

TrustChain™ Pending

Identity Based Lifecycle Management for the IoT Supply Chain

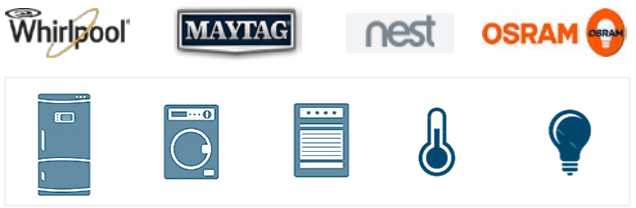
New Ventures of Mentor, a Siemens Business

Unrestricted © Siemens DI 2018

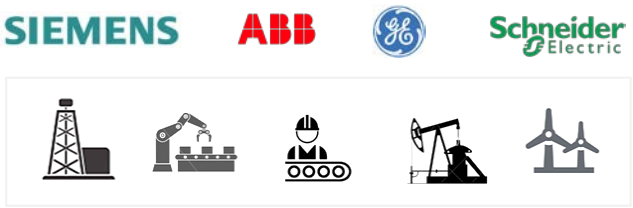
Smart-Connected Product Supplier Economics



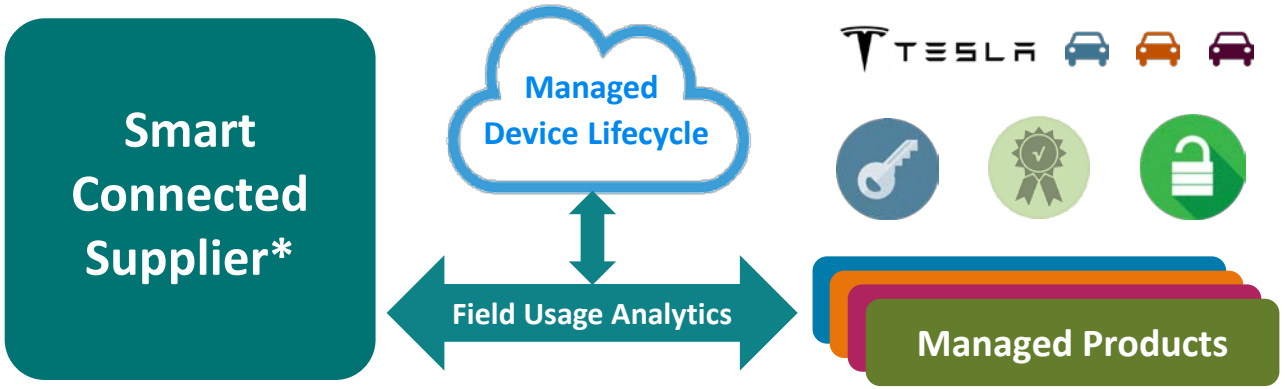
Established Connected Devices



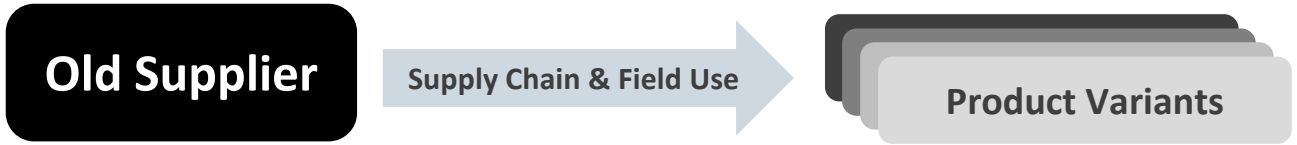
Evolving Connected Devices



Emerging Connected Devices



- Better visibility on product field use
- Remote lifecycle management
- Reduced support costs and RMAs
- Lower OPEX, higher differentiation
- New services and business models
- **Trust, security and safety issues**

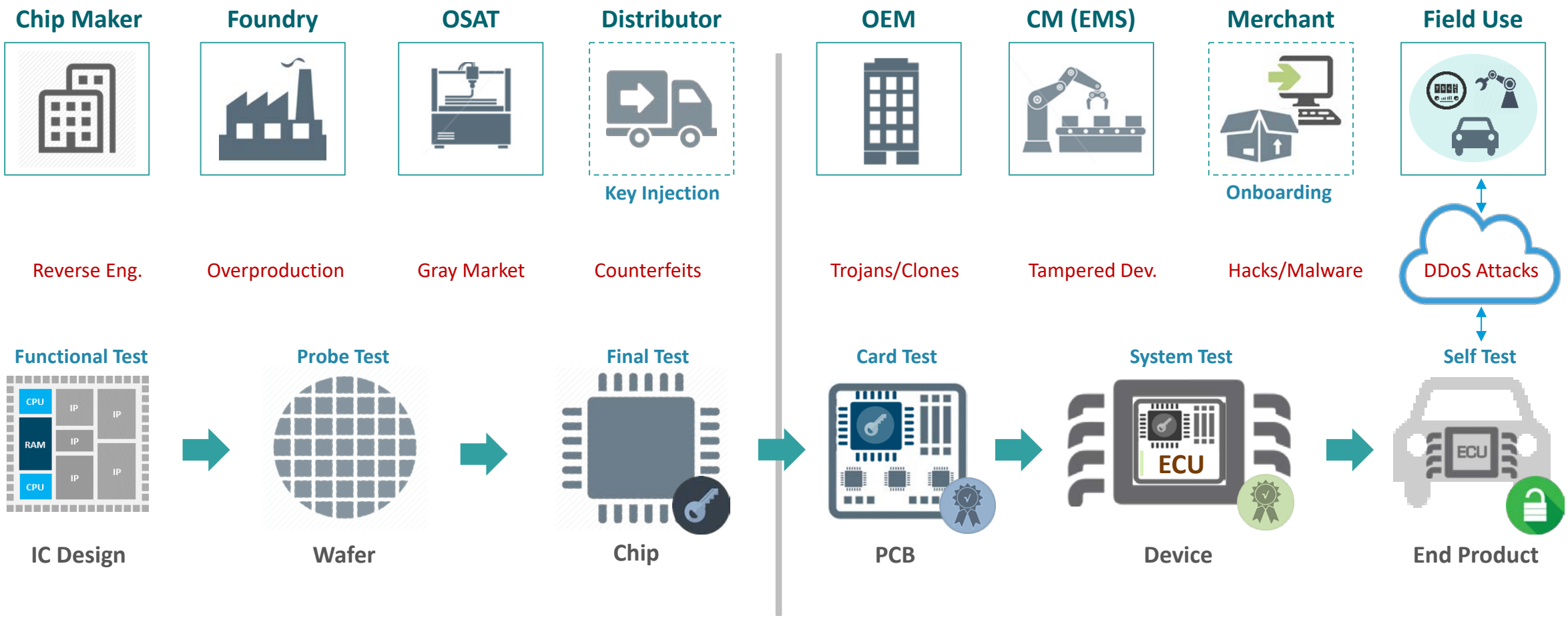


- No traceability or configurability
- High OPEX, low differentiation

*Source: Harvard Business Review

Unrestricted © Siemens DI 2018

Device Lifecycle Security & Trust in Digital Supply Chain



Can we trust a system and its parts from multiple suppliers in the supply chain?

Unrestricted © Siemens DI 2018

Security & Trust Issues - Fragmented IoT Supply Chain

Connected Things
Wearables, Homes, Cities, Industrial, Automotive, Transportation, Health Care

Applications & Services				
Device OS+Apps	**Enterprise Integ**	**IoT Platforms**	**Connectivity**	**Vertical Sol.**
Apple, Google, Microsoft	IBM, HP, Cisco, Accenture, PwC	Siemens, GE, ARM, Windriver	AT&T, Verizon, Vodafone	ADT, Comcast P&E, DIRECTV

Vertically Specialized Systems		
Embedded Systems	**Smart Industrial**	**Connected Cars**
Thales, Telit, Sierra Wireless	Schneider, GE, Siemens,	Bosch, Delphi, Denso, Yazaki

Networking Infrastructure		
Backbone (Routing/Optical)	**Access (Cellular/Wi-Fi**	**Security (Network, Edge)**
Cisco, Juniper, Alcatel, Google	Cisco, Ericsson, Nokia, Netgear	Equinix, Argus, Duo, …

Semiconductors & Components				
Comm ICs	**Processors**	**MCUs & Analog**	**Sensors**	**Storage**
Qualcomm, Broadcom	Intel, ARM, Qualcomm	Renesas, STM, Microchip, NXP	InvenSense, TI, Maxim	Micron, WD, Marvel, Hynix

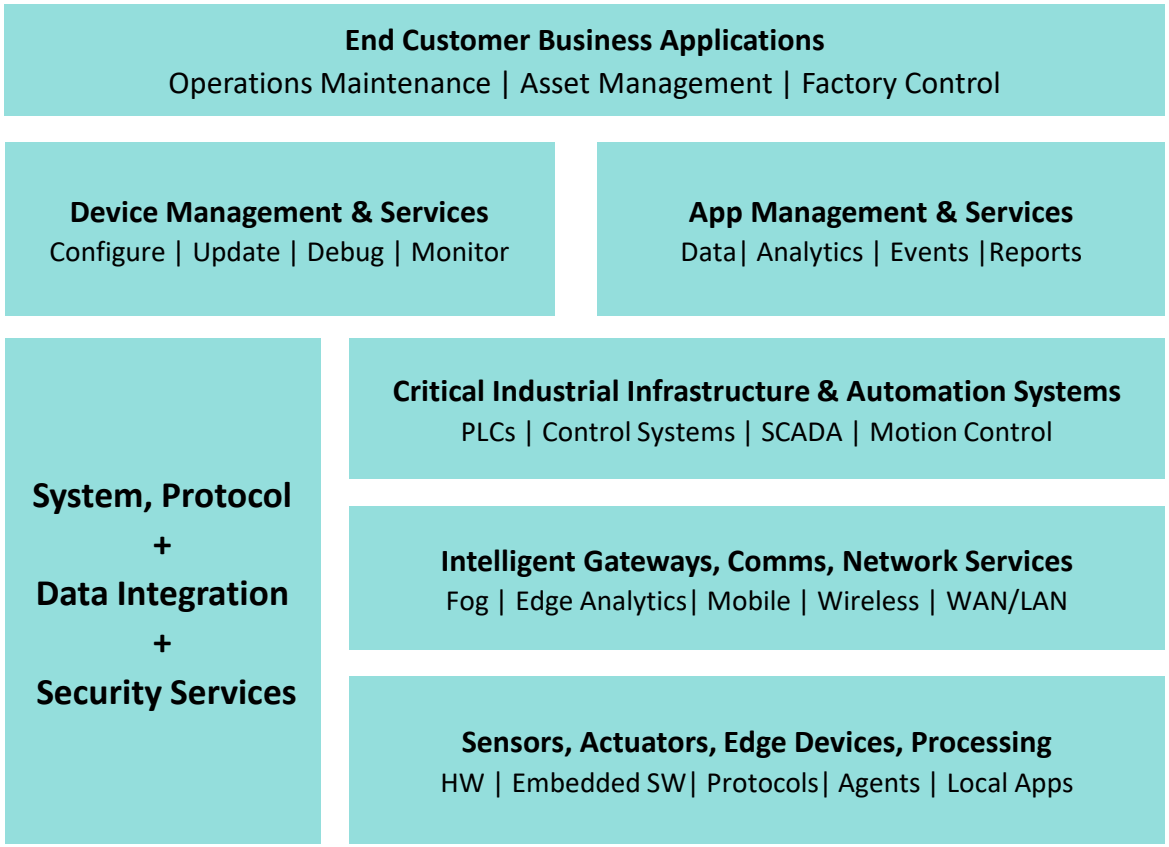
- Multiple Verticals, Varied Profiles
- Several Actors in the Value Chain
- Disparate Rules Among Suppliers
- Rebranded Low Cost Hardware
- No Economic Incentive for Security
- Untrusted Device Vulnerabilities

The roots of security issues lie in the structure of the electronics industry at large

Unrestricted © Siemens DI 2018

*Sources: Goldman Sachs, McKinsey, and others

Security & Trust Issues - Complex System & Parts



- Growing Attack Surface in System
- Breaches Impact All Suppliers
- Costly to Identify Root Causes
- Limited Knowledge Base on Attacks
- Untraceable Chain of Liability
- Critical Infrastructure Threatened

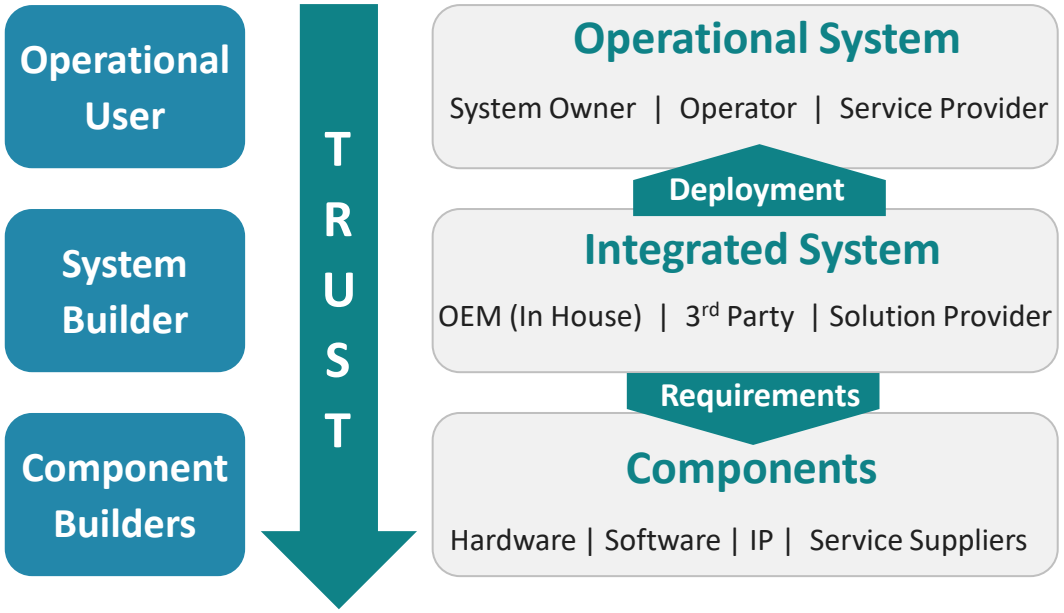
Vast attack surface making it extremely difficult to track down intrusions & hacks

Unrestricted © Siemens DI 2018

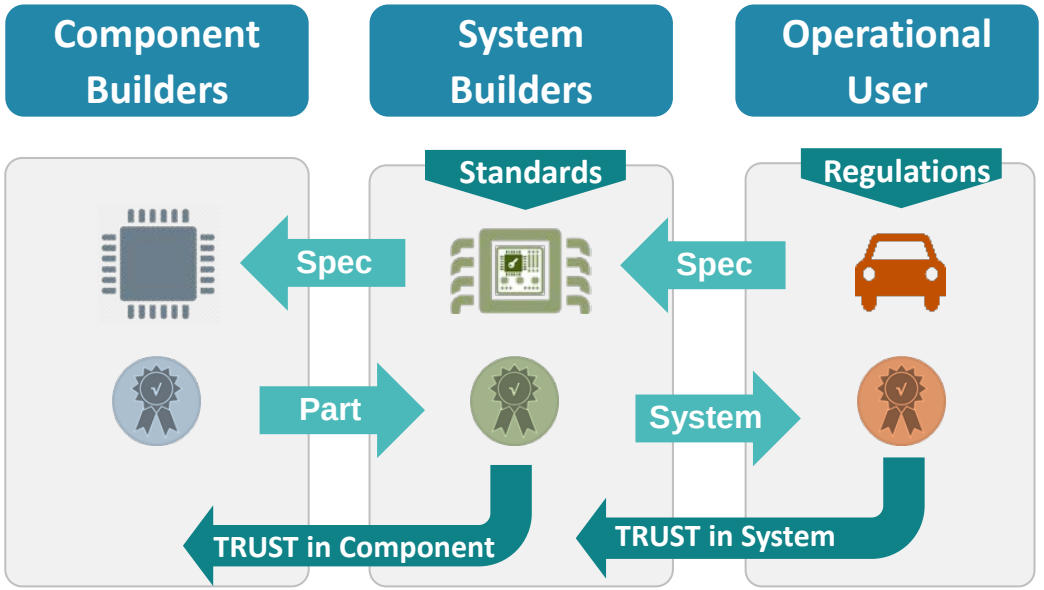
*Sources: Goldman Sachs, McKinsey, and others

Evolving Trust in Complex Supply Chains

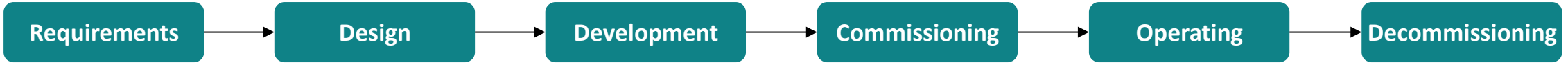
Trust Flow - Starts top-down, evolves bottom-up



Permeation of Trust - Assurance & Credentials



Device Lifecycle - Each part the system and supply chain must be monitored to preserve trustworthiness



Unrestricted © Siemens DI 2018

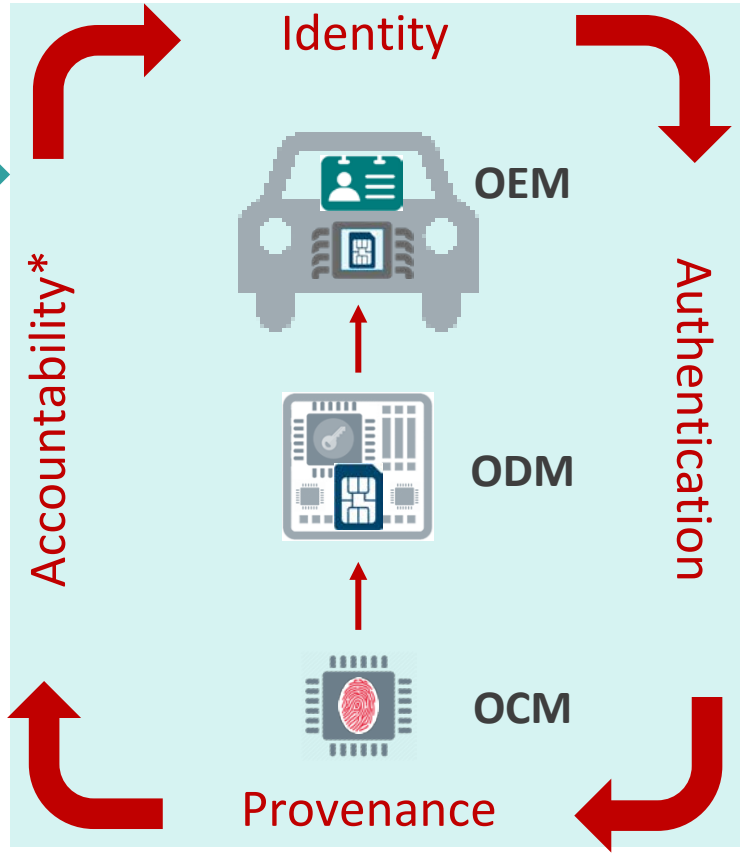
*Source: www.iiconsortium.org Internet of Things Volume G4: Security Framework

Charter of Trust and the Digital Supply Chain



www.charter-of-trust.com

1. Ownership of cyber and IT security
2. Responsibility throughout the digital supply chain
3. Security by default
4. User-centricity
5. Innovation and co-creation
6. Education
7. Certification for critical infrastructure and solutions
8. Transparency and response
9. Regulatory framework
10. Joint initiatives

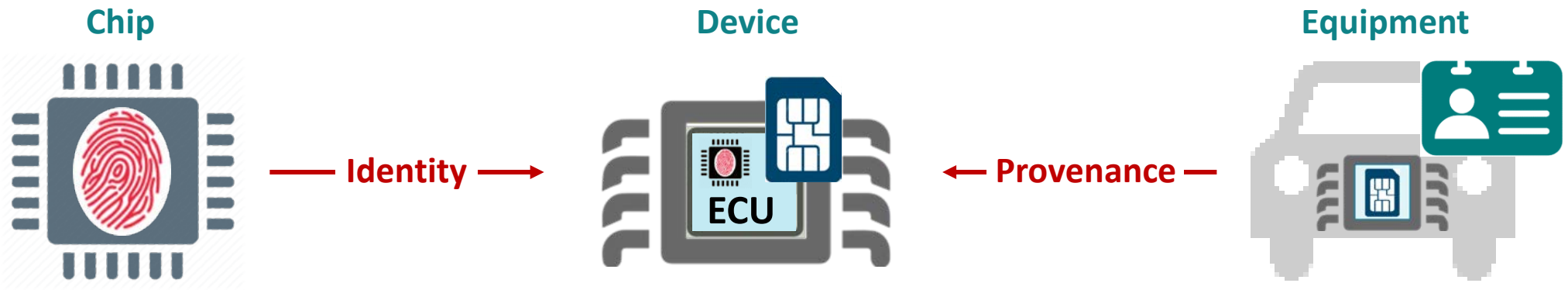


Trusted identity and provenance are key for accountability* in the supply chain

Unrestricted © Siemens DI 2018

*Source IDC: European IoT Security Why the IoT Supply Chain of Trust Matters

Identity Driven Lifecycle Management Strategy



TrustChain IP + TrustChain APIs + IC Partner

IC Design → Fab - OSAT → Distribution

TrustChain APIs + Valor + IC + OEM/ODM

System Design → Assembly → Delivery

MindSphere Services (MindApps)

Onboarding → Operating → Recycling

Traceability - Monitoring



- Establish Accountability and Trust
- Enable Identity-driven Services
- Improve Quality, Security, Safety

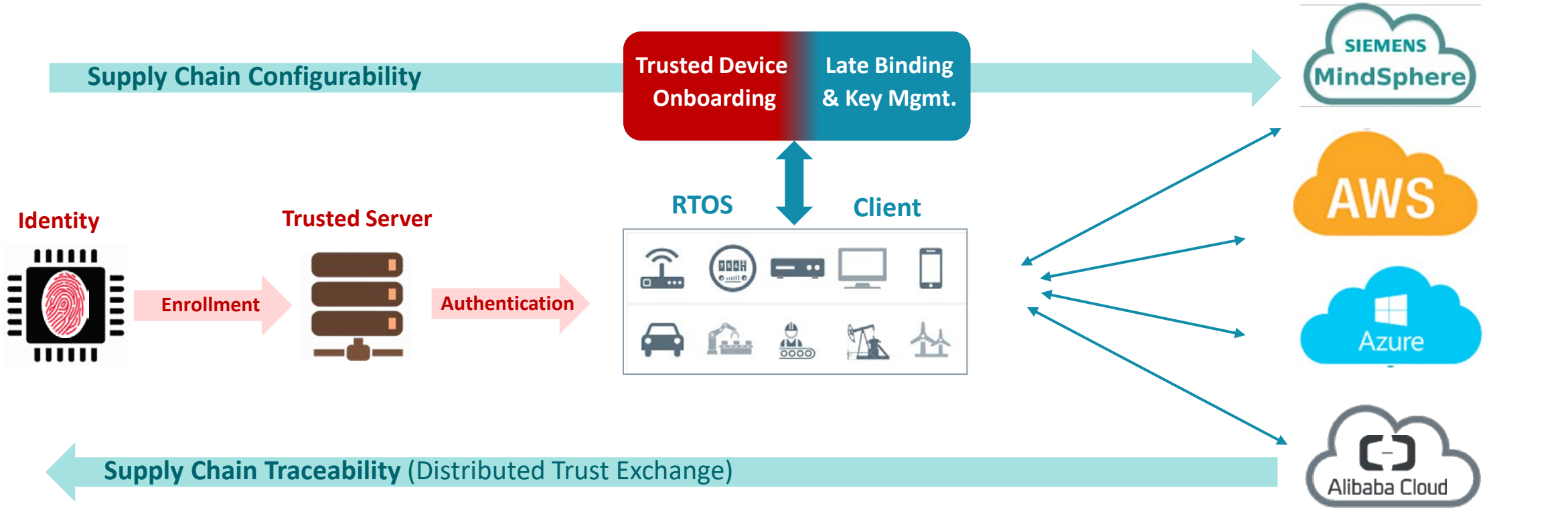


Configurability - Provisioning

- Simplify Personalization and Onboarding
- Securely Manage SKUs, Updates, RMAs
- Enable Higher Value Business Models

Unrestricted © Siemens DI 2018

Foundation for Trusted End-to-end Supply Chain Solution



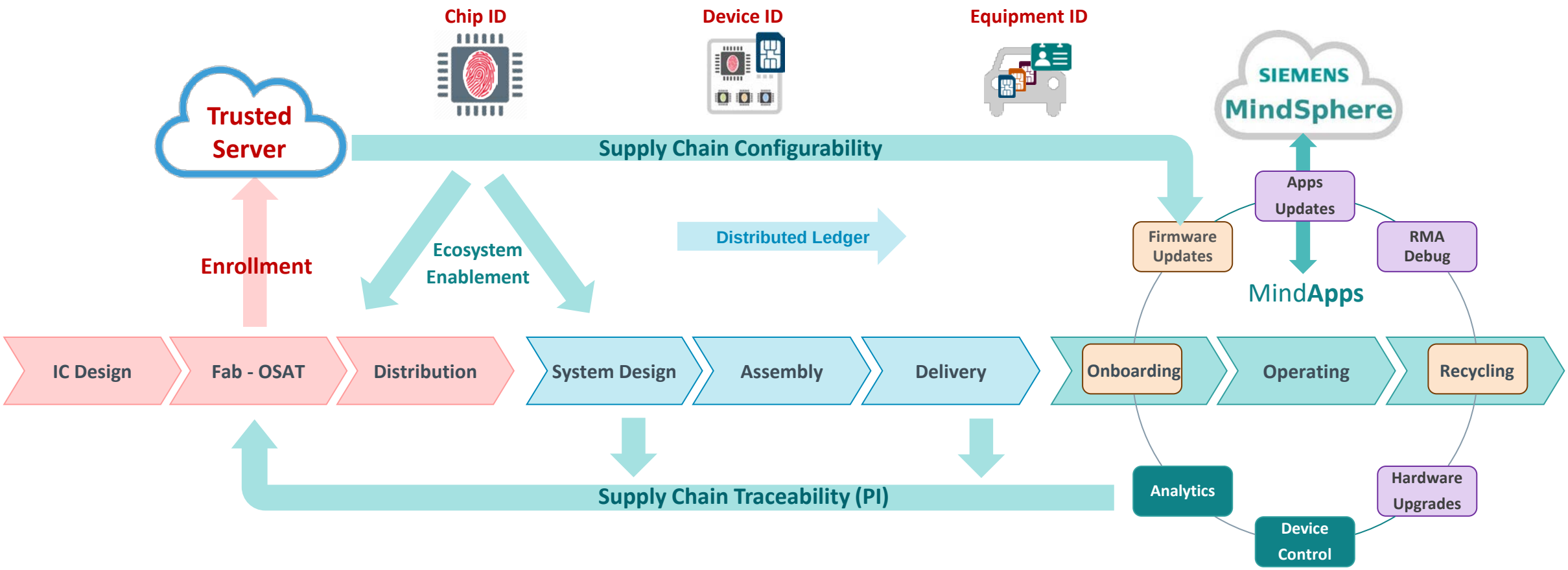
Ecosystem Enablement
Authentication, Provisioning, …

Connectivity, & Device Management
Firmware, Protocols, Applications,…

Data & Lifecycle Management
Field Operations & Services

Unrestricted © Siemens DI 2018

Identity Driven Lifecycle Management Strategy



Services

- Chip Authentication
- Chip Feature Provisioning
- Chip Authenticity Certification
- Key injection (Untrusted Facility)
- Firmware Injection (Untrusted Facility)
- Generic Data Injection / Extraction
- Identity-driven Device Onboarding
- OTA Firmware and App Updates
- RMA Debug (incl. IC Access Grant)

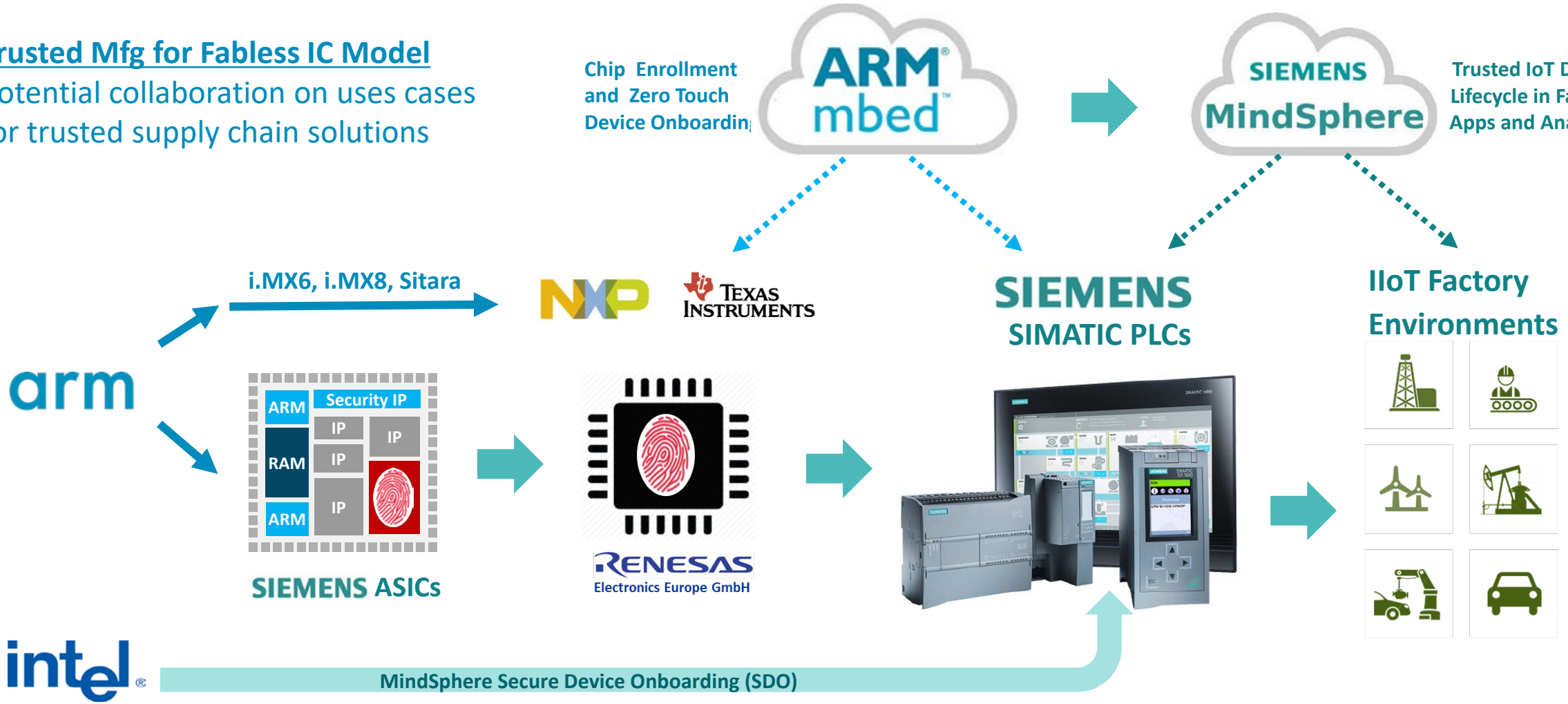
IC Partners | ODMs - OEMs | Siemens

Unrestricted © Siemens DI 2018

Siemens Digital Factory - Trusted PLC Supply Chain

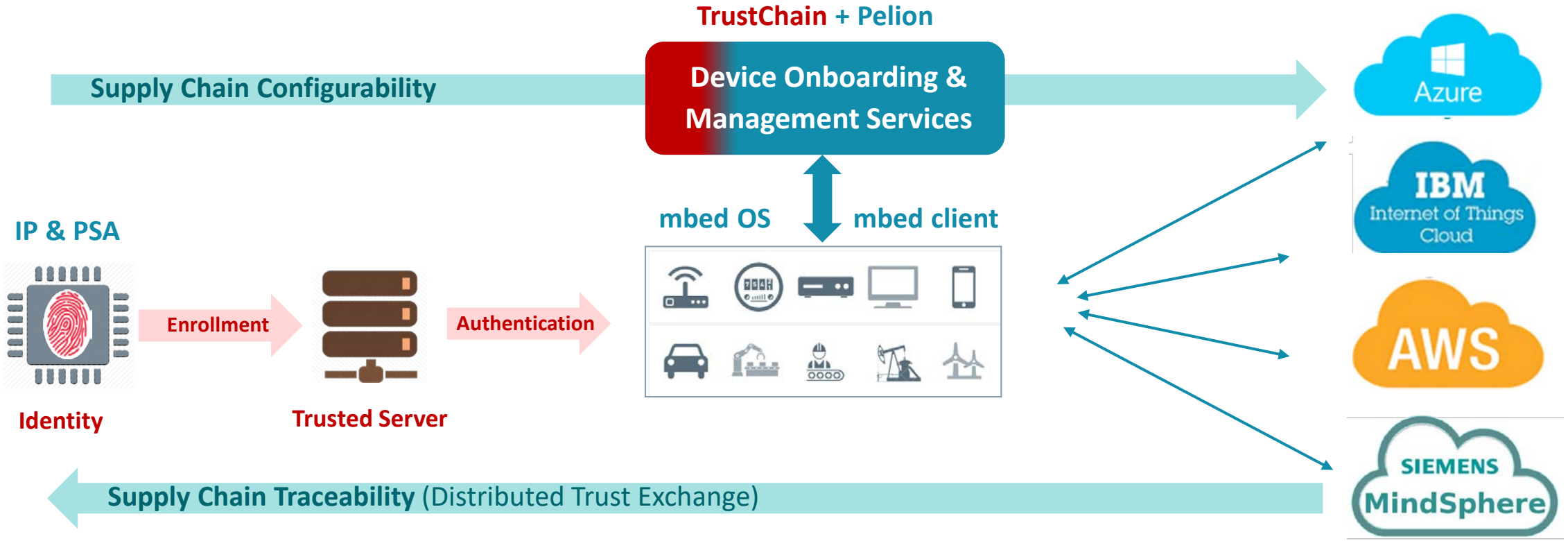
Trusted Mfg for Fabless IC Model

Potential collaboration on uses cases for trusted supply chain solutions



Restricted © Siemens AG 2018

Siemens & ARM Synergies for Trusted End-to-end Solution



Ecosystem Enablement
Authentication, Provisioning, …

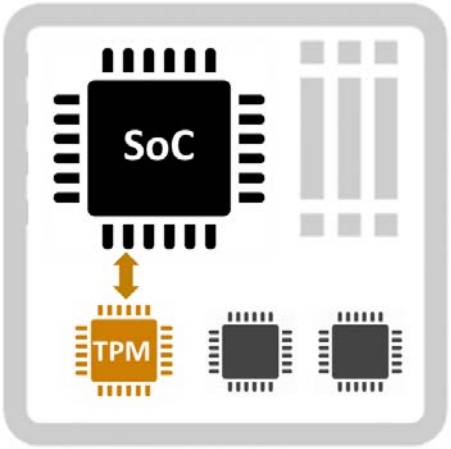
Connectivity, Device, Data Management
TLS, Firmware, Applications, …

Lifecycle Management
Trusted Field Operations

Unrestricted © Siemens DI 2018

Trusted Identity and Device Lifecycle Management

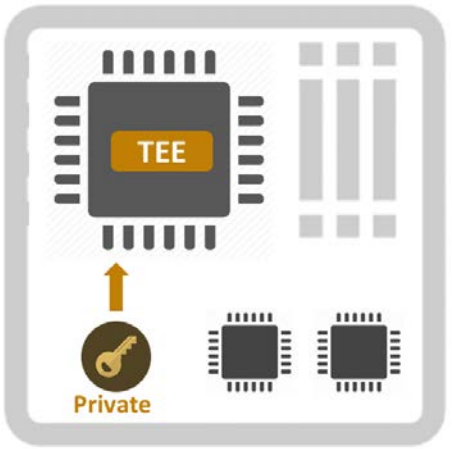
TPM Identity



*Trusted Platform Module

- Simple PCB Device ID
- BOM Cost (Extra ASIC)
- Can be compromised

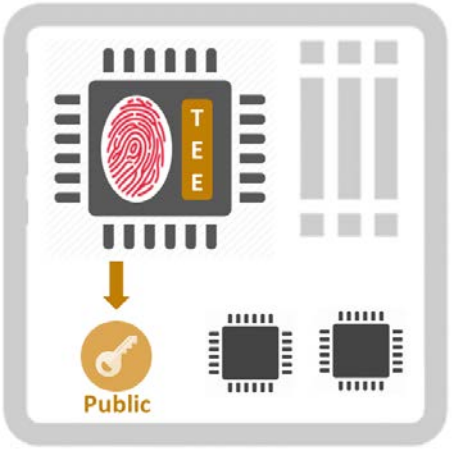
Inserted Identity



*Fused or Injected Secret

- ID Embedded in Chip
- Trusted Execution Env
- Can be tampered/cloned

Inborn Identity



*No Secret at Rest (power-off)

- ID based on Mfg process
- Trusted Execution Env
- Physically Unclonable

Enabled Services & Apps

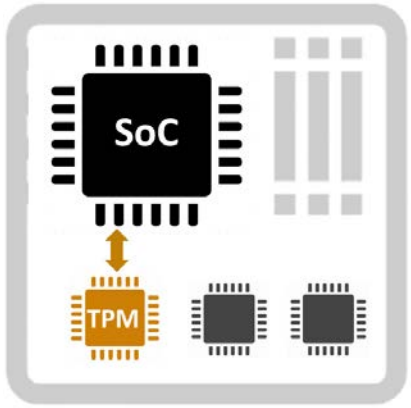
- Tracking Device Shipments
- Multi-actor Chain of Custody
- Installation and Onboarding
- Device & Service Activations
- Usage Rights and Privileges
- Device and App Management
- Parts Origin and Provenance
- Security Chain of Liability
- End-of-life, Revocations

Inborn identity provides an immutable root of trust for the IoT supply chain

Unrestricted © Siemens DI 2018

Root-of-Trust based Identity for Enabling Chain of Trust

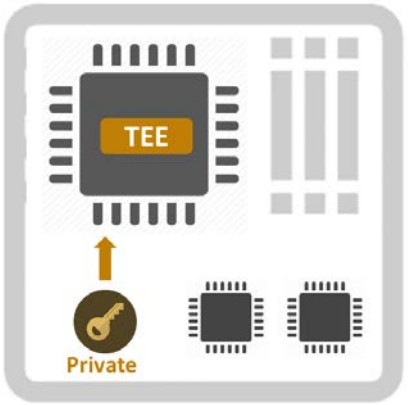
TPM Identity



*Trusted Platform Module

- Simple PCB Device ID
- BOM Cost (Extra ASIC)
- IC can be compromised
- No Chip Traceability

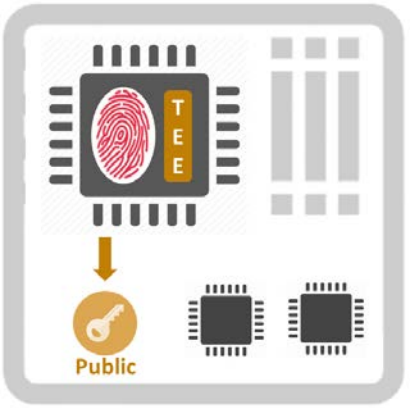
Inserted Identity



*Fused or Injected Secret

- ID Embedded in Chip
- Trusted Execution Env
- Can be tampered/cloned
- No Parts Traceability

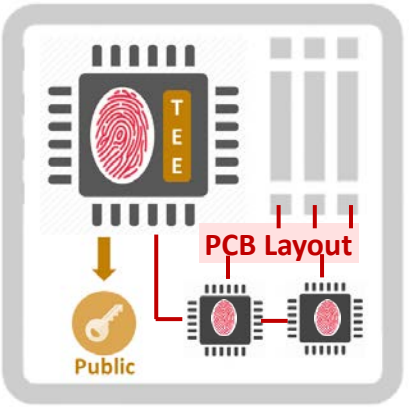
Inborn Identity



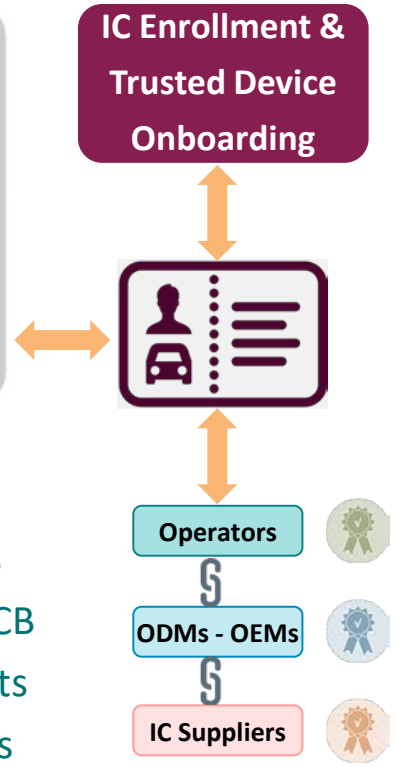
*No Secret at Rest (power-off)

- ID from Mfg process
- TEE and Secure Enclave
- Physically Unclonable
- PCB Can Be Hacked

Unified Identity + Trusted Partners



*ID linked to Ownership (PO)



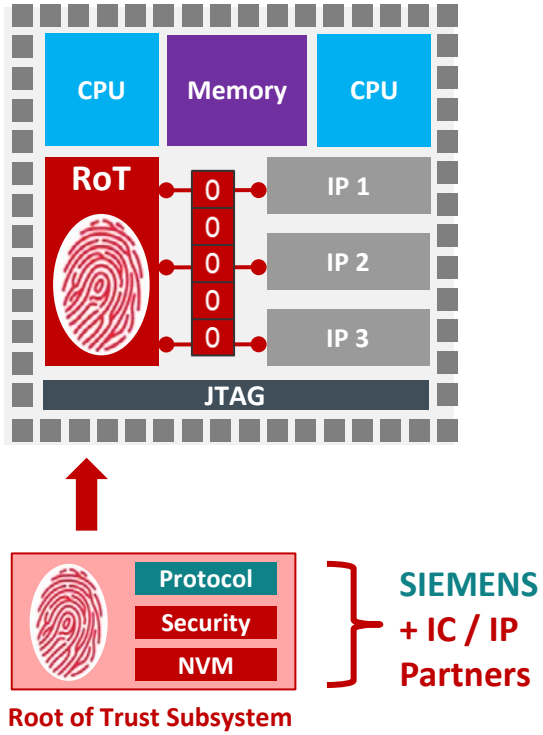
- Derived ID from all ICs
- ID factoring BOM in PCB
- Certified Device & Parts
- Trusted Suppliers Links

Inborn identity coupled with traceability infrastructure and trusted value chain

Unrestricted © Siemens DI 2018

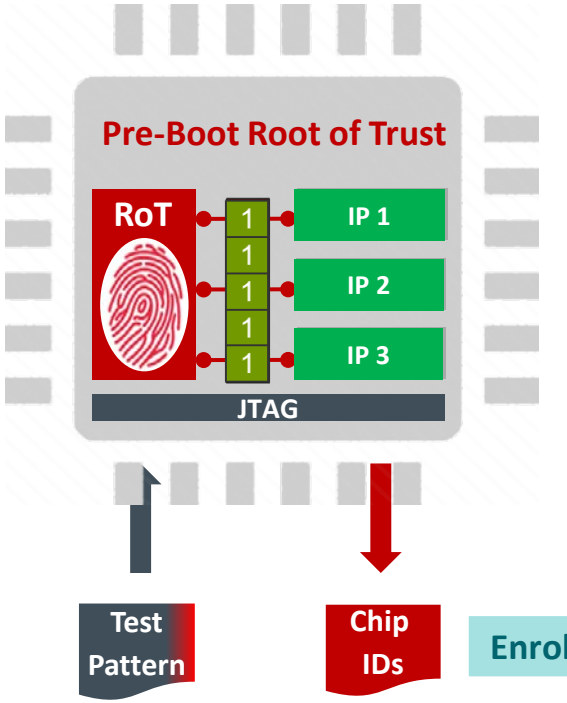
Foundation for a Trusted Value Chain

Chip Design



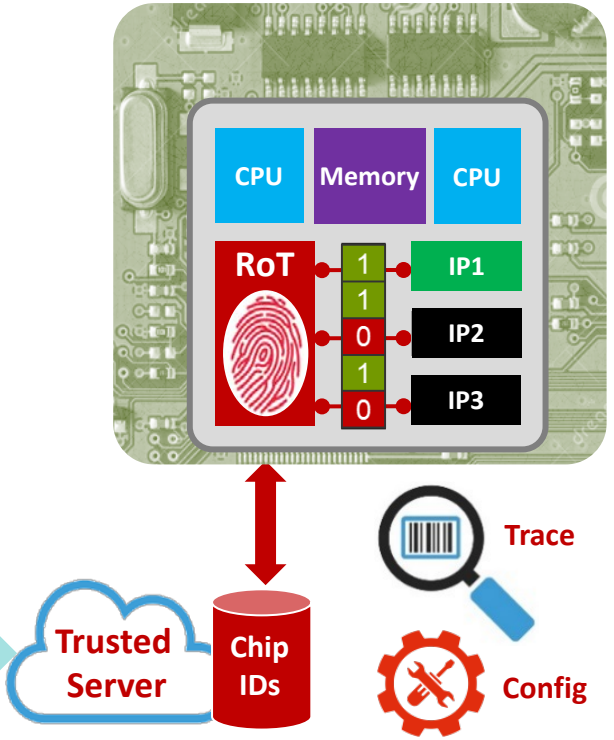
Embed Root of Trust

Manufacturing



Activate & Enroll

Field Use

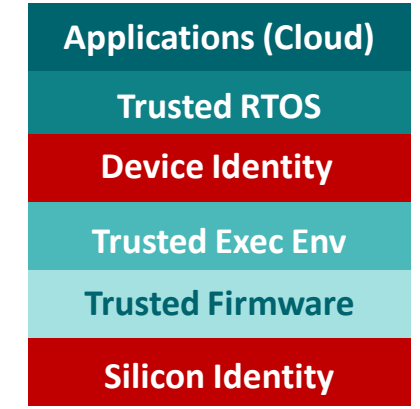


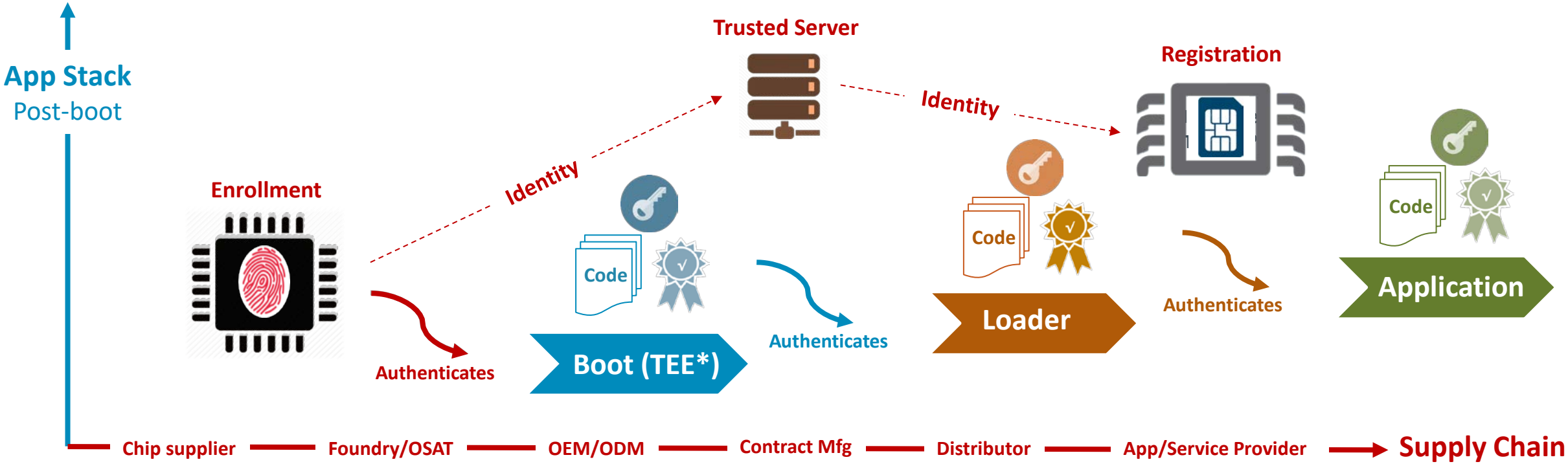
Monitor & Provision

Unrestricted © Siemens DI 2018

Root of Trust and Chain of Trust

- **Identity** is used to confirm **authenticity** and **personalization** (late binding)
- Secure Boot uses crypto to confirm authenticity of firmware before running
- A multi-stage boot process consists of each stage authenticating the next



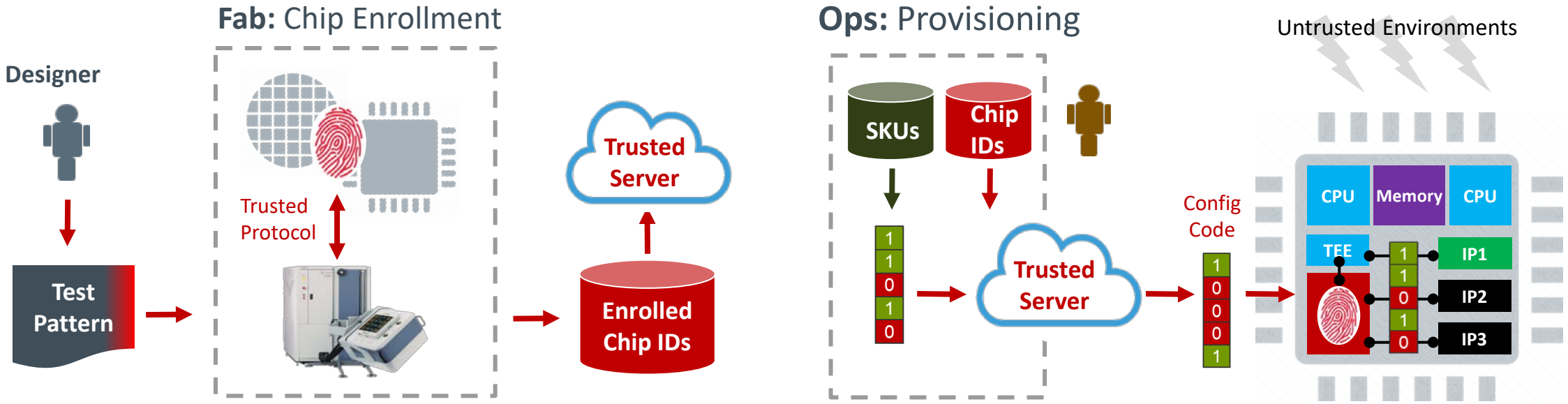


*TEE: Trusted Execution Environment and Boot Sequence (Sources: ARM & ST Microelectronics)

Unrestricted © Siemens DI 2018

PUF* is a Key Technology for Inborn Identity

PUF: Physically Unclonable Function



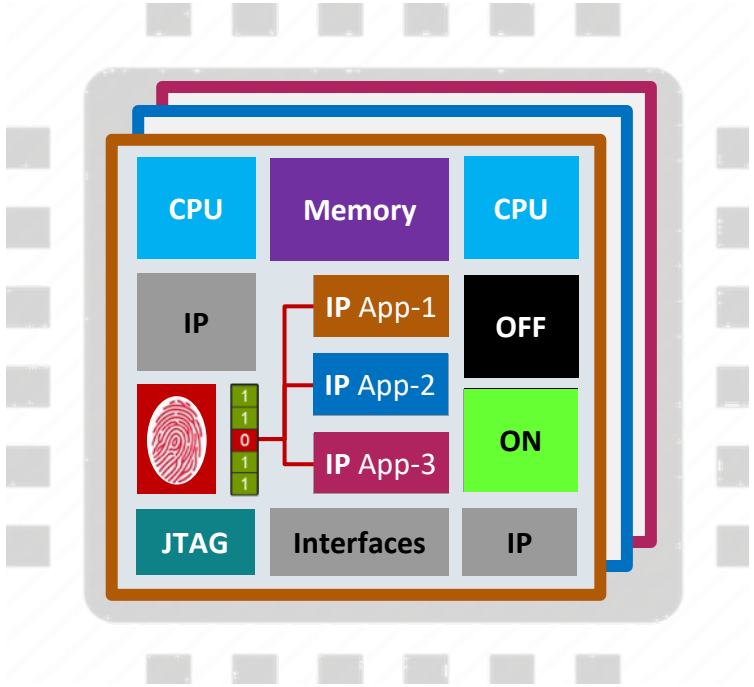
- **Trusted Foundry:** Inborn chip ID tied to mfg process
- **No Secret at Rest:** Identity exists only with power ON
- **Hard to Tamper:** Protected RoT hardware and protocol
- **Traceability + Authenticity:** Part No tied to chip ID
- **Unique Config per IC:** Features secured by chip ID
- **Field Provisioning:** Updates/Debug enabled by ID

Inborn silicon identity is essential for trusted IoT device lifecycle management

Unrestricted © Siemens DI 2018

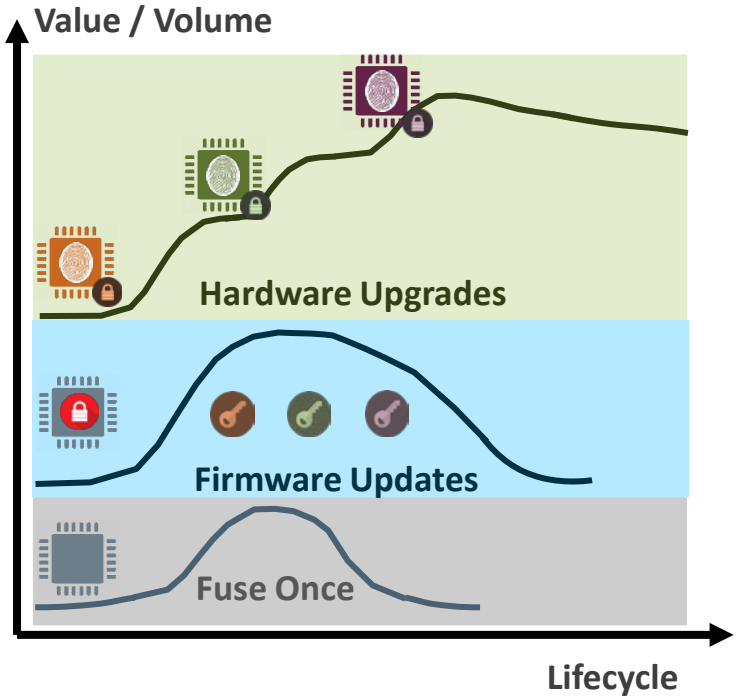
Enabling Trusted IC Partners to Increase Value

Configurable SoC → Higher Value



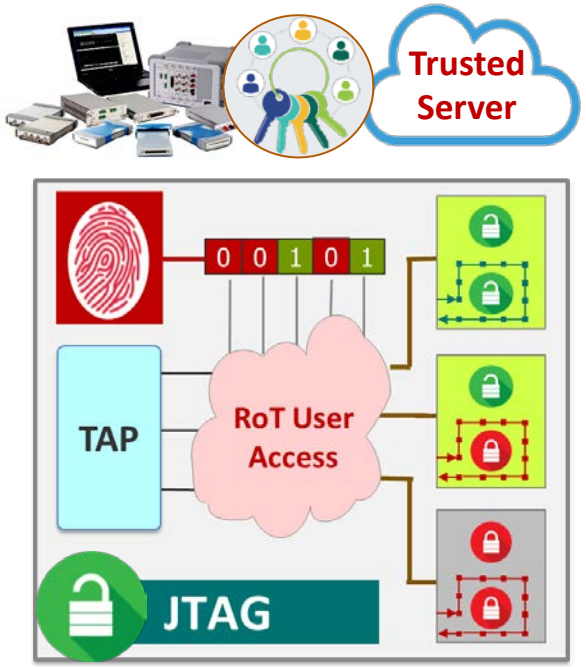
Lower Production Cost

In-field Provisioning → Better PLM



Hardware as a Service

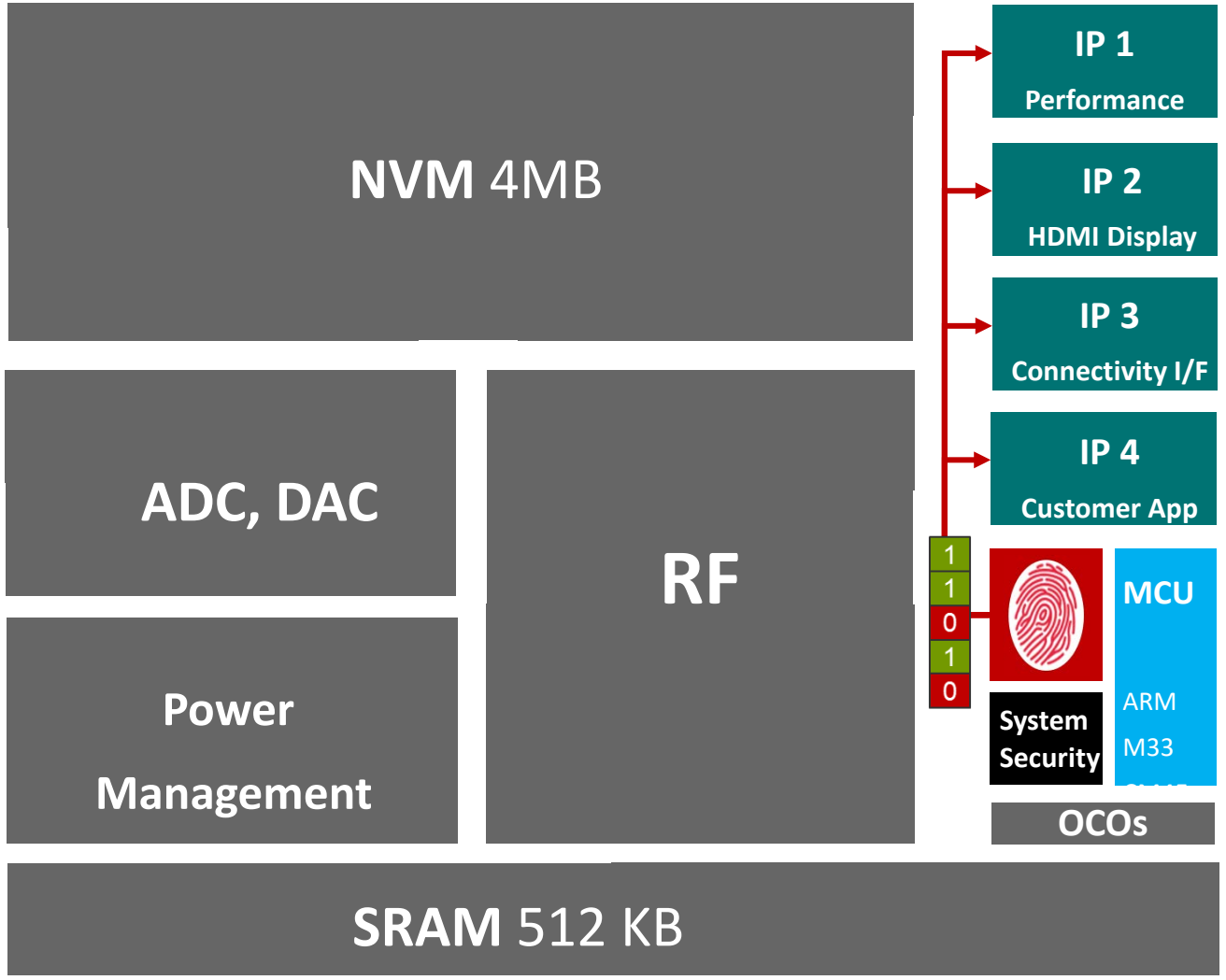
Secure Debug → Smarter RMA



Lower Support Cost

Unrestricted © Siemens DI 2018

Example - Fingerprint Configurable IoT ASSP



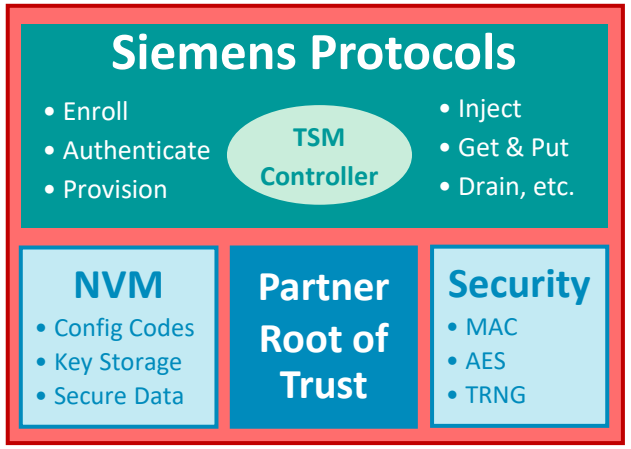
- **Superset ASSP for multiple verticals**
  - SKUs support several IoT customers
  - Traceable & configurable via fingerprint
  - Single mask set for multiple products
- **Enable in-field feature provisioning**
  - Modify SKUs for emerging markets
  - Support for multi-region products
  - Add memory as protocols increase
- **Enable Hardware-as-a-Service**
  - Start by selling low-end product
  - Upgrade later (CPUs, or other IP)
  - Add lifecycle management services

*Approx. 22 sqmm IoT ASSP for 22nm process technology

Unrestricted © Siemens DI 2018

Foundation for Trusted Lifecycle Management

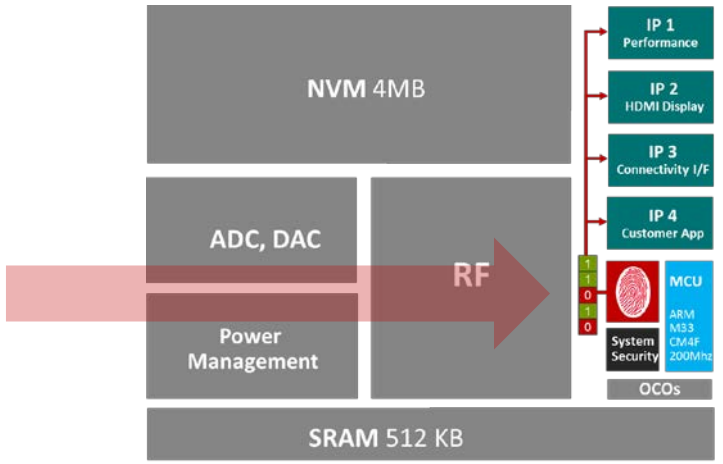
Trusted Silicon Module



*Partner and/or Third Party IP

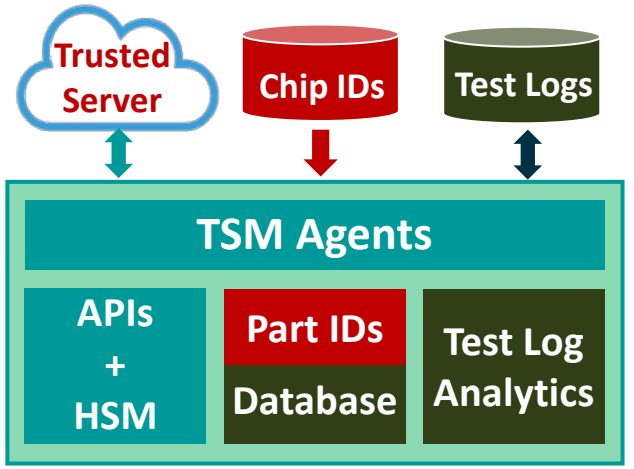
- Can support any Root of Trust
- Use partner NVM & Security IP
- Customized TSM Controller
- Utilizes **Siemens Protocols**

Configurable IoT ASSPs



- Standard IPs for IoT markets
- MCU and System Security
- Dedicated TSM Subsystem
- TSM-driven Config Register

Trusted Infrastructure

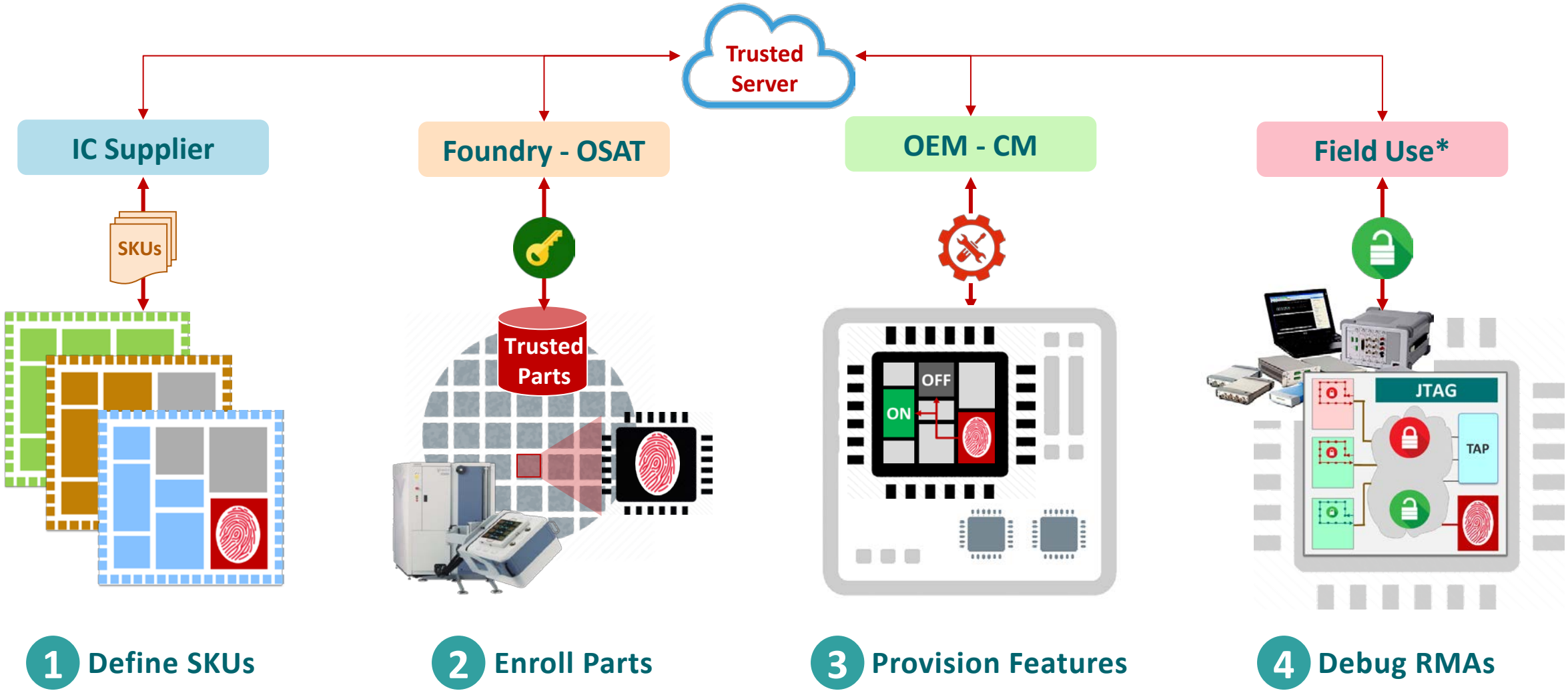


- ATE parsers, agents, APIs
- Chip Fingerprint Database
- Analytics Dashboards
- SKU Config Utility Tools

*RoT: Root of Trust

Unrestricted © Siemens DI 2018

Foundation Technology for IoT Supply Chain



*Connected IoT Device

Unrestricted © Siemens DI 2018

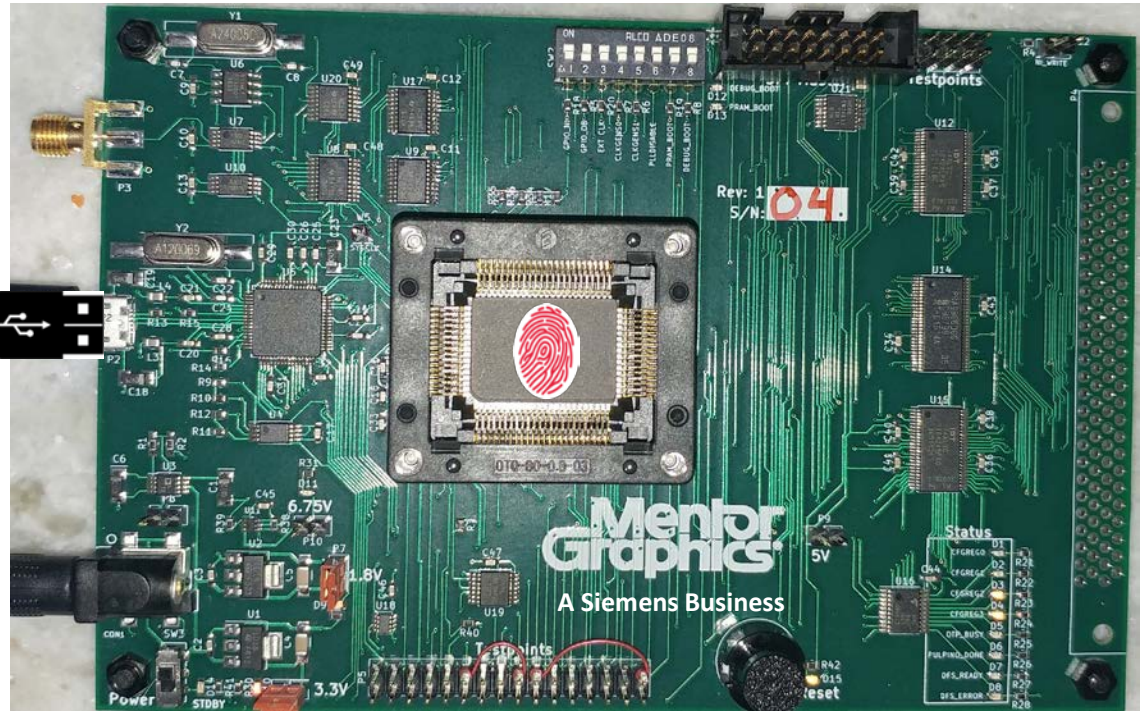
Foundation Technology Solution Demo

Software Infrastructure (Server & Supply Chain Agents) + Hardware Design (PCB + IC)

Supply Chain Agents

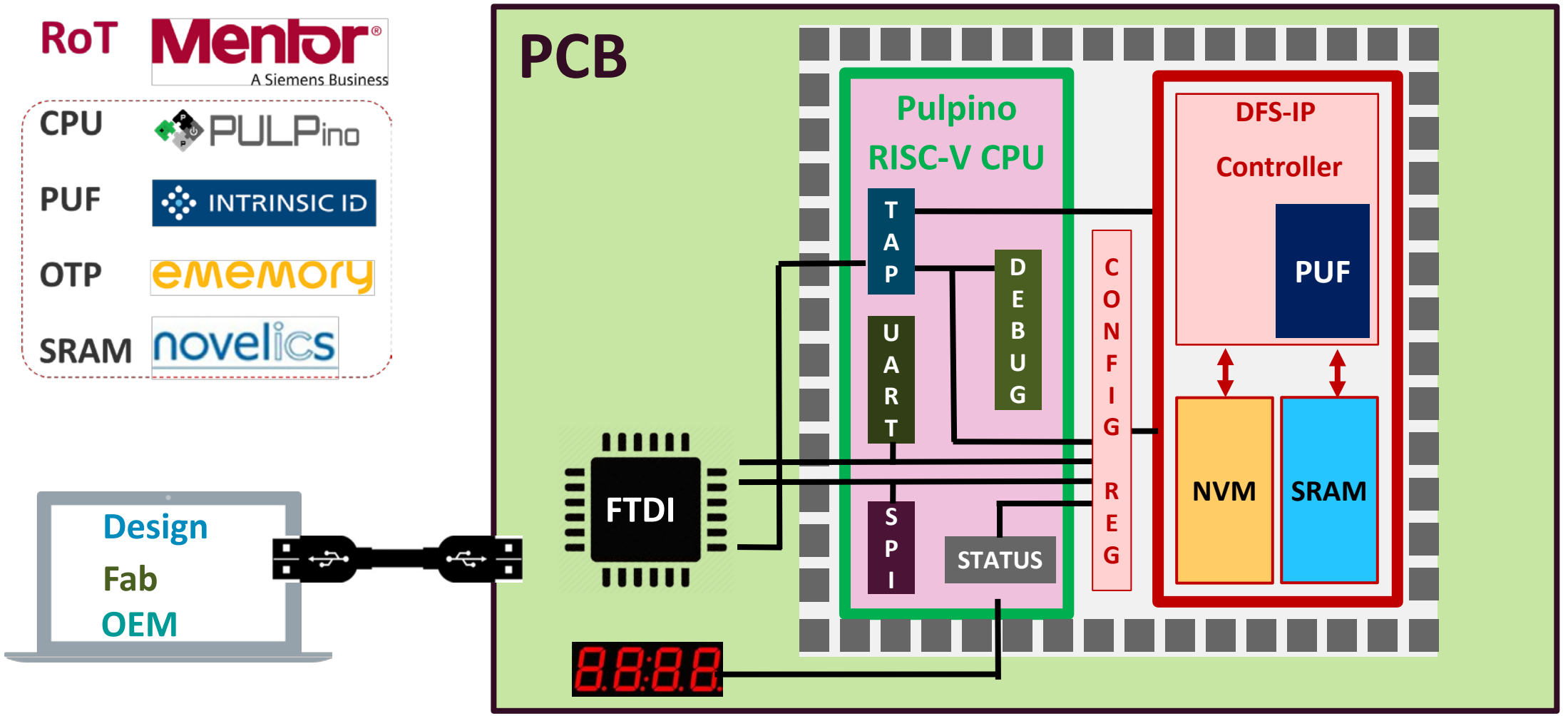


Demo Environment



Unrestricted © Siemens DI 2018

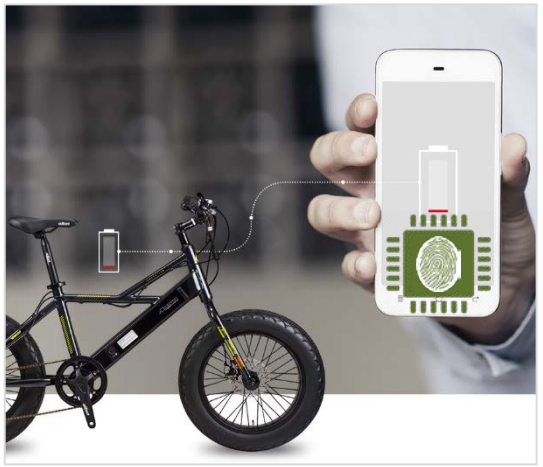
Test Chip with Root of Trust IP Subsystem



Unrestricted © Siemens DI 2018

Use Cases - Key & Feature Provisioning

Electric Bike



Offer differing charging speeds, distance and tracking service

Pet Tracker



Offer differing ranges (higher power GPS) & contract duration

Multi Market Product*



One SKU product supporting many standards provisioned on delivery

- Product performance can be increased
- Battery life can be extended (ala Tesla)
- RMAs can be diagnosed even inside chip
- Compromised systems can be disabled

Value

Remote Provisioning

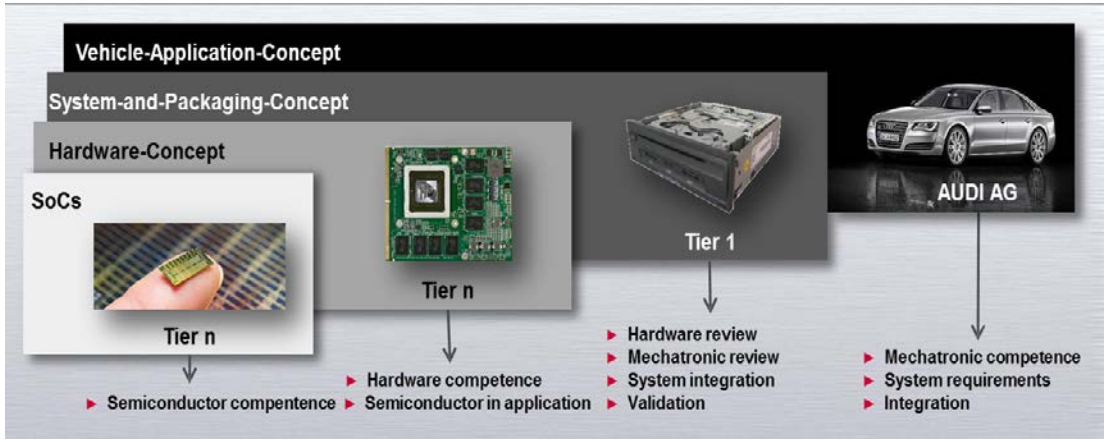
- Ease adoption of new products/services
- Reduce recalls with in-field diagnostics
- Enable Hardware-as-a-Service business
- Deactivate stolen/unauthorized products

*Assumes Managed IIoT Edge Devices

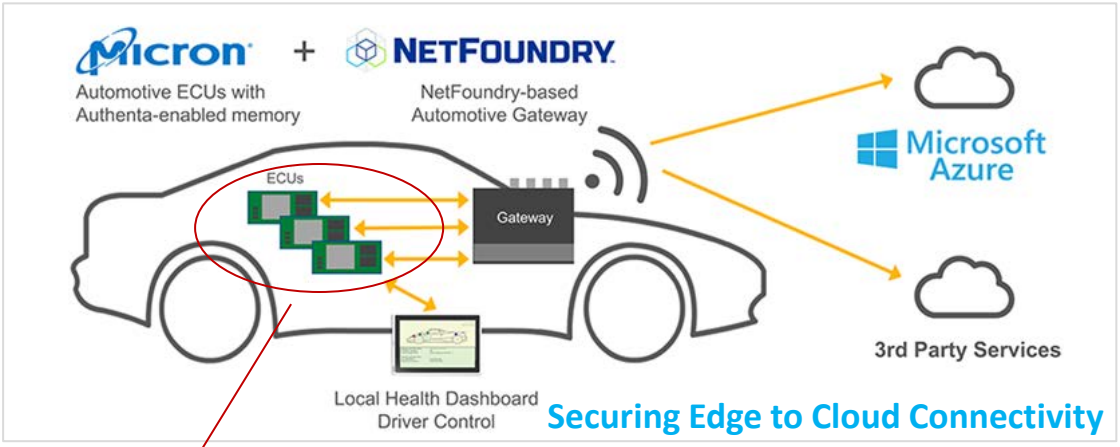
Unrestricted © Siemens DI 2018

Use Cases - Automotive Supply Chain Challenges

Quality & Reliability



Security & Safety



- 7,000 semiconductor ICs on a premium car
- 1ppm failure rate = 7 failures for 1,000 cars
- 4,000 cars build per day = 1 failure per hour*
- Production failures plus electronics failures

- **Supply Chain Security**
  - Authorized Distributors
  - Continuity of Supply
- **Counterfeit Chips in**
  - ECUs & ABS Systems
  - Airbag& Cruise control
- **Over the Air Updates**
  - Firmware Changes
  - Keys and Certificates

- Many publicized hacks, millions of recalls
- Vulnerabilities from 100s of ECUs per car
- Gray market, clones, or counterfeit ICs
- Gb of data / day / car can be compromised

Source: Automotive Megatrends, Challenges and Solutions , SEMICON Europa 2015, Dresden

Unrestricted © Siemens DI 2018

Example - Automotive Supply Chain End-to-End Solution

Traceability
Supply Chain Analytics

Trusted Services

Configurability
Provisioning and Updates

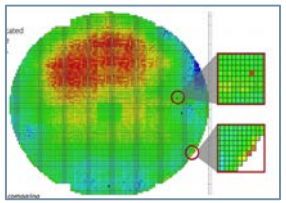
IC Supplier

Ops SKU Db

Trace where issue occurred



Predict Field Performance



Enrollment

Chip IDs

Test Logs

Foundry

Test Logs



Probe Test



OSAT

Test Logs



Final Test



Distributor

Inject Logs



Key Injection



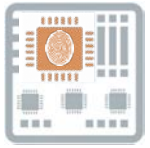
Trusted Protocol

OEM/ODM

Ops SKU Db



PCB Test



CM (EMS)

BOM + Test



System Test



Field Use

IoT Platforms



Self Test



Chain of Custody
Distributed Ledger

Supply Chain Monitoring and Certification

• Engineering • Operations • Production • Procurement • Accounting

Unrestricted © Siemens DI 2018

Identity-based Lifecycle Management – Trusted Services

Chip Supply Chain

Manufacture
- Extract IDs at Probe Test
- Enroll Identities in Server
- Configure Debug Access
- Establish Traceability DB

Package
- Authenticate Supply
- Configure Chip SKUs
- Inject Application Keys
- Install SoC Firmware

Distribute
- Activate Chip Supply
- Update Firmware
- Contract on Asset Use
- Register IoT Asset

Assemble
- Built BOM Database
- Assemble / Test PCB
- Authenticate Parts
- Configure HW SKUs

Identity





Analytics*

Traceability

*Siemens Product Intelligence

SIEMENS MindSphere

MindApps*

Configurability

*ARM, Third Party, Siemens





Device Supply Chain

Deliver
- Configure HW Supply
- Install & Preset Device SW
- Contract on asset usage
- Onboard & Register Asset

Deploy
- Add Application Signature
- Distribute to App-Stores
- Config Access Permissions
- Config Security Policy

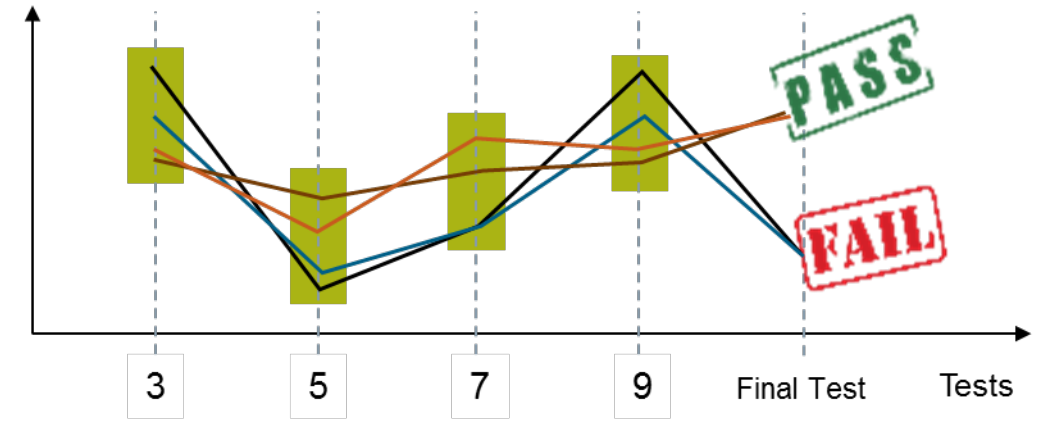
Operate (OTA)
- Monitor & Enforce Security
- Upgrade HW, Update SW
- Remote locking or clearing
- Report & Audit Assets

Decommission (OTA)
- Uninstall & Deregister Asset
- Reclaim/Clear Data & Keys
- Re-config and Re-bind HW
- Register & Redeploy Asset

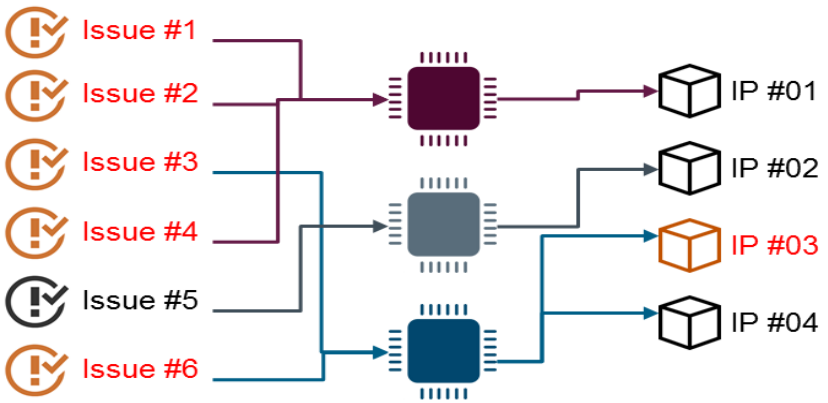
Unrestricted © Siemens DI 2018

Use Cases - Supply Chain Traceability

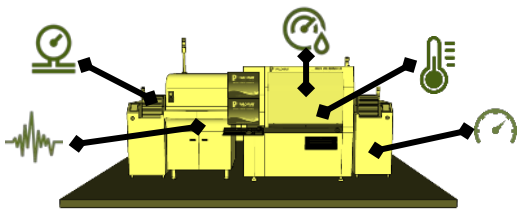
Why Did the Part Fail?



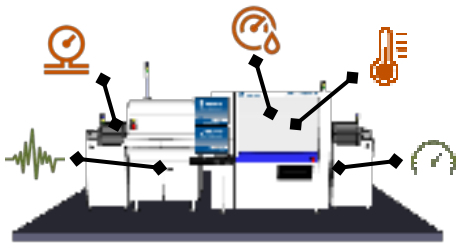
Which IP Contributed to Failure?



Why Production ATE did not work as expected?

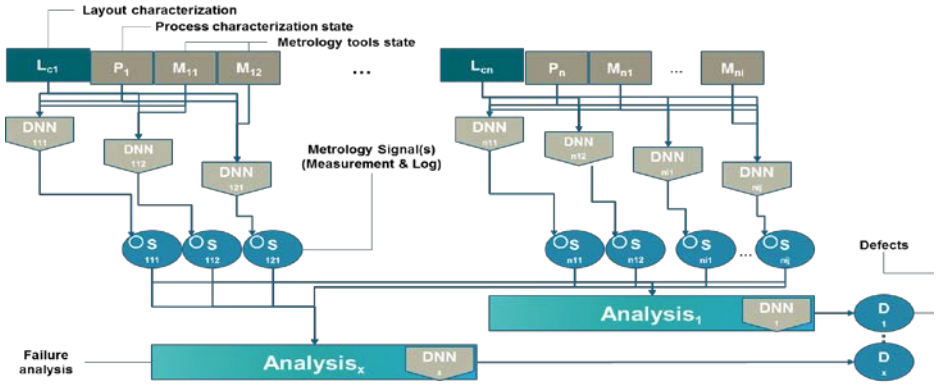


Pre-Launch ATE



Production ATE

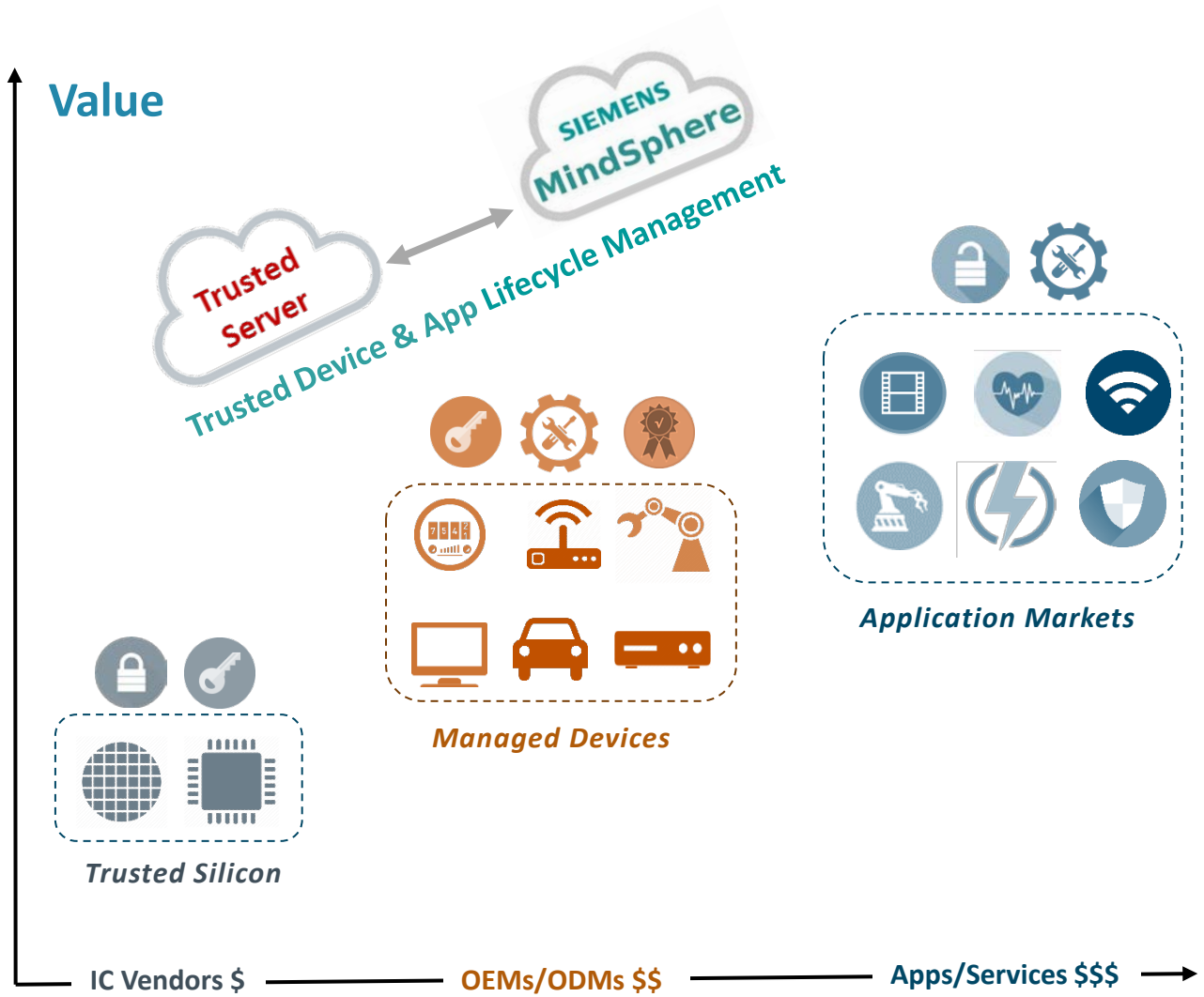
Can we use ML* Process/Defect Characterization?



*ML: Machine Learning

Unrestricted © Siemens DI 2018

Potential Evolution of Business Models

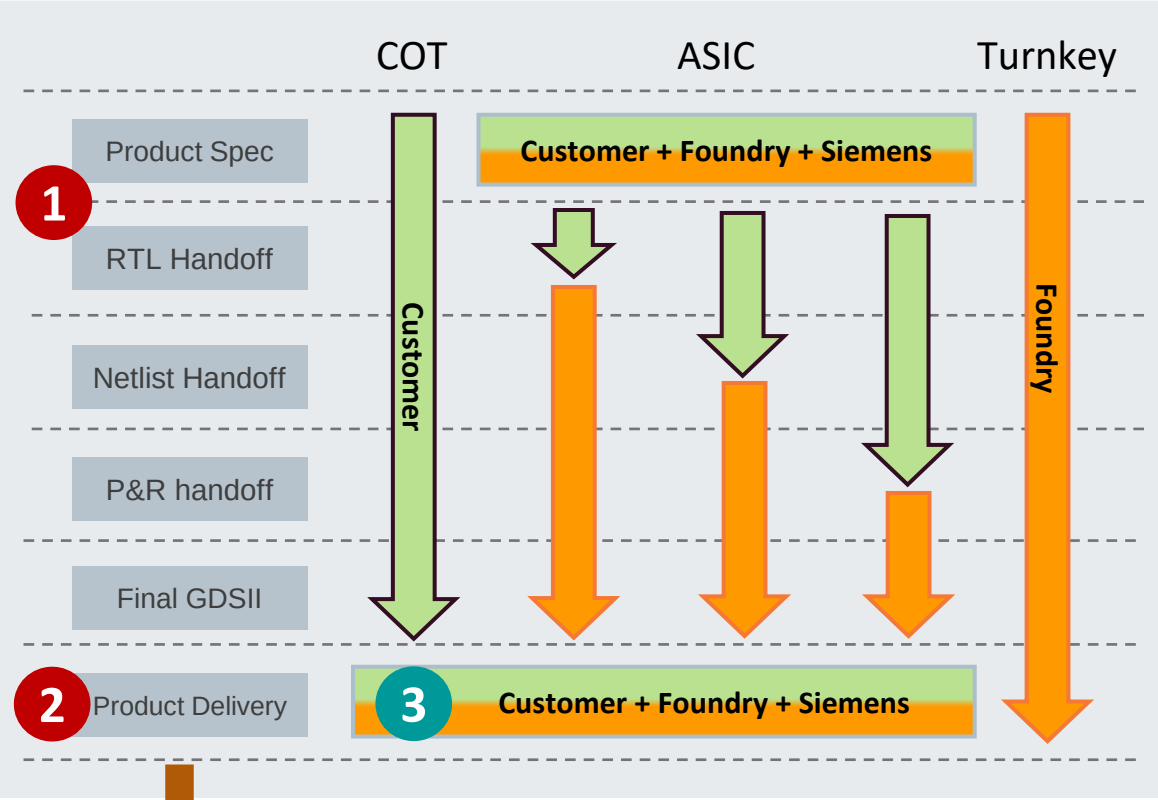


- **Enablement revenue streams**
  - Design Integration with IC Partner
  - Ops Integration with IC Partner
  - Keys injected to SoC paid by OEM
- **Per device services revenues**
  - Post-mfg chip provisioning service
  - Provisioning report to end customer
  - Services fees paid by end customer
- **Higher value business models**
  - Rev-share on Hardware-as-a-Service
  - Data analytics on quality and security
  - Trusted IoT device lifecycle services

Unrestricted © Siemens DI 2018

Evolving End-to-End Supply Chain Solution (Fabless Model)

IC Partner Engagement Models (with Foundry or IDM)



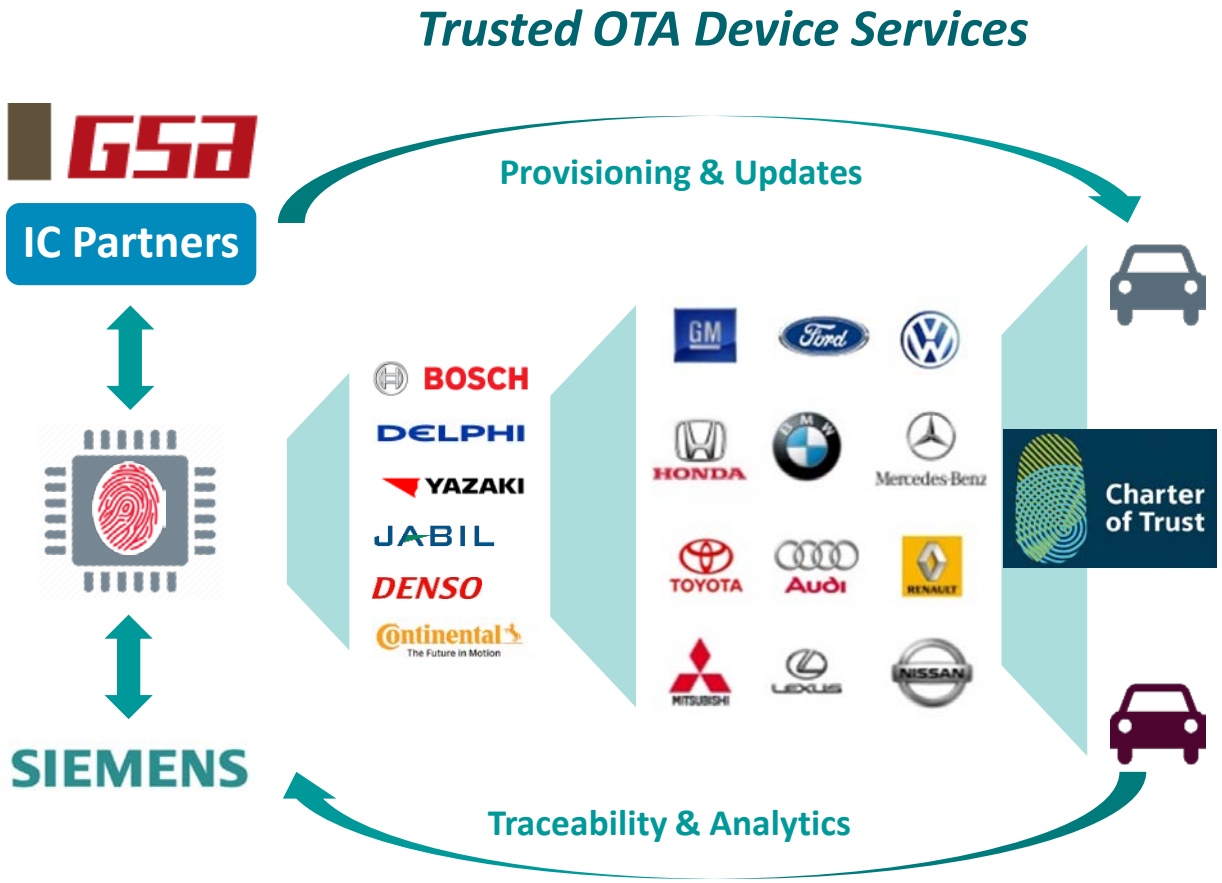
1. **IC Design Integration (TC Protocol)**
2. **IC Ops Integration (TC APIs)**
3. **Manufacturing Link (Quantix)**
4. **SubCon HSMs (Agents)**
5. **Distributor Partnerships (Data I/O)**
6. **Contract Mfg (Valor)**
7. **Field Use (MindSphere)**

Foundry - **GF** → OSAT- **Amkor** (4) → ODM - **Si-labs** → Distr - **Avnet** (5) → CM - **Jabil** (6) → Sys OEM - **Itron** → End User - **PG&E** (7)

Unrestricted © Siemens DI 2018

Evolution of Trusted Device Lifecycle Management

- Trusted Devices With Inborn Identity
- Field Traceability and Configurability
- Trusted Ecosystem Partnerships
- Authentication & Certification Process
- Identity Based Lifecycle Management



Unrestricted © Siemens DI 2018