GLOBALPLATFORM

Introduction of GlobalPlatform as partner Type 2
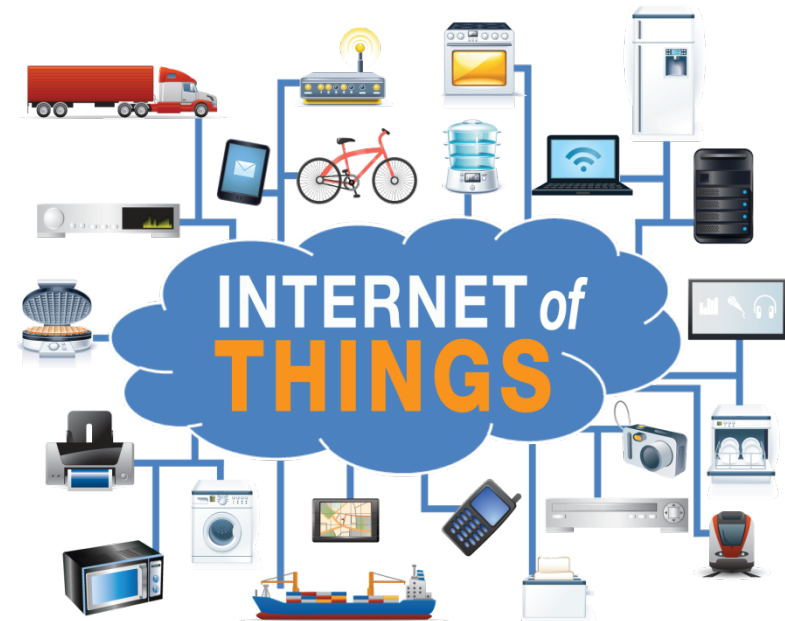
TP-2015-0748

Sebastian Hans / ORACLE

GlobalPlatform IoT Task Force chair

oneM2M TP#18

July 2015

@GlobalPlatform_

www.linkedin.com/company/globalplatform

Welcome

GlobalPlatform Mission

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

- GlobalPlatform Specifications enable trusted end-to-end solutions which serve multiple actors and support several business models

GlobalPlatform Vision

- Member-driven organization to define technology standards for cards, devices and systems and create foundation for future growth.

- License royalty-free card, device, and systems specifications.

- Compliance Program tools to verify card, device, systems compliance to GlobalPlatform technology.

- Foster adoption of secure chip technology standards and implementations across industries.

GlobalPlatform Positioning

GlobalPlatform is *the* standard for managing applications on secure chip technology

TRUSTED EXECUTION ENVIRONMENT

MESSAGING

SECURE ELEMENT

Across several market sectors and in converging sectors

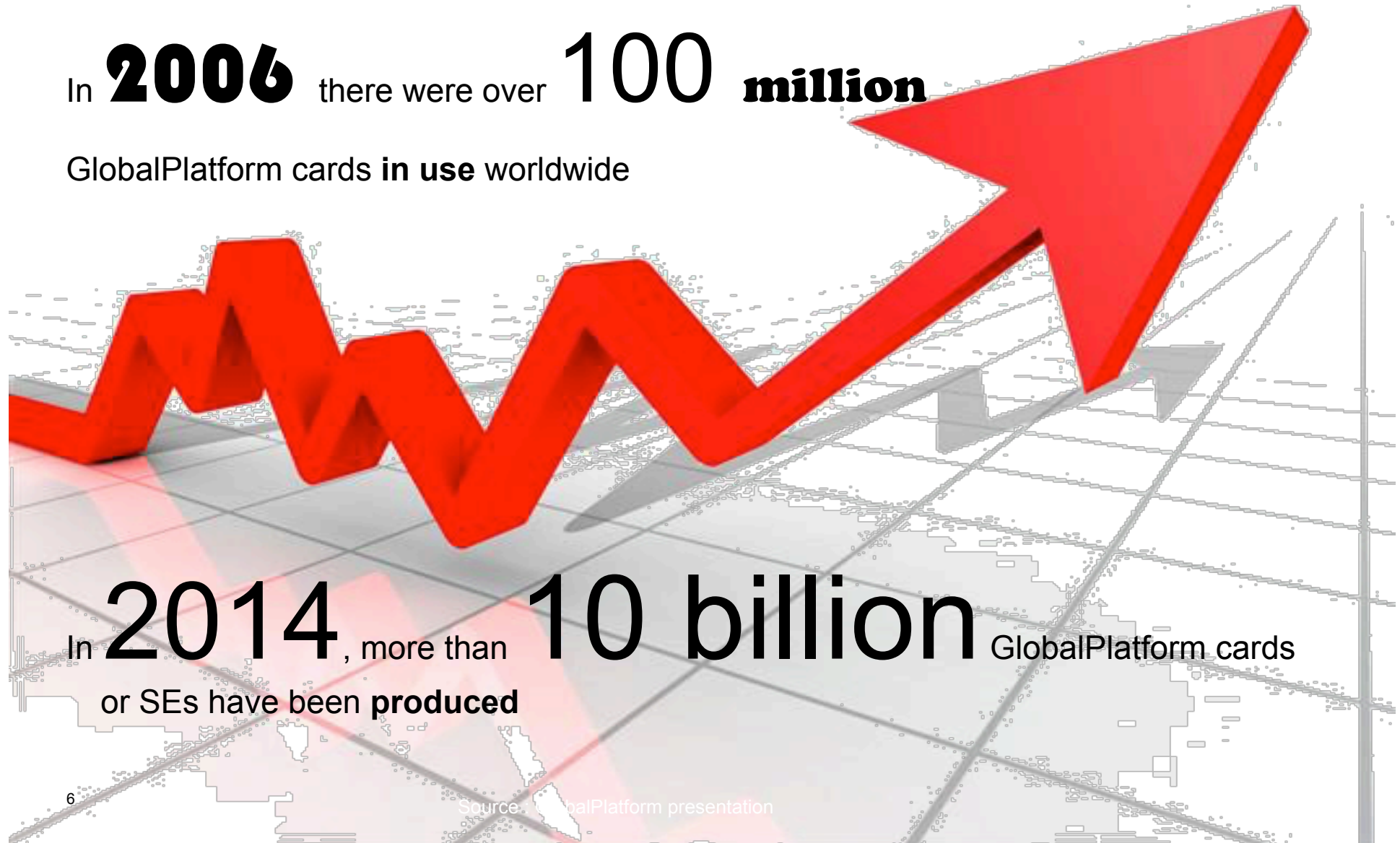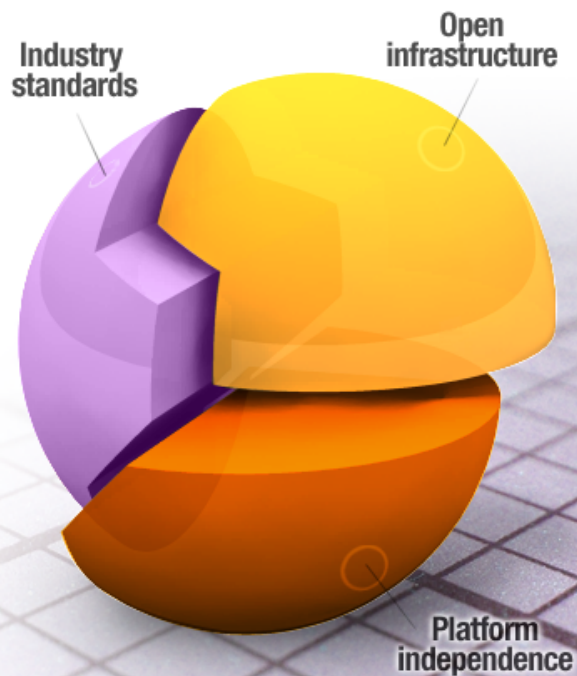| PREMIUM CONTENT | FINANCIAL | TELECOM | GOVERNMENT | AUTOMOTIVE | HEALTHCARE | RETAIL | TRANSIT |

Strong Rate of Growth

In **2006** there were over 100 **million**

GlobalPlatform cards **in use** worldwide

In 2014, more than 10 billion GlobalPlatform cards or SEs have been **produced**

6

Source: GlobalPlatform presentation

GlobalPlatform At-a-Glance

GLOBALPLATFORM

Industry standards

Open infrastructure

Platform independence

What is the output of GlobalPlatform?

Specifications – technical industry guidelines

Configurations – applying the guidelines to different market sectors

Security Certifications – streamlining security requirements & testing

Industry Compliance Program – confirming a product's functionality aligns to GlobalPlatform technology

Educating the Industry – white papers & technical documents

Workshops – specification training & educational

GlobalPlatform Members

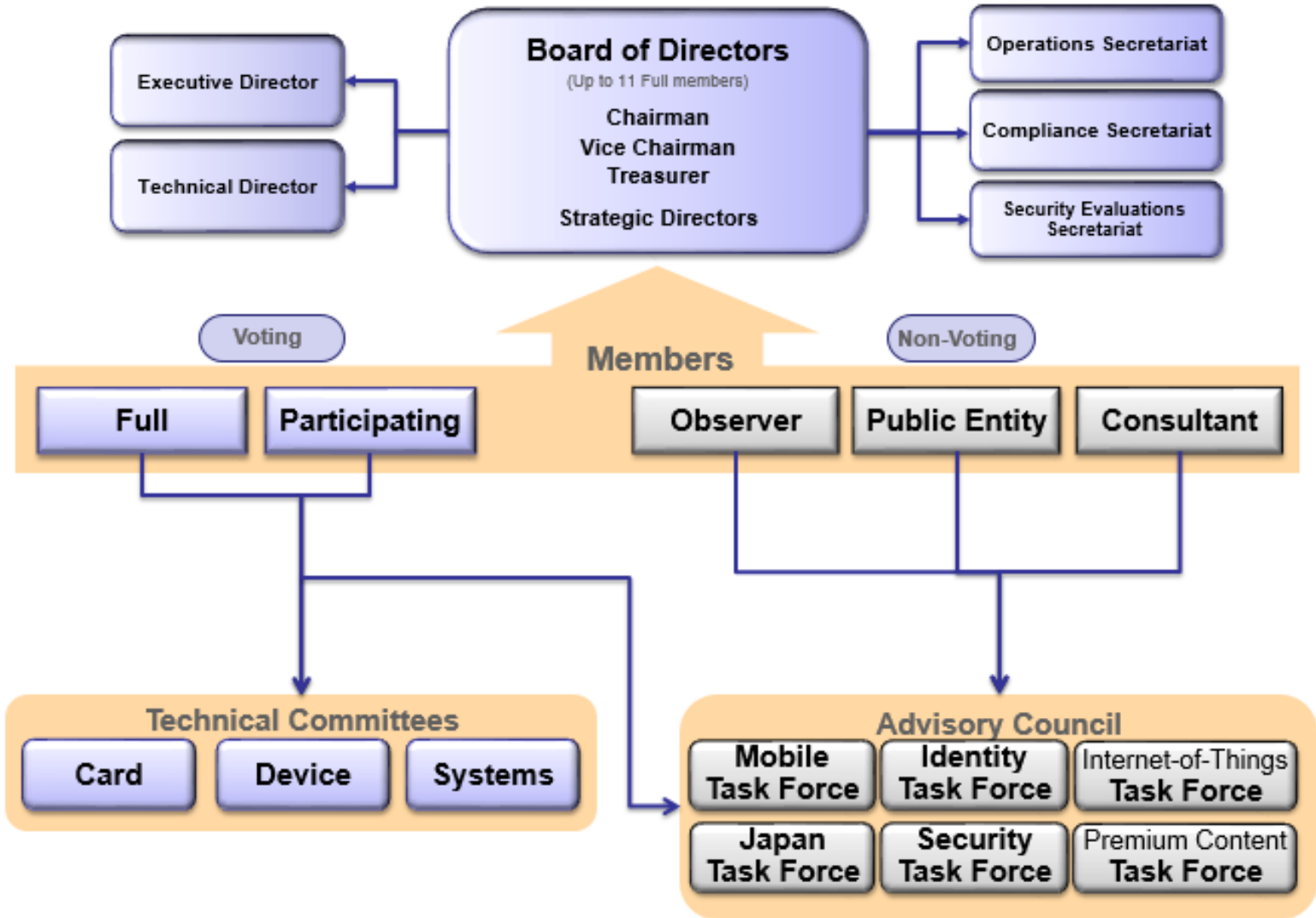# Our Collaborative Industry Partners

GlobalPlatform Structure

Organizational Structure

Board of Directors
(Up to 11 Full members)

Chairman
Vice Chairman
Treasurer

Strategic Directors

Executive Director

Technical Director

Operations Secretariat

Compliance Secretariat

Security Evaluations Secretariat

Voting

Non-Voting

Members

Full | Participating | Observer | Public Entity | Consultant

Technical Committees
Card | Device | Systems

Advisory Council
Mobile Task Force | Identity Task Force | Internet-of-Things Task Force
Japan Task Force | Security Task Force | Premium Content Task Force

Why this Impressive Success ?

- Pilots have demonstrated the attractiveness of a multi-application device to the end-user
  - Smartphone: always there, always on

- GlobalPlatform technology is neutral regarding the business model used in a project (e.g. multiple form factors, multiple businesses…)

- GlobalPlatform integrates with external standardization

- GlobalPlatform has had a strong knowledge of 'ecosystems' since 1999
  - Learned the hard way
  - Each party (with its differences) are respected

- The same 'object' supports different models
  - Investment from different actors in different models are shared
  - → eSE deployment helps UICC deployment and motivate SD deployment

In the end it's about enabling application & services whatever the business environment supported by multiple players worldwide

GlobalPlatform and IoT

Security and Privacy

- IoT devices are used in the context of critical infrastructure or potentially dangerous systems, such as transportation systems, water pumps, electric substations and medical devices.

28th Chaos Communication Congress
Behind Enemy Lines

Smart Hacking For Privacy

Advanced metering devices (aka smart meters) are nowaday
networks in Germany, in other parts of Europe and in the U
amendment especially in Germany they become more and m
new and refurbished buildings.

Unfortunately, smart meters are able to become surveillance dev
customers leading to unprecedented invasions of consumer priva
consumption data is transmitted to the utility company in princip
and monitoring of equipment within con
different reports.

This talk is about the Discovergy / Easy
our analysis we found several security b
missing security features for the meterin
unencrypted, although otherwise stated
performed on a sealed, fully functionall

In our presentation we will mainly focus

THREAT LEVEL

It's Insanely Easy to Hack Hospital Equipment

BY KIM ZETTER 04.25.14 | 6:30 AM | PERMALINK

Share 4.0k   Tweet 3,006   g+1 465   Share 1,372   Pin it

SECURITY

Students hack Tesla Model S, make all its doors pop open IN MOTION

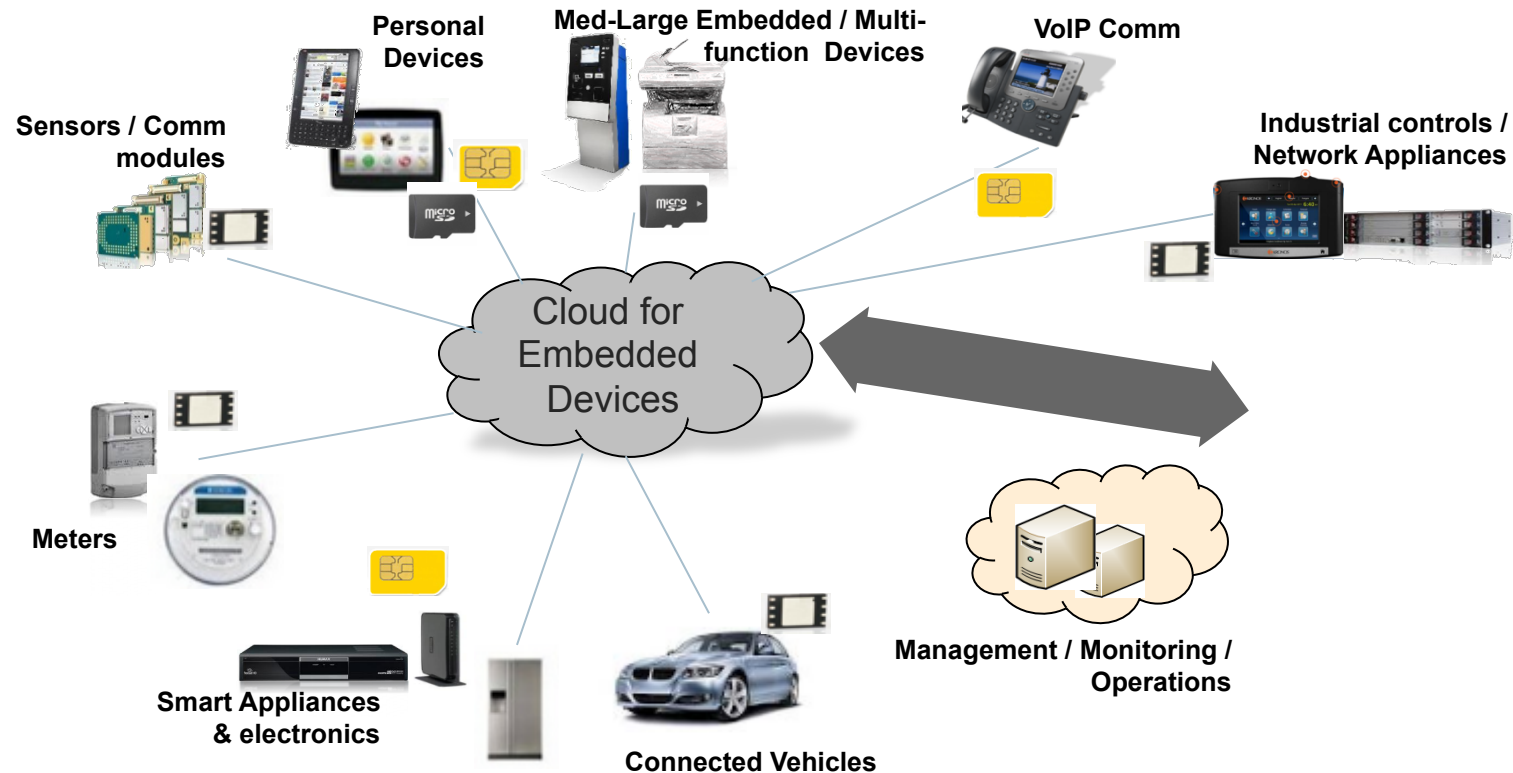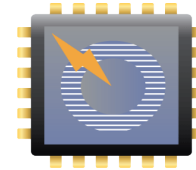### Toot the horn, too

By Darren Pauli, 21 Jul 2014   Follow 2,473 followers

13

Devices in Scope for GlobalPlatform's IoT Task Force

GLOBALPLATFORM

- The IoT Task Force is focusing on M2M/IoT devices with a secure element (SE) or a TEE
  - the SE is a tamper resistant element
  - no restrictions on the form factor

GlobalPlatform Assets

- What can be the role of GlobalPlatform in the IoT market ?
  - Focus on our existing assets and how they can be leveraged in this new market

- GlobalPlatform specifications define a Secure Element (SE), which is a removable or non-removable semiconductor device. These are often used in the form factor of a SIM/UICC card, a generic smart card, or a solderable secure device.

- GlobalPlatform defines the TEE platform as secure environment running in an isolated process on the device to protect assets and execute trusted code

- *Specifically, GP assets can be used in the following IoT contexts:*
  - Secure Environment for IoT Device/Gateway (SE,eSE,TEE)
  - Trust Management in Multi-Application and Multi-Actor Environments
  - Provisioning of Credentials and Applications
  - Compliance Testing and Security Evaluation

Remote Management

- One category of IoT devices is those required to have long lifetimes because they are built-in or part of an infrastructure that is amortized over decades

- For a service to remain competitive throughout such a time span it must be possible to efficiently manage:
  - patching, updating, reconfiguring, or changing data or software of the devices

- It is not practical in many IoT deployments to manage devices on-site:
  - the actual device may be hard to access due to its placement
  - the device may not even have a user interface
  - the cost of a person visiting sites may not be supported by the business model

- Such lifetime constraints are particularly sensitive for security, as threats are continuously evolving

- *GlobalPlatform sees a strong need for 'efficient and standardized' remote management of secure elements in IoT*

Remote Management

GlobalPlatform's in IoT/M2M

- Examples of IoT/M2M organisations that leverage already existing GlobalPlatform technology:
  - oneM2M devices with a security environment
    - can be a UICC but can be any other type of secure environment, e.g. SE, or Trusted Execution Environment (TEE)
    - oneM2M leverages extensively the technology from GlobalPlatform in their security specification
  - OMA Lightweight M2M device
    - configuration of the device security from the smart card
    - loading data and credentials for the initial setup of the device from a file system in the card
    - secure channel protocol from GlobalPlatform between SE and Application in the device
  - GSMA
    - GlobalPlatform technology is the baseline for their eUICC specification targeting the M2M market

Current Work in the IoT Task Force

- Threat analysis of IoT architecture and deployments
  - Mapping of GlobalPlatform technology to security requirements and development of new requirements for further development in GlobalPlatform

- Adoption of existing and development of new specification for the management of eSE/TEE in IoT deployments
  - Today we can handle perform management based on the direct communication between Admin Server and UICC or Admin Server and hosting device
  - Need to further development for end-to-end security with multiple hops between Admin Server and end device

- Integration of the eSE/TEE with Bluetooth LE
  - Discovery and communication

- Integration with the TPM world for new markets like IoT and Automotive
  - Increasing the value of the Secure Component

www.globalplatform .org

Thank you!