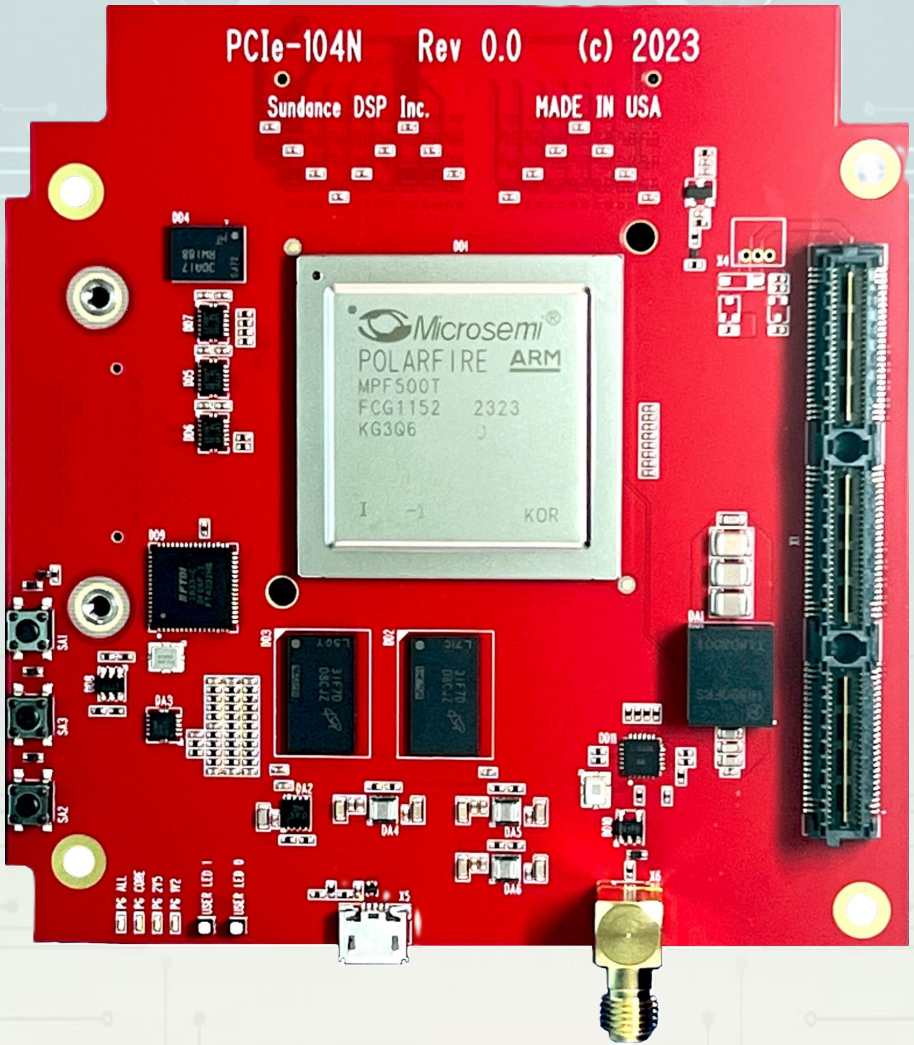
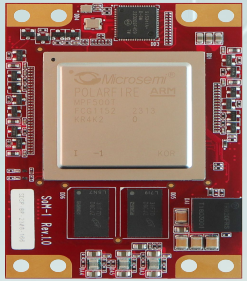
Hardware-Rooted Bitstream Security & Secure Manufacturing Workflow

Defense-Grade Implementation Using PolarFire FPGA on PCIe104N

Mans Ahmadian, PhD, CEng, MIET
CInO, Sundance

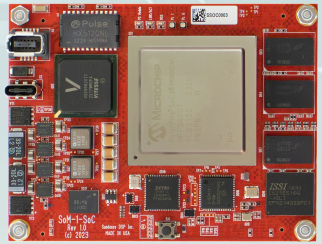

PCIe-104N Rev 0.0 (c) 2023
Sundance DSP Inc.
MADE IN USA
Microsemi
POLARFIRE ARM
MPF500T
FCG1152 2323
KG3Q6
KOR



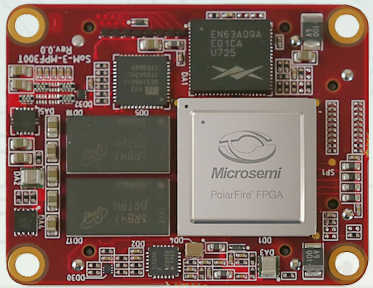
SOM1

SE300

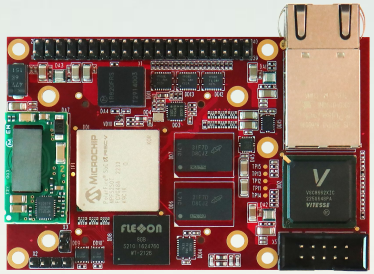
MICROCHIP



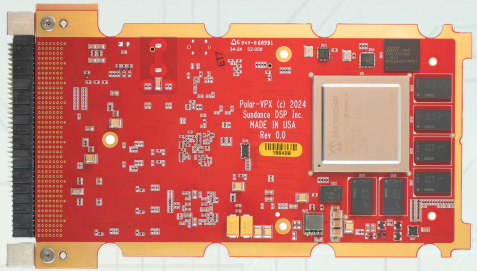
SOM1-SOC



SOM3



PolarBerry



Polar-VPX

CONTEXT

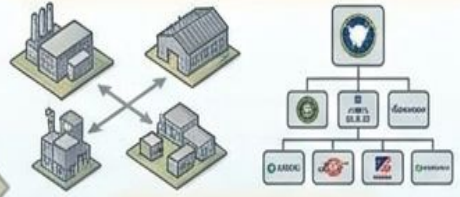
FPGA ADOPTION IN DEFENSE & AERO

- INCREASING USE OF FPGAs IN DEFENSE & AEROSPACE SYSTEMS

Flexibility
Power
Performance

CHALLENGES IN FPGA DEPLOYMENT

- OPERATIONAL ENVIRONMENT



- DEPLOYMENT IN DISTRIBUTED & MULTI-PARTY ENVIRONMENTS

Supply Chain Risks

SYSTEM SECURITY SCOPE

- SECURITY MUST EXTEND BEYOND FIELD OPERATIONS
  - Protect bitstream integrity
  - Ensure IP confidentiality
  - Point of manufacturing securement

THE CRITICAL NEED FOR COMPREHENSIVE SECURITY

THE CORE PROBLEM

TRADITIONAL FOCUS: RUNTIME AND FIELD SECURITY

SECURITY EFFORTS: Runtime encryption, Secure boot, tampering detection.

OVERLOOKED RISK: MANUFACTURING AND PROVISIONING PHASE

VULNERABILITIES: Unsecured programming hosts, Untrusted facilities, Lack of key management.

RESULT: BITSTREAM EXPOSURE BEFORE DEPLOYMENT

Breach unacceptable in defense: Compromised security & Mission failure.

THE VULNERABILITY: UNSECURED PROVISIONING AT MANUFACTURING

THREAT LANDSCAPE

INTELLECTUAL PROPERTY THEFT

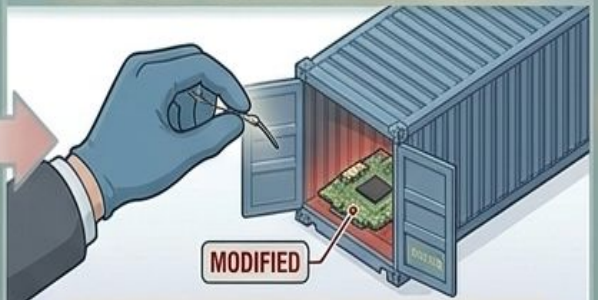
HARDWARE SUBSTITUTION

OVERBUILDING OF DEVICES

BITSTREAM INTERCEPTION

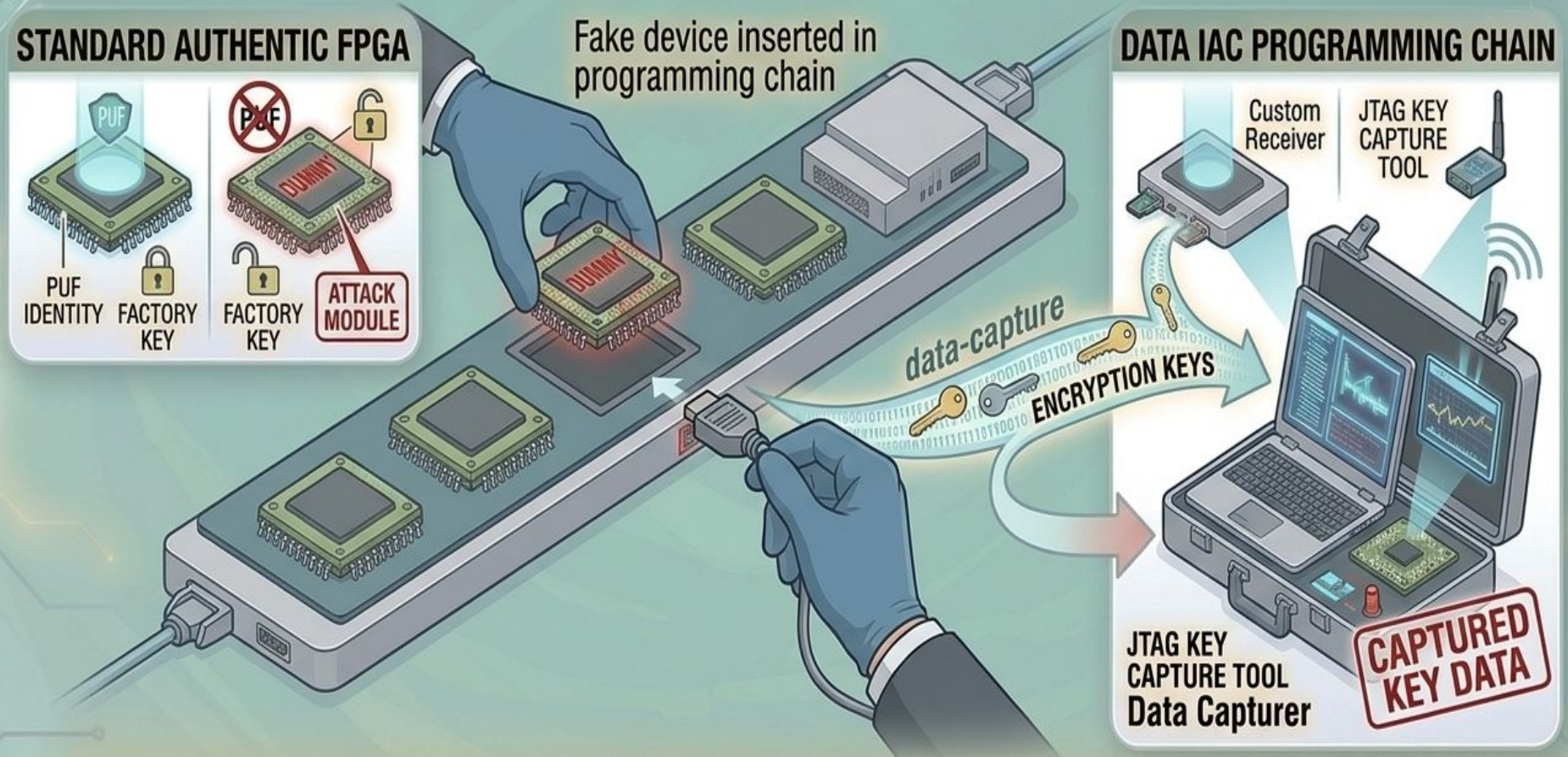
BITSTREAM INTERCEPTION

SUPPLY CHAIN TAMPERING



SUPPLY CHAIN TAMPERING

REAL ATTACK SCENARIO



SECURITY REQUIREMENTS

A defense-grade system must provide:

DEVICE AUTHENTICITY

Uniquely identifies each FPGA to ensure genuine hardware.

BITSTREAM CONFIDENTIALITY

Protects data during transit and provisioning, keeping design secure.

ANTI-CLONING GUARANTEES

Robust protection against unauthorized device duplication or counterfeiting.

SECURE KEY LIFECYCLE

Tightly controls cryptographic keys from creation through deployment.

SUPPLY CHAIN TRUST

Ensures disciplined and traceable operations from manufacturing through deployment.

SOLUTION OVERVIEW

Integrated Secure Provisioning Approach

HARDWARE-ROOTED SECURITY FEATURES

- Hardware-rooted security features in PolarFire FPGA

ANTI-CLONING GUARANTEES

- Cryptographic architecture from Microchip Technology

SECURE KEY LIFECYCLE

- Secure workflow built on Microchip architecture and implemented within Sundance's controlled production environment

SYSTEM STAKEHOLDERS

Integrated Secure Provisioning Ecosystem

1. THE CUSTOMER

- Securely defines and manages system requirements
- Receives and authenticates final deployed units

2. SUNDANCE

- Microchip solution provider
- Design services for secure architectures
- Hardware and software development

3. SECURE TEST & PROGRAMMING CENTER

- Manages the secure root of trust
- Programs devices with authorized bitstreams
- Validates individual device keys and identities

Separation of responsibilities is a *deliberate security design principle.*

ROLES AND RESPONSIBILITIES

CUSTOMER

- Firmware
- Keys
- Production Control

The customer owns the intellectual property, generates the encryption keys, and defines the production limits.

SUNDANCE

- Hardware Manufacturing
- Integrity

Sundance manufactures the hardware while ensuring component provenance and integrity.

TEST CENTER

- Validation
- Secure Programming

The secure test center performs validation and executes programming under controlled conditions.

CUSTOMER'S ROLE

CUSTOMER

- Firmware
- Keys
- Production Control

The customer owns the intellectual property, generates the encryption keys, defines the production limits.

Generates bitstream

01010101010101
11010110101101
01010101
01010111
11001110

Creates UEK

Maintains full key ownership

Defines production limits

00010

SUNDANCE'S ROLE

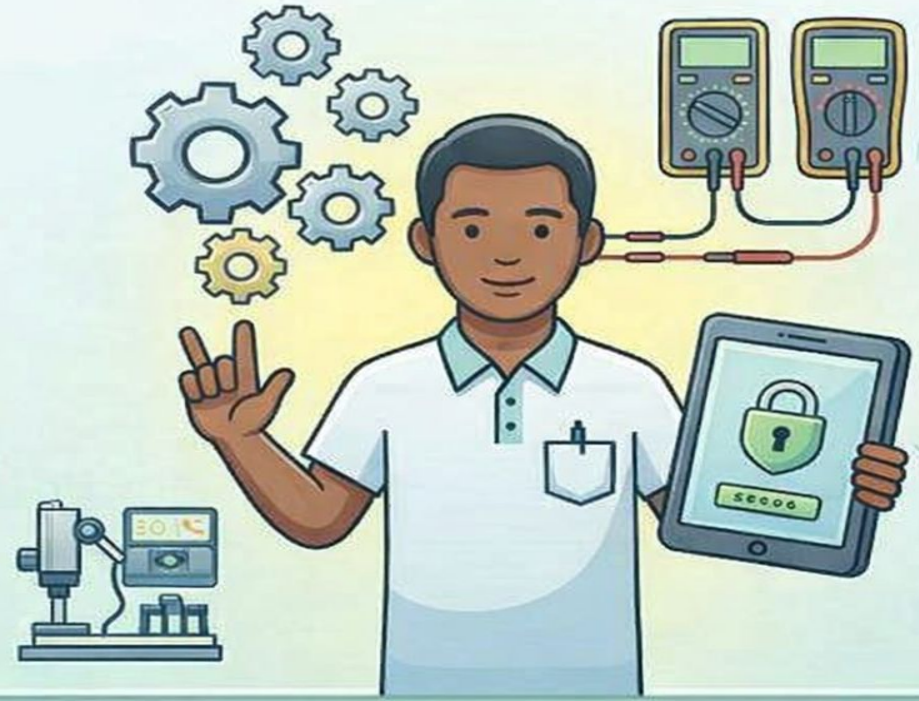
TEST CENTER'S ROLE

T CENTER

ms electrical testing
es secure
oning
es authentication
s

nentication policies

Performs electrical testing



Ensures secure provisioning

Test Center R

No
Plaintext
bitstream
Keys

TRUST BOUNDARY MODEL

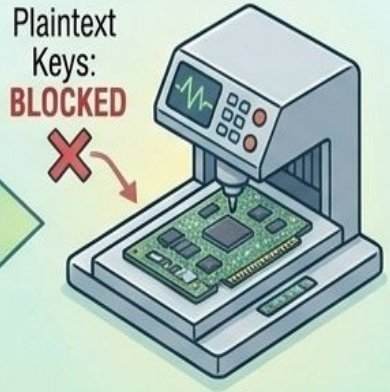
Customer

- Owns keys and IP
- Defines security policy
- Generates credentials

Encrypted Data Only

Manufacturer

- Builds hardware
- Ensures physical integrity
- No access to keys



Trusted Hardware

Test Center

- Performs provisioning
- Validates hardware
- Cannot modify firmware

- No single party has full control

DATA & CONTROL SEPARATION

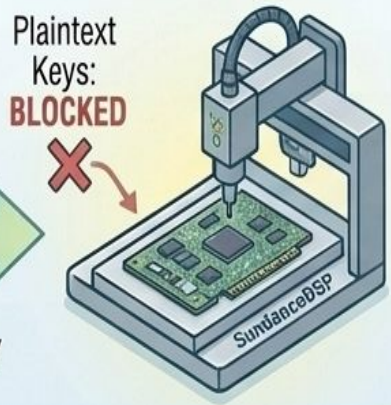
Customer

- Keys controlled by customer

TRUST BOUNDARY

Manufacturer

- Hardware controlled by manufacturer



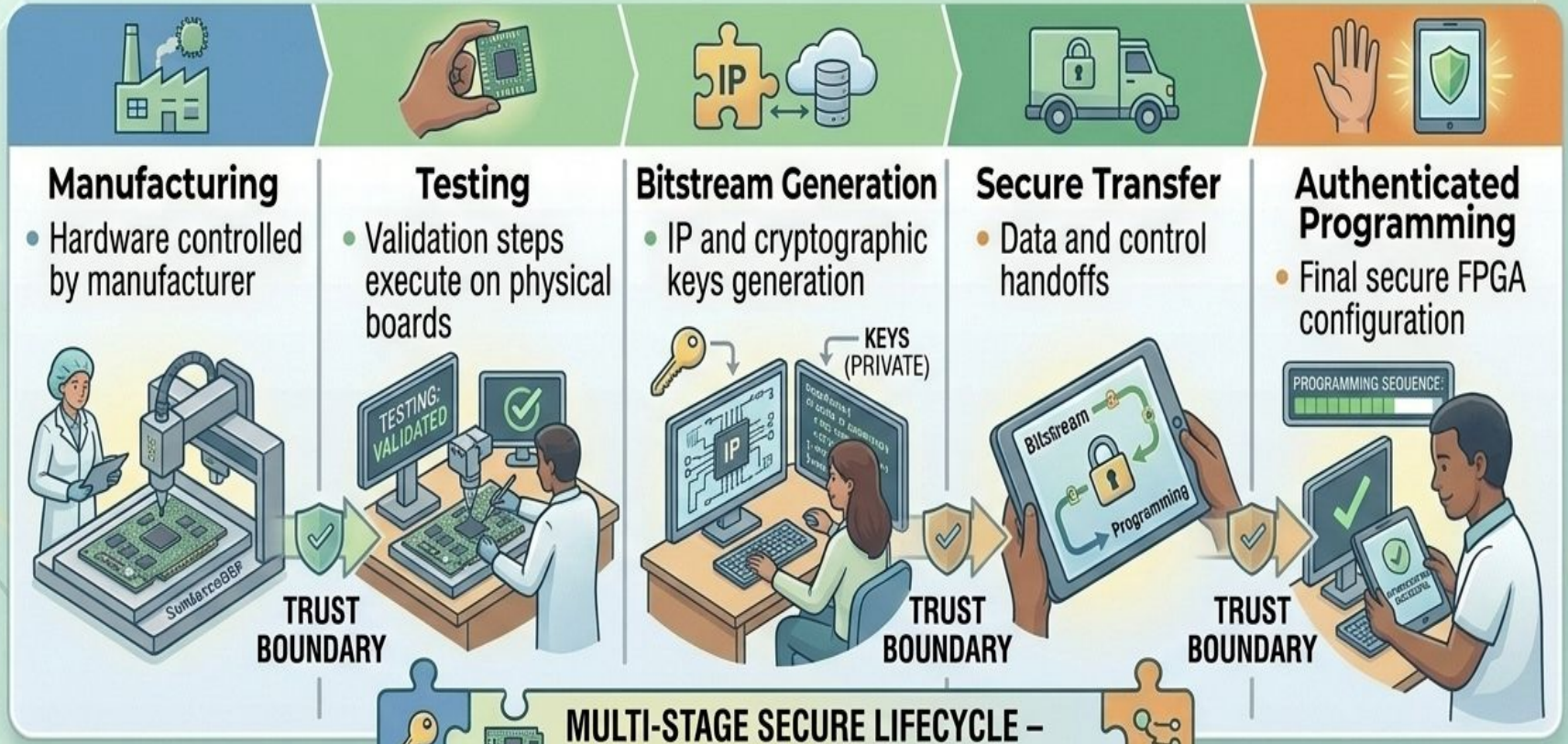
TRUST BOUNDARY

Test Center

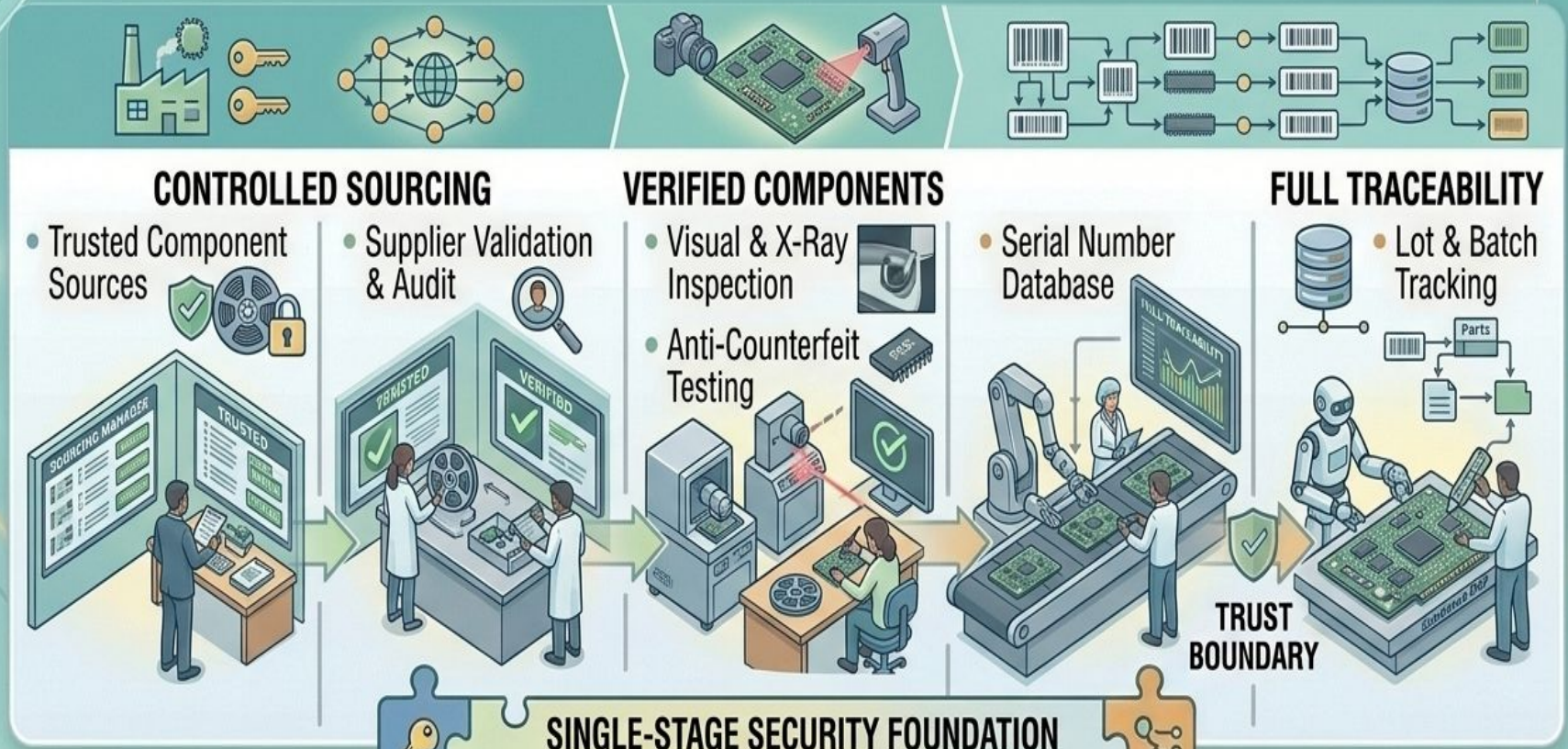
- Programming controlled by test center

NO SINGLE PARTY HAS FULL CONTROL -
Control and Access are **INTENTIONALLY FRAGMENTED**

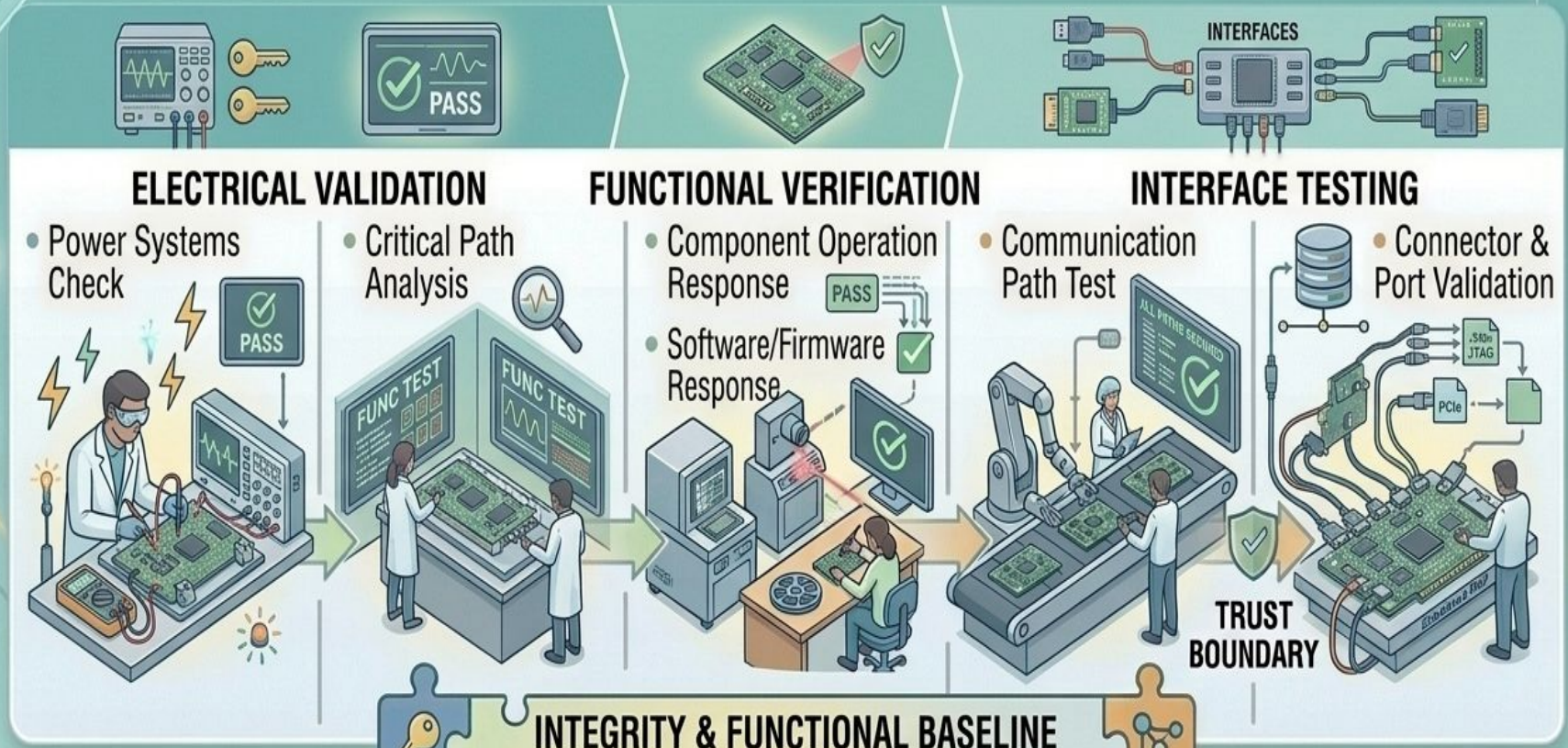
WORKFLOW OVERVIEW



MANUFACTURING PHASE



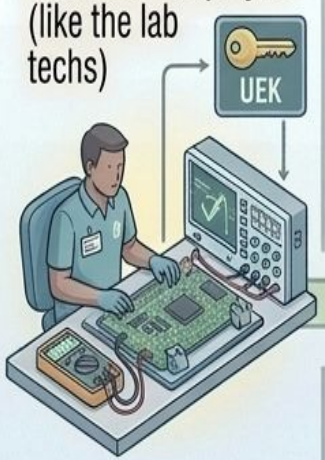
TESTING PHASE



BITSTREAM CREATION

CUSTOMER GENERATES

- Customer-employee (like the lab techs)



- Encryption Desktop

ENCRYPTION INSIDE HSM

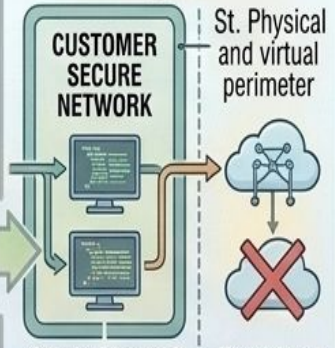
- Secure Key Isolation within HSM
- ENCRYPTED BITSTREAM

UEK CREATED SECURELY

- TRNG-based Key Generation

ISOLATED ENCRYPTION

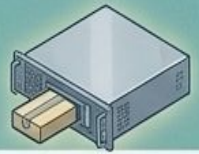
- No External Connectivity During Creation



SECURE INTELLECTUAL PROPERTY BASELINE

Isolated generation of bitstream and UEK prevents external key exposure.

SECURE TRANSFER



ENCRYPTED ASSET PACKAGE

- Gloved Technician prepares sealed asset canister.

Gloved Technician prepares sealed asset canister.

M-HSM INPUT

- M-HSM authenticates transfer source and validates integrity.

M-HSM authenticates transfer source and validates integrity.

PROTOCOLS & LOGS

- **SECURE TRANSFER PROTOCOLS**
- Cryptographic protocols prevent Signatures

Cryptographic protocols prevent eavesdropping.

CONFIDENTIALITY GUARD

- **NO PLAINTEXT EXPOSURE**

Only encrypted assets are handled.

SECURE HANDOFF

- Comprehensive, auditable log of assets.

Comprehensive, auditable log of assets.

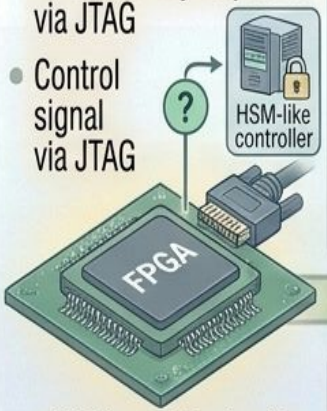
VERIFIED ASSET HANDOVER

Encrypted bitstream and UEK transferred with full auditability.

DEVICE AUTHENTICATION

FPGA IDENTITY REQUESTED

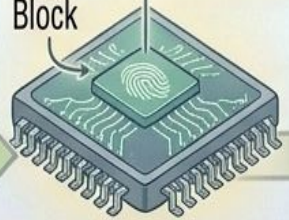
- FPGA identity requested via JTAG
- Control signal via JTAG



- PUF-based Device ID generated

PUF ID GENERATION

- PUF Block activates a unique digital fingerprint.



PUF Blocks activating a unique digital fingerprint.

HSM VERIFICATION

- Verified before programming
- Device ID to trusted database

- Verified before programming

AUTHENTICATION STATUS

- If **PASS**, connection with key

If connection with key is proceeds.

LOGGED AUTHENTICATION

- Comprehensive, auditable log of assets.

Comprehensive, auditable log of assets.

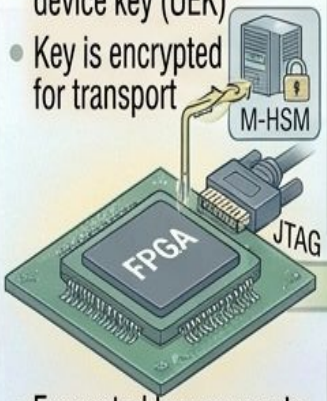
VERIFIED DEVICE HANDOVER

Genuine hardware confirmed with full audibility.

PROGRAMMING PHASE

UEK TRANSFERRED SECURELY

- HSM creates unique device key (UEK)
- Key is encrypted for transport



- Encrypted key moves to FPGA internal storage

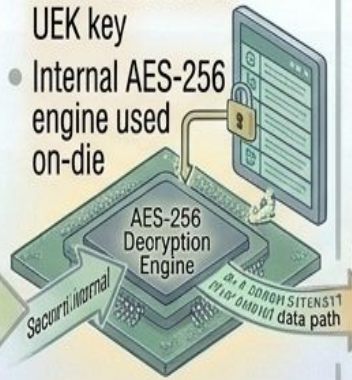
ENCRYPTED BITSTREAM LOADED

- M-HSM retrieves encrypted bitstream
- Authenticated link active

- Bitstream loaded into FPGA configuration memory

INTERNAL FPGA DECRYPTION

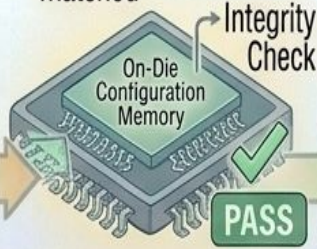
- FPGA uses stored UEK key
- Internal AES-256 engine used on-die



- Bitstream is decrypted on-die

CONFIGURATION VERIFIED

- Decrypted configuration is verified
- Checksum/Signature matched



- Genuine and correct bitstream confirmed

PROGRAMMING COMPLETED

- Device configured and operational

- Detailed programming log generated

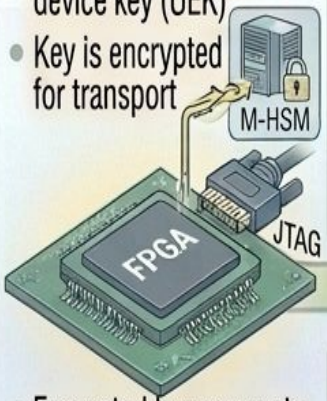
PROGRAMMED DEVICE READY

FPGA configured with secure bitstream and keys, fully ready for deployment.

KEY BINDING

UEK TRANSFERRED SECURELY

- HSM creates unique device key (UEK)
- Key is encrypted for transport
- Encrypted key moves to FPGA internal storage



ENCRYPTED BITSTREAM LOADED

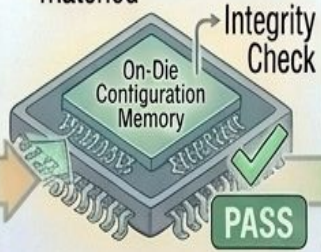
- M-HSM retrieves encrypted bitstream
- Authenticated link active
- Bitstream loaded into FPGA configuration memory

INTERNAL FPGA DECRYPTION

- FPGA uses stored UEK key
- Internal AES-256 engine used on-die
- Bitstream is decrypted on-die

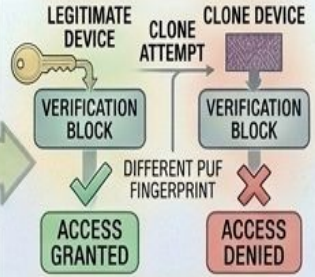
CONFIGURATION VERIFIED

- Decrypted configuration is verified
- Checksum/Signature matched
- Genuine and correct bitstream confirmed



CANNOT BE REUSED

- Clone device has a different, incompatible PUF fingerprint
- Device-bound key is invalid on any other hardware
- Re-use and cloning are prevented

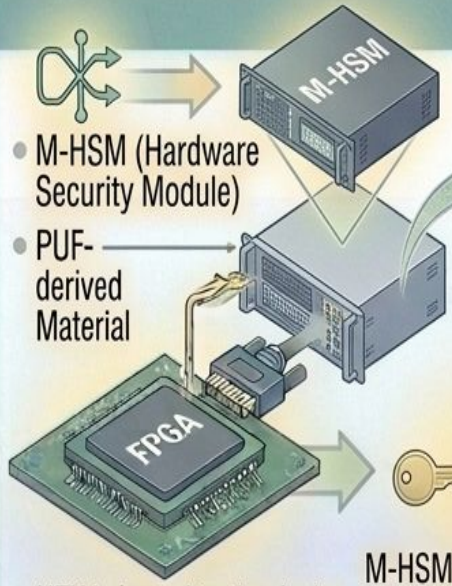


BINDING CONFIRMED

Device uniquely bound to the configuration using inherent hardware identifiers.

PRODUCTION CONTROL

STRENGTHENING PRODUCTION CONTROL



- M-HSM (Hardware Security Module)
- PUF-derived Material
- UEK is bound to the device using PUF-derived material

Authorized Number Count

100

Pre-defined production Count set

M-HSM PROGRAMMING LIMITS

PROGRAMMING CONTROL

- Programming count enforced by M-HSM
- Pre-defined production count set ot.
- Authorized firmware only

DEPLOYED BOARDS

PREVENTING OVERBUILDING

NORMAL PRODUCTION

PROGRAMMING STATION

AUTHORIZED QUANTITY (e.g., 100/100)

QUANTITY LIMIT CHECK

PRODUCTION COUNT VALID: Devices Programmed & Deployed.

OVERBUILD ATTEMPT

STOP

COUNT EXCEEDED (e.g., 101/100)

STOP PROGRAMMING

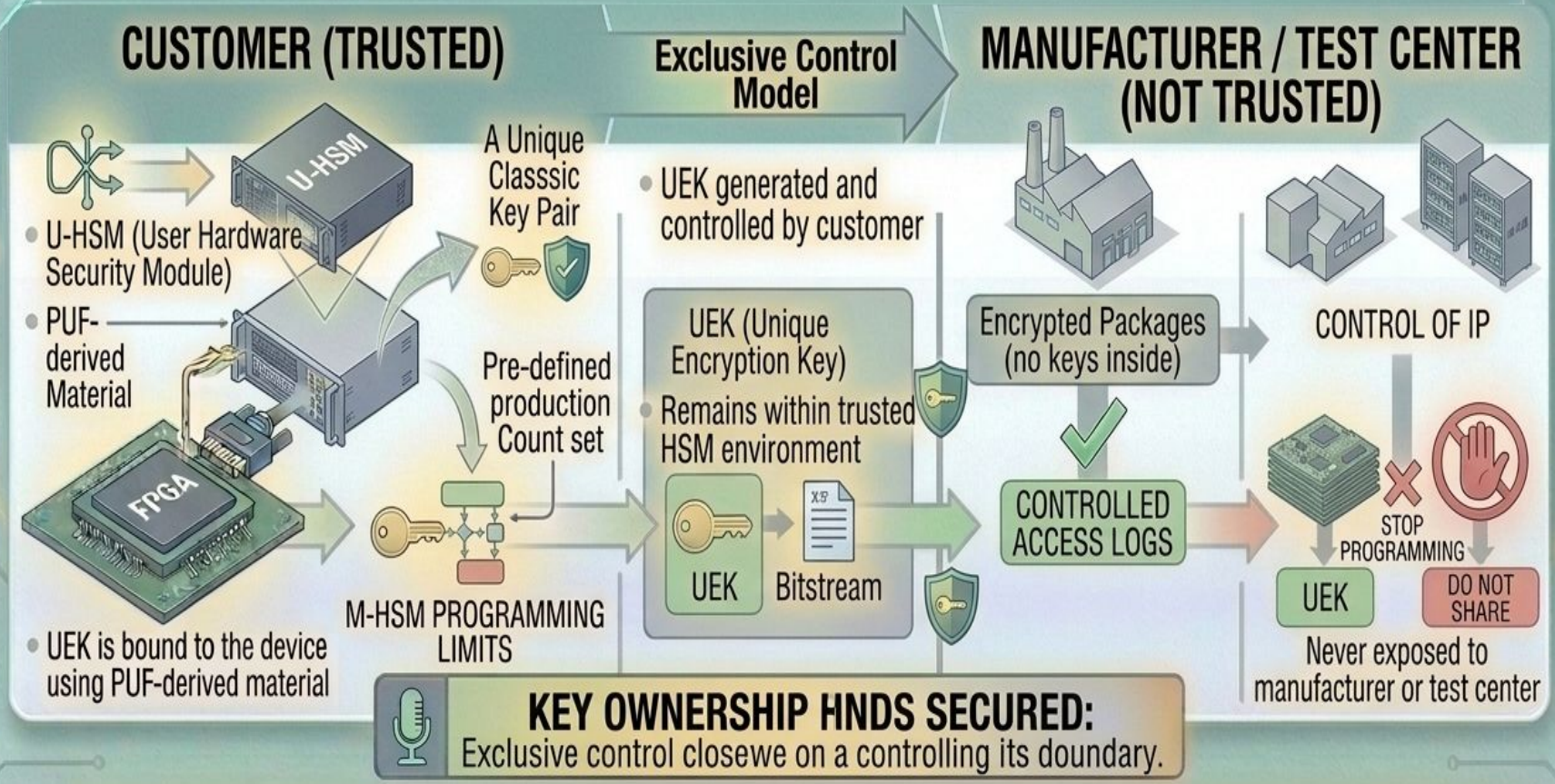
COUNT EXCEEDED

PRODUCTION HALTED

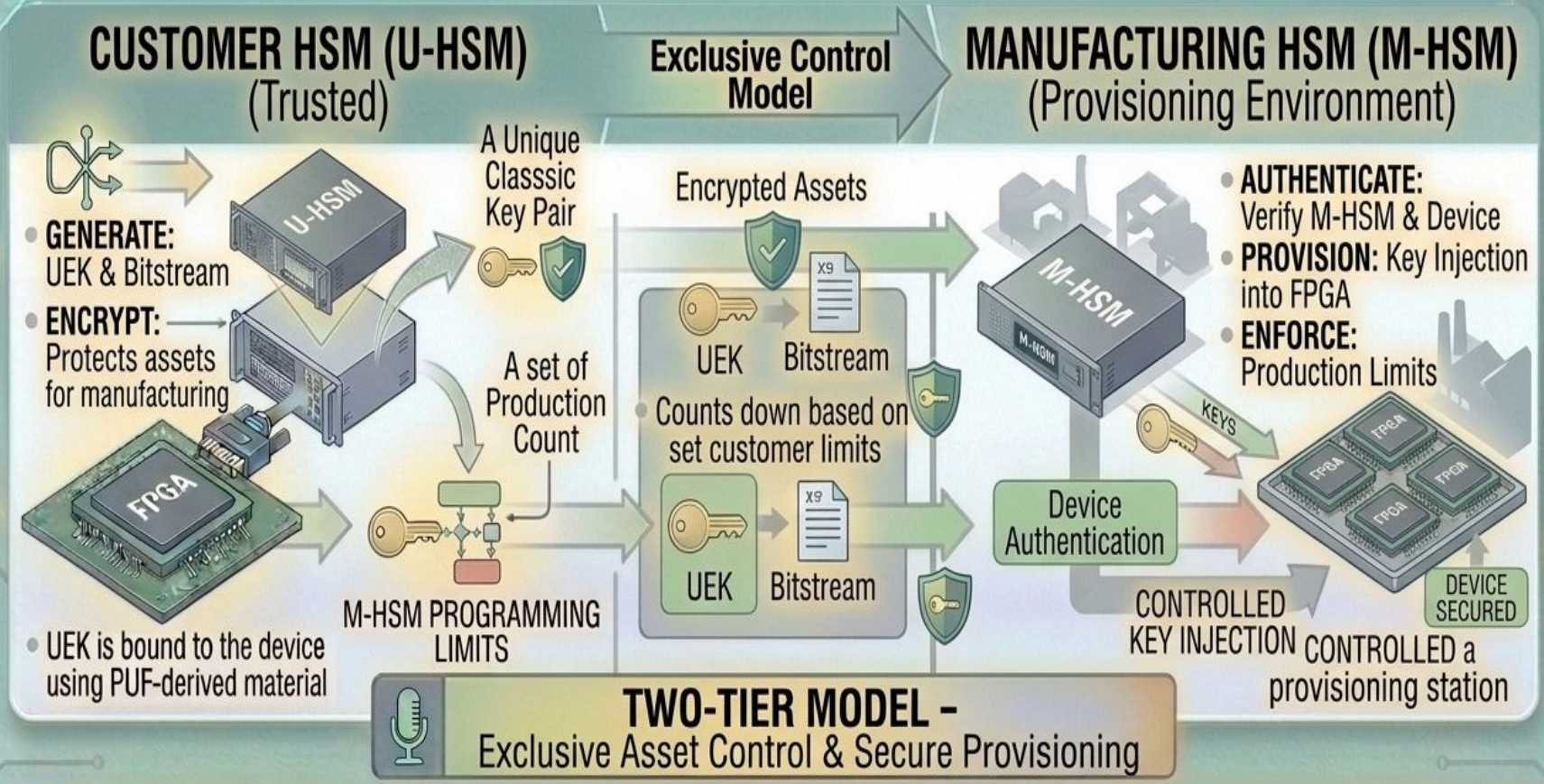
Programming Stops Automatically.

PRODUCTION CONTROL SECURED:
Precise control over device manufacturing quantity.

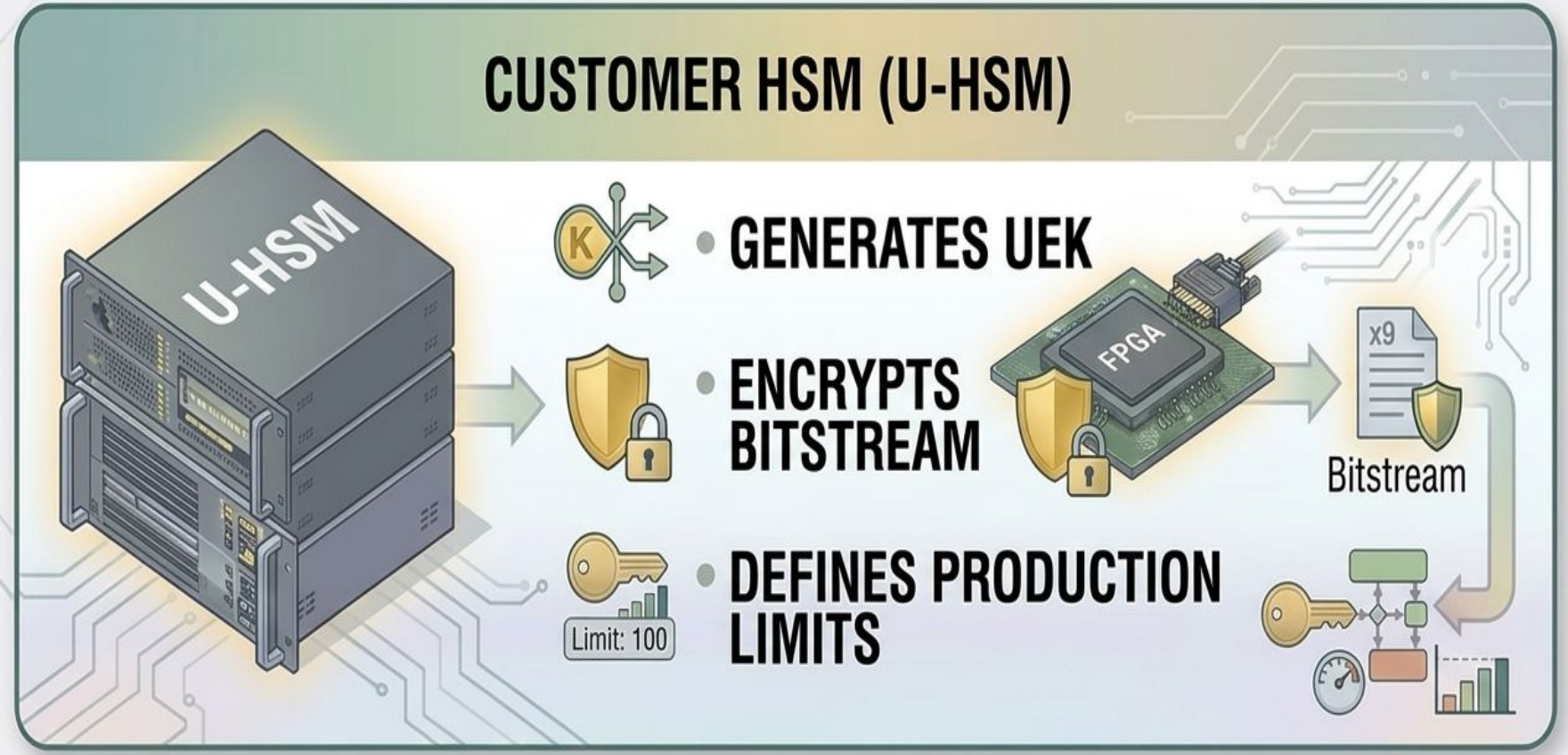
KEY OWNERSHIP



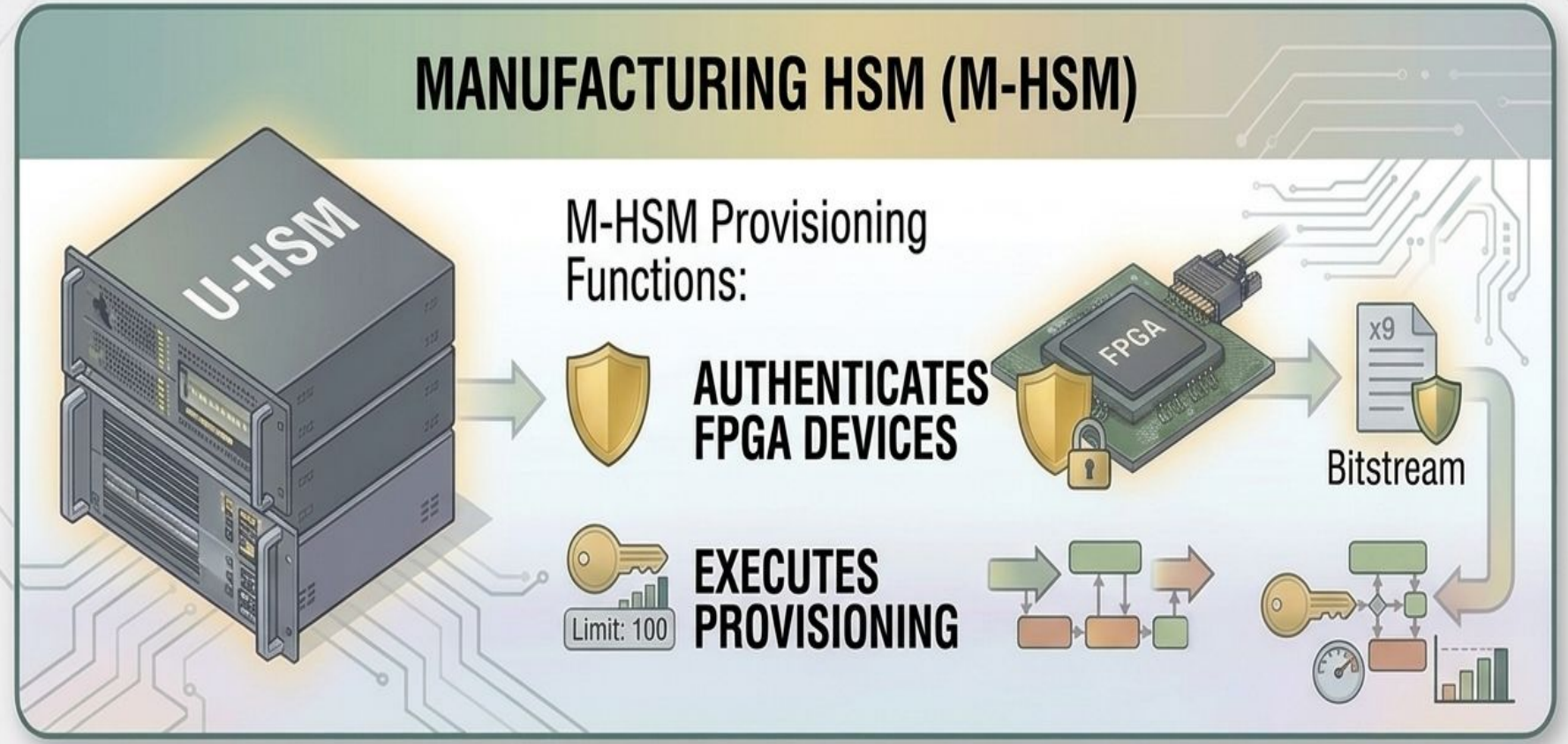
HSM ARCHITECTURE



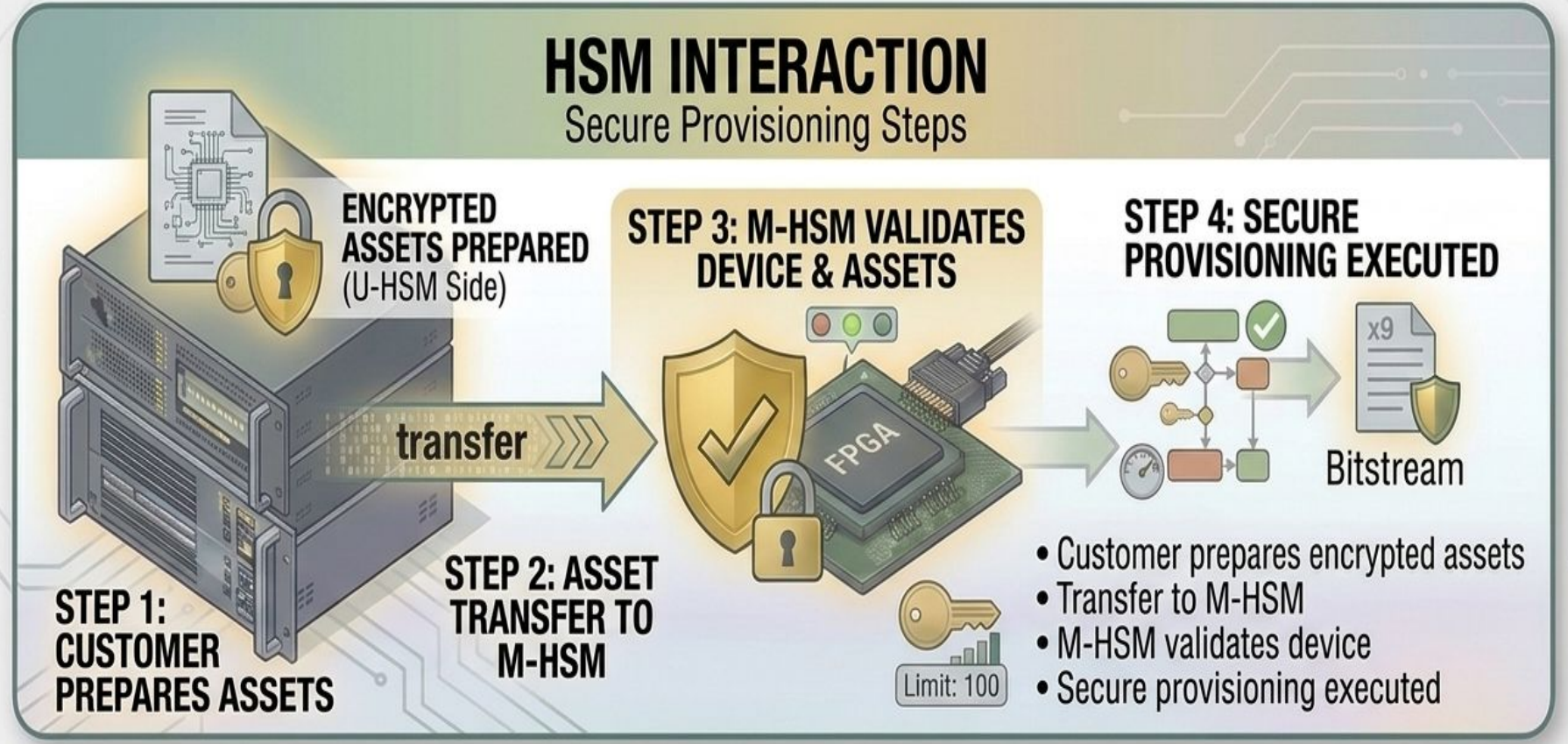
CUSTOMER HSM (U-HSM) ARCHITECTURE



MANUFACTURING HSM (M-HSM) ARCHITECTURE



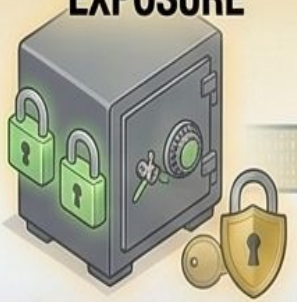
HSM INTERACTION WORKFLOW



SECURITY PROPERTIES

SECURITY PROPERTIES
Key System Safeguards

NO KEY EXPOSURE



NO KEY EXPOSURE
Keys and assets remain encrypted from preparation to final use

STRONG DEVICE AUTHENTICATION

STRONG DEVICE AUTHENTICATION
Multi-factor authentication required for M-HSM access

ENFORCED PRODUCTION LIMITS

ENFORCED PRODUCTION LIMITS
Hardware-level counter prevents unauthorized provisioning beyond set caps

FULL AUDITABILITY

- No key exposure
- Strong device authentication
- Enforced production limits
- Full auditability

POLARFIRE SECURITY ARCHITECTURE

POLARFIRE SECURITY ARCHITECTURE

Hardware Root of Trust

PUF-BASED IDENTITY

A unique, unforgeable fingerprint is generated from inherent physical properties of each device.

FACTORY-PROGRAMMED KEYS

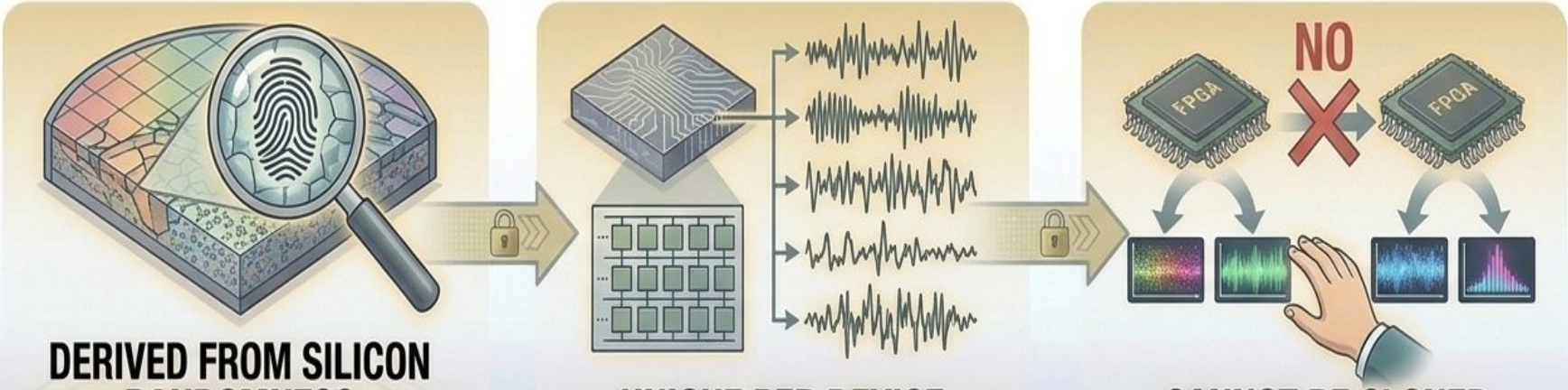
Cryptographic keys are pre-installed in a secure, controlled manufacturing environment.

DEVICE-SPECIFIC AUTHENTICATION

Each device has a globally unique identity and key, enabling tamper-proof authentication.

PUF CONCEPT

Silicon-Level Randomness and Uniqueness



DERIVED FROM SILICON RANDOMNESS

Microscopic variations in the manufacturing process create distinct electrical fingerprints.

UNIQUE PER DEVICE

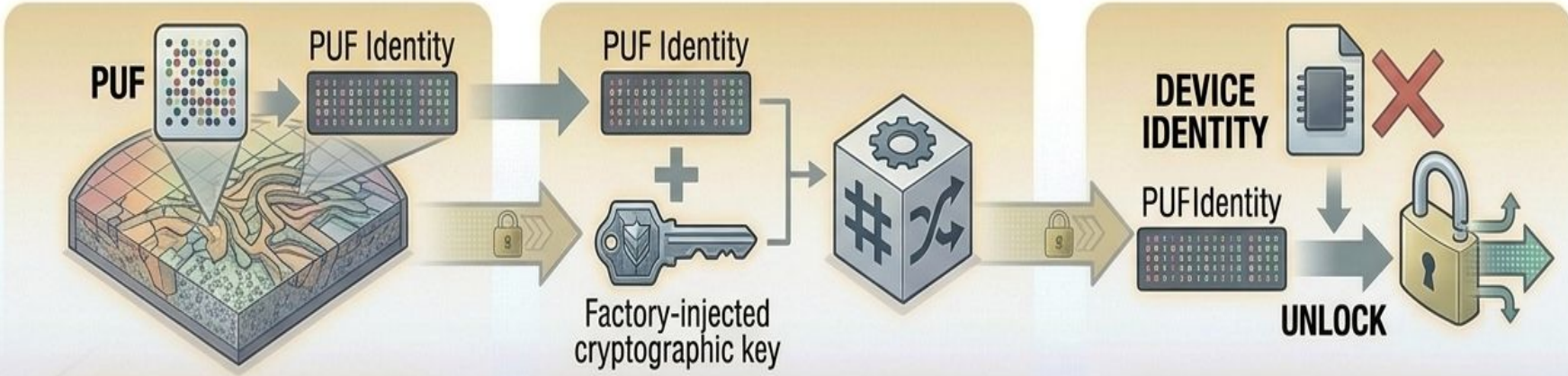
Each individual chip possesses a one-of-a-kind identity that cannot be predicted.

CANNOT BE CLONED

Physical characteristics are impossible to replicate, ensuring true hardware security.

DEVICE IDENTITY

Generated from PUF and Factory Keys



GENERATED FROM PUF

Based on unique silicon variations; the chip's core digital fingerprint.

COMBINED WITH FACTORY KEYS

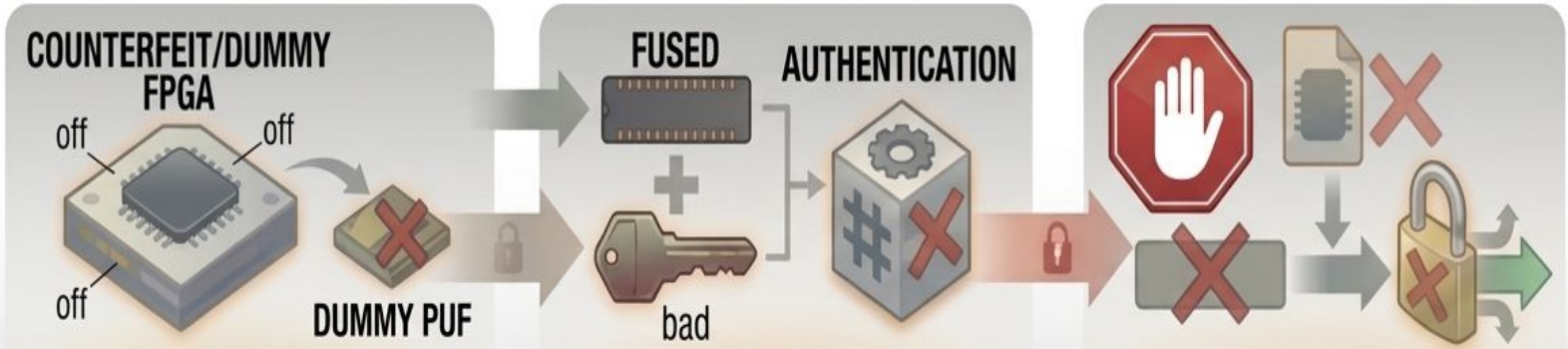
Unique PUF-derived data is integrated with pre-existing manufacturing factory keys.

NOT STORED IN MEMORY

Dynamically generated only when required; zero persistence in memory; maximum security.

ATTACK RESISTANCE

Authentication Failure Prevents Provisioning



DUMMY FPGA CANNOT REPLICATE IDENTITY

Based on a counterfeit or generic chip; lacks the unique digital fingerprint.

COMBINED DATA FORGES FAILED SIGNATURE

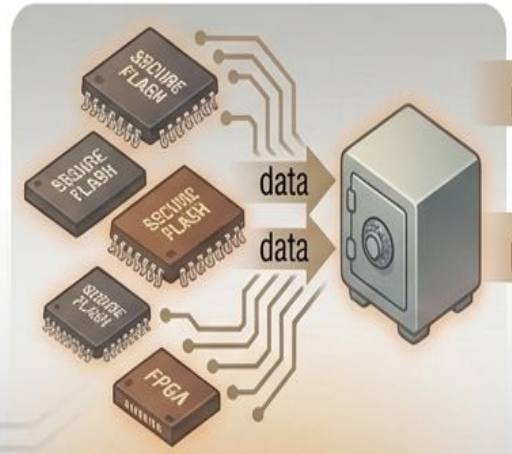
Dummy PUF and factory keys cannot create a valid unique device signature.

AUTHENTICATION FAILURE STOPS PROVISIONING

Zero key exposure; the process is terminated. No key is provided to an unauthenticated device.

Bitstream Protection

Encrypted Bitstream Storage



- AES-256 (CTR mode)
- SHA-256 authentication

Authentication

AUTHENTICATION VERIFICATION

SHA-256 is used to verify the bitstream's integrity before decryption.

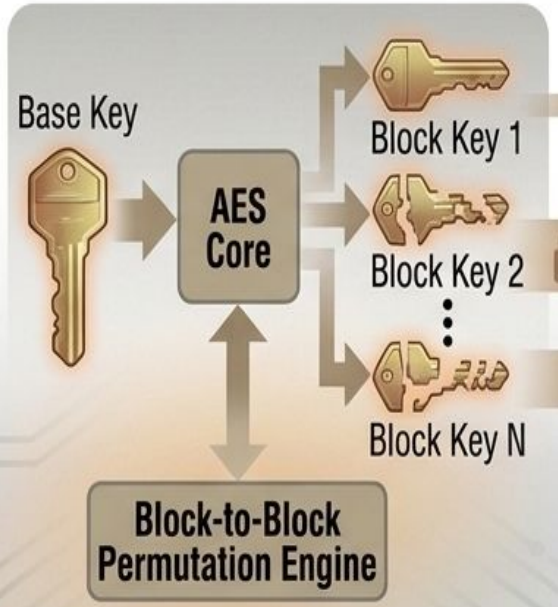
Bitstream Decryption

DECRYPTION AND LOADING

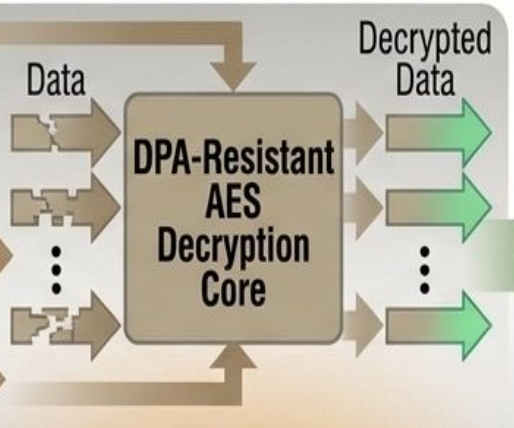
Authenticated bitstream is decrypted by the secure UEK and loaded onto the FPGA.

DPA Protection

Continuous Key Permutation

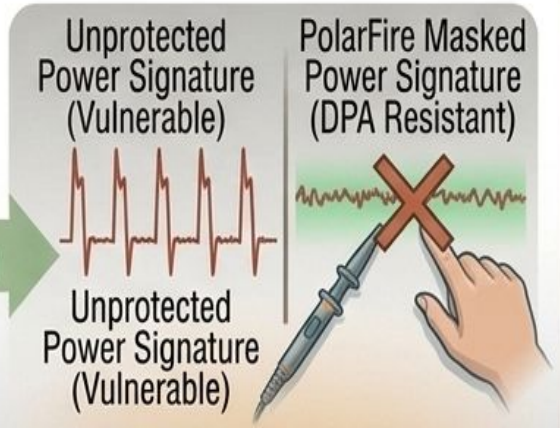


Encrypted Block Processing



- Built-in DPA resistance in PolarFire
- Uniquely permutes keys per 128-bit block

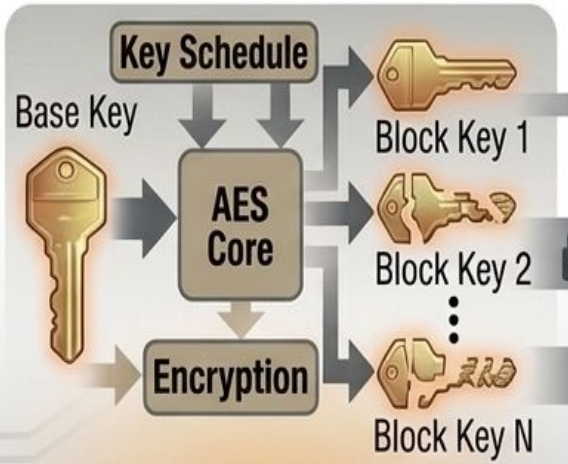
Side-Channel Data Masking



- Obfuscates key-dependent power patterns
- Effectively prevents key extraction

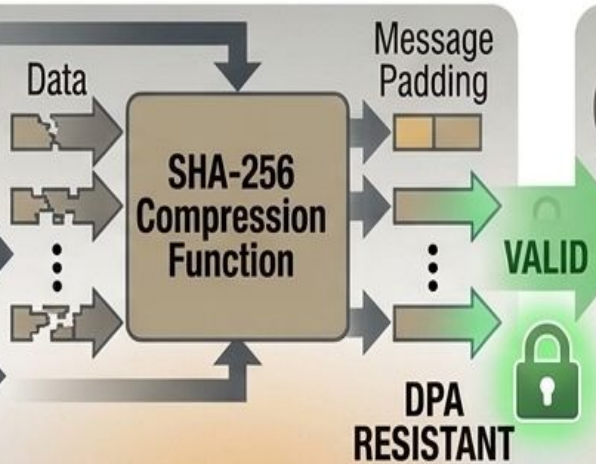
Compliance

AES (FIPS 197)



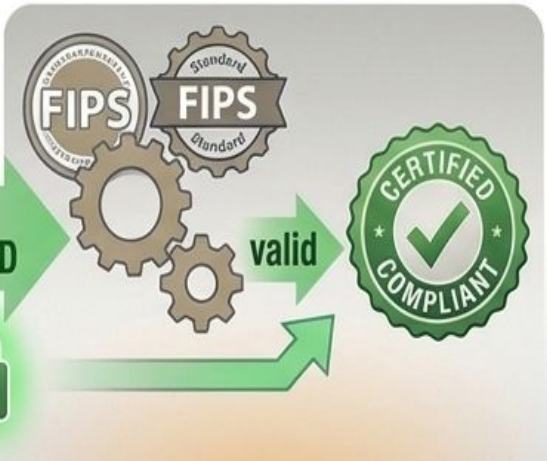
- Verified AES implementation

SHA-256 (FIPS 180-4)



- Validated hashing function

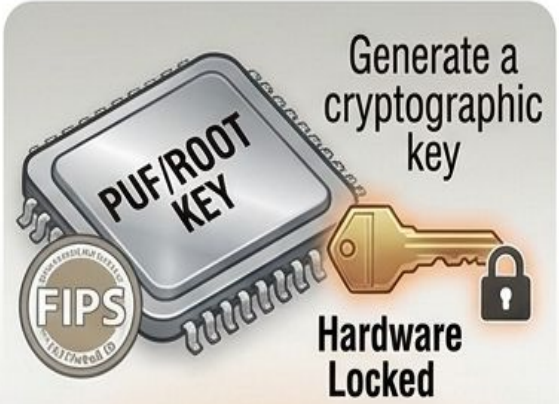
Industry Cryptographic Standards



- Meets defense application requirements

Key Takeaways

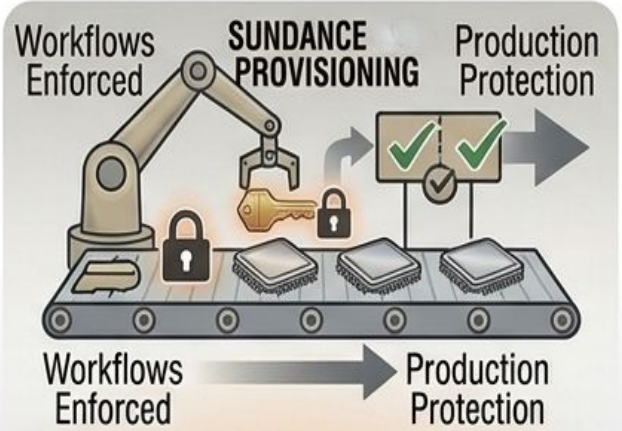
Secure Foundations



- Hardware-rooted identity is critical

- End-to-end device security

Controlled Workflows



- Secure workflows enforce real protection

- Protection from cloning/overbuilding

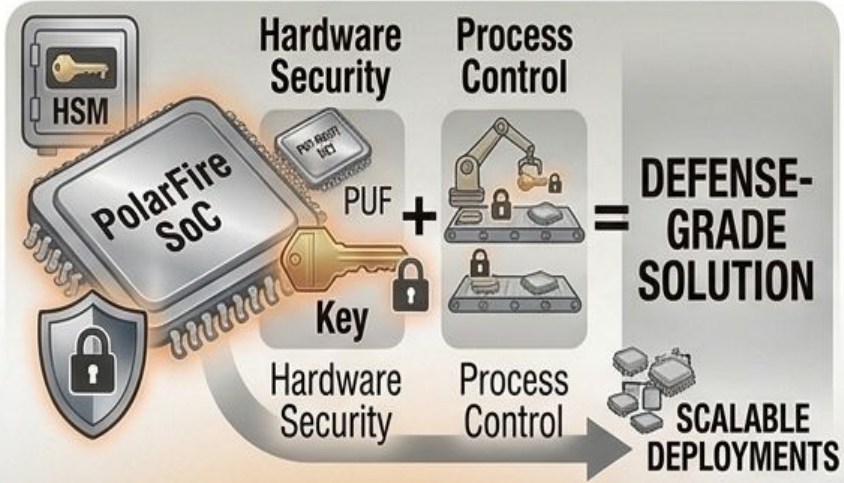
Operational Integrity

- Separation of roles reduces risk

- Resilient defense supply chain

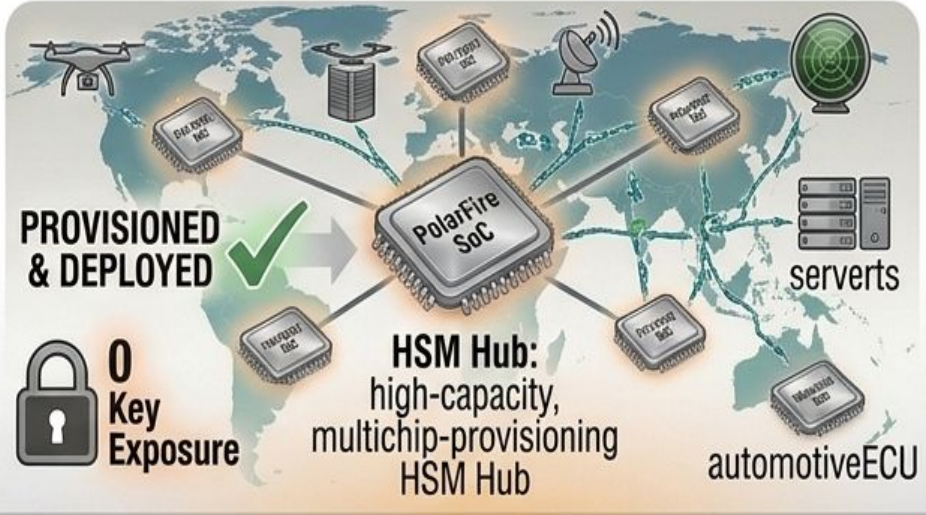
Conclusion

Defense-Grade FPGA Security



- Hardware security + process control = defense-grade solution
- Authenticated encryption & key management

End-to-End Scalability & Protection



- Secure provisioning prevents key exposure and overbuild
- Approach is scalable across secure FPGA deployments

Q & A

Thank you

Questions?