Joint Workshop: Internet of Things for Smart Cities & Communities

IoT Standards Trends and Convergence

IoT Standards in the Convergence Turmoil

Presented by: **Emmanuel Darmois**   For: **IoT Week 2019**

20.06.2019

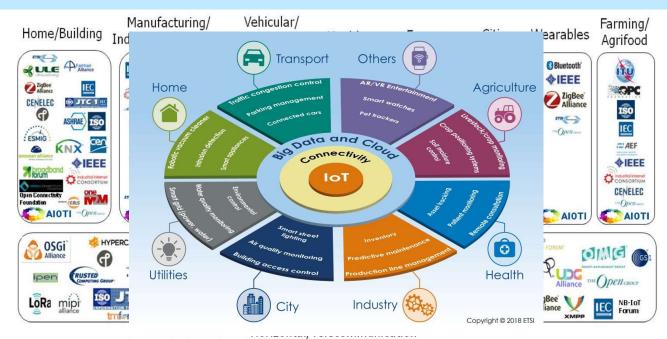# Trends

IoT Week 2019 - IoT Standards Trends and Convergence

The intrinsic complexity of IoT have a profound impact on IoT Standardisation and how standards are actually used

Pervasive ICT technologies, Multiple Point Solutions (e.g. protocols)

Sector-specific solutions (and silos), Cross-sector system deployment

Source: AIOTI WG3 (IoT Standardisation) – Release 2.8

How to Make Decisions in a Fragmented Standards Landscape?

Another complication: Standards and Standardisation are only a small part of the solutions

Standards	Open Source	Regulation
Industry	**Stakeholders**	**Research**
Skills	**Strategies**	**Organisations**

Addressing IoT Systems Complexity

Dealing with IoT characteristics

High-level issues in support of strategy

- Stakeholders Involvement
- Technical strategy
- Deployment models
- Integration of/with legacy

Specific technical elements

- Interoperability
- Privacy
- Security

Integrating some important aspects

Stakeholders and roles

- Many roles (not just technical)
- Potentially conflicting requirements

Reference Architecture

- Shared understanding
- Documented technical choices

Support to the non-specialist

- Guidelines for decision and usage
- Teaching material

Possible Ways to Operate in the IoT Ecosystem
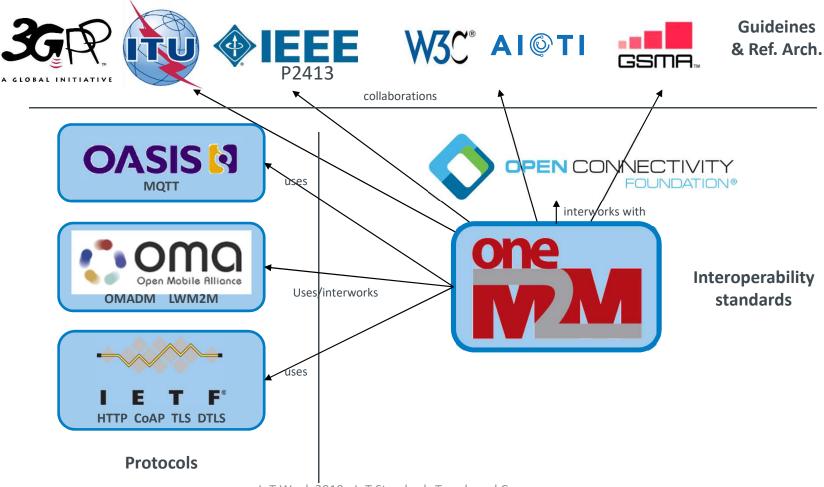
SDO collaboration
the example of oneM2M

ETSI

3GPP A GLOBAL INITIATIVE   **ITU**   **IEEE** P2413   **W3C®**   **AI TI**   **GSMA**   **Guideines & Ref. Arch.**

collaborations

OASIS MQTT ←uses

OPEN CONNECTIVITY FOUNDATION®

interworks with

oma Open Mobile Alliance OMADM LWM2M

one M2M **Interoperability standards**

Uses/interworks

IETF® HTTP CoAP TLS DTLS ←uses

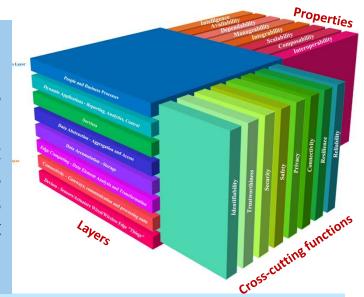**Protocols**

Meta Standards
the example of the Reference Architecture

The LSP 3D Architecture Model (developed in the LSP Activity Group 02) extends some of the current IoT reference architectures and is aiming at:

- Ensuring a common view of the different layers of the IoT systems from Physical up to Business;

- Providing additional viewpoints to the different stakeholders (not just to the developers) regarding some additional cross systems functions such as security, privacy or safety and the shared analysis of some properties (e.g., integrability) between different stakeholders.

The additional dimension of properties is a new way to discuss the properties of the IoT system between different involved parties (e.g., users, contractors, designers) and identify the elements in support (e.g., functional building blocks, APIs) and those missing.

The 3D Model is meant to be contributed to standardisation (not yet another Reference Architecture)

Co-funded by the European Commission

Stakeholders guidelines
the example of ETSI STF 547

An holistic approach to IoT Systems

- A solid standardized architectural framework, addressing interoperability across IoT domains
- Focusing on major aspects:
  - (Semantic) Interoperability
  - A User-centric approach to Privacy
  - Methods and techniques for Secure IoT

Whose essential objectives are to

- Identify guidelines and best practices
- Build a bridge for potential designers / implementers of IoT systems
- Provide comprehensive material for information, teaching/learning and demonstration with a very practical usage and implementation perspective

A Set of Coordinated Deliverables

An umbrella Special Report

- Dedicated to all stakeholders
  - Not just for the technology happy few
- Based on the analysis of relevant use cases

Seven Technical Reports

- Privacy; Standards Landscape and best practices
- Security; Standards Landscape and best practices
- Teaching material; Part 1: IoT Security
- Teaching material; Part 2: IoT Privacy
- Guidelines for using semantic interoperability in the industry
- Strategic / technical approach on how to achieve interoperability / interworking of existing standardized IoT Platforms
- Plugtests™ preparation on Semantic Interoperability

IoT Week 2019 - IoT Standards Trends and Convergence

Citizens involvement
the example of ETSI STF 561

Engage ALL stakeholders

The problem

- How many smart city/community technology initiatives actually mention **citizens and their needs** like accessibility, security, privacy, services that function correctly and listen to them?
- Projects, research and industry factor in standards – but **how many standards factor in the citizen**?
- How many cities actually believe standards can help them address citizen needs? And have they been involved in the standardisation process?

The objective

- Take a first overview of what the needs of citizens in smart communities are
  - Relate those needs to standardisation activities, ongoing or foreseen, and assess if they are being met;
  - If not, make recommendations as to how to rectify this;
- Lay down some basic principles as to how citizen needs should be addressed
- Make recommendations to standardisation (not standards)

An open process with stakeholder consultation   (see: https://standards4citizens.etsi.org/)
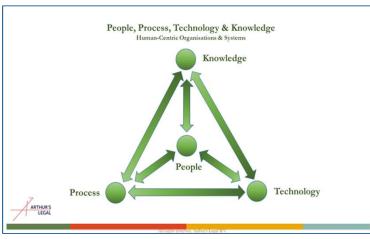
Some issues here to stay

Privacy

The challenge of Privacy in IoT

- IoT is an example of hyper connectivity and distributed control
- Appropriate safeguards are needed to ensure that individuals' right to privacy is **effectively** protected
  - Box ticking does not guaranty effective protection
- Some of the challenges in ensuring privacy in practice:
  - Identifying the entire chain of stakeholders that have responsibilities in relation to processing of personal data
  - Understanding the role of the context
  - How stakeholders need to think of Privacy as part of design not an afterthought
  - Raising awareness that protection of privacy is mandatory: GDPR forms binding law, not just a standard

Some take-aways

- GDPR is mandatory
- No new standards or regulation needed on privacy but:
  - There is a significant gap in application of privacy protection in general
  - Any new IoT standard should be adapted to GDPR
  - Need for new codes of conduct and certification

People, Process, Technology & Knowledge
Human-Centric Organisations & Systems

Knowledge

People

Process   Technology

ARTHUR'S LEGAL

Security
From IoT to Secure IoT

Identify where devices sit on the acceptable risk scale

- Highly risk averse:
  - All devices have to identify themselves and their function to their attached correspondents
  - All data passed from device to device has to be visible only to identified and authenticated, and authorized parties
  - All data protected against malicious manipulation (e-signature or MAC)
- Less risk averse
  - Use secure nodes as security anchors and liability anchors; Allows for devices without security processing

Apply Security Principles to IoT

- General Security Guidance and Best Practices
  - Provide security functions when required by law
  - Provide mitigations to quantified risk
  - Know who is acting on your device and why (security in depth)
- Specific (Cryptography) Security Guidance and Best Practices
  - Security should be centred on the key (and not on the algorithm)
  - Key management rigour determines system vulnerability

Semantic Interoperability

The Semantic Interoperability Challenge

- � Adopt the most flexible adapted of many approaches
- � Make sure this is used in the industry, not just labs

High expectations

- � Improve existing services, provide new ones; support public policy, …
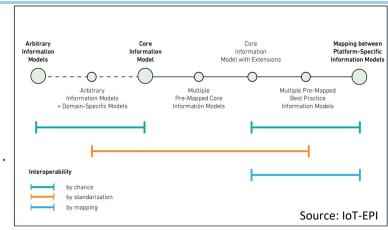- � Expected benefits e.g., data exposure, improved integration

Difficult road ahead

- � A complex landscape
  - � Glossary, Dictionary, Taxonomy, Thesaurus, Topic map, Meta data repository, Microformat, Ontology
- � The ontology problem: fragmentation (no upper-ontology in use); integration nightmare
- � Various level of adoption

Some guidelines and recommendations (ETSI TR 103 535)

- � Strategic guidelines: what to adopt; investment shaping (incl. training), internal promotion of success, …
- � Technical recommendations: use upper ontology, reuse domain ontology, adapt the development process, …

Source: IoT-EPI

However …

IoT Week 2019 - IoT Standards Trends and Convergence

No real chance to reduce complexity anyway …

Today

A plethora of standards
- ⱱ ICT is pervasive, its standards too
  - ⱱ 10 000 standards for Smart Cities

A plethora of standards organisations
- ⱱ Uncoordinated, sometimes competing
  - ⱱ 100+ initiatives for Smart Cities

Emergence of new actors and solutions
- ⱱ Open Source communities
  - ⱱ Often a complete alternative to standards
- ⱱ (Open) APIs; market places

Tomorrow

A plethora of
- ⱱ Standards
- ⱱ (Open) APIs and Data Models

A plethora of community initiatives
- ⱱ Growing role of Open Source

Emergence of new promises and issues
- ⱱ Big Data (aka IA) and Semantic Interop.
- ⱱ Effective privacy; Secure IoT
- ⱱ Growing role of (proprietary) ecosystems
- ⱱ Standards & OSS: collaboration or replacement
- ⱱ …

Thank you for your attention!

Contact Details: Emmanuel Darmois
                     CommLedge
                     emmanuel.darmois@commledge.com
                     +33 6 3151 5393

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

STF561:   https://standards4citizens.etsi.org

CREATE-IoT: https://european-iot-pilots.eu/project/create-iot/