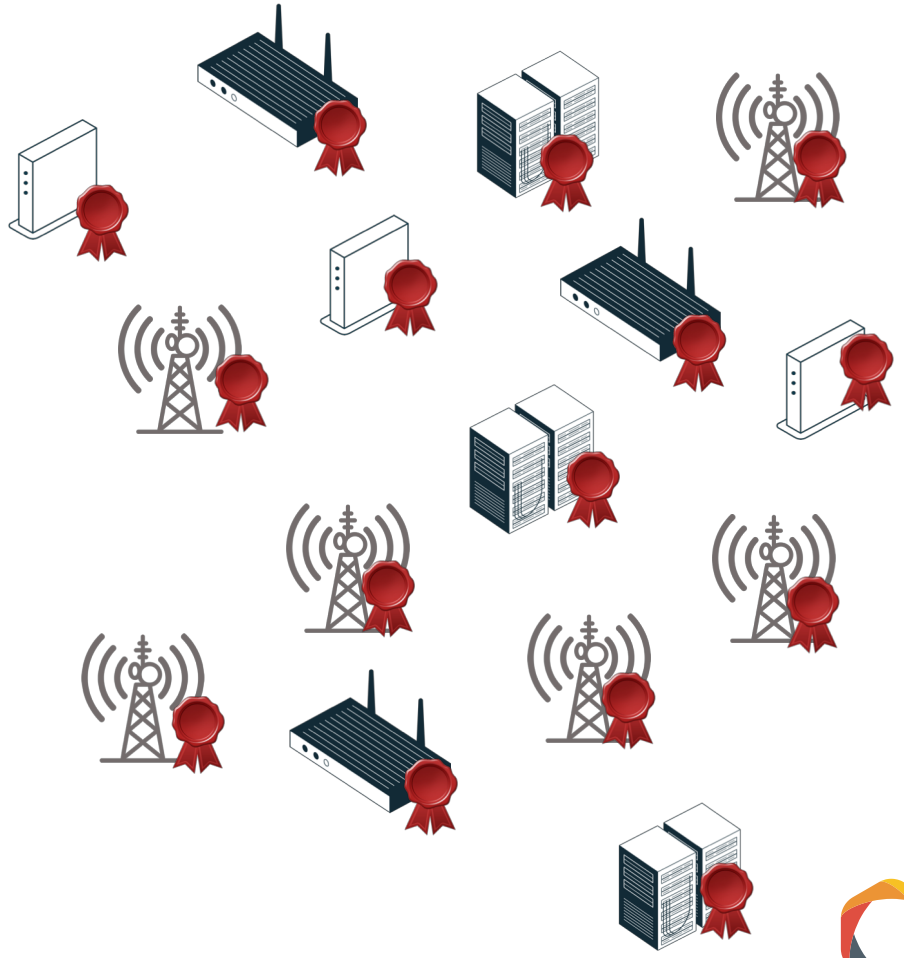
Symmetric is simple…



…but becomes unwieldy at large scales

Asymmetric/PKI Identity is Scalable

- Asymmetric is highly scalable
- Each certificate is uniquely identifiable
- Device identity is difficult to spoof
- Individual or groups of certificates can be revoked

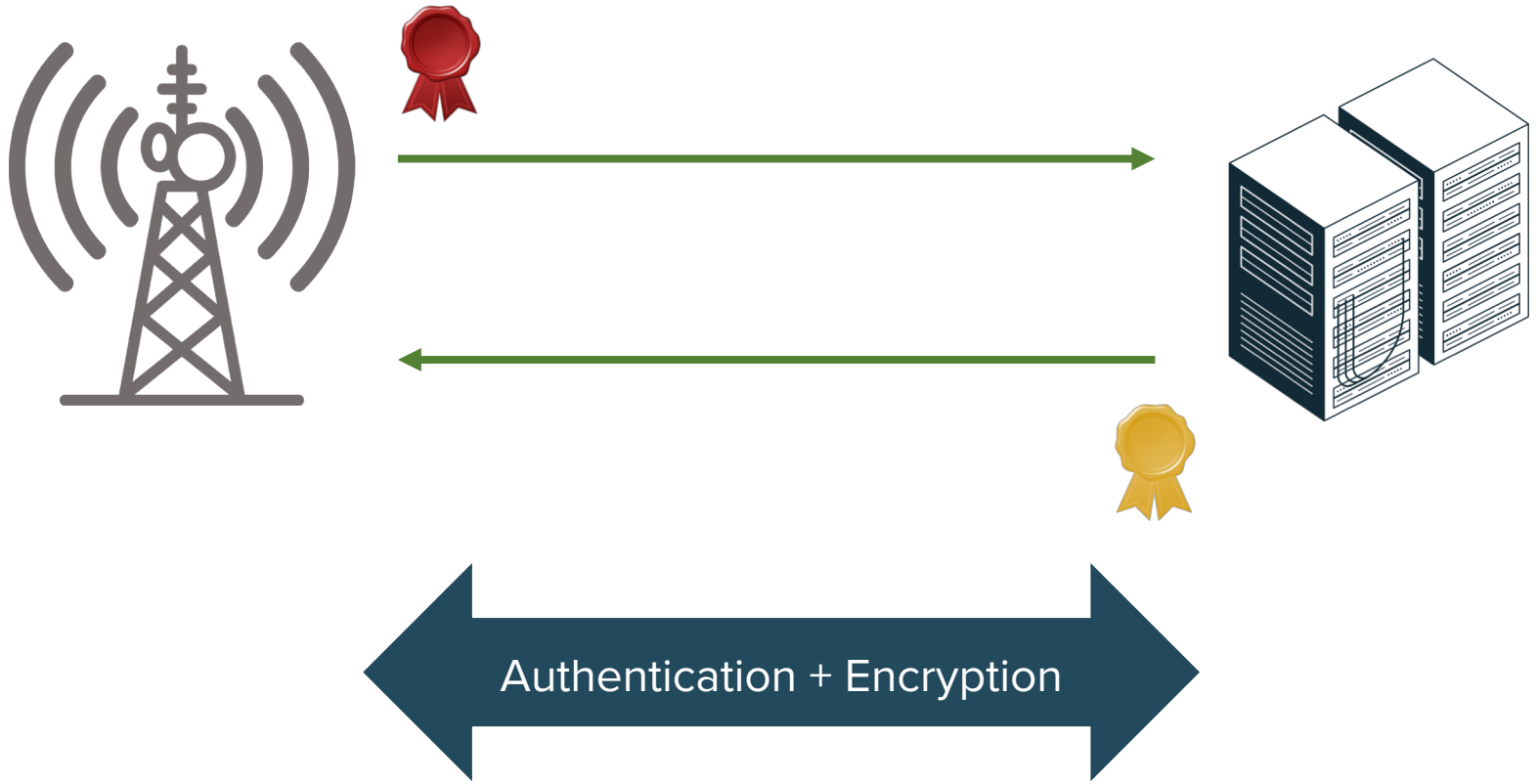


Digital Certificates as Tamper-Resistant Identities

Establishing Verifiable Identities

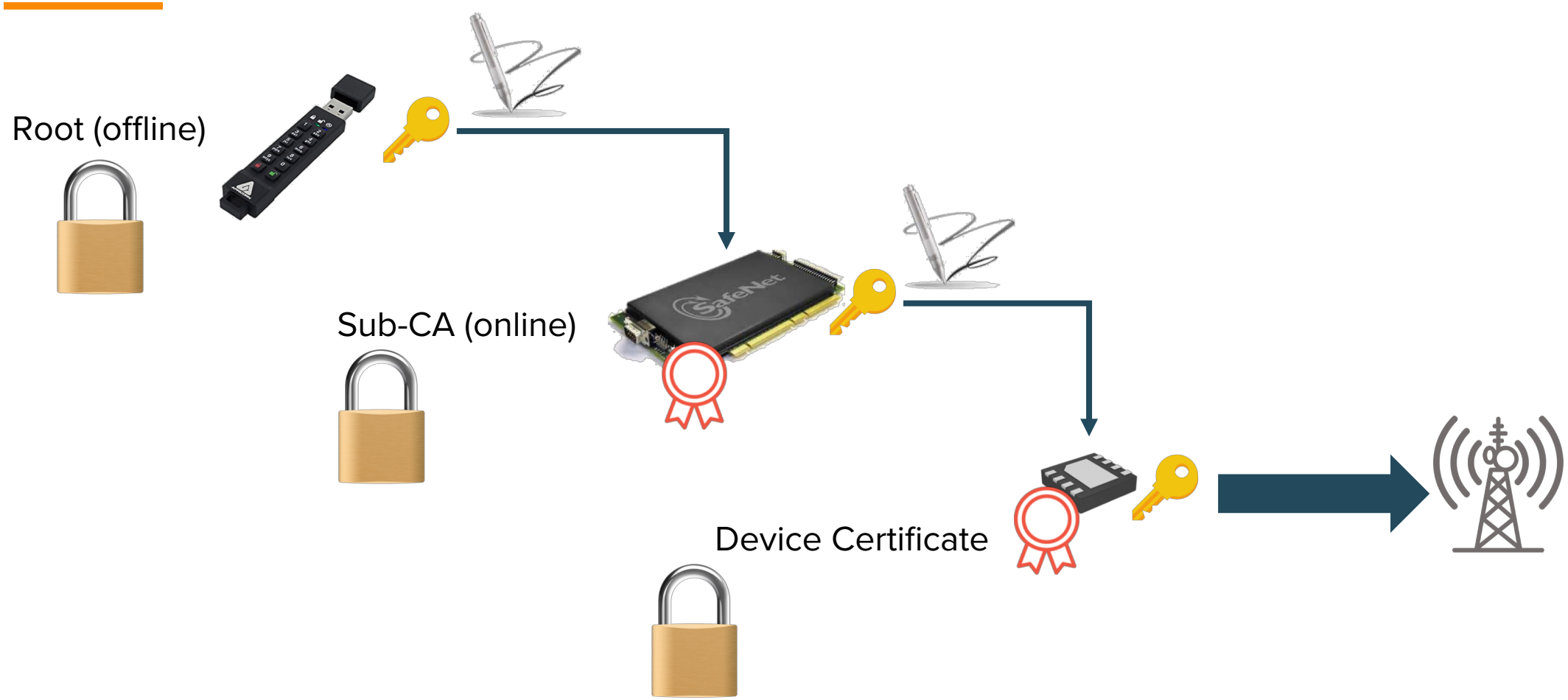
Controlled Issuing Authority			**Controlled Source**
Credential			
Authenticity Verification	Holograms	Digital Signature	**Credential is Real and Valid**
Ownership Verification	Picture	Private Key	**Credential Belongs to Bearer**

PKI Functional Summary – Mutual Authentication

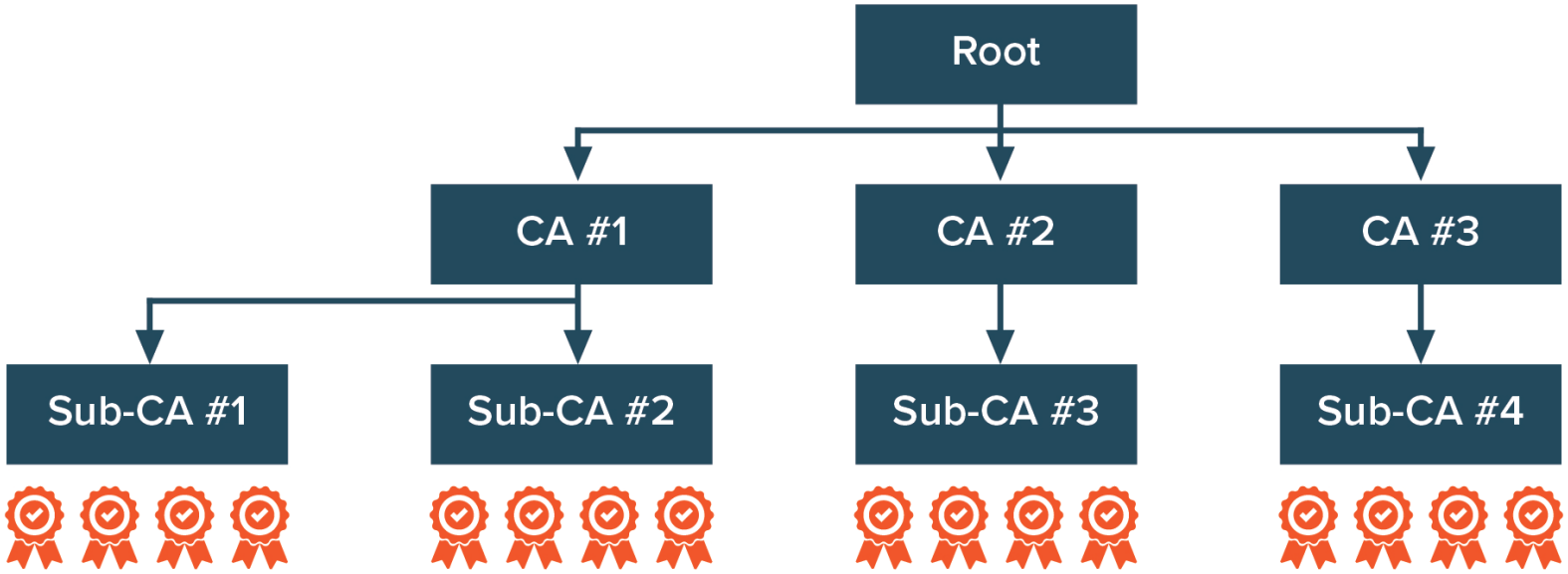


PKI/Credential Management Certificate Authorities as a Controlled Source of Certificates

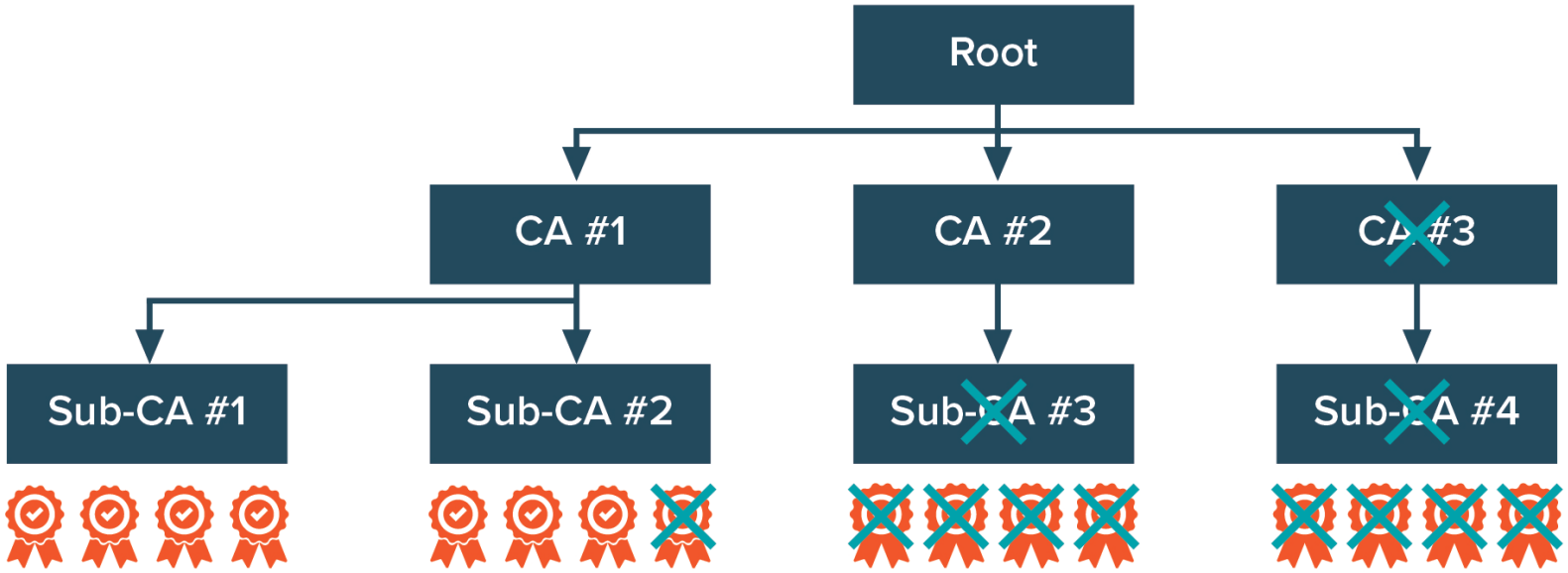
PKI Functional Summary – Trust Chain



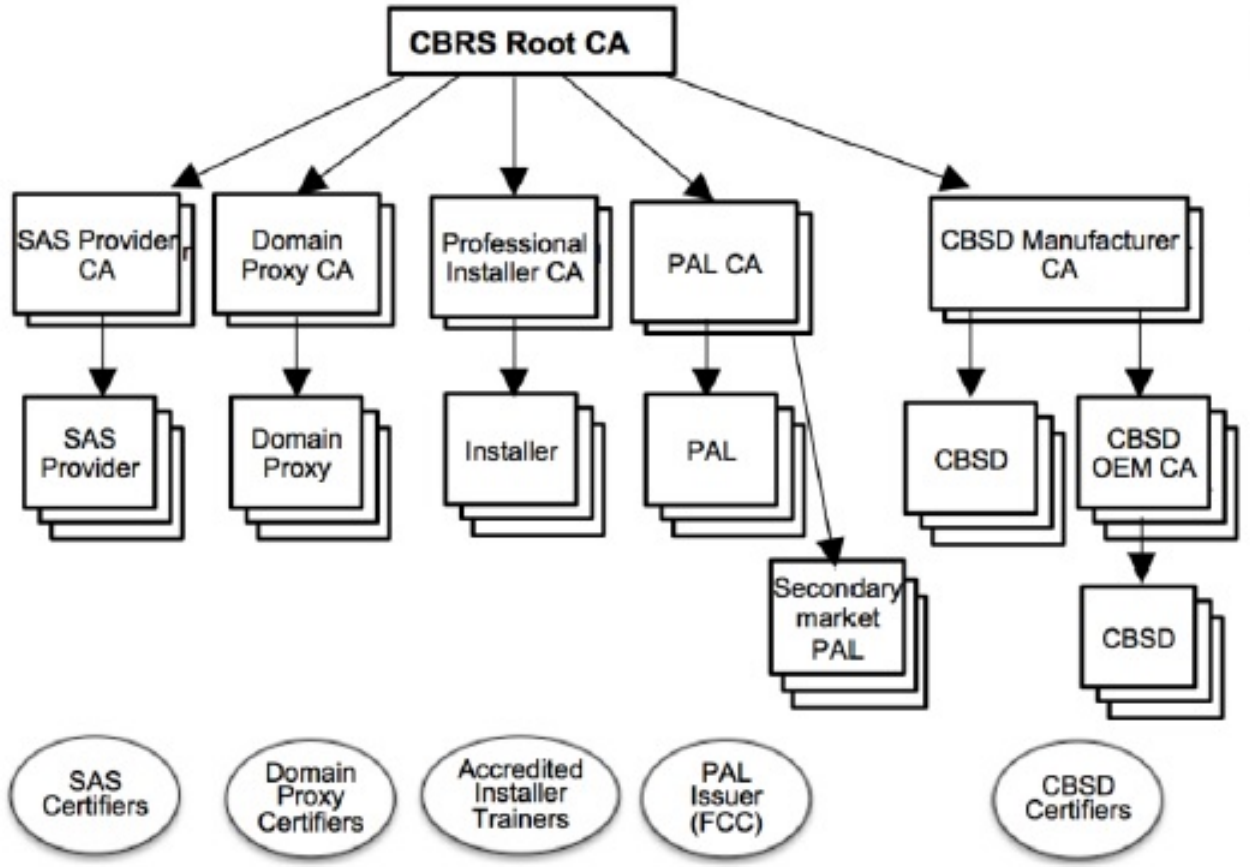
PKI Architecture



PKI Architecture - Revocation

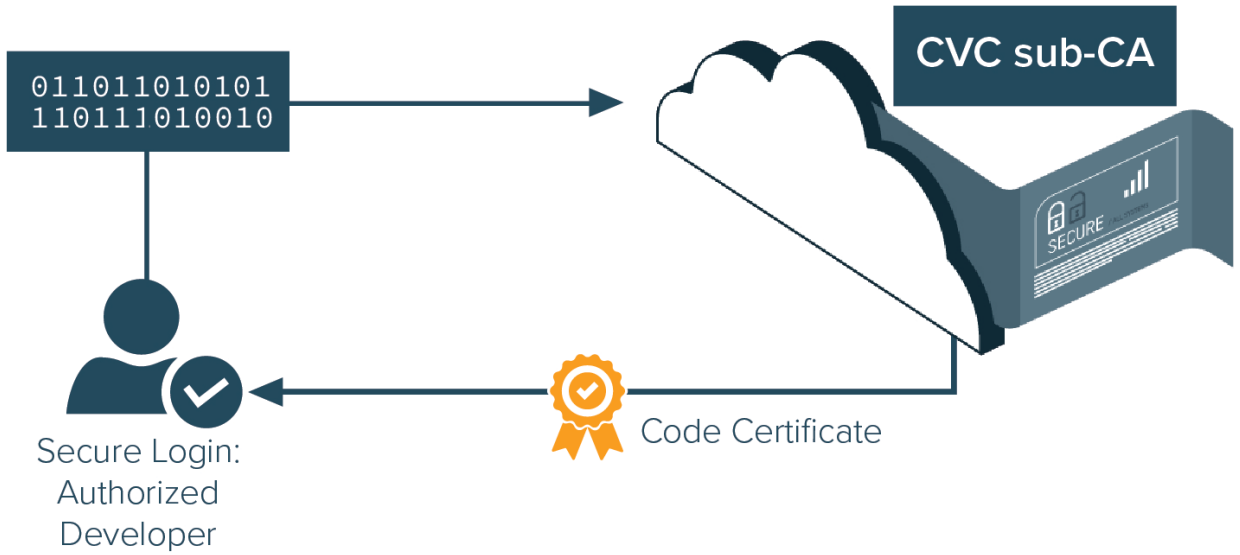


CBRS PKI Hierarchy



PKI Architecture – Code Signing

Use Certificates to Protect Your Firmware/Code

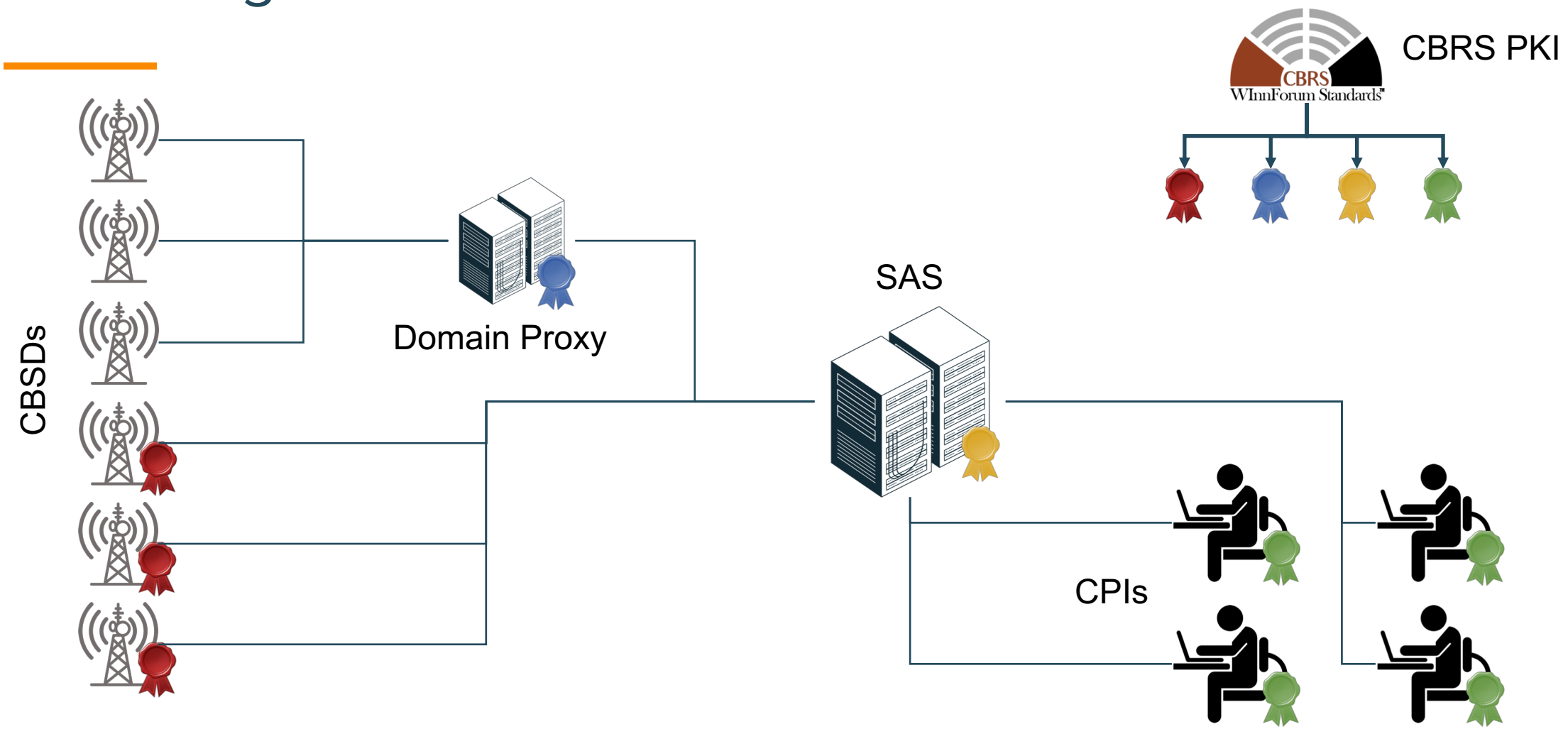


Certificate Authorities - Function

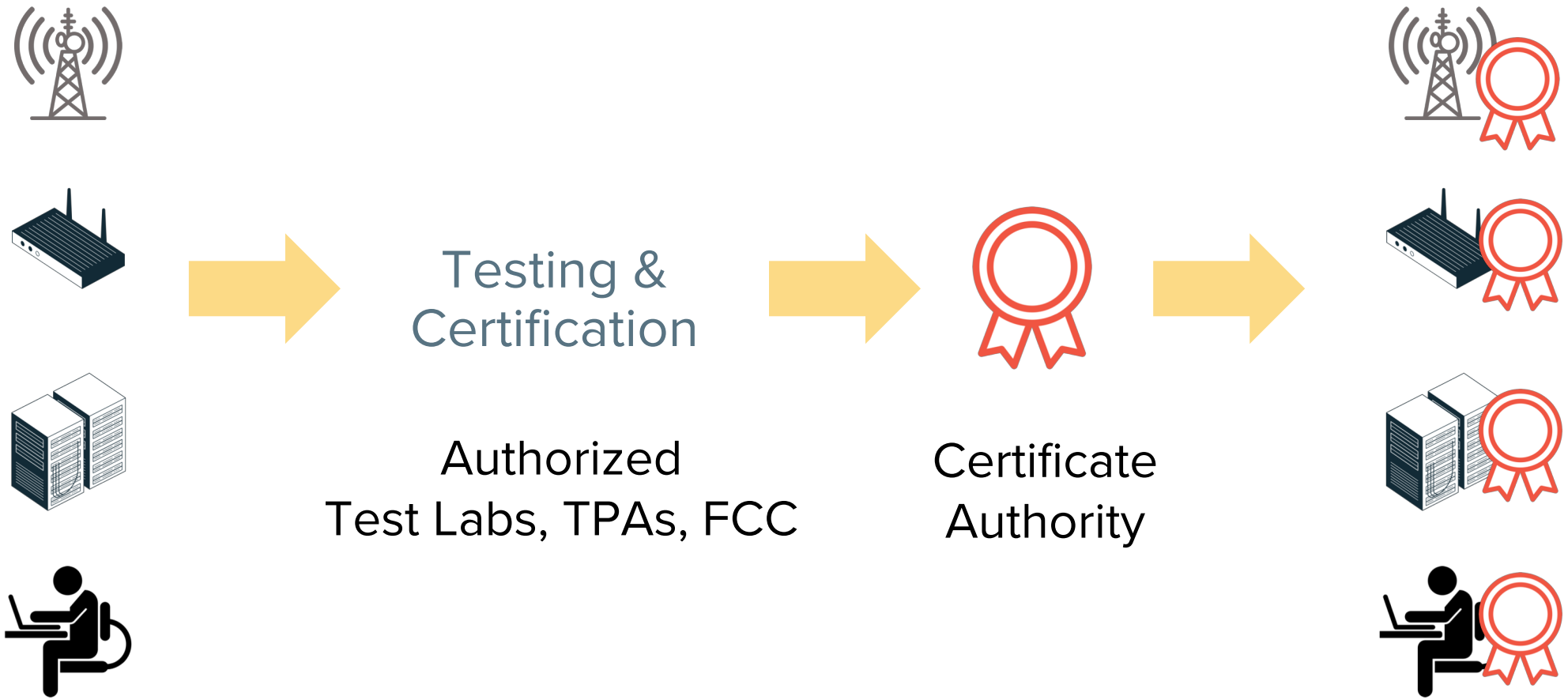
- Help Define Ecosystem Certificate Policy (CP)
- Architect, construct and operate the PKI according to the CP and Security Specifications
- Enforce procedural and physical security requirements around controlling certificate issuance
- Acts on behalf of the owners/BoD of the ecosystem
- Audit/WebTrust and contractual requirements limit CA activity to what is defined by the *current* fully approved specification

Using Certificates for Ecosystem Integrity

Providing Access Control for CBRS

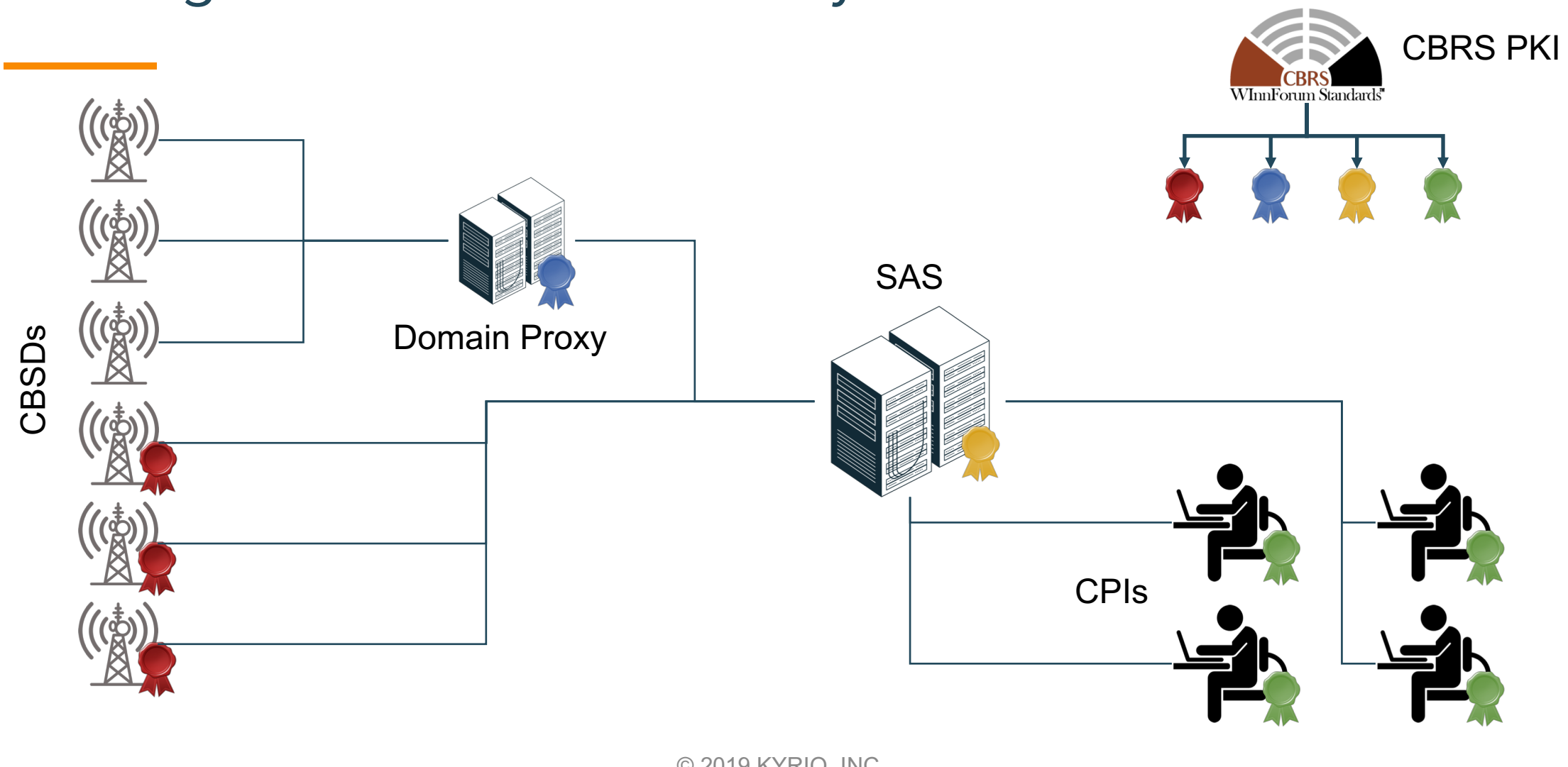


Maintaining Security and Spec Compliance



Getting Started with CBRS Certificates

Making CBRS a Trusted Ecosystem



CBRS Certificates

- Who needs certificates?
  - All entities connecting to a SAS must have a digital certificate to access the network
  - EnodeB (CBSD), High power CPEs, Domain Proxy Servers, SAS and CPIs
  - Devices behind a DP that will never directly connect to a SAS might not need a certificate but do require a means of authentication between the CBSD and DP
- Types of Certificates
  - SAS – 15 month validity
  - Domain Proxy – 15 month validity
  - CPI – 5 years
  - CBSD – 10 years
  - PAL – TBD

  - CBSD OEM sub-CA – 30 years

Timeline for Production Certificates

- Production certificates available mid to late February
  - V1.1.2 CP approved 1/29/2019
  - FCC approvals of SAS systems
- Corporate managed CRA (Certificate Requesting Accounts) require ~2-3 days for authentication/verification and processing
- CPI Accounts (Individuals) can be authorized users under TPA corporate accounts; ~48 hours

Get Started with a CA Secure Portal

- SAS, CBSD, DP Corporate CRA Accounts
  - Contact Kyrio to sign a DCSA – Digital Certificate Subscriber Agreement
  - Kyrio will validate company and key contact info for each corporate account
- TPA – CPI Training Program Administrator
  - Create Corporate Account through DCSA as above
  - TPA can operate their own sub-CA (compliance to CP required), or outsource to a CA
- CPIs
  - Personal identity will be validated by TPA
  - CPIs will be an authorized user under each TPA Main account after successfully completing their training course

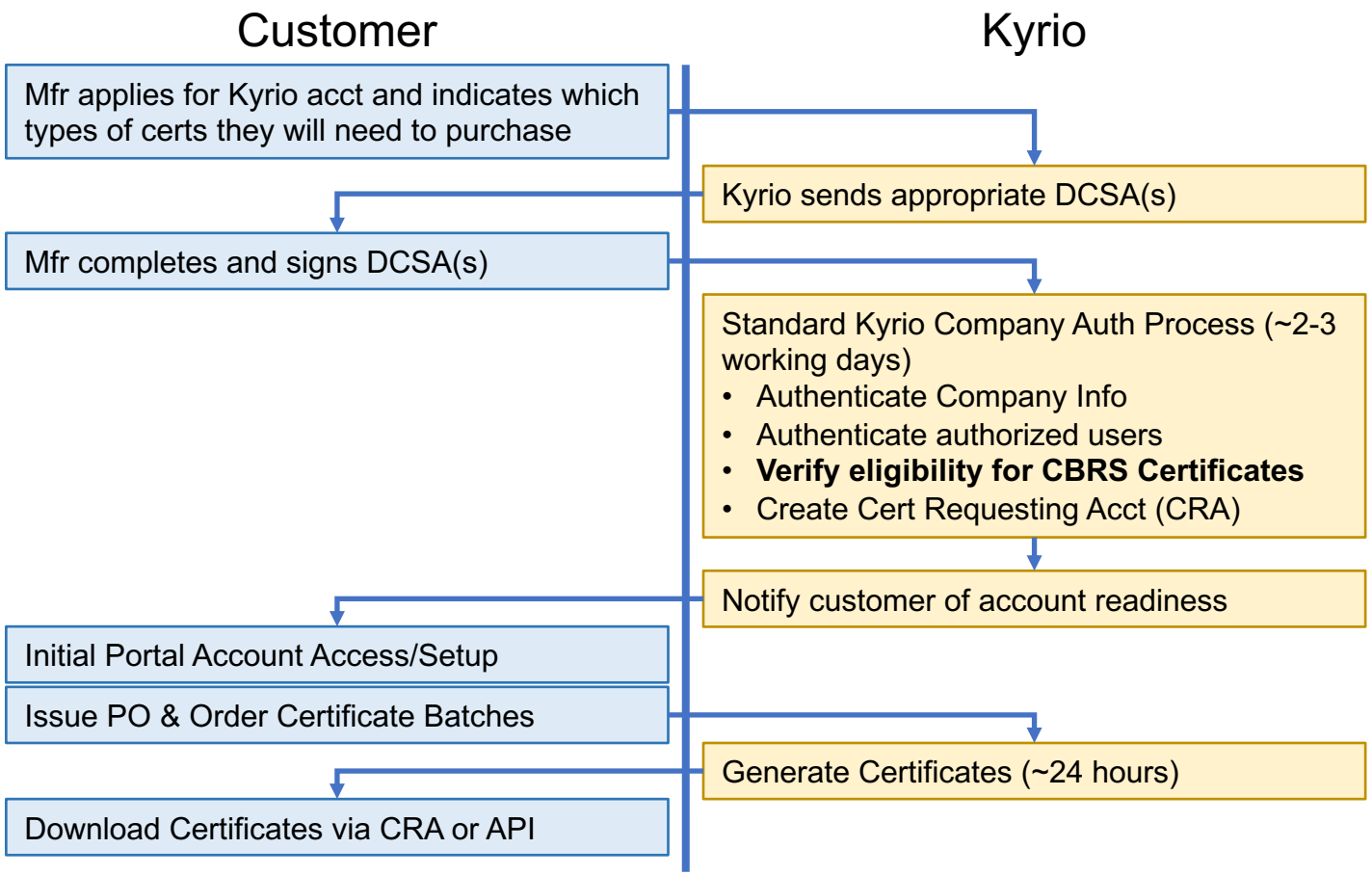
Certificate Issuance for TPA, SAS, CBSD, DP vendors

- **2-3 working day account setup processing time**
  - Digital Certificate Subscriber Agreement (DCSA)
  - Company verification
  - Authorized users/account admin authentication
  - Account setup
- Company Information Needed
  - **Designated Account admins**
  - **Authorized users**
  - **Legal, technical contacts**
  - Corporate Address/Location
  - Country/State of incorporation

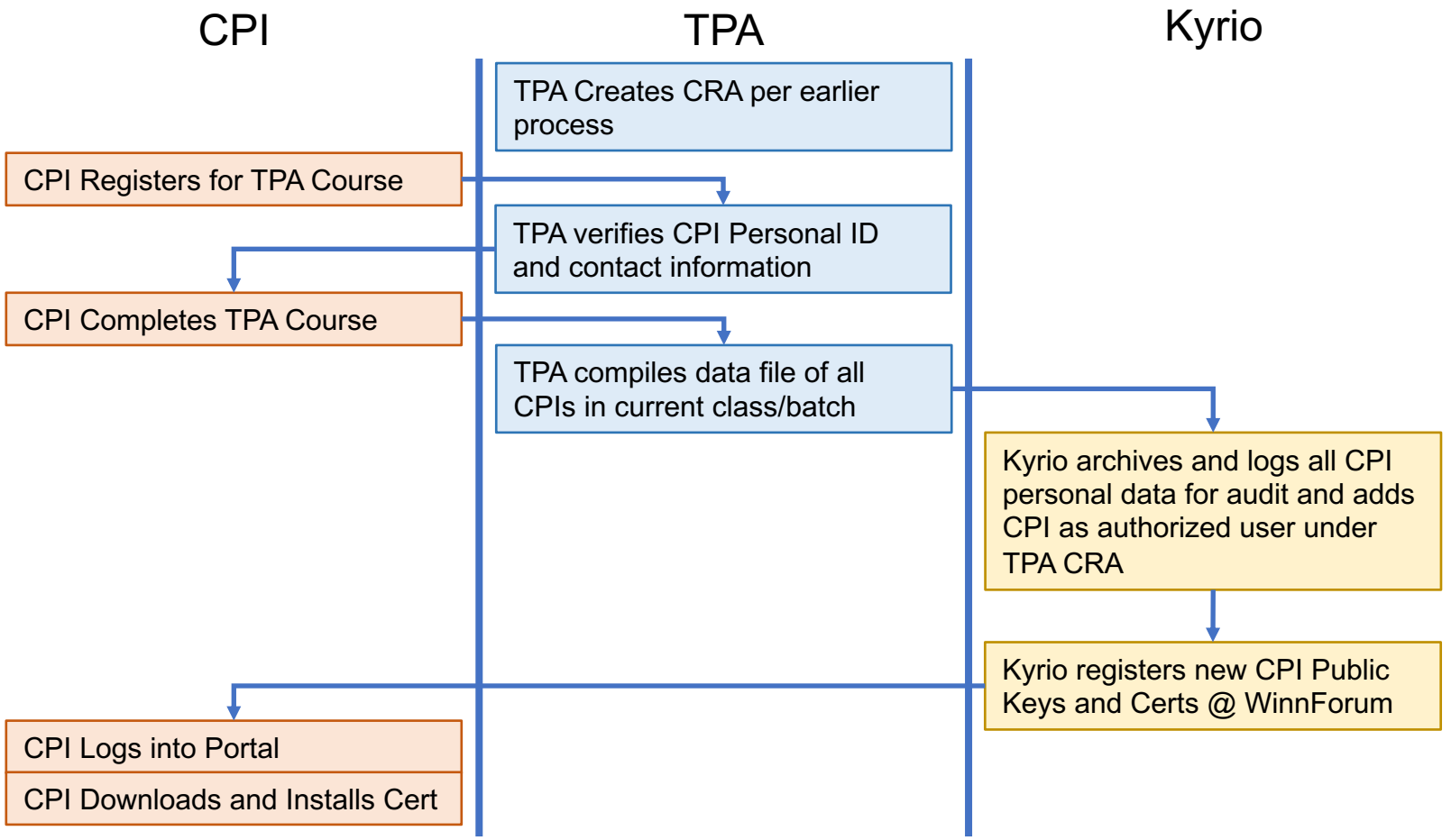
Certificate Purchase

- Certificates can be thought of as “virtual components”
  - Each is unique and individually generated and signed within the PKI Trust chain
  - Certificates are inventoried like physical goods, but not taxed as such
- Certificates are purchased in blocks
  - Certificate per-unit pricing varies with volume very similar to hardware
  - Larger blocks have lower per-certificate prices
  - Block purchases are added to an account owner’s inventory
- Downloaded certificates are decremented from owner’s inventory

TPAs, CBSD, SAS and DP Mfr CRA Process Flow



Certificate Issuance for CPIs



Work with a CBRS CA

- Kyrio
  - Sales - Ron Ih, Director of Bus Dev, r.ih@kyrio.com
  - Operations - pkiops@kyrio.com
  - Website - https://www.kyrio.com/security-services
- Insta
  - https://www.instadefsec.fi/cbrs
- Digicert
  - https://www.digicert.com

Questions?

KYRIO™

THANK YOU

We **CONNECT** People, Places and Things at the Speed of Business