Alliance for Internet of Things Innovation

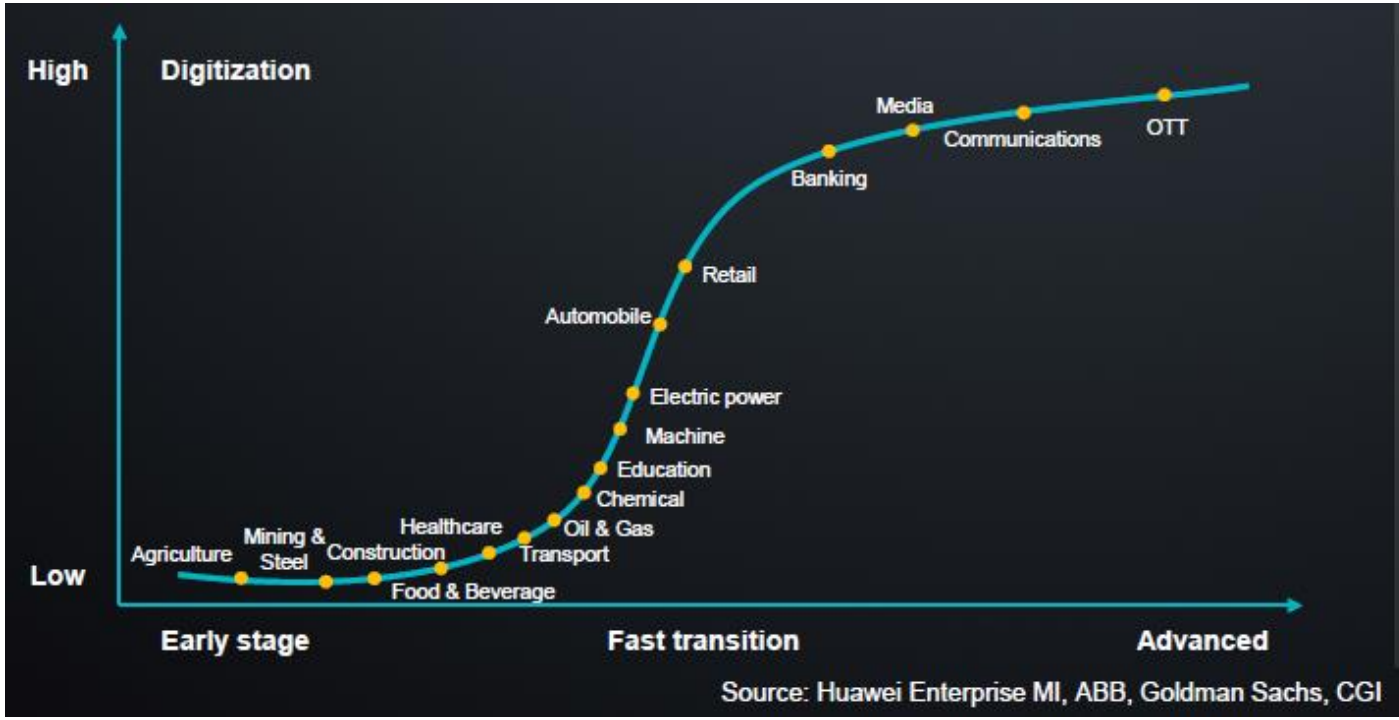
IoT Week 2018, 7th June 2018

Strengthening Trust in IoT using Standardization/Certification

Georgios Karagiannis

Huawei / AIOTI WG03 Vice-Chairman

Trends in Digital Transformation



Source: Huawei Enterprise MI, ABB, Goldman Sachs, CGI

- 64% of enterprises are already exploring and trying digital transformation. (Source: IDC)
- 67% of CEOs in 2,000 multinational companies have set digitization at the center of their corporate strategy. (Source: Gartner)
- Digital transformation is an imperative for all industries.

Internet of Things and Risks

- Digital Transformation changes the world at fast pace
- Internet, digital services and cloud computing are the living proof at a massive scale
- Internet of Things technologies accelerate this process even more by hyper-connecting people, organizations and data with billions of objects
- Risks:
  - Every networked device is potential target for hackers
  - New cyber threats linked to monetization methods, attacks on democracies and personal data theft
  - No user of a networked device can be absolutely sure that device only features functions and executes data flows specified by persons or bodies authorized to do so

AIOTI

Strengthen Trust in IoT

- Standardization / certification provides means to minimize risks and strengthen trust of citizens, consumers, businesses and other persons and organizations on demand side

Security by design and by default:

define/select a reference architecture model

apply on complete supply chain of IoT products and services

agree on security standards, procedures, processes and risk and impact management

well understood and securely managed and up-datable settings

Privacy by design:

minimize use of personal data

protect personal data in all phases of personal data life cycle:

obtain/collect, create/derive, use, store, share/disclose, archive, destroy/delete

Certify IoT security assurance levels to increase Trust in IoT:

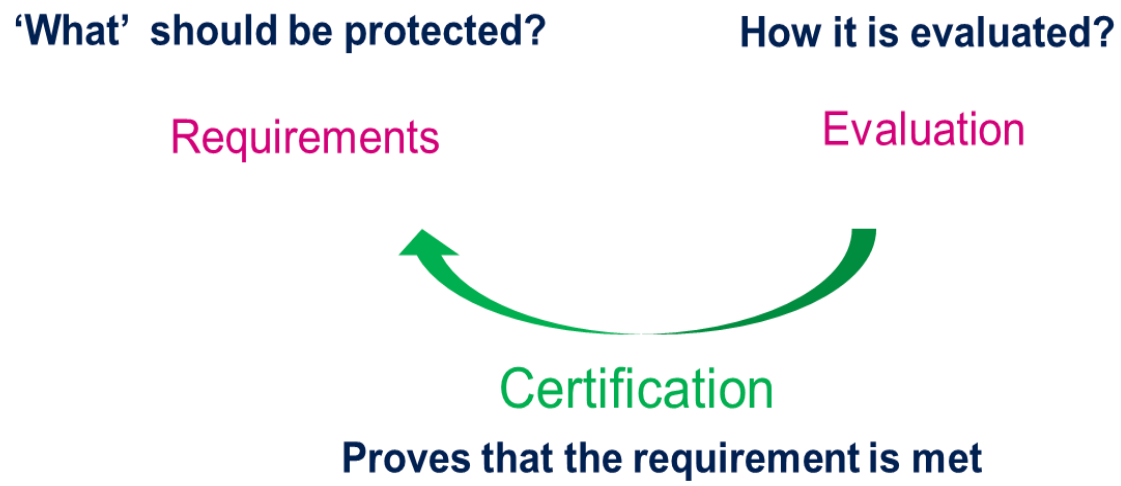
basic, substantial and/or high security assurance levels – EU CyberSecurity Act

depending on risk use self-assessment and third party assessment by accredited third party

AIOTI

Samples from AIOTI position on EU CyberSecurity Act:

- Scalable certification framework
  - Adopt scalable risk based approach according to risks and criticality of products and services to be covered by EU certification schemes



Samples from AIOTI position on EU CyberSecurity Act:

- Three AIOTI views on Security Assurance Levels of a certification scheme (basic, substantial and/or high, for ICT products and services):
  I. Welcome three security assurance levels since they provide a degree of confidence in the claim of asserted security qualities of a process or service:
     - basic security level assessment done by checklists
     - substantial and/or high done by accredited laboratories
  II. Levels need to be further expanded to alleviate fear of security as a barrier for small and medium sized enterprises
  III. Move definition of assurance levels to each specific certification scheme that will have different assurance levels depending on e.g., goals, sector, stakeholder

Samples from AIOTI position on EU CyberSecurity Act:

Certification Assessment	Both self-assessment and third party assessment depending on risk assessment, e.g., critical infrastructures
Muti-stakeholder Participation	CyberSecurity can be addressed in private-public ecosystem, where also society and relevant stakeholders, e.g., from industry are involved
Transparency	Transparency and openness of certification information
Validity of Certificate	EU certification framework need to be agile and flexible to adapt to wide scope of ICT products and services, e.g., validity of certificate should be defined in each scheme on a case-by case basis
Reference to Standards	For competiveness purposes, certification schemes shall be based on international and European standards to provide common rules, increase transparency and allow for a fair comparison of products and suppliers
Sector Specific Requirements on standards which certification will be made against	Standard levels applicable to all sectors as common baseline; Complemented by sector specific standards level according to targeted products/services/ sectors

Alliance for
Internet of Things
Innovation