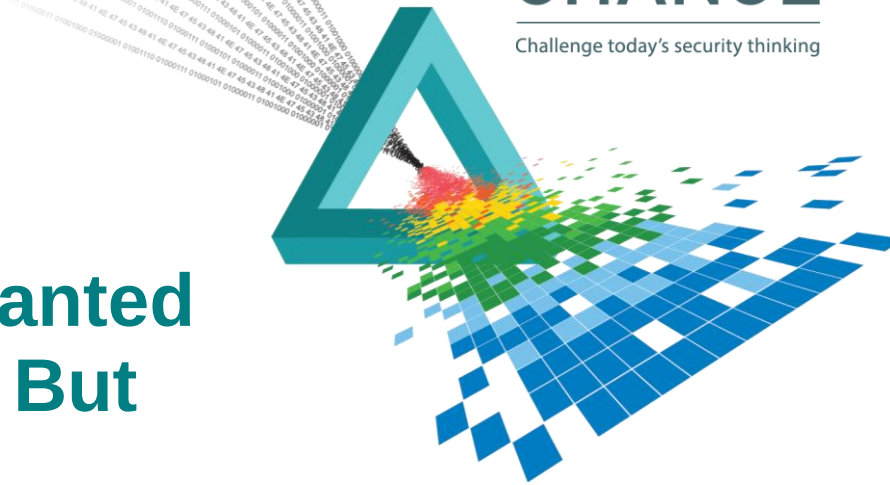
RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking



SESSION ID: MBS-F03

Mobile Security: All You Wanted To Know About Standards But Were Afraid To Ask

Hadi Nahari

Chief Security Architect

NVIDIA

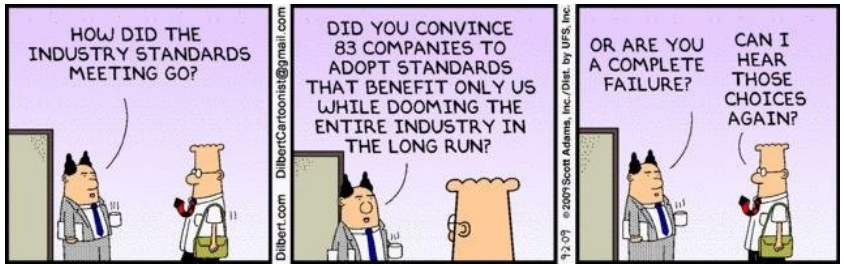
hadinahari

Background

- Trusted & secure computing base, cryptography, complex system analysis, HPC, massively scalable systems design, implementation, and governance
- Identity management, asset protection, information-assurance schemes, vulnerability assessment and threat analysis
- Enterprise & Embedded (Netscape, Sun Microsystems, USG, Motorola, Zaplet, MontaVista, eBay, PayPal, NVIDIA…)
- Author of “Web Commerce Security: Design and Development.”
- Currently Chief Security Architect at NVIDIA

Disclaimer

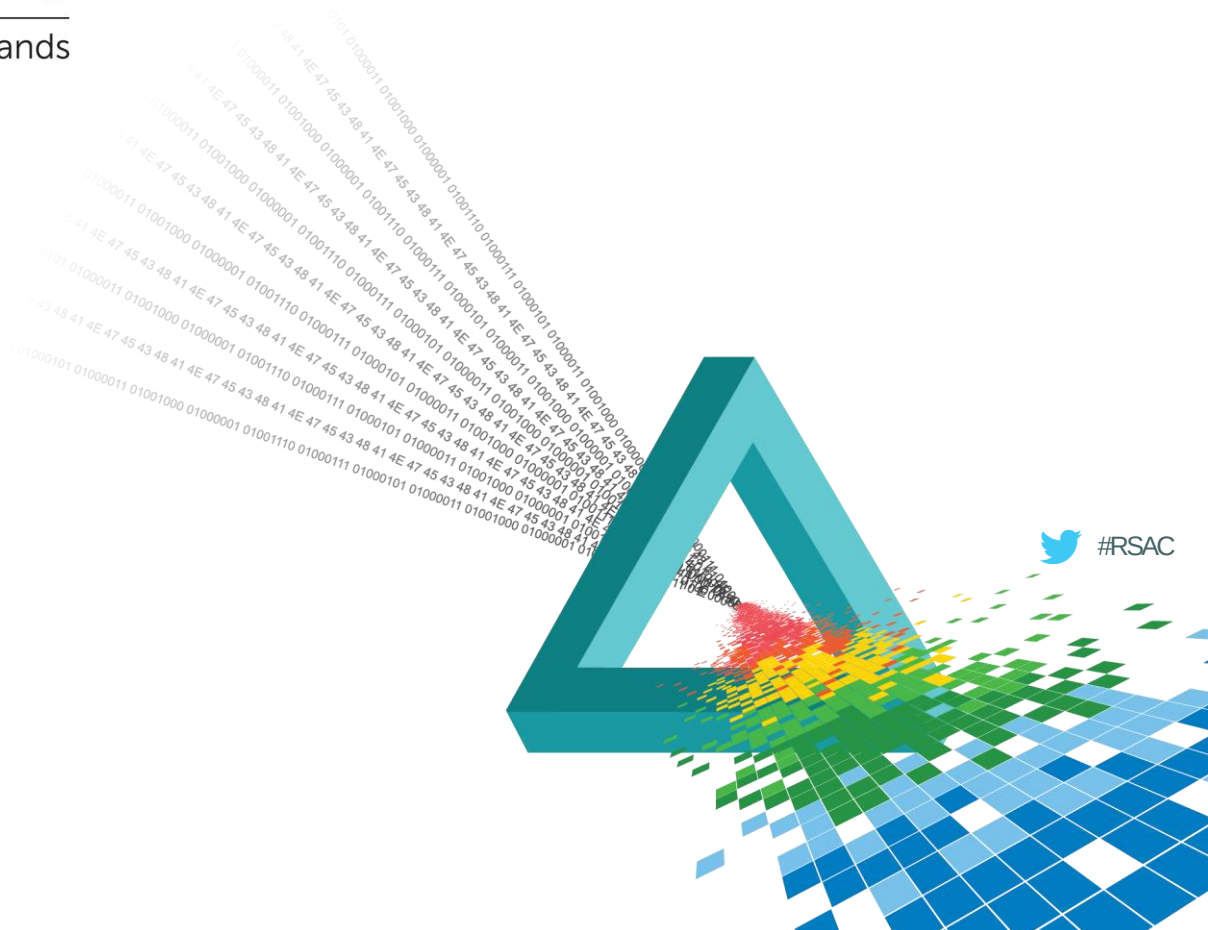
I'm not representing GP (GlobalPlatform), TCG (Trusted Computing Group), or ETSI (European Telecommunications Standards Institute), or my past/current/future employer in this session, thus the opinions do not reflect the official stance of the said-entities. Furthermore, the contents presented here are all based on publically-available material. Opinions are mine: your personal mileage may vary…



Agenda

- Motivations
- Mobile & IoT
- Standards
  - GP*
  - TCG
  - ETSI
- Conclusion

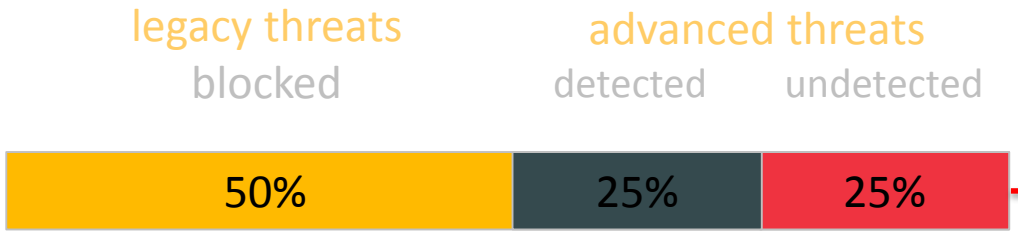
Motivation



General Threat Landscape

>3,000,000,000,000

threats annually



Standardization can help!

(avg. $27.3 loss per incident)

1.6 B

number of records lost globally in 2014

$236 M

recovery cost of Target breach (so far)

15 B

connected devices in 2015

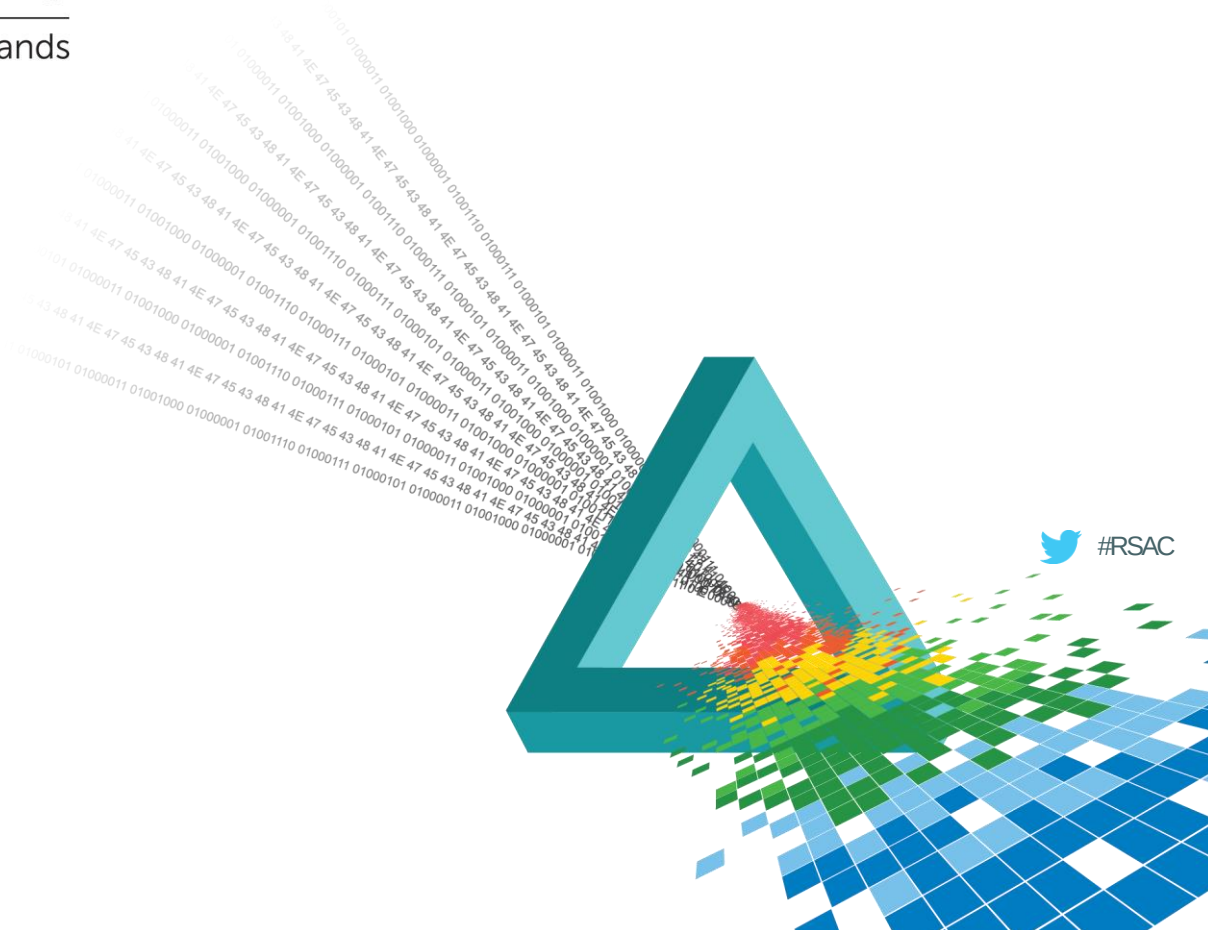
$110 BN

annual price tag of cybercrime

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Mobile



#RSAC

Evolution

- Two-way radio
- Mobile phone
- 06/29/2007: iPhone
- !Smart phone
- Tablets/Phablets enter the party
- Everything starts looking the same
- Mobile is being commoditized: transitioning out to IoT

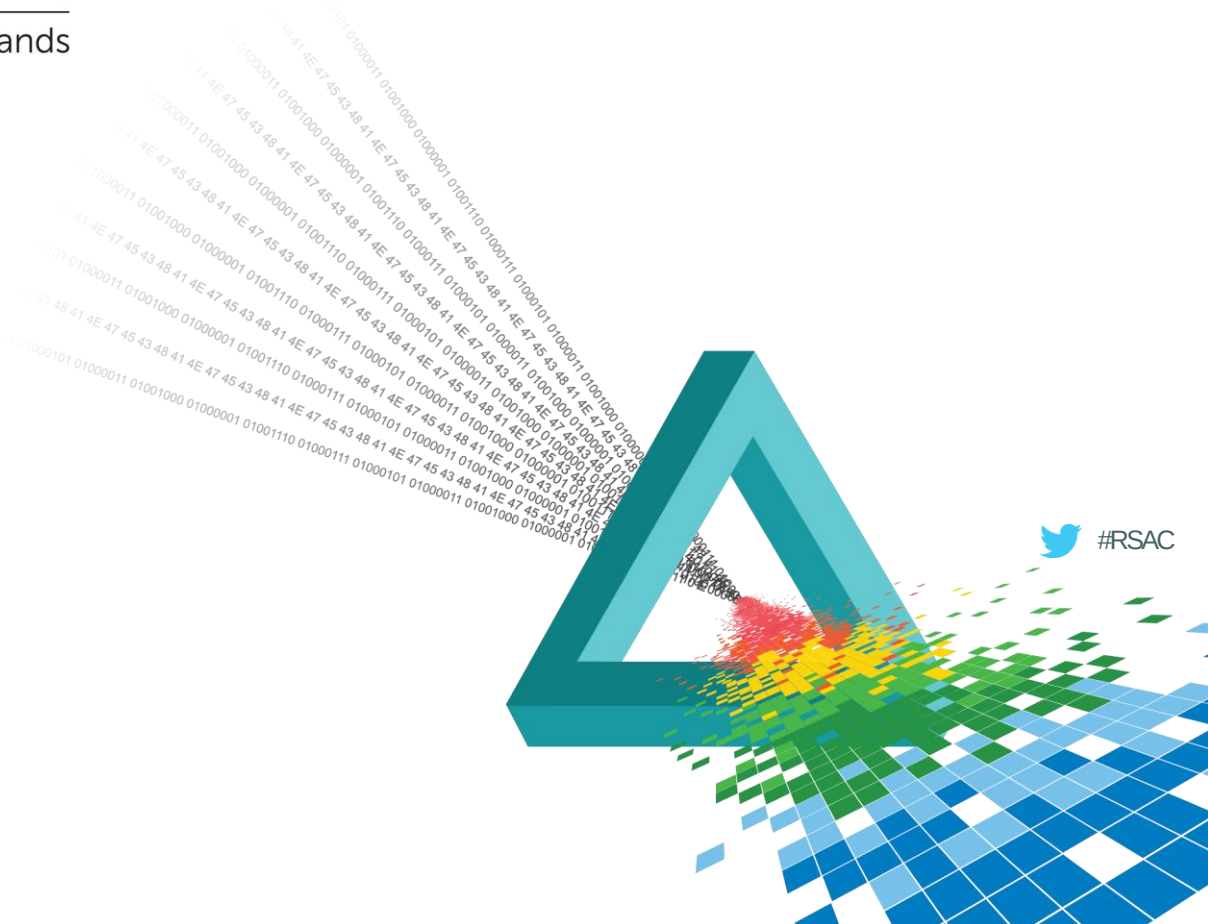
Mobile Security Observations

- Mobile security posture is [kind of] stabilizing*
- Core framework and device technologies are finally maturing
  - ROT/COT, SEforAndroid, ARM TrustZone, Mobile TPM/HSM, e/SE, etc.
  - Foundation technologies have/are being commoditized
- Ecosystem(s) consolidating:
  - SoC, OEM/ODM, Stack/OS, MNO, SP, MDM
- Liability boundaries are clearer now than in early days
- More capable [& cheaper] devices → more value-added auxiliary services
- Mobile attack surface hardening → attackers transitioning to softer targets

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

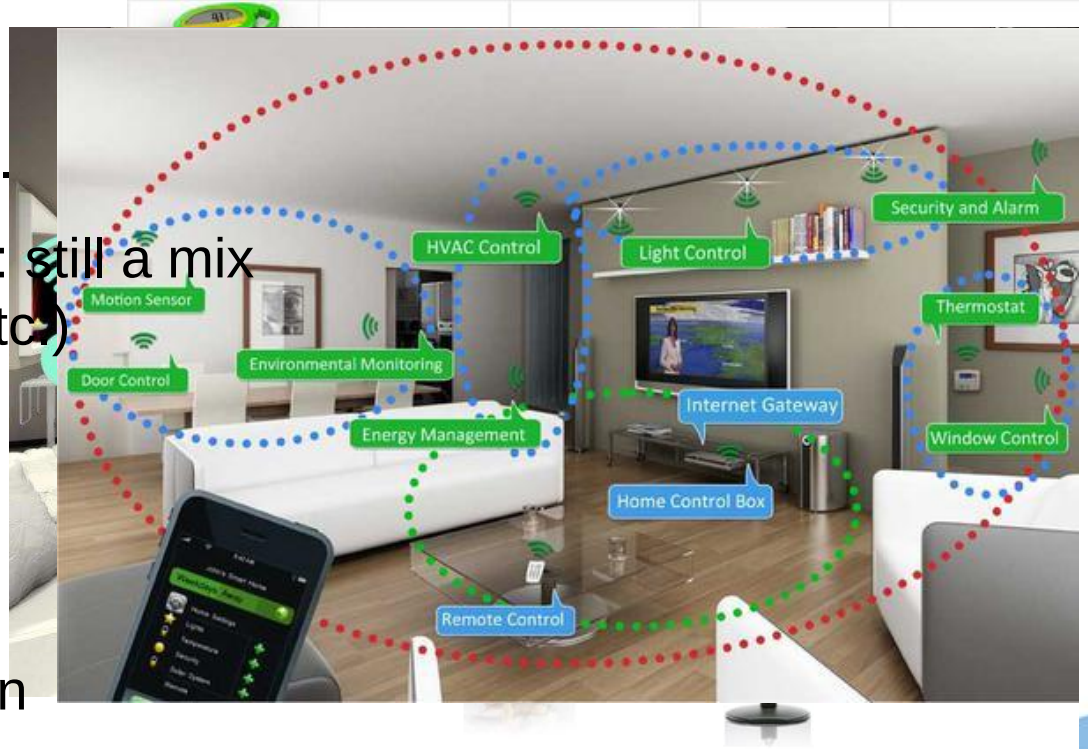
IoT



#RSAC

IoT

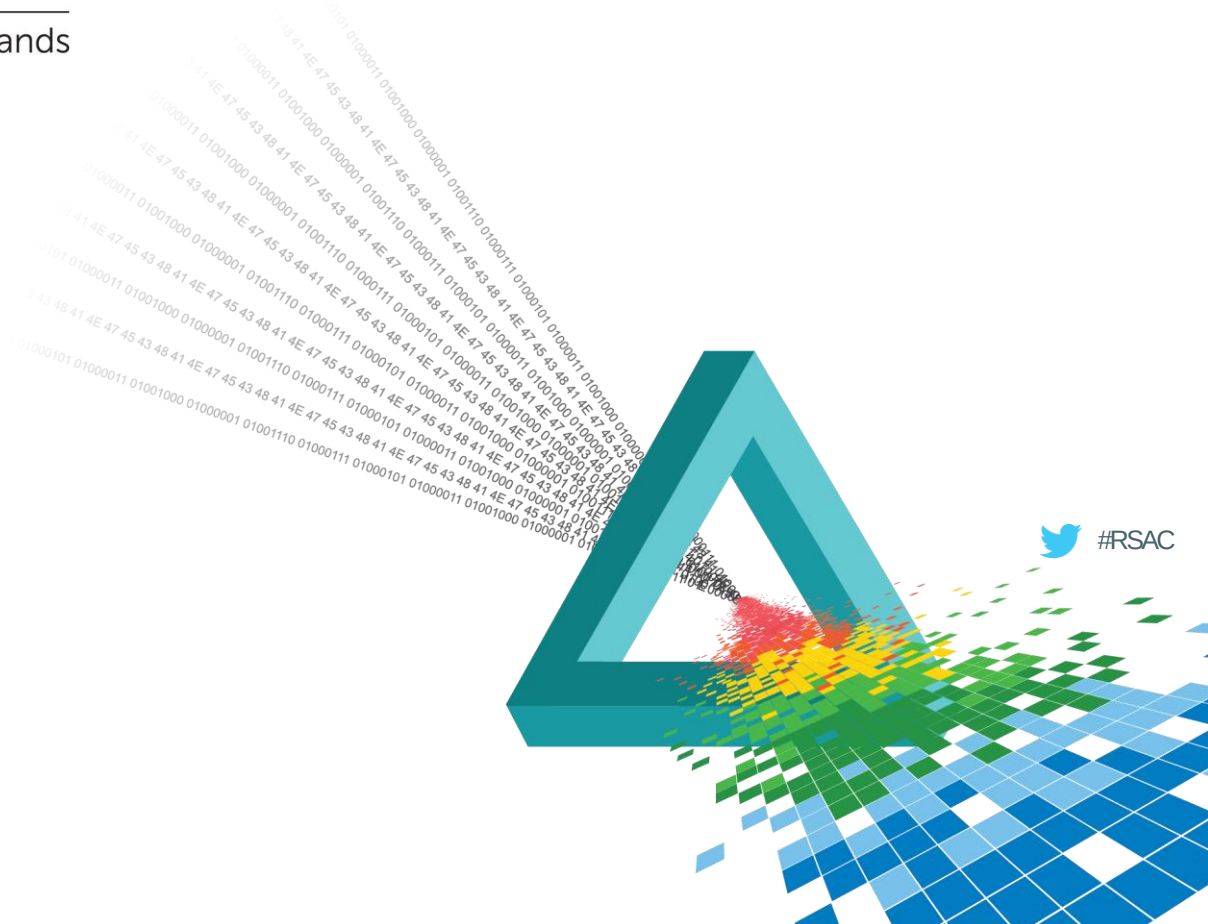
- Controllers, processors, CPUs. No standard comm.
- ~standard comm. stack(s): still a mix (WiFi, BT, NFC, ZigBee, etc.)
- Apps and ecosystem
- Transition to services
- Scaled-up connection
  → massive data generation



IoT Security Observations

- Lack of standardized orchestration layer
- Heterogeneous security capabilities
- Multi device management
  - Prone to TOCTOU attacks, among others
- Dangerous “atomic” view of the IoT devices
  - False sense of security
- Technologies, usecases, attacks, and standards still evolving

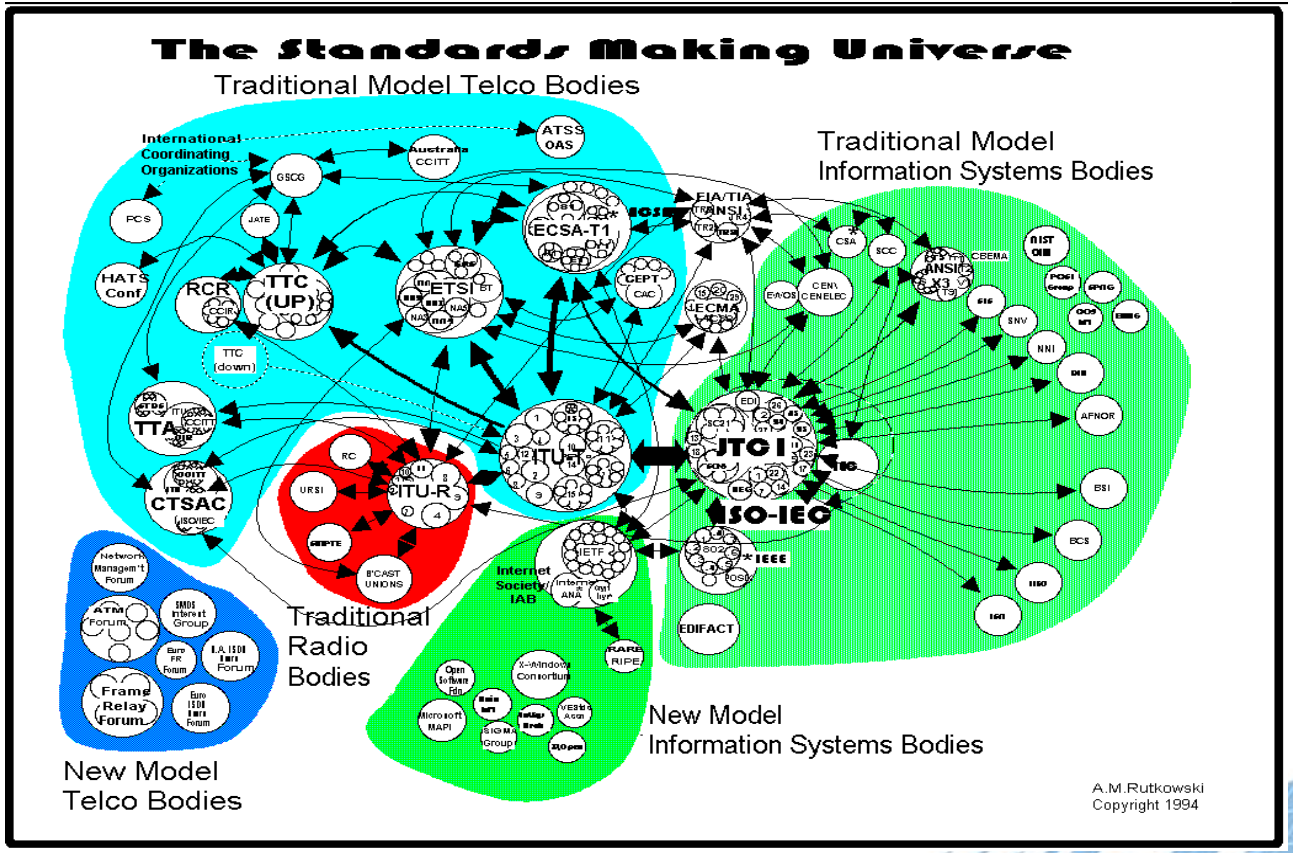
Standardization



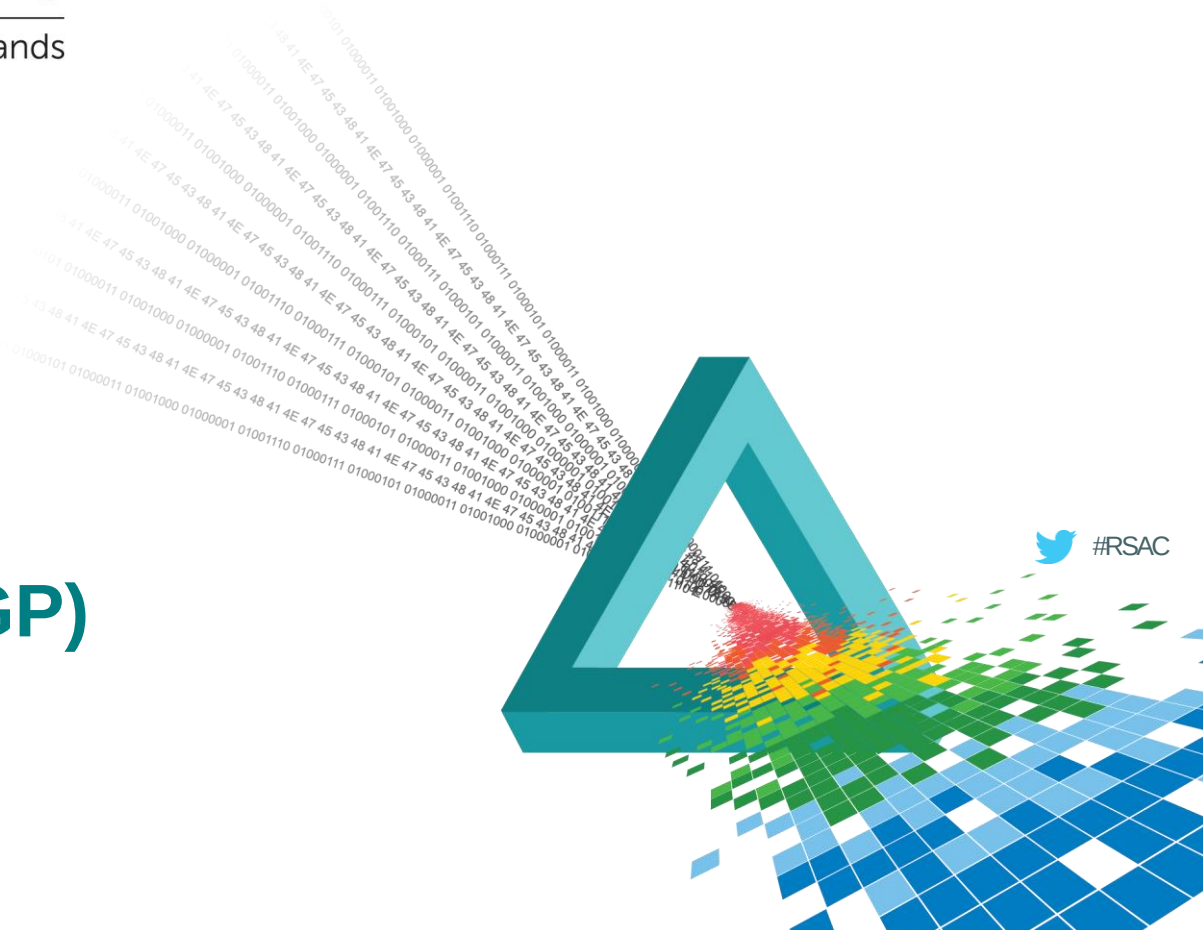
Why Standardization?

- Inherently a political process based on coopetition model
  - Most of the time, by mutually distrusting parties
- Similar to legislation: ineffective without meaningful implementation
- General benefits
  - Safety, reliability, business growth, interoperability, compatibility, repeatability, commoditization, support of policies & legislation
  - Quality: security is a subset of QA
    - i.e. verifying that the specifications are met and nothing else

Many Standardization Organizations (SO)



GlobalPlatform (GP)



GP Charter

- Working across industries to identify, develop and publish specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technologies

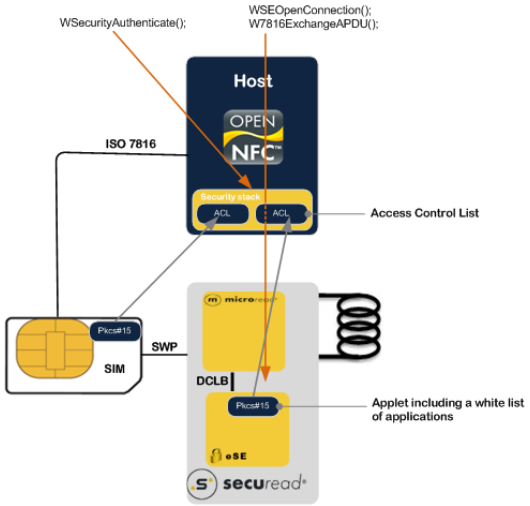
GLOBALPLATFORM®

GP Specifications Categories

- **Card**: Configurations, Composition Model, Security Guidelines for Basic Applications, Amendments A, B, C, D, E, F, APIs, Requirements Docs, Alternative Frameworks
- **Device**: TEE, TEE System Architecture, Client API, Internal APIs, Trusted Applications APIs, Internal Core API, SE API, Trusted User Interface API, Protection Profile, TEE TA Debug Specs., SE Management, SE Remote Application Management, SEAC
- **Systems**: System Messaging Specification, Systems E2E Simplified Service Management Framework, …

GP First Class Citizens: SE

- Secure Element (SE): a tamper-resistant platform (typically a one-chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data in accordance with the rules and security requirements set forth by a trusted authorities.



GP SE Relevant Specifications

GlobalPlatform Card Specification v2.2.1

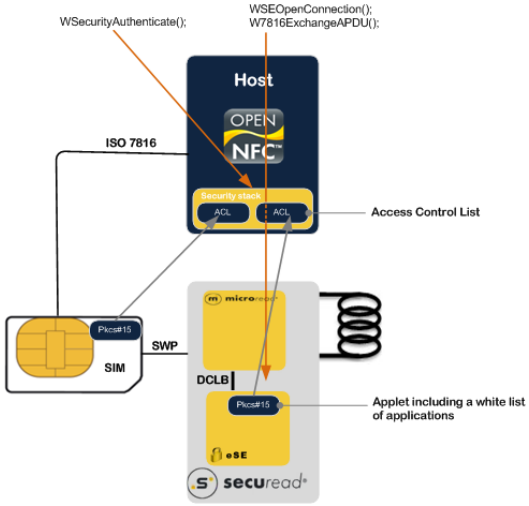
- Configurations
  - GlobalPlatform Card Common Implementation Configuration v1.0
  - GlobalPlatform Card Secure Element Configuration v1.0
  - GlobalPlatform UICC Configuration v1.0.1
  - GlobalPlatform Card ID Configuration v1.0
  - GlobalPlatform UICC Configuration - Contactless Extension v1.0
  - Mapping Guidelines of Existing GlobalPlatform Card Specification v2.1.1 Implementations v1.0.1
- Security Documents
  - GlobalPlatform Card Composition Model v1.1
  - GlobalPlatform Card Composition Model FAQs v1.1
  - GlobalPlatform Card Composition Model Security Guidelines for Basic Applications v1.0
  - GlobalPlatform Card Composition Model Security Guidelines for Basic Applications v2.0
- Amendments
  - Confidential Card Content Management – GlobalPlatform Card Specification v2.2 - Amendment A v1.0.1
  - Card Remote Application Management over HTTP Card Specification v2.2 – Amendment B v1.1.3 NEW
  - Card Technology Contactless Services Card Specification v2.2 – Amendment C V1.1.1
  - Card Technology Secure Channel Protocol '03' Card Specification v2.2 – Amendment D V1.1.1
  - Card Technology Security Upgrade for Card Content Management Card Specification v2.2 – Amendment E V1.0.1
  - Card Secure Channel Protocol '11' Card Specification v2.2 – Amendment F v1.0 NEW

GP SE Relevant Specifications

- Application Programming Interfaces
  - Java Card API and Export File for Card Specification v2.2.1 (org.globalplatform) v1.6
  - Card Contactless API and Export File for Card Specification v2.2.1 (org.globalplatform.contactless) v1.2
  - MULTOS(TM) API v1.0 for GlobalPlatform Card Specification v2.2.1
- Requirements Documents
  - Requirements for NFC Mobile: Management of Multiple Contactless Secure Elements v2.0
- Alternative Frameworks
  - Card Specification - ISO Framework v1.0
  - GlobalPlatform Card Networked Framework v1.0
  - HTML Java Card 3.0 API and ASN.1 Command for GlobalPlatform Card Networked Framework v1.0

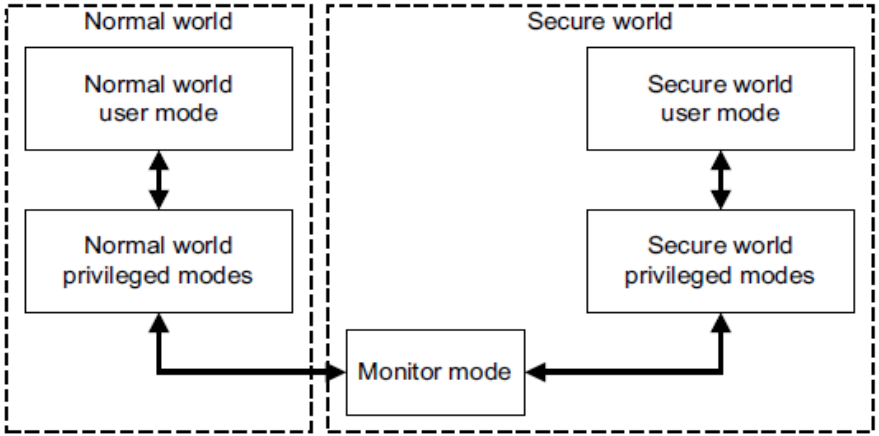
SE Security Observations

- Most prevalent form of hardware security chip
- Limited processing and storage capabilities
- Protection Profile (PP) defined and validated*
- Standardized by GP & Smart Card Alliance
- Majority of instances (UICC/SIM) use *proprietary** crypto algos (A3, A5, etc.)
- Security interactions among different types of SEs still somewhat wild and undefined
  - ROT, ACL, OTA, etc.?



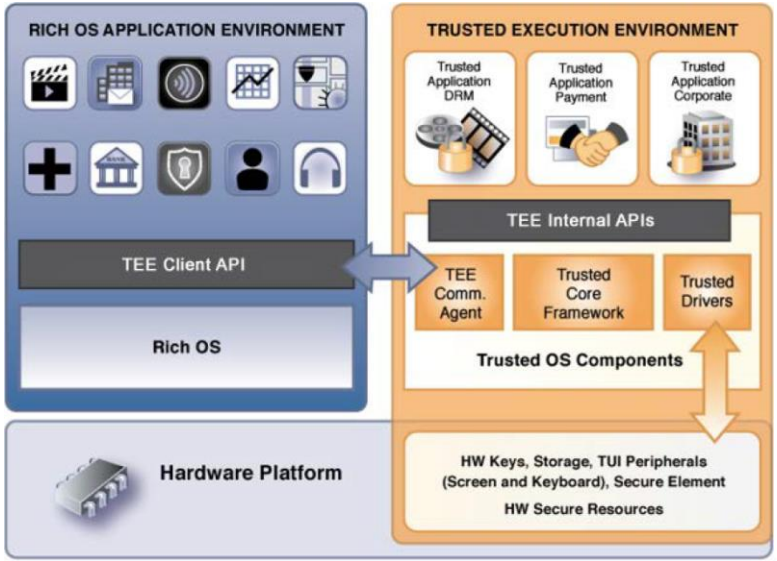
TrustZone®

- A carve out within Application Processor (AP) for
  - Running Trusted Applications (TA)
  - Providing HW-based isolation
  - Enabling privileged-access to system resources
- NS bit in the SCR in CP15 sets the “security state” of the complex
  - NS = 1 → processor in non-secure
  - NS = 0 → processor in secure state



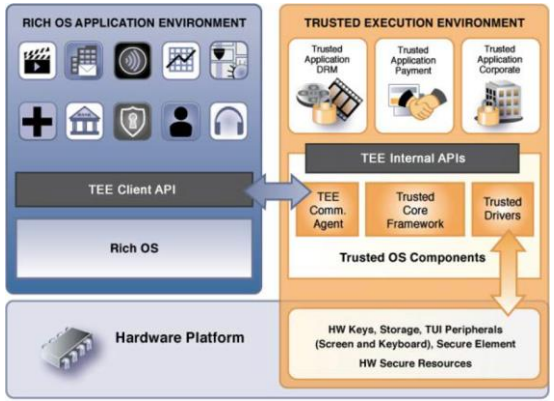
GP First Class Citizens: TEE

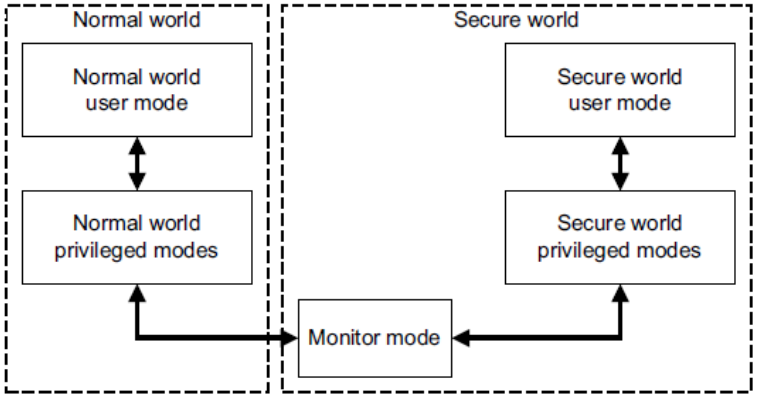
- Trusted Execution Environment (TEE): a separate execution environment that runs alongside a Rich OS and hosts trusted services offered to that rich environment.



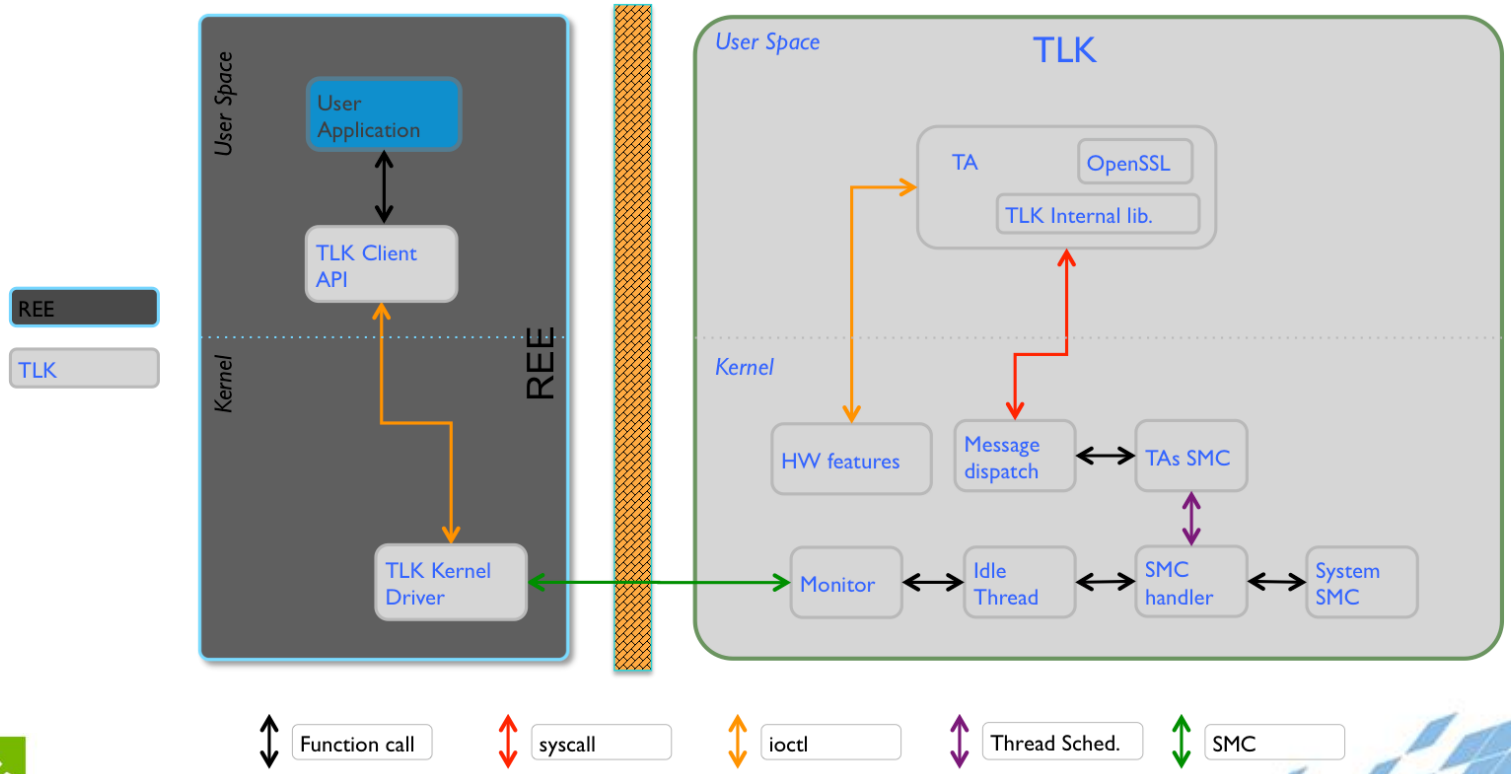
GP First Class Citizens: TrustZone®-based TEE

- Trusted Execution Environment (TEE): a separate execution environment that runs alongside a Rich OS and hosts trusted services offered to that rich environment.





TEE Software Stack: TrustedOS



GP TEE Relevant Specifications

Trusted Execution Environment (TEE)

- TEE System Architecture v1.0 | GPD_SPE_009
- TEE Client API Specification v1.0 | GPD_SPE_007
  - > Supporting Documentation
    - TEE Client API Specification v1.0 Errata and Precisions v2.0 | GPD_EPR_028

APIs for Trusted Applications

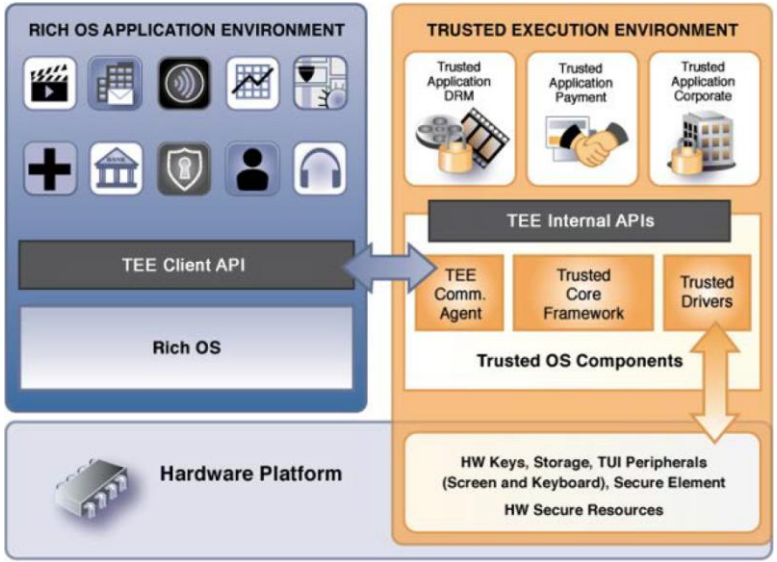
- TEE Internal API Specification v1.0 | GPD_SPE_010
  - > Supporting Documentation
    - TEE Internal API Specification v1.0 Errata and Precisions v1.0 | GPD_EPR_017
    - TEE Internal API Specification v1.0 Errata and Precisions v3.0 | GPD_EPR_017
- TEE Internal Core API Specification v1.1 | GPD_SPE_010

GP TEE Relevant Specifications

- TEE Secure Element API Specification v1.0 | GPD_SPE_024
  - > Supporting Documentation
    - TEE Secure Element API Specification v1.0 Errata and Precisions v1.0 | GPD_EPR_030
- TEE Sockets API Specification v1.0 | GPD_SPE_100 NEW
- Trusted User Interface API Specification v1.0 | GPD_SPE_020
- TEE Protection Profile v1.2 | GPD_SPE_021
- TEE TA Debug Specification v1.0 | GPD_SPE_025
- TEE Initial Configuration Test Suite 1.1.0.1

TEE Security Observations

- Interaction model
  - Dichotomized application
  - Secure World slave*
- Programming model
  - Primitive (ANSI C)
  - Isolation: challenging
- Security model
  - Prone to DOS attack
  - “Busy” Secure World
- Increasingly-complex TrustedOS*
  - Trusty, TLK, <t-base, SecuriTEE, OP-TEE, etc.
  - Reliance on Secure Boot



GP Specifications Sum Up

Card

- Specifications
- Application model
- Lifecycle
- Security

Device

- Specifications
- TEE Architecture
- REE/TEE Interaction model
- Security

Systems

- Messaging specifications
- E2E Simplified Service Management Framework
- Ecosystem, TSM

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

#RSAC

Trusted Computing Group (TCG)

TCG Charter

- The Trusted Computing Group (TCG) is a non-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of hardware-based root of trust, for interoperable trusted computing platforms
- Members include manufacturers, governments, and academics – Cloud computing, operating systems, security research, aeorospace, automotive, SoC, IoT, embedded systems, mobile phones, servers, PCs, laptops, tablets, memory, hard drives, etc.

TCG At A Glance

Solutions

- Authentication
- Cloud Security
- Data Protection
- IoT
- Mobile Security

First Class Citizens

- Trusted Platform Module (TPM)
  - Currently at TMP 2.0
- TCG Software Stack (TSS)

Other TCG Solutions

- Infrastructure
- PC Client
- Server
- Storage
- Trusted Mobility Solutions
- Trusted Multi-tenant Infrastructure
- Trusted Network Communications
- Network Access & Identity
- Trusted Platform Module
- Virtualized Platform

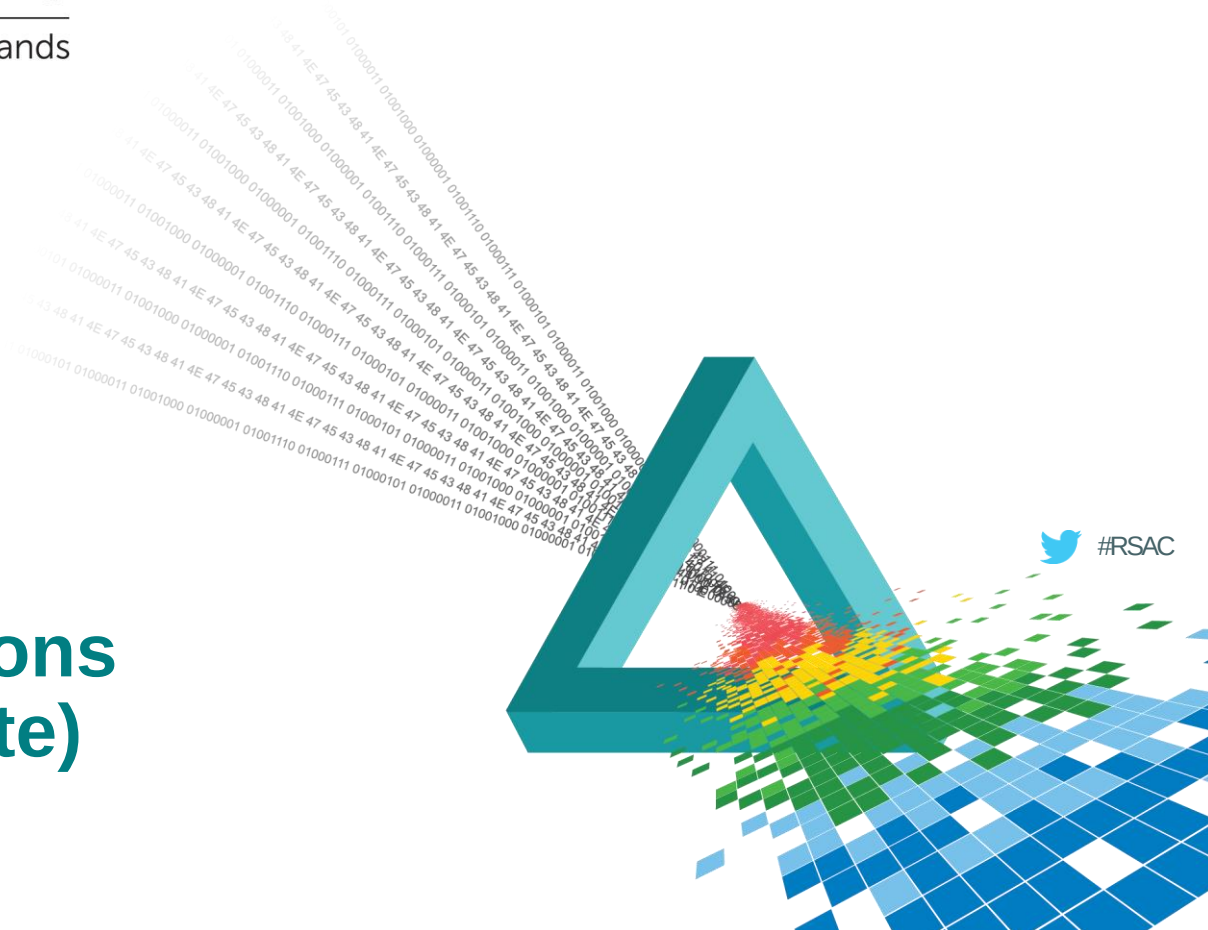
Notable Specifications & Resources

- **Embedded Systems:** TCG TPM 2.0 Library Profile for Automotive-Thin, TCG Guidelines for Security IoT
- **Mobile:** TPM 2.0 Mobile CRB (Command Response Buffer) Interface Specification, TCG TPM 2.0 Mobile Common Profile, TPM 2.0 Mobile Reference Architecture Specifications
- **TSS:** TSS TAB (TPM Access Broker) Interfaces and Resource Manager, TSS System Level API and TPM Command Transmission Interface Specification, TSS Feature API Specification, TSS Specification, TCG Architecture Overview

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

ETSI (European Telecommunications Standards Institute)



ETSI Charter

- An independent, not-for-profit organizationETSI's Mission Statement describes the primary task to produce top-quality standards for information and communications technologies, including fixed, mobile, radio, converged, broadcast and Internet technologies.
- ETSI has a special role in Europe, including supporting European regulations and legislation through the creation of "Harmonised European Standards."

ETSI
World Class Standards

ETSI Technology Clusters

ETSI Standards Types

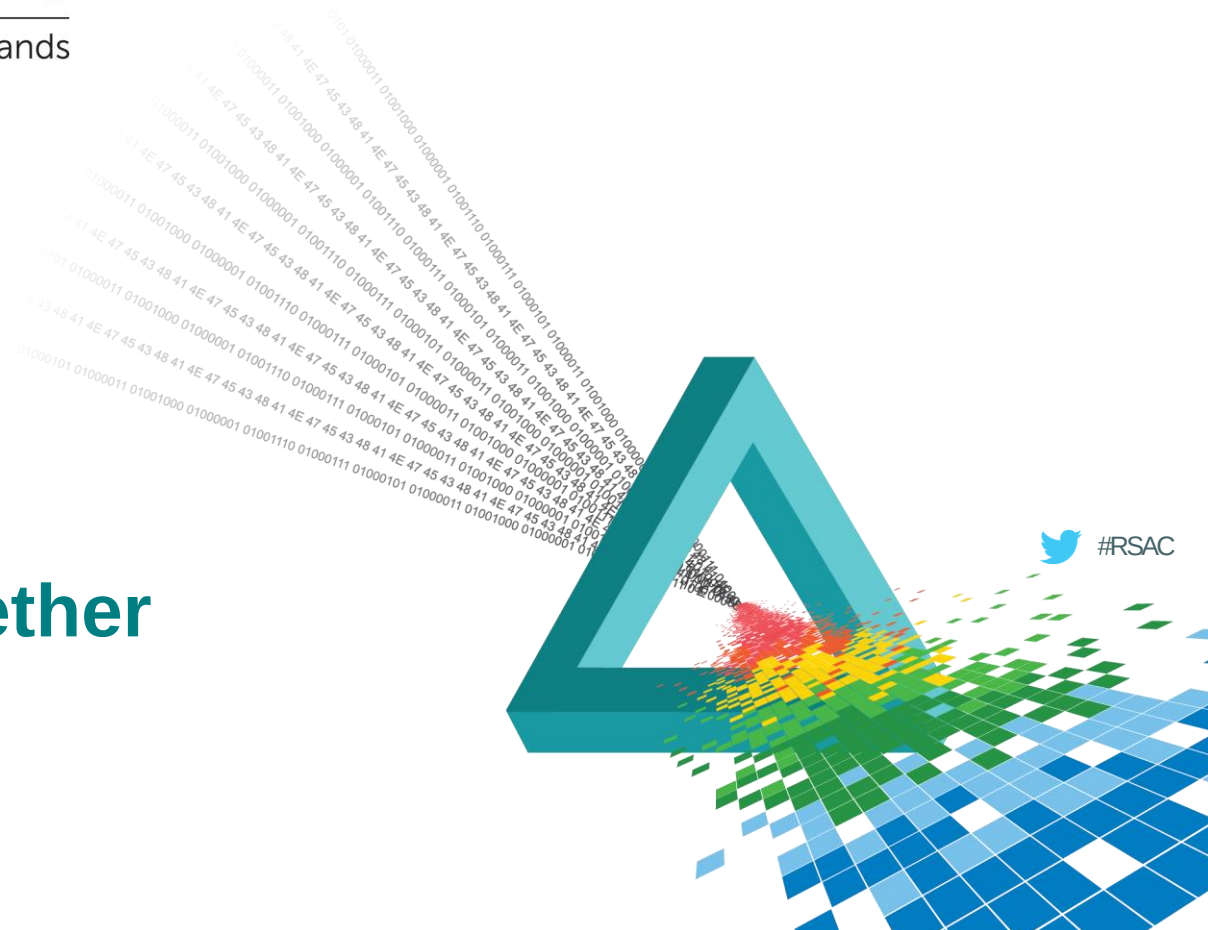
- European Standard (EN)
- ETSI Standard (ES)
- ETSI Guide (EG)
- ETSI Technical Specification (TS)
- ETSI Technical Report (TR)
- ETSI Special Report (SR)
- ETSI Special Report (SR)
- ETSI Group Specification (GS)
- Harmonized Standards
- Community Specifications

Notable Technologies & Standards

- M2M (Interoperability, Communications, Automotive, Smart Metering)
- Mobile (UMTS, 3GPP, GPRS, PCC)
- Security (ESI, CAT, HCI, SWP, LI, SSD)

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

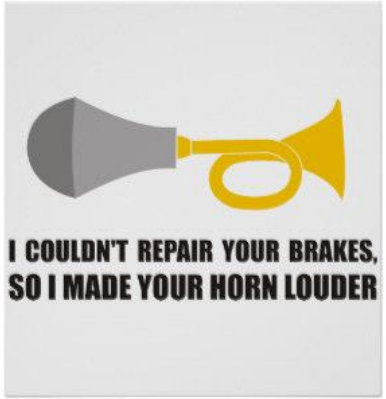


#RSAC

Putting It All Together

Apply

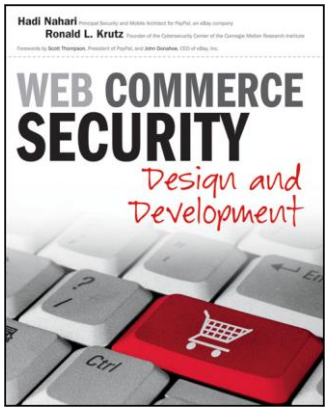
- If you're dealing with any of these use cases, then get acquainted with GlobalPlatform
  - (mobile) payment, Trusted User Interface, DRM, HDCP, multiple TA
- If you rely on or interact with low-level [HW] system security constructs, then you must be well-versed with TCG standards
- If your products or services rely on telecommunications, and/or you operate in Europe, then follow ETSI



RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Thank You!



http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470624469.html

Hadi Nahari
hnahari@nvidia.com
hadinahari

#RSAC