

COMMSCOPE®



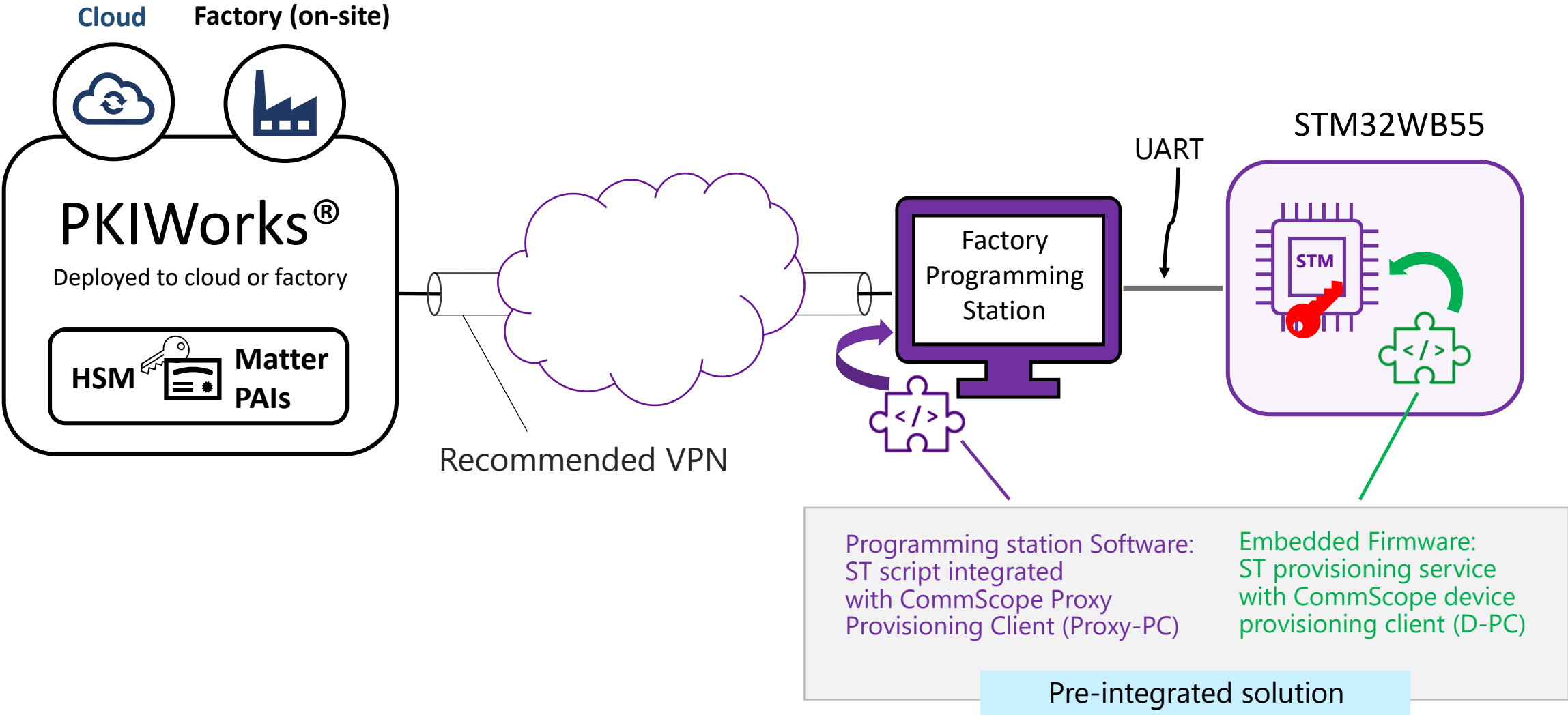
How to Provision STM32WB55 with Matter DAC



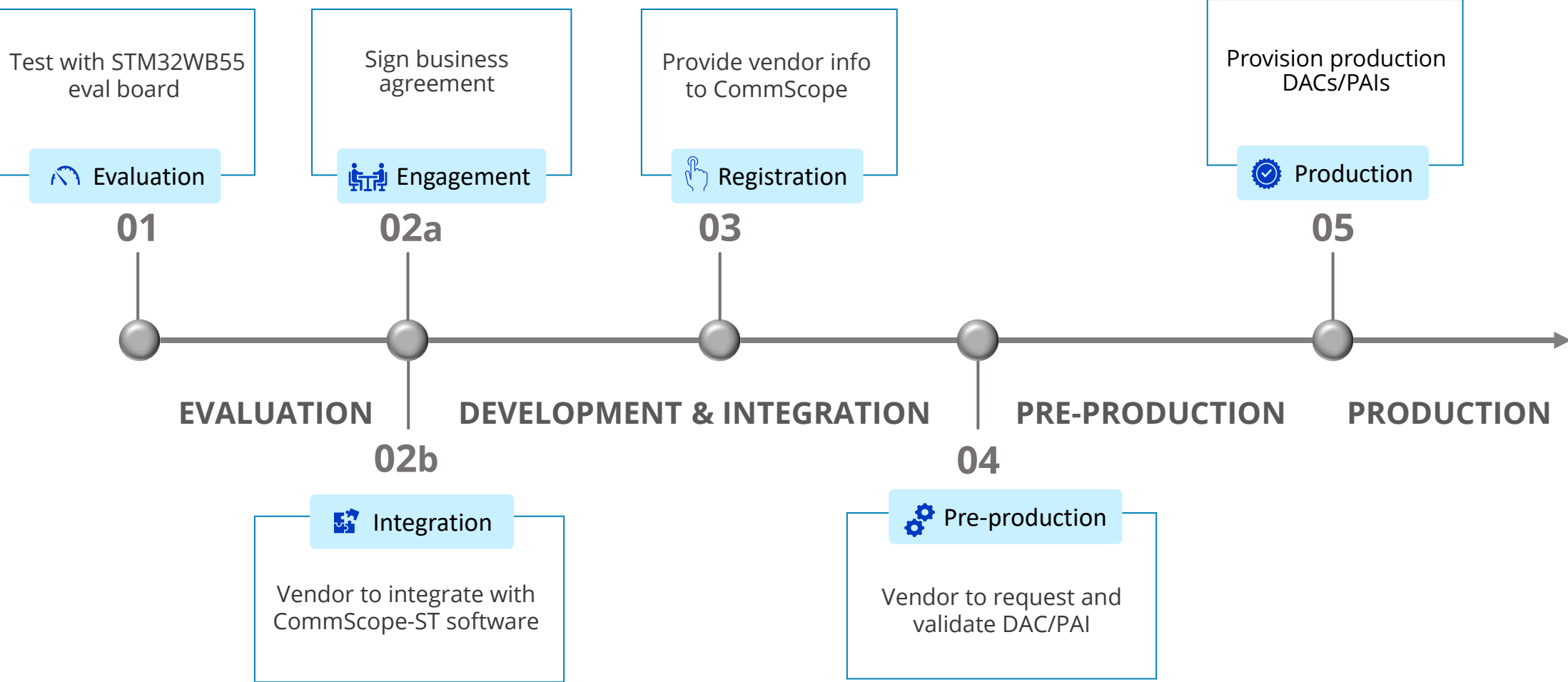
Joint Effort Makes
Matter Device Attestation Credential Provisioning

Simple **Streamlined** **Secure**

Pre-integrated Solution for Factory Configuration



Step-by-Step: Working with CommScope and ST



Easy Integration & Quick Turn-around

Working with CommScope: DAC Provisioning Journey



Evaluation

- Obtain CommScope-ST pre-integrated device provisioning client and programming station proxy client solution
- Test DAC provisioning on targeted STM32WB55 device evaluation board with CommScope test DACs/PAI



Integration

- Vendor to integrate device client & programming station proxy client with their own software



Business Engagement

- Sign business agreement



Vendor & Product Registration

- Vendor registration via CommScope intake portal (VID, PID, PAI(s), information, Product parameters etc.)
- CommScope to vet VID/PID information & to create vendor/product specific PAI(s)



Pre-Production Setup

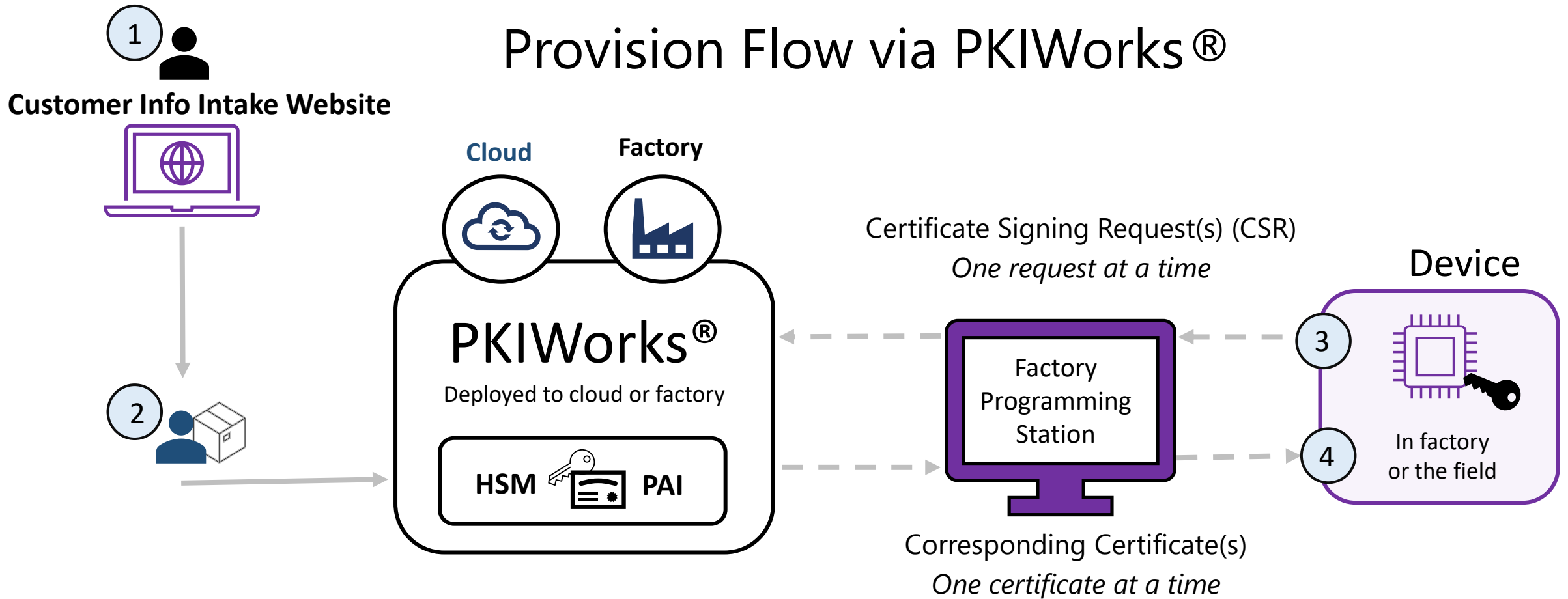
- CommScope to release vendor-specific production parameters for customers/products
- Vendors to use production parameters to request DACs/PAI from PKIWorks® production server



Production

- DAC/PAI provisioning in production run with PKIWorks® production server
- Inventory mgmt.: alert customer to place additional DAC orders to maintain balance when the stock is low.

Provision Flow via PKIWorks®



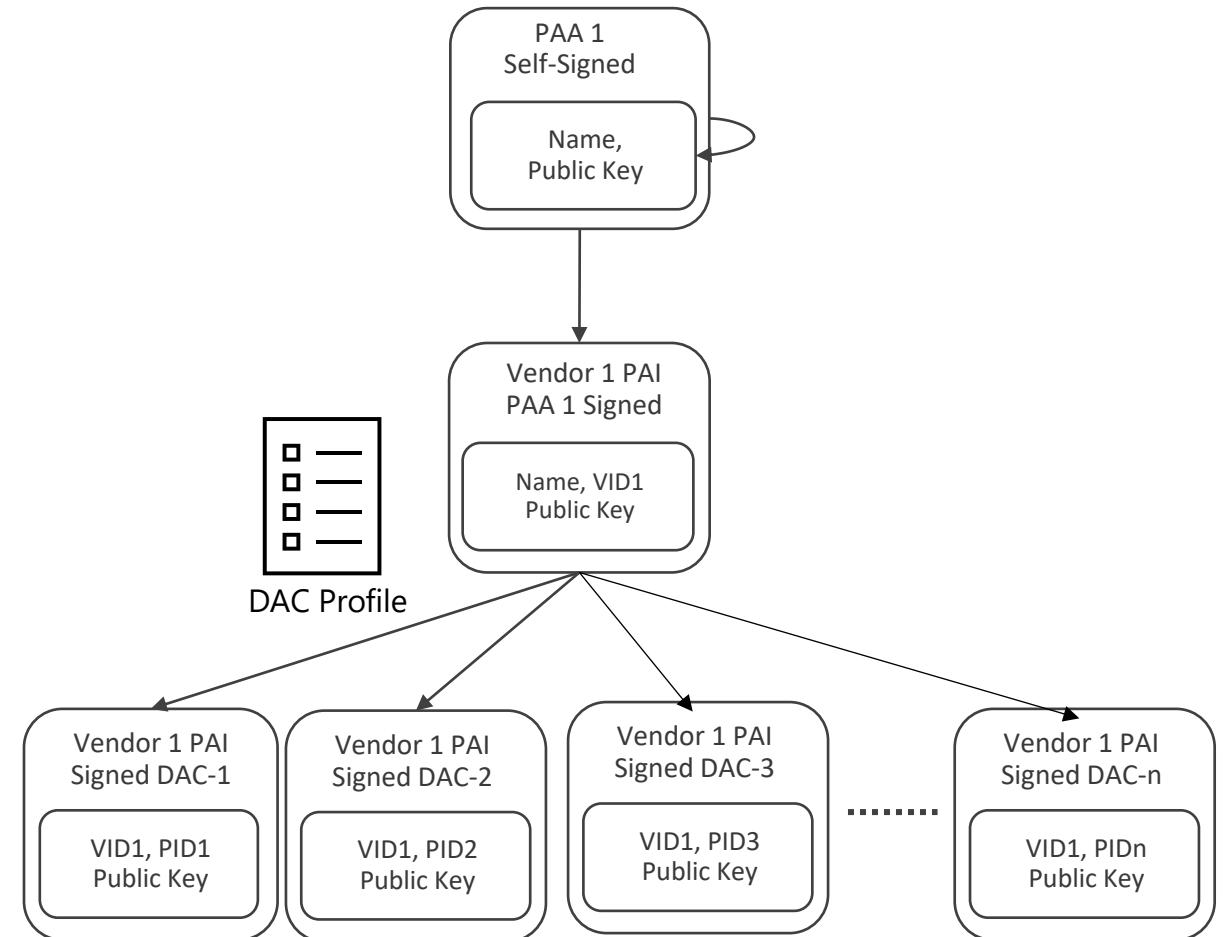
1. A vendor or distributor (on behalf of a vendor) enters required information into the PKIWorks® Starter website.
2. CommScope creates customer specific PAI(s) and deploys it to PKIWorks®.
3. The device/STM32WB55 generates key pair and sends request to PKIWorks®.
4. The device receives the matching certificate, save back to STM32WB55.

Vendor & Product Registration with CommScope

A customer or distributor on behalf of customer to submit parameters to CommScope intake portal

<https://starter.pkiworks.com>

- VID → to be used in PAI
- PID → to be used to create DAC certificate profiles
- Other administrative information
 - Company name
 - Contact person information



Configuration: CommScope-ST Pre-integrated Solution



Programming station



STM32WB55 device

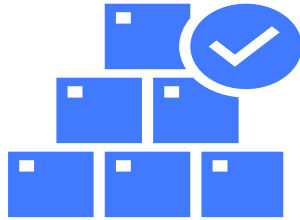


ST Device Programming Script integrated with CommScope Proxy Provisioning Client (Proxy-PC)



ST embedded provisioning firmware with CommScope device provisioning client (D-PC)

Main Features and Functions



PKIWorks®

Validate CSRs against DAC profile, preventing unauthorized requests

Reject duplicated public keys in CSRs, enhancing security to ensure uniqueness and minimizing error to save cost

Generate DAC certificates



Programming Station Client

Offer additional protection over the factory programming station

Enhance security with additional authentication for device CSRs

Provide assurance to authenticate customer VID and PIDs, reducing the risk of mismatched DACs



Device Provisioning Client

Generate DAC key pairs inside STM32WB55 for enhanced security

Safely store private keys inside STM32WB55, preventing exposure

Generate CSR within the chip

Validate received certificates to match with original key pairs, minimizing errors

CommScope CSA Matter PKI Service Values



Pre-integrated with STM32WB55, fast tracking device maker's own development



Designed for a factory-deployable workflow to minimize production errors, ensuring cost-effectiveness



Best security practice; DAC private keys never exposed outside devices



CSA approved CommScope PAA with customizable PAIs to align with customers' Matter product roadmap



Free test DACs available to facilitate end-to-end testing, chained to CSA Testnet



Additional product related security services available (like code signing for secure boot or OTA provisioning)

ST & CommScope Resources and Support

Evaluation Phase Instructions:

- STM32WB55 eval. board: <https://estore.st.com/en/stm32wb5mm-dk-cpn.html>
- Request sample software for the eval board via matter@pkiworks.com
- Watch video at: <https://tinyurl.com/43nx55wm>

Development Integration:

- CommScope support for integration via matter@pkiworks.com
- **ST support contact: to be provided later**

Pre-production Run (PPR) and Production Run (PR):

- Register VID and PID with CommScope at <https://starter.pkiworks.com>
- PPR and PR using vendor specific production DACs and PAI(s)
- Worldwide 24x7 support at sdnoc@commscope.com or call +1 858.404.2465

For more information: <https://www.pki-center.com/partner/STMicroelectronics>