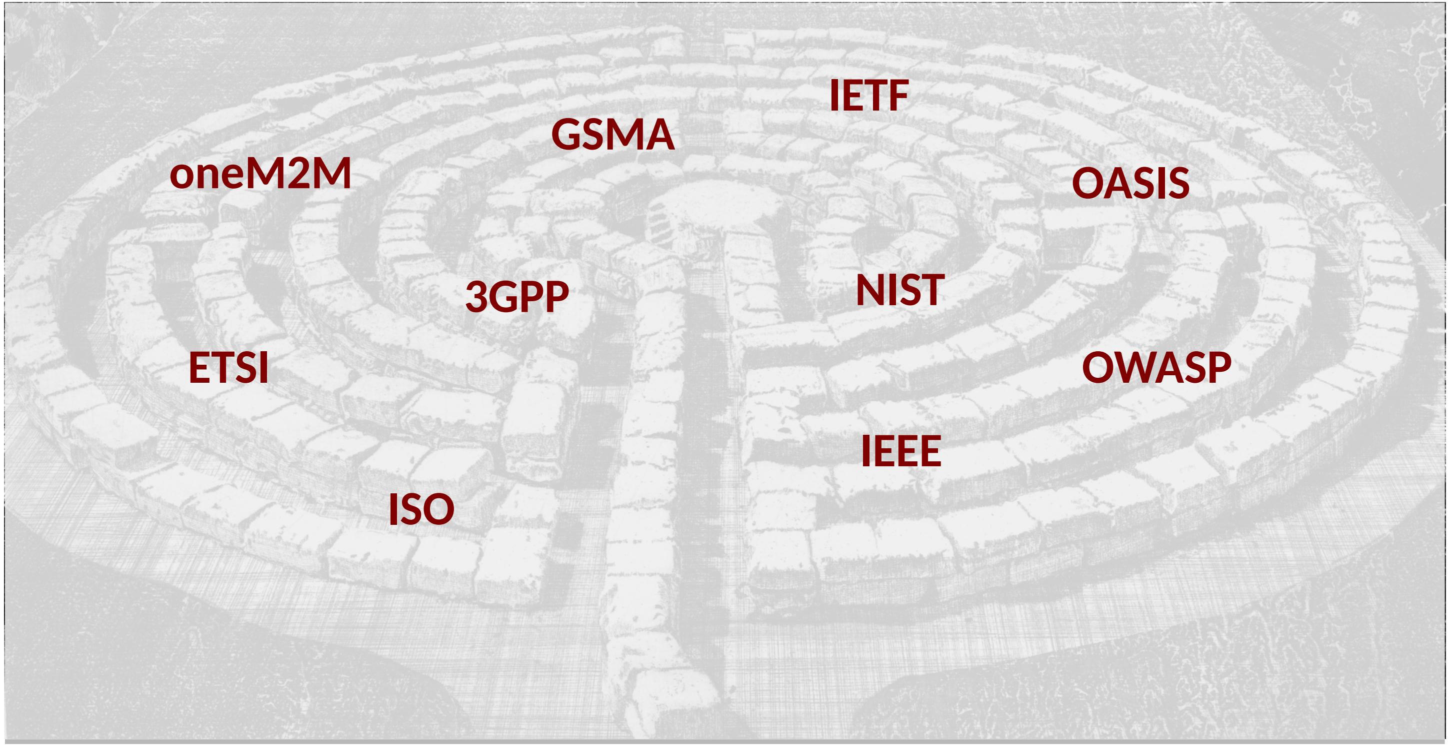
Internet of Things
Security standards

Vangelis Gazis (vangelis.gazis@huawei.com)
Chief Architect Security Internet of Things (IoT)
Security Solution Planning & Architecture Design (SPD)

HUAWEI

Security standards for IoT… where does one start?



Let's look at automotive (as an example)

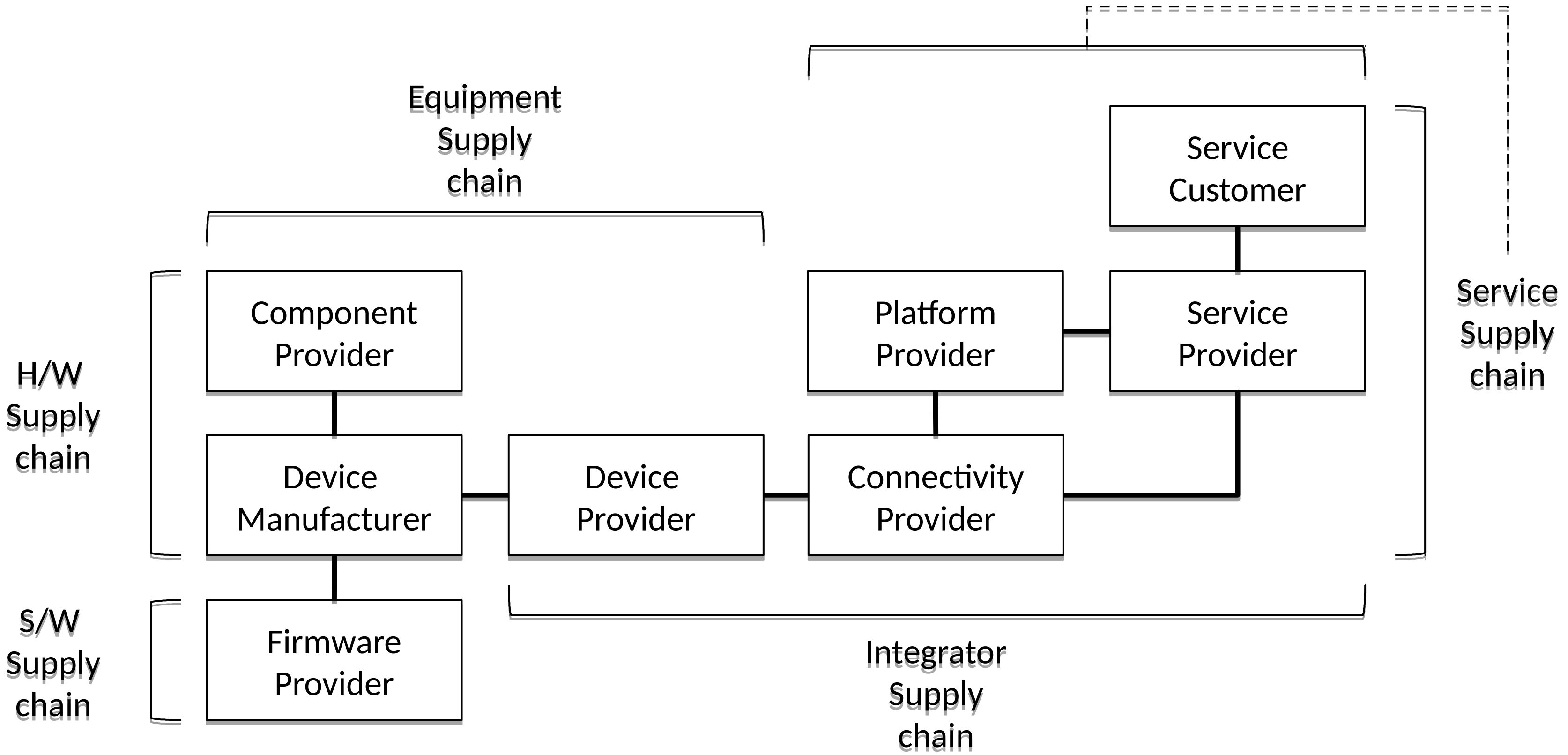
Study Groups		Standardization Bodies		Other Bodies	
ITU-T	SG 11	ISO	TC 22	GSMA	
	SG 13		TC 204	Standards Development Organizations	ATIS
	SG 16	ISO/IEC	JTC1/SC6		CCSA
	SG 20		JTC1/SC27		TIA
ITU-R	WP5A	SAE	Vehicle Cyber Security		TTA
CITS – Collaboration on ITS Communication Standards		IEEE	802.11 WG		TTC
			1609 WG		
		ETSI	TC ITS	UNECE WP29 TFCS	
		W3C	Automotive WG	AGL – Automotive Grade Linux	

https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201708/Documents/S2-Lee.pdf

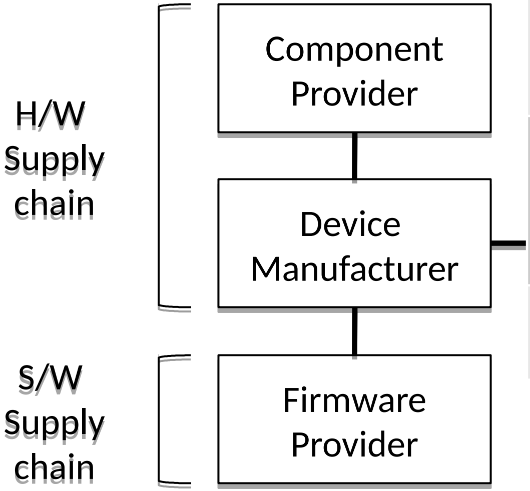
Standards in the risk ecosystem of IoT

HUAWEI

The risk ecosystem of IoT

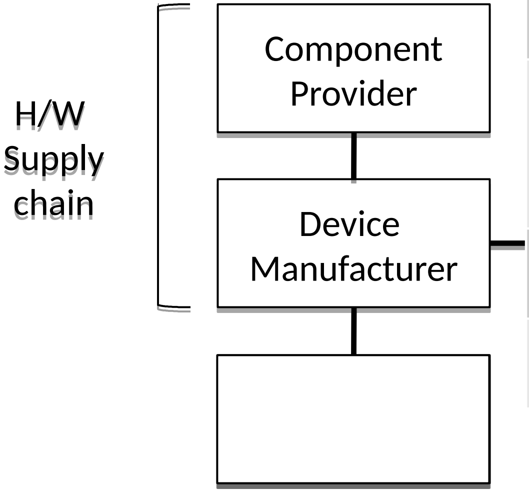


The risk ecosystem of IoT
Security standards: ISO



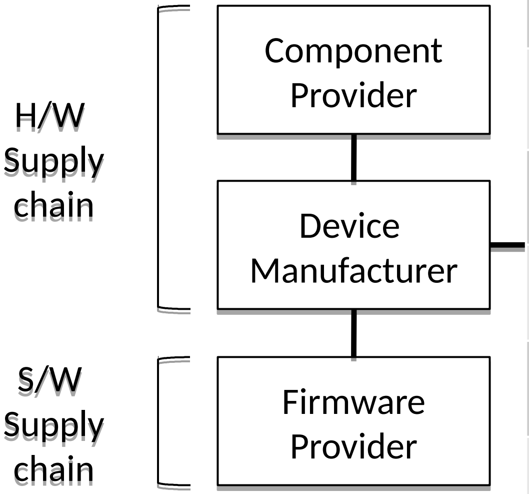
Standard	Title
ISO 28000:2007	Specification for security management systems for the supply chain
ISO 28001:2007	Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance
ISO 28003:2007	Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems
ISO 28004-1:2007	Guidelines for the implementation of ISO 28000 Part 1 – General principles

The risk ecosystem of IoT
Security standards: ISO



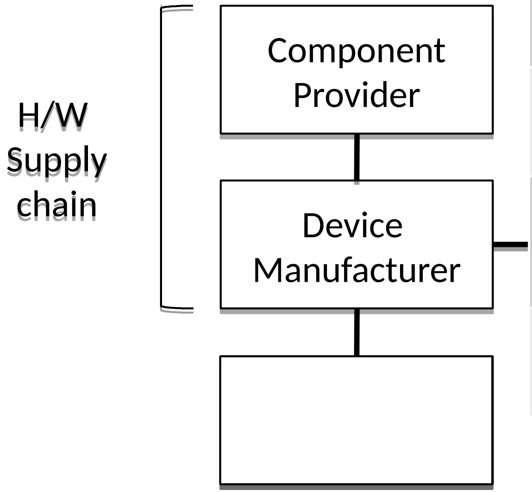
Standard	Title
ISO 20243-1:2018	Information technology – Open Trusted Technology Provider Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products – Part 1: Requirements and recommendations
ISO 20243-2:2018	Information technology – Open Trusted Technology Provider Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products – Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018

The risk ecosystem of IoT
Security standards: NIST



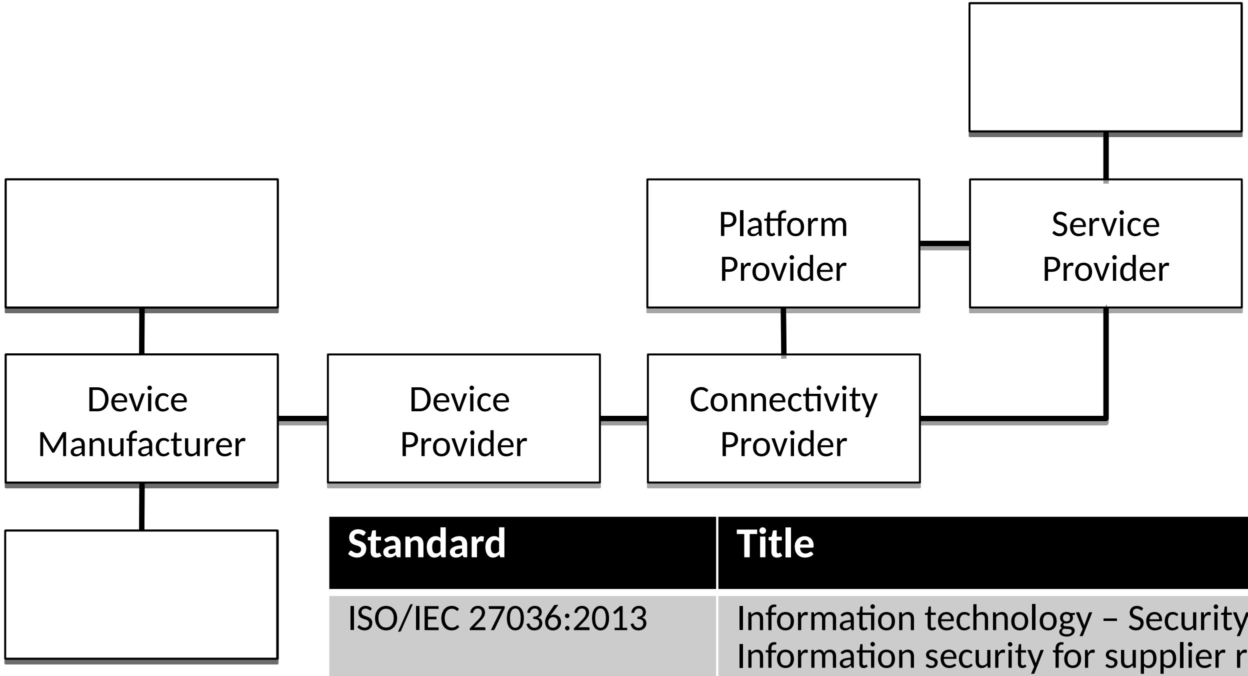
Standard	Title
SP 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations

The risk ecosystem of IoT Security standards: SEMI



Standard	Title
SEMI T21-0314	Specification for Organization Identification by Digital Certificate Issued from Certificate Service Body (CSB) for Anti-Counterfeiting Traceability in Components Supply Chain
SEMI T22-0212	Specification for Traceability by Self Authentication Service Body and Authentication Service Body
SEMI T20-0710 (Reapproved 0416)	Specification for Authentication of Semiconductors and Related Products
SEMI E169-0414	Guide for Equipment Information System Security

The risk ecosystem of IoT
Security standards: ISO



Standard	Title
ISO/IEC 27036:2013	Information technology – Security techniques – Information security for supplier relationships

The risk ecosystem of IoT
Security standards: ISO

Standard	Title
ISO/IEC 27036-1:2014	Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts
ISO/IEC 27036-2:2014	Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements
ISO/IEC 27036-3:2013	Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security
ISO/IEC 27036-4:2016	Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services

The risk ecosystem of IoT
Framework standards

Standard	Title
ISO/IEC 21827:2008	Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model (SSE-CMM)
ISO/IEC TR 15446:2009	Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets
ISO/IEC 29100:2011	Information technology – Security techniques – Privacy framework

Approaching cyber security in IoT
Key observations

- **Market lacks economic incentives for cyber security**
  - Customers prioritize functional features over security ones
- **Depreciation of security assurances given at product/service launch**
  - New vulnerabilities are being discovered daily (discovery ≠ disclosure)
- **The value chain may distribute the liabilities associated to cyber security assurances in a disproportionate manner**
  - DDoS attacks launched by a globally distributed population of low-cost end-user devices (e.g. as in IoT) under the control of malicious actor bring no additional cost to the manufacturer of any of these devices
- **Consumers of products and/or services often lack in security awareness**

Approaching cyber security in IoT

- **Scale**
  - Devices are low-cost
  - Lack of incentives for engineering robust security at device level
  - Low security awareness

Compromise one type of device ⇨ Own millions of devices

- **Economics**
  - Lack of liability structures in the security of products and services
  - Externalities of lack in security

Device players don’t care enough ⇨ Poor security to start with and gradual security depreciation

- **Practice**

Approaching cyber security in IoT

Lightweight (cost-efficient) root-of-trust

- **Scale**
  - Devices are low-cost
  - Lack of incentives for engineering robust security at device level
  - Low security awareness

Compromise one type of device ⇨ Own millions of devices

- **Economics**
  - Lack of liability structures in the security of products and services
  - Externalities of lack in security

Device players don't care enough ⇨ Poor security to start with and gradual security depreciation

- **Practice**

Approaching cyber security in IoT

- **Scale**
  - Devices are low-cost
  - Lack of incentives for engineering robust security at device level
  - Low security awareness
- **Economics**
  - Lack of liability structures in the security of products and services
  - Externalities of lack in security
- **Practice**

Compromise one type of device ⇨ Own millions of devices

Enablement of markets for DDoS mitigation

Device players don't care enough ⇨ Poor security to start with and gradual security depreciation

Approaching cyber security in IoT

- **Scale**
  - Devices are low-cost
  - Lack of incentives for engineering robust security at device level
  - Low security awareness
- **Economics**
  - Lack of liability structures in the security of products and services
  - Externalities of lack in security
- **Practice**

Compromise one type of device → Own millions of devices

Device players don't care enough → Poor security to start with and gradual security depreciation

Standards for firmware and/or software updates

Approaching cyber security in IoT

- **Scale**
  - Devices are low-cost
  - Lack of incentives for engineering robust security at device level
  - Low security awareness
- **Economics**
  - Lack of liability structures in the security of products and services
  - Externalities of lack in security
- **Practice**

Balancing stakeholders incentives

Compromise one type of device ⇨ Own millions of devices

Device players don't care enough ⇨ Poor security to start with and gradual security depreciation

Approaching cyber security in IoT

- **Scale**
  - Devices are low-cost **TCG DICE**
  - Lack of incentives for engineering robust security at device level
  - Low security awareness

  } Compromise one type of device ⇨ Own millions of devices **IETF DOTS** **OASIS CTI**

- **Economics** **UNECE WP29**
  - Lack of liability structures in security of products and services
  - Externalities of lack in security

  } Device players don't care enough ⇨ Poor security to start with and gradual security depreciation **IETF SUIT**

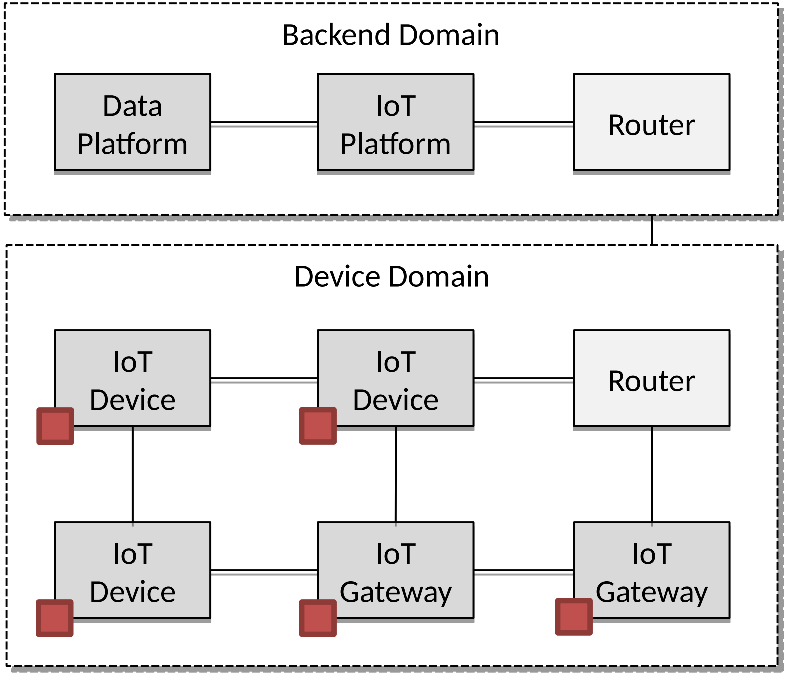
- **Practice** **ENISA GSMA NIST OWASP CSA ISO/IEC**

Standards for lightweight Root-of-Trust

HUAWEI

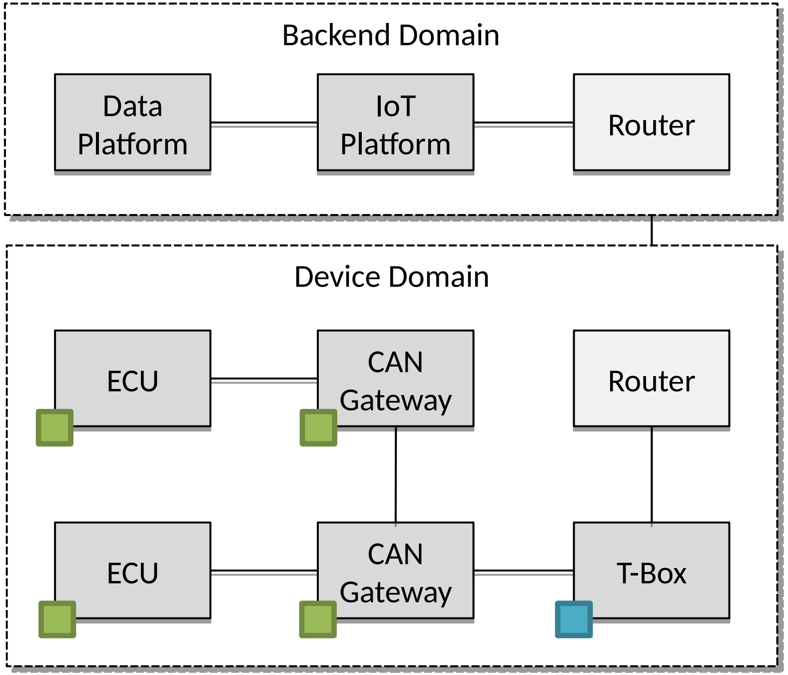
Hardware Root-of-Trust (RoT)

- **General (TCG)**
  - [Trusted Platform Module (TPM)]
- **Lightweight (TCG)**
  - [Device Identity Composition Engine (DICE)]



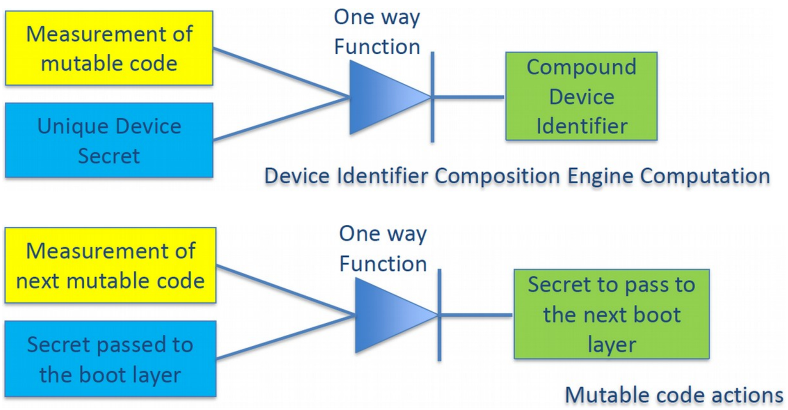
Hardware Root-of-Trust (RoT)

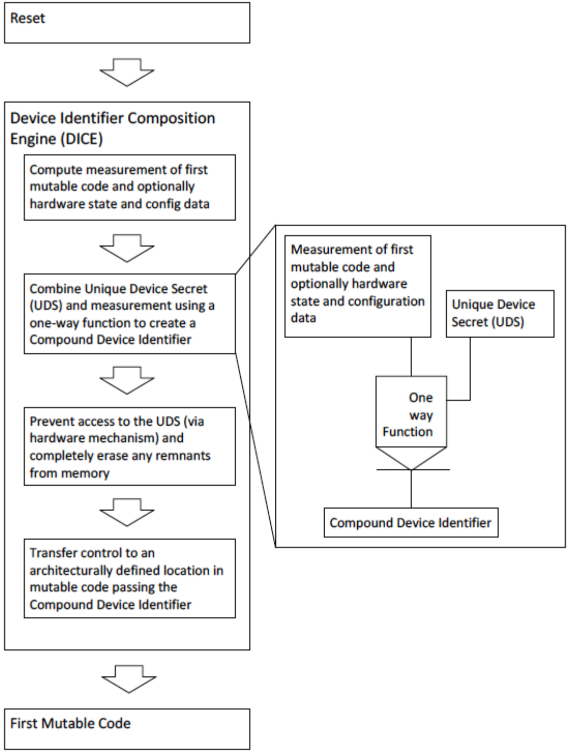
- **General (TCG)**
  - Trusted Platform Module (TPM)
- **Lightweight (TCG)**
  - Device Identity Composition Engine (DICE)
- **Automotive (TCG)**
  - TPM 2.0 Profile for Automotive Thin
  - TPM 2.0 Profile for Automotive Rich



Hardware Root-of-Trust (RoT)
TCG DICE

- **Compound Device Identifier (CDI)**
  - Unique Device Secret (UDS)
  - Measurement of the first mutable code that runs on the platform





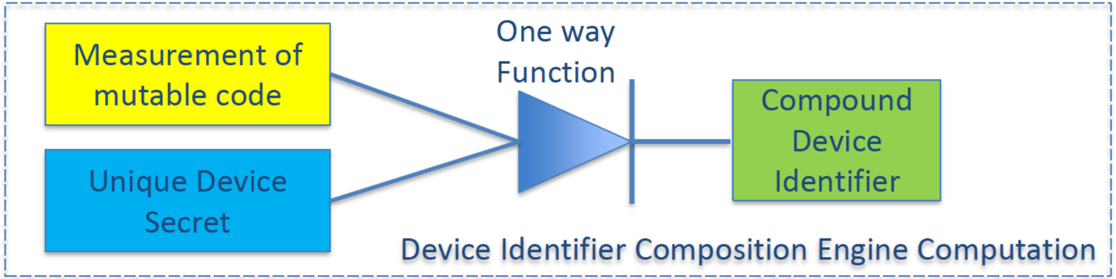
https://trustedcomputinggroup.org/wp-content/uploads/3.4_Trusted-Computing-and-Securing-Devices-2017.04.06-Final.pdf

Hardware Root-of-Trust (RoT)
TCG DICE

TRUSTED COMPUTING GROUP

Generating the Compound Device Identifier

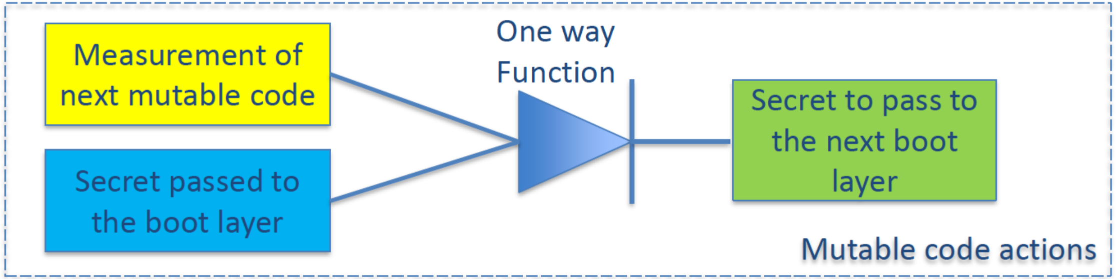
- Immutable code has access to the Unique Device Secret, but the mutable code does not
- Immutable code only passes the Compound Device Identifier to the first mutable code



Hardware Root-of-Trust (RoT)
TCG DICE

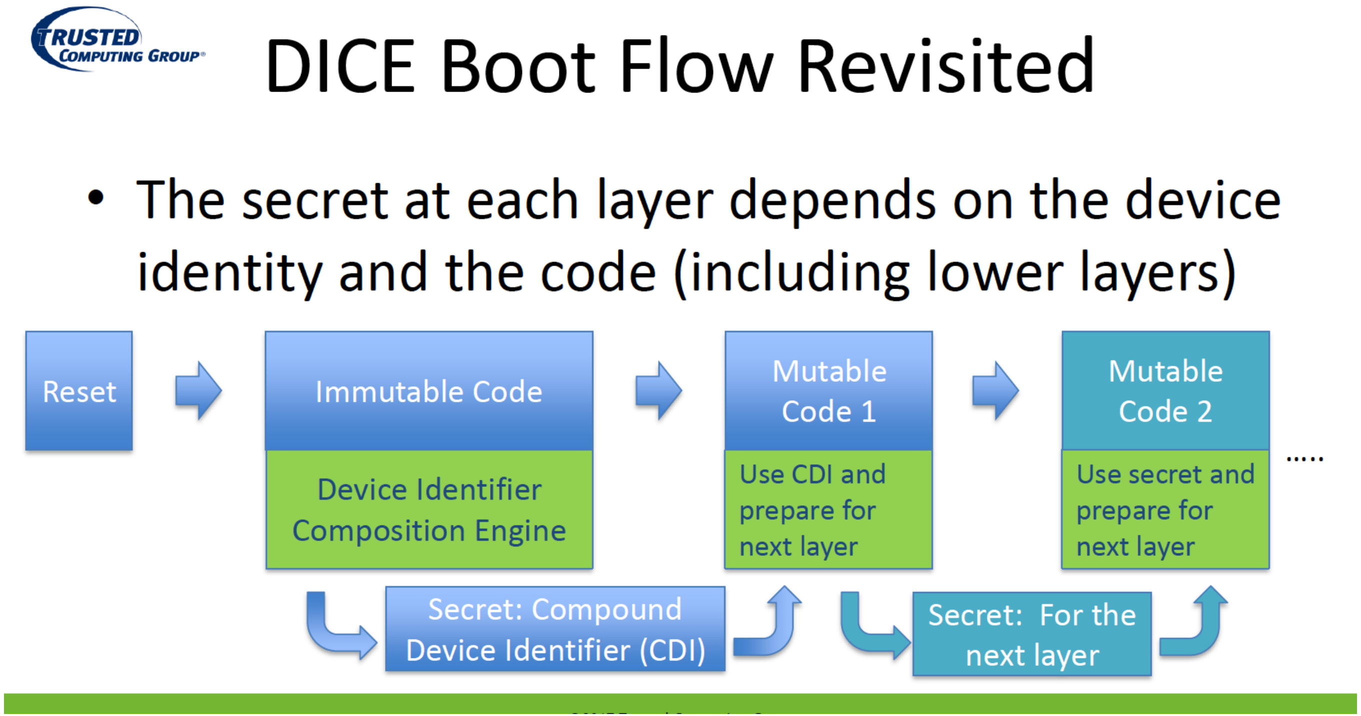
Mutable Code Actions

- Each layer of mutable code receives a secret
- The secret can be used to prove the identity and software booted
- Secret is combined with a measurement of the next boot layer



https://trustedcomputinggroup.org/wp-content/uploads/3.4_Trusted-Computing-and-Securing-Devices-2017.04.06-Final.pdf

Hardware Root-of-Trust (RoT)
TCG DICE



Hardware Root-of-Trust (RoT)
TCG DICE

- **Proving device identity and integral state of software**
  - Composite Device Identity (CDI) can be used with a Key Derivation Function (KDF) to produce an asymmetric key with (private, public) parts
  - A change in the CDI and the derived asymmetric key means that there has been a change in the first mutable code
  - The manufacturer can issue for the first layer of software a certificate for each device and include the public part of the asymmetric key
  - The device proves its identity and its boot software when it performs a computation using the private part of the asymmetric key

https://trustedcomputinggroup.org/wp-content/uploads/3.4_Trusted-Computing-and-Securing-Devices-2017.04.06-Final.pdf

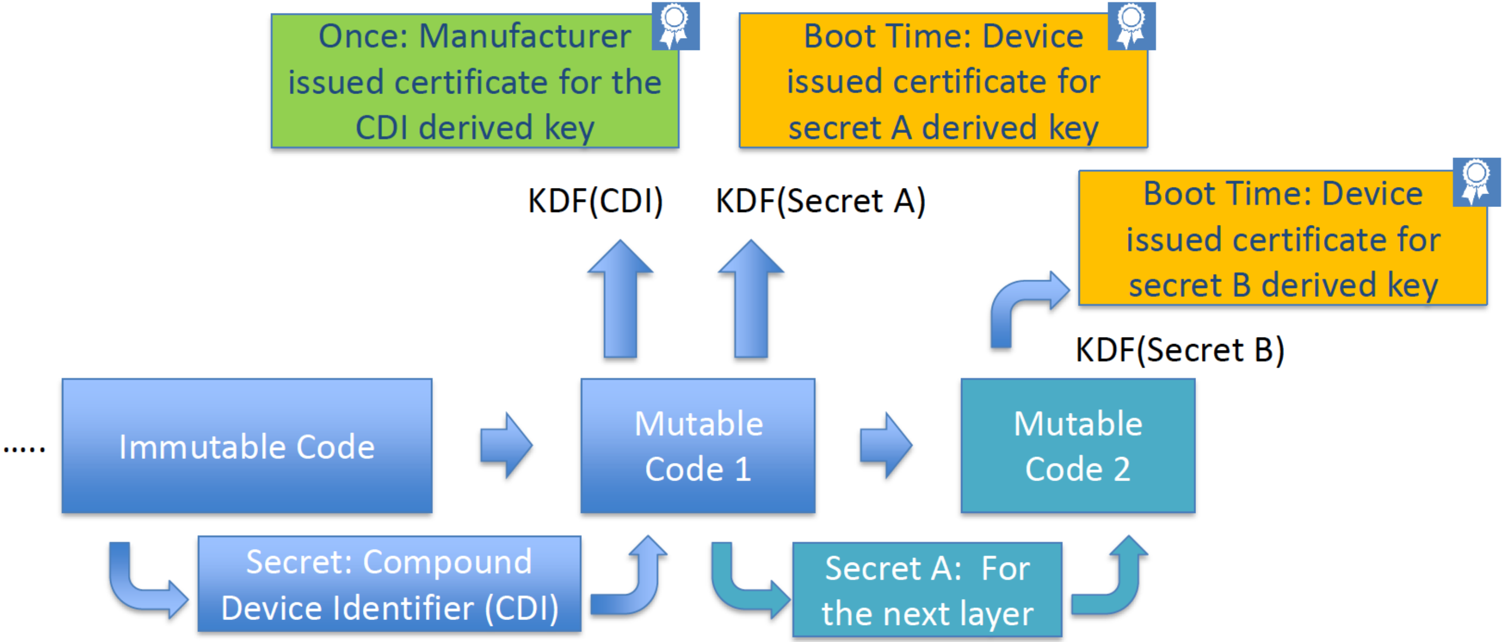
Hardware Root-of-Trust (RoT)
TCG DICE

- **Proving software state for later in the boot process**
  - The first layer of software has a certificate issued by the manufacturer
  - Each layer of software can use its private key and certificate to issue a certificate for the next layer of software
  - Each successive layer can repeat the process
  - The final certificate chain can be used in the establishment of TLS sessions and prove the device's identity and the integral state of its software

https://trustedcomputinggroup.org/wp-content/uploads/3.4_Trusted-Computing-and-Securing-Devices-2017.04.06-Final.pdf

Hardware Root-of-Trust (RoT)
TCG DICE

- ❑ **Chained Certificate issuance**



https://trustedcomputinggroup.org/wp-content/uploads/3.4_Trusted-Computing-and-Securing-Devices-2017.04.06-Final.pdf

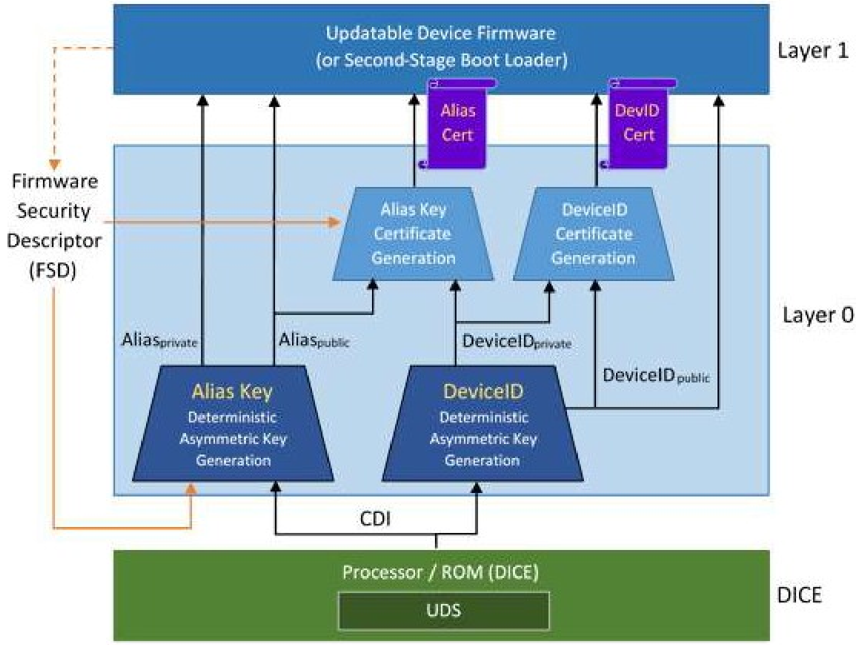
Hardware Root-of-Trust (RoT)
TCG DICE

- **Requirements (non-exhaustive list)**
  - Strength of the Composite Device Identifier (CDI) should be at least 256 bits
  - Update of the CDI requires a secure software update process (otherwise the CDI is immutable)
  - Protection offered by one-way function as in NIST SP800-57 Part 1
  - Any values that can be used to determine the Unique Device Secret (UDS) are erased before execution of the first mutable code (NIST SP800-88r1)
- **Key enabler**
  - Implicit identity-based device attestation

https://trustedcomputinggroup.org/wp-content/uploads/3.4_Trusted-Computing-and-Securing-Devices-2017.04.06-Final.pdf

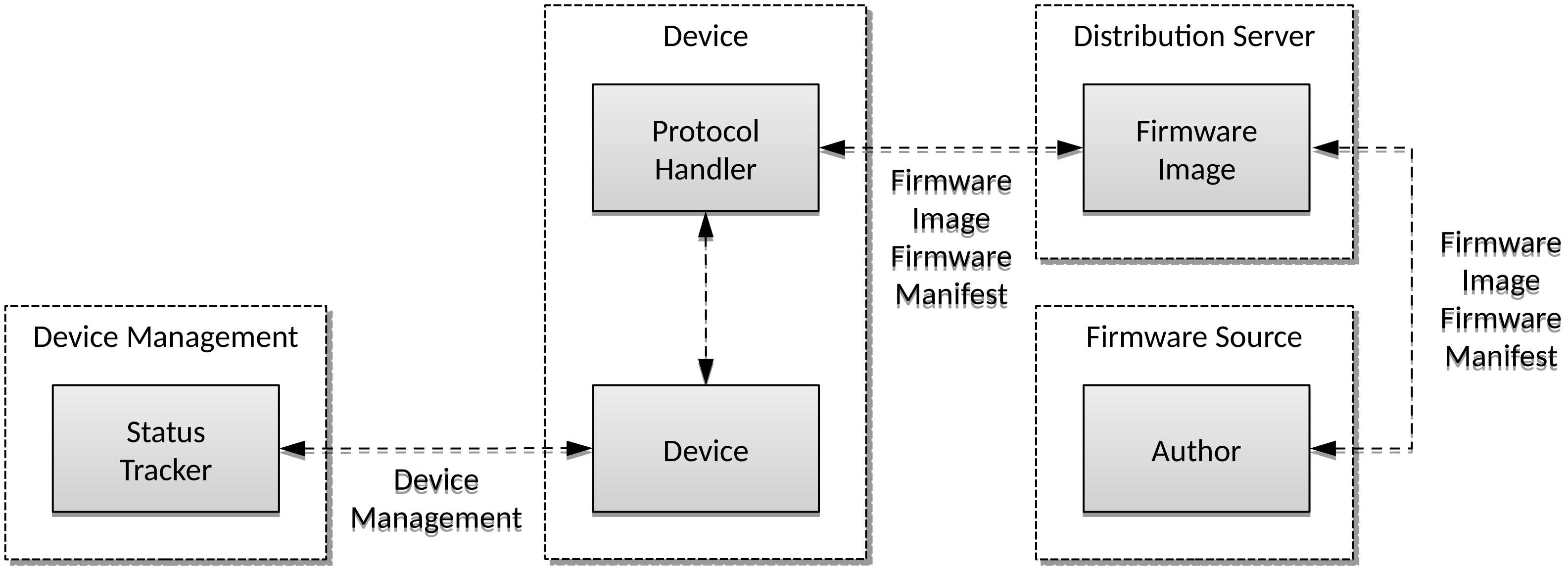
Hardware Root-of-Trust (RoT)
TCG DICE

- **Implicit attestation**
  - First mutable code uses CDI to generate Device Identity (DI) asymmetric key pair
    - Can be done at manufacture time
    - Manufacturer may certify the public key of DI key pair
  - DI is best kept secret (e.g. from L1)
  - Device generates Alias asymmetric key whose public key is certified by DI key



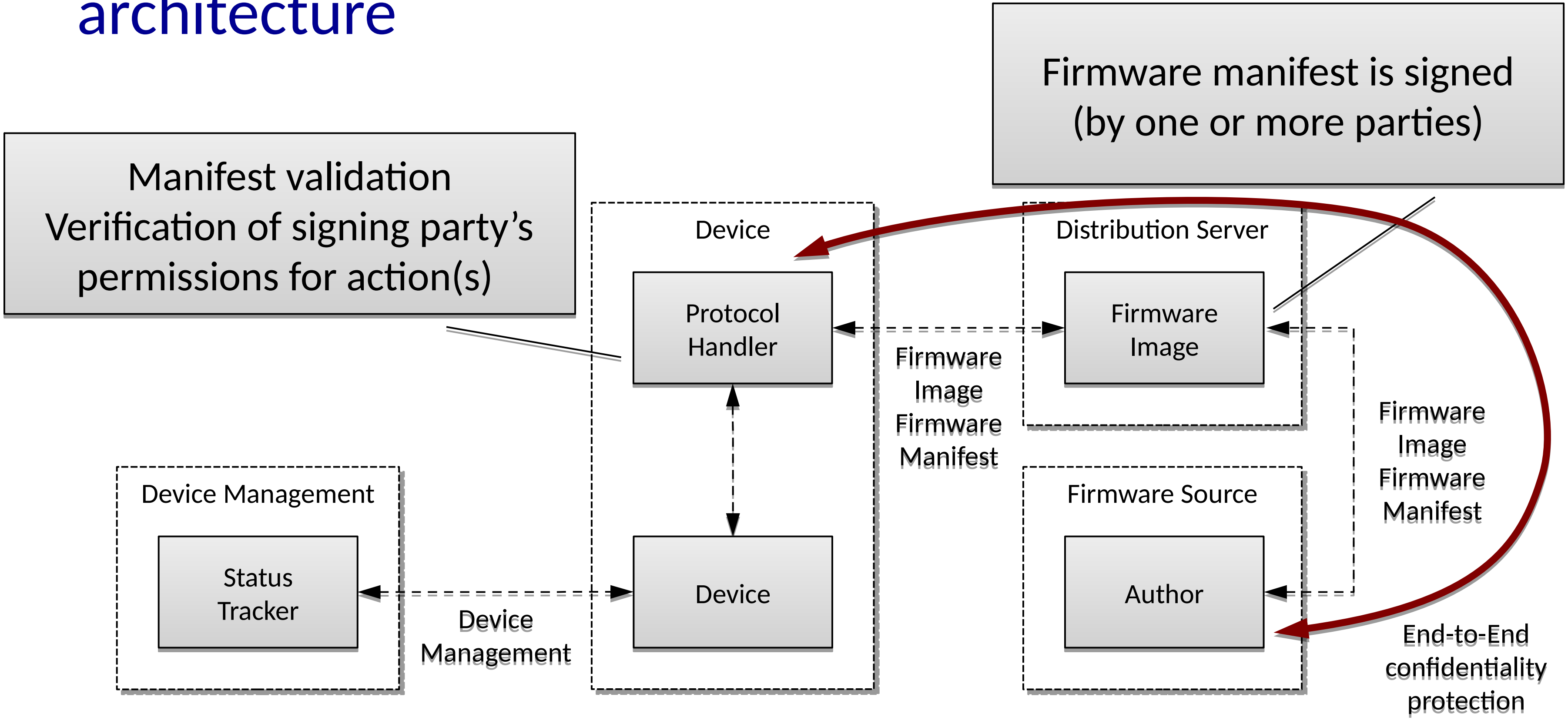
Standards for firmware updates

IETF Software Updates for Internet of Things (SUIT) architecture



https://datatracker.ietf.org/wg/suit/about/

IETF Software Updates for Internet of Things (SUIT) architecture



https://datatracker.ietf.org/wg/suit/about/

IETF Software Updates for Internet of Things (SUIT) requirements

- **Old firmware**
- **Mismatched firmware**
- **Offline device and old firmware**
- **Target device misinterprets the type of payload**
- **Target device installs payload to wrong location**
- **Redirection**
- **Payload verification on boot**
- **Unauthorized updates**
- **Unexpected precursor images**
- **Unqualified firmware**
- **Reverse analysis of firmware images for vulnerability discovery**
- **Overriding critical manifest elements**

https://datatracker.ietf.org/wg/suit/about/

IETF Software Updates for Internet of Things (SUIT) information model

- Version identifier of the manifest structure
- Monotonic sequence number
- Vendor ID condition
- Class ID condition
- Precursor image digest condition
- Required image version list
- Best-before timestamp condition
- Payload Format
- Processing steps
- Storage location
- Component identifier
- URIs
- Payload digest
- Size
- Signature
- Directives
- Aliases

https://datatracker.ietf.org/wg/suit/about/

IETF Software Updates for Internet of Things (SUIT) information model

- **Dependencies**
- **Content key distribution method**
- **XIP address**

https://datatracker.ietf.org/wg/suit/about/

Balancing stakeholders incentives

HUAWEI

IETF
Manufacturer Usage Description (MUD)

- **The activity pattern of an IoT device is unlike a human one**
  - An IoT device serves a single purpose or a small set of purposes
  - A IoT device communicates to a few services
    - Local network services
      - DHCP
      - NTP
      - DNS
    - Possibly services supporting its purpose (e.g. services accessible over the Web)
  - An IoT device cannot be expected to protect itself (even if it does so today)
- **The activity pattern of an IoT device is largely known to its manufacturer**
  - Remedy can applied at the IoT device class level

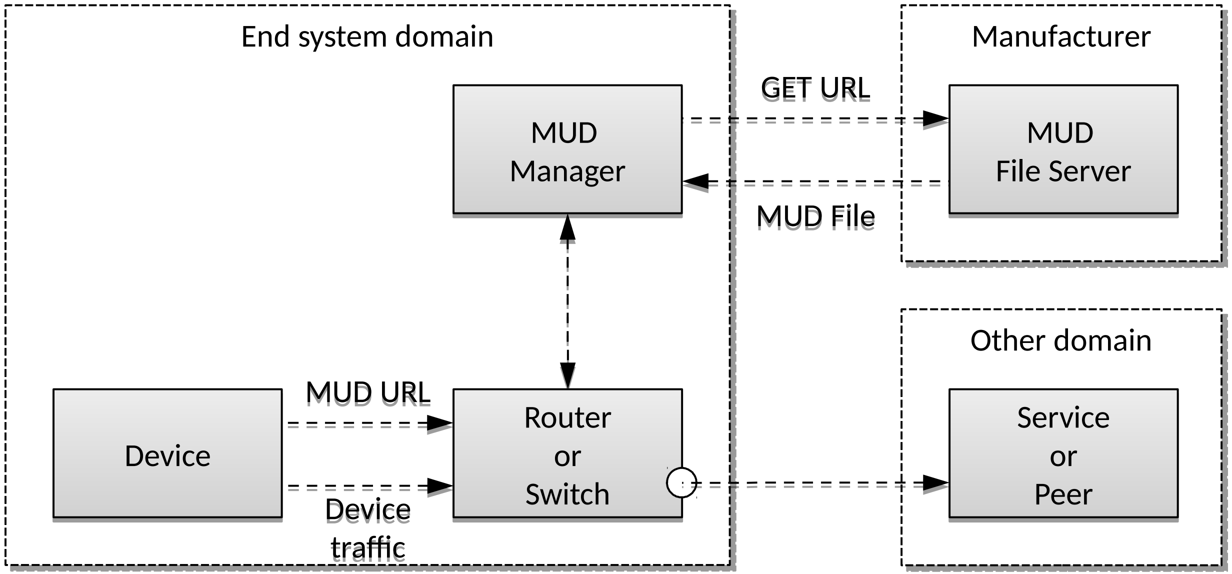
http://www.ieee802.org/1/files/public/docs2017/new-lear-iot-mud-0217-v01.pdf

IETF
Manufacturer Usage Description (MUD)

- **Assumptions**
  - The network is able to identify in some way the remote endpoints that a “thing” will talk to
- **Objective**
  - Provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function (i.e. intended use)
- **Building blocks**
  - A URL that can be used to locate a description
  - The description itself (including how it is interpreted)
  - A means for local network management systems to retrieve the description

https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/

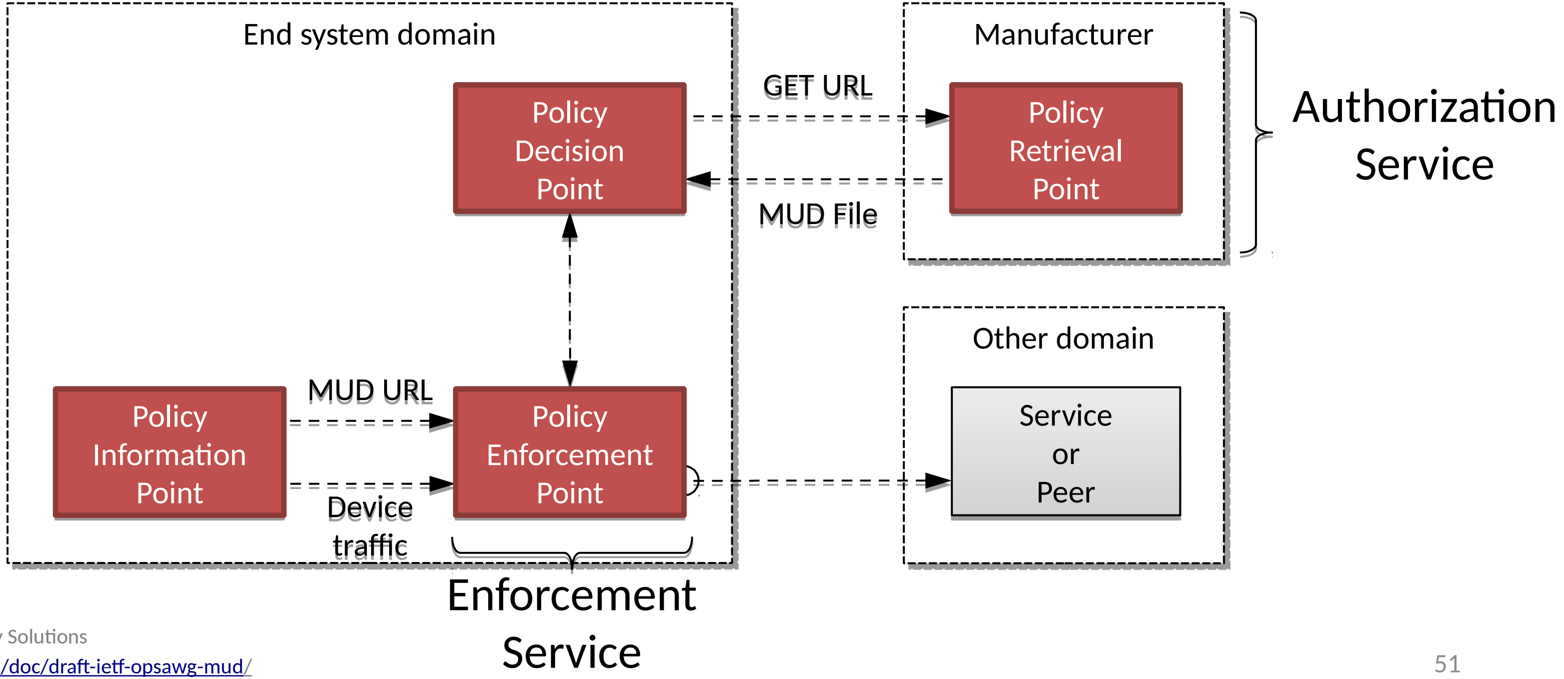
IETF
Manufacturer Usage Description (MUD)



https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/

IETF
Manufacturer Usage Description (MUD)

- **Mapping MUD to the oneM2M authorization architecture**



OneM2M TS-0003 Security Solutions
https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/

IETF
Manufacturer Usage Description (MUD)

```
module: ietf-mud
  +--rw mud!
     +--rw mud-version           uint8
     +--rw mud-url               inet:uri
     +--rw last-update           yang:date-and-time
     +--rw mud-signature?        inet:uri
     +--rw cache-validity?       uint8
     +--rw is-supported          boolean
     +--rw systeminfo?           string
     +--rw mfg-name?             string
     +--rw model-name?           string
     +--rw firmware-rev?         string
     +--rw software-rev?         string
     +--rw documentation?        inet:uri
     +--rw extensions*           string
     +--rw from-device-policy
     |  +--rw acls
     |     +--rw access-list* [name]
     |        +--rw name    -> /acl:acls/acl/name
     +--rw to-device-policy
        +--rw acls
           +--rw access-list* [name]
              +--rw name    -> /acl:acls/acl/name
```

```
augment /acl:acls/acl:acl/acl:aces/acl:ace/acl:matches:
  +--rw mud
     +--rw manufacturer?         inet:host
     +--rw same-manufacturer?    empty
     +--rw model?                inet:uri
     +--rw local-networks?       empty
     +--rw controller?           inet:uri
     +--rw my-controller?        empty
augment
  /acl:acls/acl:acl/acl:aces/acl:ace/acl:matches
     /acl:l4/acl:tcp/acl:tcp:
  +--rw direction-initiated?   direction
```

https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/

IoT Security
Recommendations and guidelines (non-exhaustive list)

- **ENISA**
  - Baseline security recommendations for IoT in the context of critical information infrastructures
- **CSA**
  - 13 steps to developing secure IoT products
- **GSMA**
  - IoT security guidelines for endpoint ecosystems
  - IoT security guidelines for service ecosystems
  - IoT security guidelines for network operators

IoT security
ENISA baseline security recommendations for IoT

Policies	Organizational People Processes	Technical Measures	
Security by design	End-of-life support	Trust and integrity management	Secure software/firmware update
Privacy by design	Proven solutions	Strong default security	Authentication
		Strong default privacy	Authorization
Asset management	Vulnerability management	Hardware security	Access control
Risk identification and assessment	Incident management	Data protection and compliance	Secure interfaces and network services
Threat identification and assessment	Security training and awareness	System safety and reliability	Secure and trusted communications
	3rd party relationship management	Secure handling of input/output data	Logging
			Monitoring and auditing

IoT security
CSA recommendations

Policies	Organizational People Processes	Technical Measures	
	Secure development methodology	Secure key management	Secure update capability
	Secure development and integration environment		Authentication
			Authorization
		Hardware security	Access control
	Establish privacy protections	Data protection	Secure associated Applications and Services
			Protect logical and API interfaces
	Identify framework security		Logging
	Identify platform security		Security reviews

IoT security
GSMA recommendations

Policies	Organizational People Processes	Technical Measures	
	Sunset model	Manage cryptographic architecture	Network authentication services
		Server provisioning	System hardening
		Bootstrap method	Communications model
	Data breach policy	Root of Trust (RoT)	Update model
Set of security classifications	Incident response model Recovery model	Persistent storage model	Security infrastructure for exposed systems
	Communications privacy model	Input validation Output filtering	Define an application execution environment
	Authorization model	Service Trusted Computing Base (TCB)	Logging and monitoring
	Strong password policy		

Thank you.

HUAWEI

Annex

Cyber security standards for IoT
IETF

- **Security Automation and Continuous Monitoring (SACM)**
  - Security Automation and Continuous Monitoring (SACM) Requirements
  - Security Automation and Continuous Monitoring (SACM) Architecture
  - The Data Model of Network Infrastructure Device Data Plane Security Baseline
  - The Data Model of Network Infrastructure Device Infrastructure Layer Security Baseline
  - The Data Model of Network Infrastructure Device Management Plane Security Baseline

https://datatracker.ietf.org/wg/sacm/about/

Cyber security standards for IoT
IETF

- **Trusted Execution Environment Provisioning (TEEP)**
  - Trusted Execution Environment Provisioning (TEEP) Architecture
  - The Open Trust Protocol (OTrP)

- **Cyber Threat Intelligence (CTI)**
  - RFC 4765 Intrusion Detection Message Exchange Format (IDMEF)
  - RFC 5070 Incident Object Description Exchange Format (IODEF)
  - RFC 5901 Extensions to the IODEF for Reporting Phishing
  - RFC 6545 Real-time Inter-network Defense (RID)

https://datatracker.ietf.org/wg/teep/about/

Cyber security standards for IoT
ETSI

- **Technical Committee (TC) CYBER**
  - TR 103 306 Global Cyber Security Ecosystem
  - TR 103 421 Network Gateway Cyber Defense
  - TR 103 305-1 Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls
  - TR 103 305-2 Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and Auditing
  - TR 103 305-3 Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations
  - TR 103 305-4 Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms

https://portal.etsi.org//STF/STFs/STFHomePages/STF547#deliverables

Cyber security standards for IoT
ETSI

- **Technical Committee (TC) CYBER**
  - TS 103 532 Attribute Based Encryption for Attribute Based Access Control
  - TR 103 167 Threat Analysis and Countermeasures to M2M Service Layer
  - TR 103 303 Protection Measures for ICT in the Context of Critical Infrastructures
  - TR 103 331 Structured Threat Information Sharing
  - TR 103 369 Design Requirements Ecosystem
  - TS 103 460 Malicious Behavior Detection
  - TR 103 370 Practical Introductory Guide to Privacy
  - TR 103 533 Security Standards Landscape and Best Practices from Initiatives

https://www.etsi.org/technologies-clusters/technologies/cyber-security

Cyber security standards for IoT
ETSI

- **Intelligent Transport Systems (ITS)**
  - TR 103 375 IoT Standards Landscape and Future Evolutions
  - TS 103 097 ITS Security; Security Headers and Certificate Formats
  - TS 102 940 ITS Security; ITS Communications Security Architecture and Security Management
  - TS 102 941 ITS Security; Trust and Privacy Management
  - TS 102 893 ITS Security; Threat Vulnerability and Risk Analysis (TVRA)
  - TS 102 723-8 OSI Cross-Layer Topics; Interface Between Security Entity and Network and Transport Layer

https://www.etsi.org/technologies-clusters/technologies/automotive-intelligent-transport

Cyber security standards for IoT
ITU-T

- **JCA-IoT**
  - Global online IoT standards roadmap
- **ITU-T SG17**
  - X.1362 Simple encryption procedure for IoT environments
  - X.1361 Security framework for IoT based on the gateway model
  - X.1373 Secure software update capability for ITS communication devices
  - X.secup-iot IoT Software Update Procedure (WiP)
  - X.ssp-iot Security requirements and framework for IoT service platform (WiP)
  - X.ibc-iot Security framework for use of identity-based cryptography in support of IoT services over telecom networks (WiP)

https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

Cyber security standards for IoT
ITU-T

- **X.1500 Series for Structured Cyber Security Information Exchange (CYBEX) Techniques**
  - X.1520 Common vulnerabilities and exposures (CVE)
  - X.1521 Common vulnerability scoring system (CVSS)
  - X.1524 Common weakness enumeration (CWE)
  - X.1525 Common weakness scoring system (CWSS)
  - X.1544 Common attack pattern enumeration and classification (CAPEC)

https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybex.aspx

Cyber security standards for IoT
3GPP

- **Security specifications**
  - 21.133 Security Threats and Requirements
  - 33.187 Security aspects of Machine-Type Communications (MTC)
  - 33.120 Security Principles and Objectives
  - 33.310 Network Domain Security (NDS) Authentication Framework (AF)
  - 33.102 3G Security Architecture
  - 33.401 Security Architecture SAE
  - 33.501 Security Architecture and Procedures for 5G System
  - 33.163 Battery Efficient Security for Very Low Throughput Machine Type Communication (MTC) Devices (BEST)

https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybex.aspx

Cyber security standards for IoT
3GPP

- **Security specifications**
  - 33.220 Generic Bootstrapping Architecture (GBA)
  - 33.221 Generic Bootstrapping Architecture (GBA) Support for Subscriber Certificates (SSC
)
  - 33.222 Generic Authentication Architecture (GAA); Access to network application functions using
HTTPS
  - 33.116 Security Assurance Specification (SCAS) for the MME network product class
  - 33.117 Catalogue of general security assurance requirements
  - 33.250 Security assurance specification for the PGW network product class

https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybex.aspx

Cyber security standards for IoT
3GPP

- **Security specifications**
  - 33.805 Security Assurance Methodology (SECAM) for 3GPP Nodes
  - 33.855 Study on Security Aspects of SBA
  - 33.821 Rationale and Track of Security Decisions in LTE RAN / 3GPP SAE
  - 33.863 Study on battery efficient security for very low throughput Machine Type Communication (MTC) devices
  - 33.885 Study on security aspects for LTE support of Vehicle-to-Everything (V2X) services
  - 33.926 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes

https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybex.aspx

Cyber security standards for IoT
3GPP

- **Security specifications**
  - 33.905 Recommendations for Trusted Open Platforms
  - 33.919 Generic Authentication Architecture (GAA)
  - 33.889 Study on Security Aspects of Machine-Type Communications (MTC) Architecture and Feature
    Enhancements
  - 33.899 Study On The Security Aspects Of The Next Generation System

https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybex.aspx

Status of Standards across Security Domains

Core Areas of Cybersecurity Standardization	Examples of Relevant SDOs	Connected Vehicles	Consumer IoT	Health IoT & Medical Devices	Smart Buildings	Smart Manufacturing
Cryptographic Techniques	ETSI; IEEE; ISO/IEC JTC 1; ISO TC 68; ISO TC 307; W3C	Standards Available Slow Uptake	Standards Available Slow Uptake	Some Standards Slow Uptake	Standards Available Slow Uptake	Some Standards Slow Uptake
Cyber Incident Management	ETSI ; ISO/IEC JTC 1; ITU-T; PCI	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
Identity and Access Management	ETSI; FIDO Alliance; IETF; OASIS; OIDF; ISO/IEC JTC 1; ITU-T; W3C	Standards Available Slow Uptake	Standards Available Slow Uptake	Some Standards Slow Uptake	Standards Available Slow Uptake	Standards Available Slow Uptake

Status of Standards across Security Domains

Information Security Management Systems	ATIS; IEC; ISA; ISO/IEC JTC 1; ISO TC 223; OASIS; The Open Group	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
IT System Security Evaluation	ISO/IEC JTC 1; The Open Group; UL	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented
Hardware Assurance	ISO/IEC JTC 1; SAE International	Some Standards Slow Uptake	Some Standards Not Implemented	Some Standards Slow Uptake	Some Standards Not Implemented	Some Standards Not Implemented

Status of Standards across Security Domains

Network Security	3GPP; 3GPP2; IEC; IETF; IEEE; ISO/IEC JTC 1; ITU-T; The Open Group; WiMAX Forum	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented
Security Automation & Continuous Monitoring	IEEE; IETF; ISO/IEC JTC 1; TCG; The Open Group	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
Software Assurance	IEEE; ISO/IEC JTC 1; OMG; TCG; The Open Group; UL	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
Supply Chain Risk Management	IEEE; ISO/IEC JTC 1; IEC TC 65; The Open Group; UL	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake

Status of Standards across Security Domains Lightweight cryptography

Standard	Description
ISO/IEC 29192-1:2012	Information technology – Security techniques – Lightweight cryptography – Part 1: General
ISO/IEC 29192-2:2012	Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers
ISO/IEC 29192-3:2012	Information technology – Security techniques – Lightweight cryptography – Part 3: Stream ciphers

Status of Standards across Security Domains
Lightweight cryptography

Standard	Description
ISO/IEC 29192-4:2013	Information technology – Security techniques – Lightweight cryptography – Part 4: Mechanisms using asymmetric techniques
ISO/IEC 29192-4:201 Amd.1: (2016)	Information technology – Security techniques – Lightweight cryptography – Part 4: Mechanisms using asymmetric techniques
ISO/IEC 29192-5:2016	Information technology – Security techniques – Lightweight cryptography – Part 5: Hash-functions

Status of Standards across Security Domains
Incident management

Standard	Description
ISO/IEC 27035-1:2016	Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management
ISO/IEC 27035-2:2016	Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response
ISO/IEC PDTS 27035-3	Information technology – Security techniques – Information security incident management – Part 3: Guidelines for incident response operations
ITU-T X.1056	Security incident management guidelines for telecommunications organizations

Status of Standards across Security Domains
Incident management

Standard	Description
RFC 4765	Intrusion Detection Message Exchange Format (IDMEF)
RFC 5070	Incident Object Description Exchange Format (IODEF)
RFC 5901	Extensions to the IODEF for Reporting Phishing
RFC 6545	Real-time Inter-network Defense (RID)
OASIS STIX 2.0	Structured Threat Information Expression (STIX) V2.0
OASIS TAXII 2.0	Trusted Automated Exchange of Indicator Information (TAXII) V2.0
OASIS OpenC2	Machine to machine exchange of commands to achieve investigative, remediation and/or mitigation effects