Presentation Will Begin Shortly

4:00

MATTER

FEB 15TH	The Final Step Matters: Scaling Secure Products into Volume Production
MAR 21ST	Matter Technology and Market Updates and Q&A with the Connectivity Standard Alliance
APR 25TH	Future Proofing your Matter Products
MAY 30TH	Matter Specification Updates and Enhanced Support for Low Power Sensor Devices

Welcome

The Final Step Matters

Scaling secure products into volume production. Featuring Matter

Introduction

- **Matt Maupin**
  - Matt is a Senior Marketing Manager at Silicon Labs where he leads a Marketing team for IoT wireless hardware and software. Matt joined Silicon Labs in 2012 and has been responsible for defining and launching wireless ICs and modules, including Wi-Fi®, Bluetooth®, Zigbee, Z-Wave and proprietary solutions.

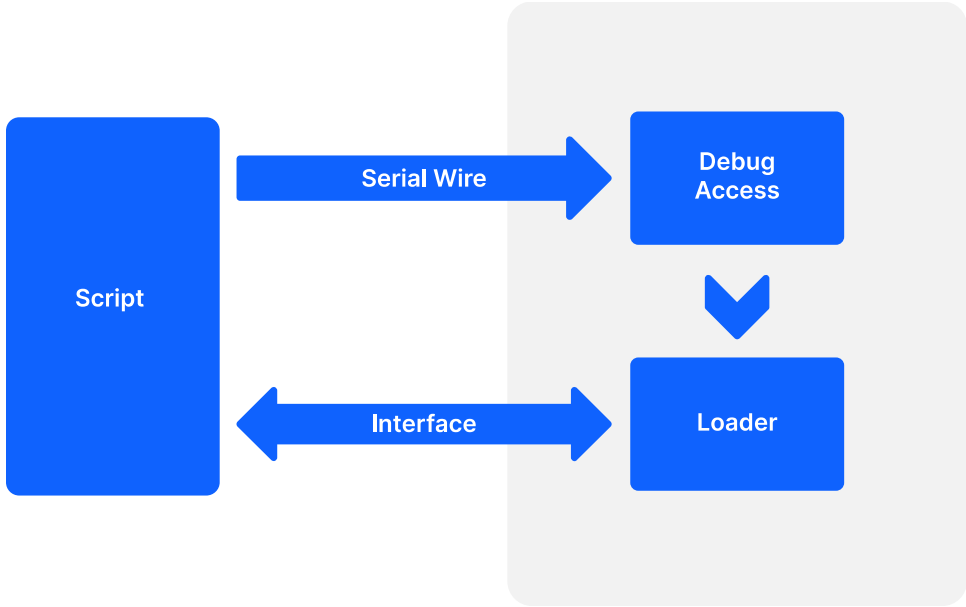
- **Josh Norem**
  - Josh is a Senior Staff Engineer who's been with Silicon Labs for over fifteen years. He has been in Product Test Engineering, Applications and is now in our Security Systems group where he helps to define our security capabilities for our wireless products.

The World, it is a' Changing

- **Manufacturing used to be simple**
  - All items were identical
  - Maybe they had serial numbers
- **Now, each copy of a product is unique**
- **Example: Matter**
  - Unique keys and certs
  - Unique labels
- **AND products need to keep things secure**

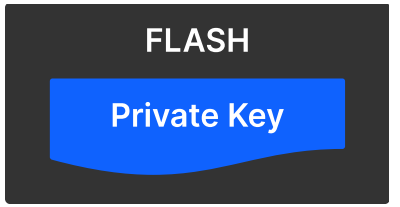
How Does Provisioning Actually Work?

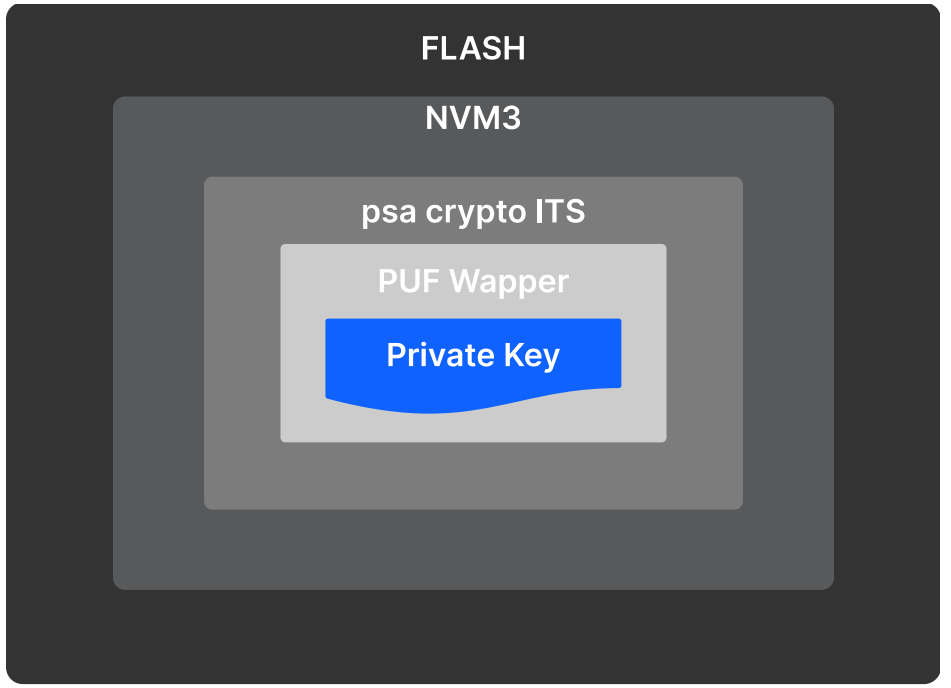
- **There is a standard method of provisioning.**
  - Program a loader application via Debug
  - Send the Loader information
  - Let the loader program the device



Challenge 1: Storage Gets More Complex

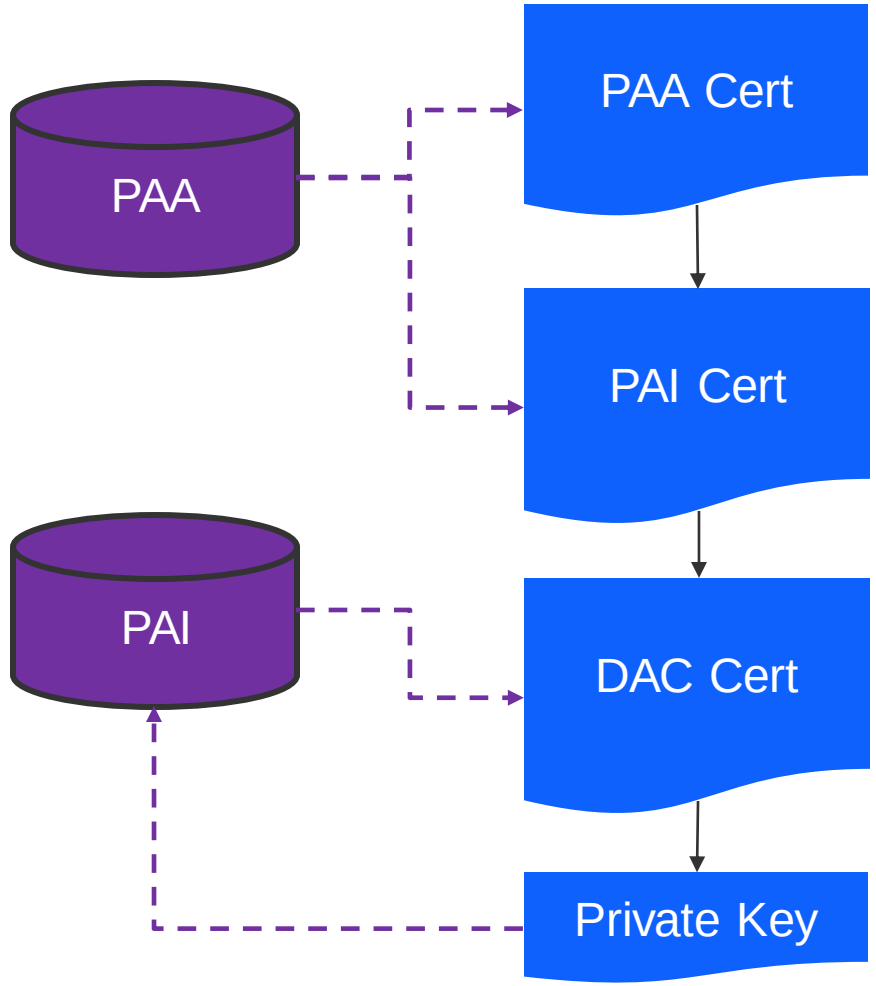
- **In Matter each device has to store a unique private key**
- **The simple way to do this is to put it in Flash**
  - This is not secure
  - This is not easily updatable
- **Proper storage can be more complex**
  - Key wrapped with PUF for security
  - Stored in psa_crypto ITS format for consistence and ease of use
  - Stored in an NVM database so it can be efficiently updated
- **Good News! Our loader can handle all this easily for us**
  - But it is now larger and more complex





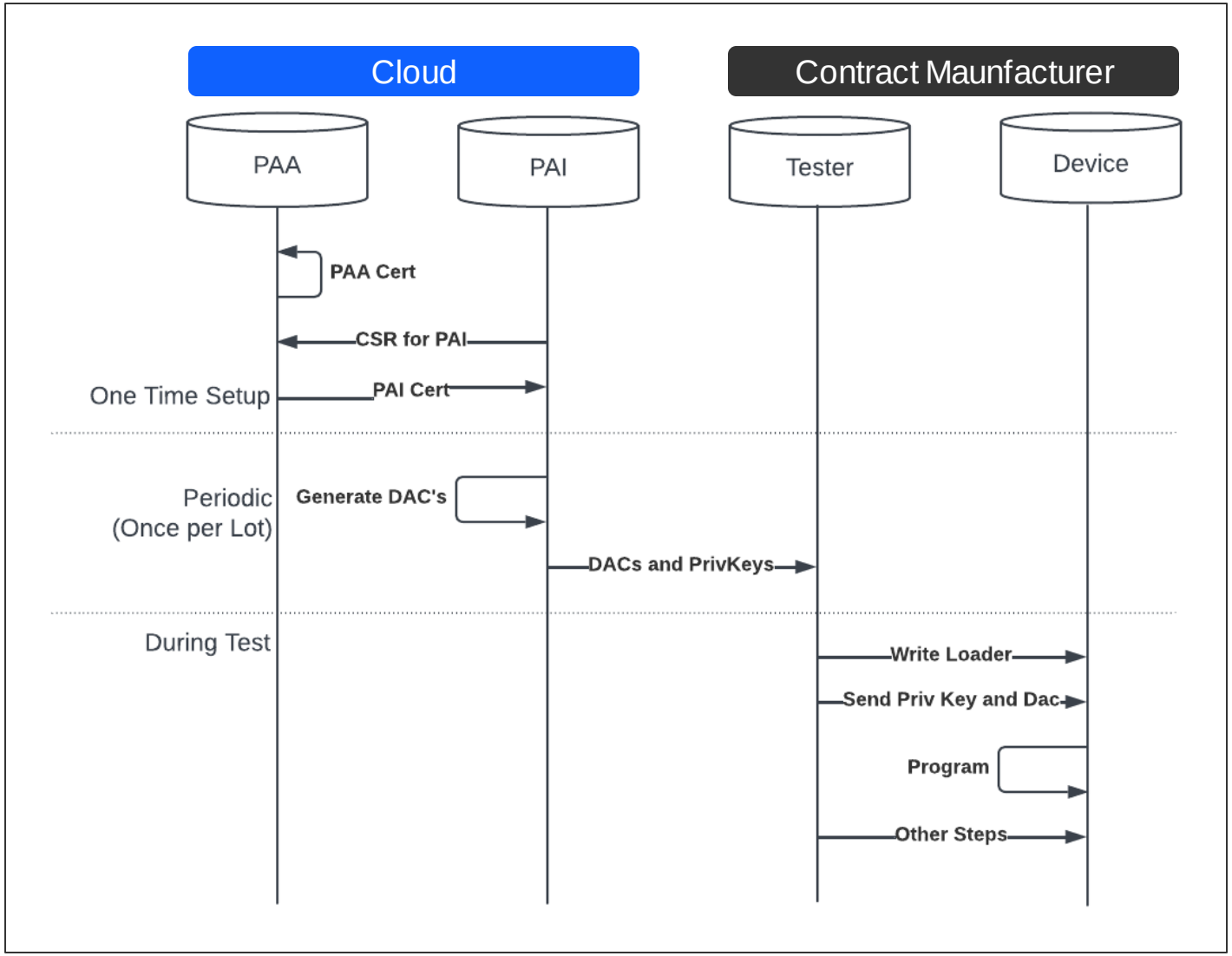
Challenge 2: How Do We Get Our Data?

- **Some things we can generate on the fly**
  - Serial numbers
- **Secure things need to come from a secure source**
- **Where does the private key come from?**
  - If it's made by the device it's most secure BUT w can't create our DAC ahead of time
  - If it's made by the PAI then we can make it ahead but it's vulnerable in transport



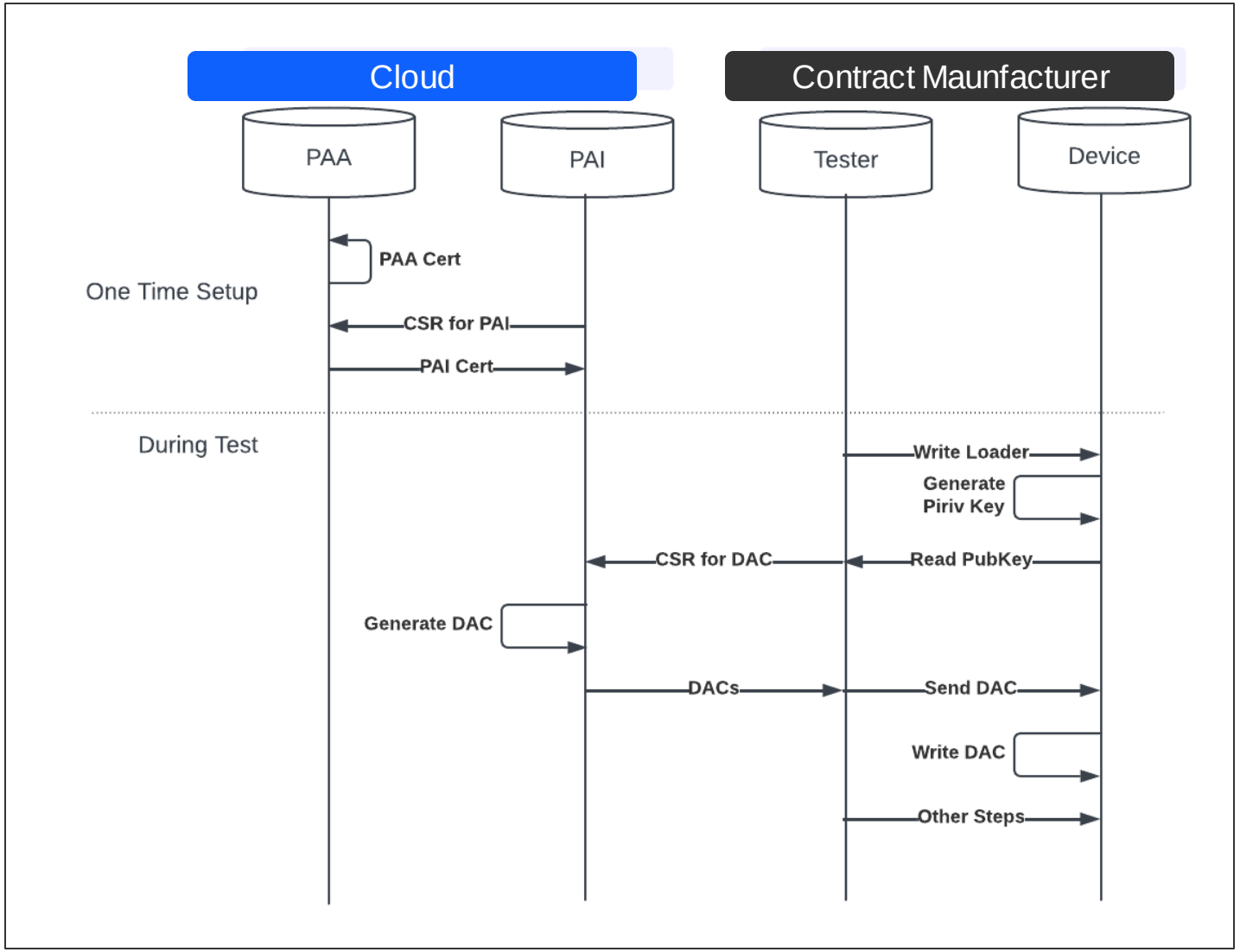
The Simplest Setup

- **This is the simplest setup**
  - Build a database of credentials
  - Send them to the tester
  - Inject the credentials
- **This is good for manufacturing**
  - Low cost
  - Low risk of interruptions
  - Simple
- **This is bad for security**
  - Private keys are transported and stored in multiple places
  - Private keys are ultimately sent to the device which is hard to protect
- **This solution would be a good fit for products that**
  - Don't support secure key storage
  - Prioritize cost over security



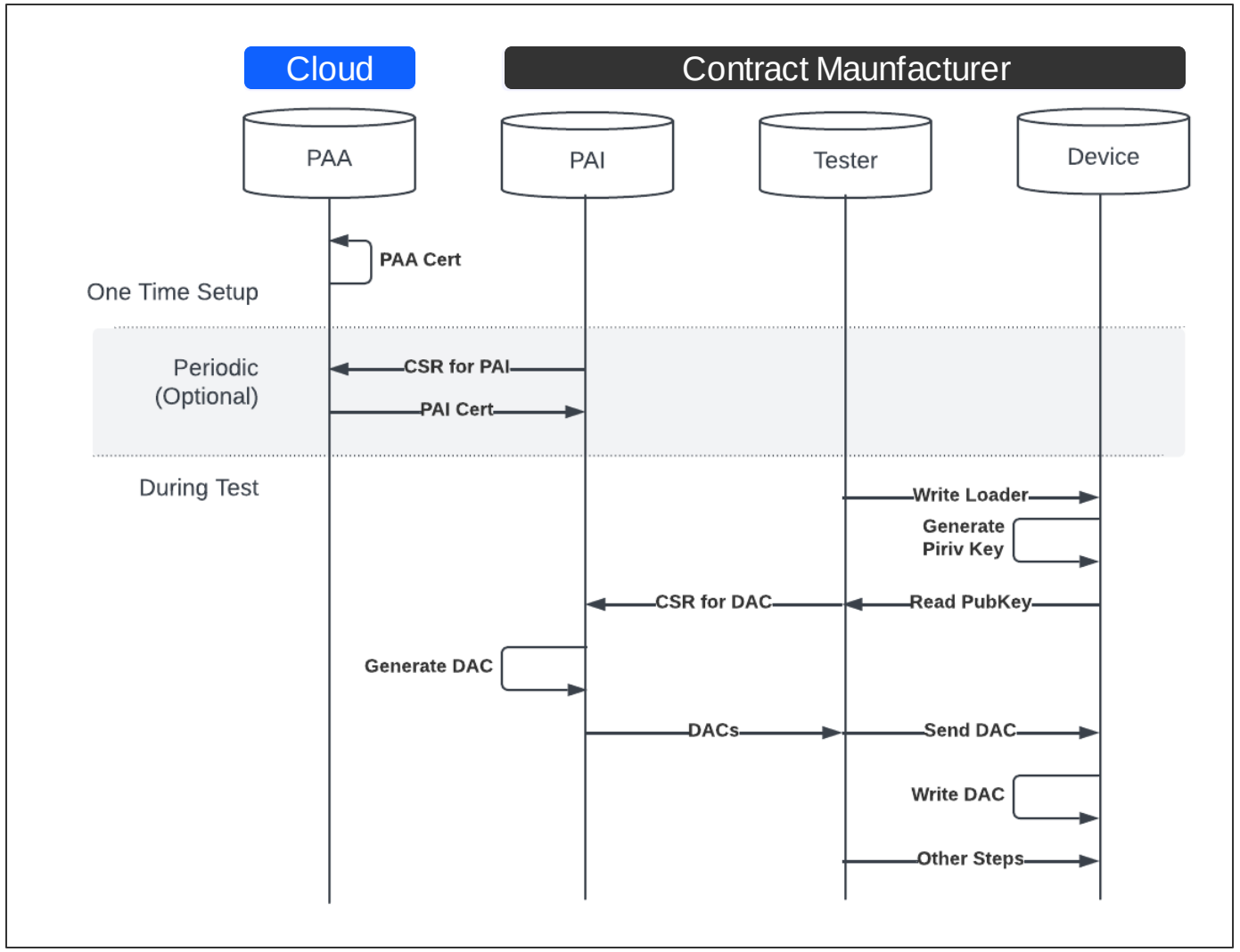
On-Line Manufacturing

- **Device Generates its own Key**
  - Key is never exposed
- **This comes with dangers of its own**
  - How much test time does that communication add?
    - CM may have 100's of systems running
  - What happens if the internet connection fails or degrades?
  - What happens if someone targets the CM with a dDoS?
- **This solution is good for**
  - OEM's who can tolerate production interruptions and value the security increase



The Most Secure Solution

- **On-Site PAI Address the On-Line risks**
- **Rotating PAIs increase security**
  - Keys are now time-bounded
  - Provides good revocation granularity
- **The PAI is on-site**
- **For Matter this is difficult due to the way the requirements are structured**
  - Especially at a site owned by a 3rd party
- **This solution is good for**
  - Products that need high security and can tolerate high cost
  - OEM's who own their own manufacturing sites



SILICON LABS

We Still Must Be Proactive About Manufacturing

- **Develop with the same script and loader that will be used in production**
  - Ensures no surprises when going to production
  - Production is debugged during development
- **Tools can easily support this**
  - Post build steps can run provisioning scripts
  - If structured properly firmware can be updated without changing provisioned data for faster firmware development
- **Silabs Provisioning Support**
  - Support all provisioning needs with scripts and loaders
    - For development AND for production
  - CPMS available to do custom part provisioning
    - Pre-program loaders or applications
    - Pre-provision credentials
    - Pre-configure device settings
  - Provide consistency between protocols and ecosystems

Conclusion

- **Matter credentials present an interesting challenge to volume manufacturing**
- **But many other problems are addressed by the same pattern**
- **There is no “Best” solution. Each product has its own needs.**
- **It’s important to plan for these new manufacturing needs up front**
  - It’s easy to run into months of delay and potentially need significant changes to a product if manufacturing is not accounted for
  - But if you know it’s coming it doesn’t have to be a problem

Q&A

Thank You

tech talks

MATTER

FEB 15TH	The Final Step Matters: Scaling Secure Products into Volume Production
MAR 21ST	Matter Technology and Market Updates and Q&A with the Connectivity Standard Alliance
APR 25TH	Future Proofing your Matter Products
MAY 30TH	Matter Specification Updates and Enhanced Support for Low Power Sensor Devices

MATTER