

CHARIOT – 3rd Workshop

Wednesday 22 October 2020 (online)

IoT DATA SECURITY AND PRIVACY SOLUTIONS – CHALLENGES AND OPPORTUNITIES FOR AIRPORTS

AIOTI WG03 IoT Standardization Challenges and Activities

Georgios Karagiannis (with input from AIOTI WG03 taskforce leaders)
AIOTI Steering Board Chair, AIOTI WG03 co-chair

Outline

- AIOTI Overview
- AIOTI WG03 IoT Standardisation Overview
- AIOTI WG03 Gap Analysis
- Challenges in Green Airports

Outline

- **AIOTI Overview**
- AIOTI WG03 IoT Standardisation Overview
- AIOTI WG03 Gap Analysis
- Challenges in Green Airports

AIOTI Vision, Mission & Founding Members

- AIOTI strives to leverage, share and promote best practices in the IoT eco-system, and to be a one stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT Innovation in Society



Deployment

- Identify barriers
- Gather evidence
- Contribute to the Digital Single Market



IoT Ecosystem

- Build across different application areas
- Mapping and bridging of IoT innovation activities
- Encourage the growth of SMEs and startups in IoT



IoT Uptake

- Identify spearhead players
- Communicate
- Champion



Large Scale Pilots

- Experimentation, replication and deployment
- Convergence
- Interoperability
- H2020

Founding Members



AIOTI Structure

	WG 05	WG 06	WG 08	WG 09	WG 10	WG 11	WG 12	WG 13
WG 01 IoT Research								
WG 02 Innovation Ecosystems								
WG 03 IoT Standardisation								
WG 04 IoT Policy								
SME Interests								
Distributed Ledger Technologies								
	Smart Living Environment for Ageing Well	Smart Farming and Food Security	Smart Cities	Smart Mobility	Smart Water Management	Smart Manufacturing	Smart Energy	Smart Buildings and Architecture



Outline

- AIOTI Overview
- AIOTI WG03 IoT Standardisation Overview
- AIOTI WG03 Gap Analysis
- Challenges in Green Airports

Chair

Patrick Guillemin

ETSI



Co-Chair

Georgios Karagiannis

Huawei



The vision for WG03 is to be recognized as a major contributor to the worldwide interoperability, security, privacy and safety of IoT systems and applications, and particularly for the development of the market in Europe.

Scope: (1) Maintaining an IoT standards framework landscape, (2) Consolidation of architectural frameworks, reference, architectures, and architectural styles in the IoT space, (3) HLA / High Level Architecture, (4) IoT identifiers, (5) IoT relation and impact on 5G, (6) (Semantic) Interoperability, (7) Personal data protection/privacy to the various categories of stakeholders, in the IoT space (with WG04 IoT Policy), (8) IoT Security (with WG04 IoT Policy)

WG03 Highlights (ref. <https://aioti.eu/aioti-wg03-reports-on-iot-standards/>)

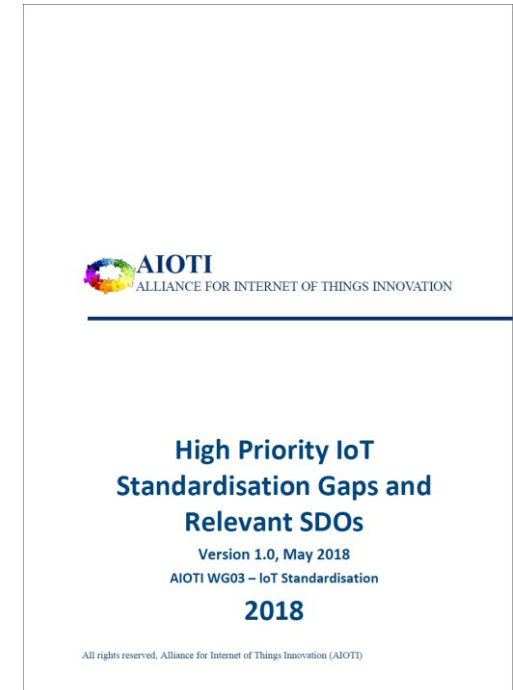
- **IoT Landscape** Georgios Karagiannis (Huawei)
 - **IoT Landscape maintenance** is key to keep the liaisons alive and maintain dialogue on how to foster collaboration to improve interoperability & security, v2.9 published in October 2019
 - **Gap Analysis** and recommendations Michelle Wetterwald (Netellany), Emmanuel Darmois (Commledge) 1st release published May 2018, 2nd release published in January 2020
 - **Cooperation with SDOs/Alliances** to foster co-creation and interworking Georgios Karagiannis (Huawei), Patrick Guillemin ETSI (e.g., Liaisons: 3GPP, ITU-T, ISO, OSGi Alliance, BBF, 3GPP; MoUs – signed: All, OSGi Alliance, BDVA, SCIA.0, ISO/IEC JTC1 SC41, under discussion OPC Foundation
 - **IoT relation and impact on 5G** Thomas Klein (IBM) ; Georgios Karagiannis (Huawei), 1st release published in June 2018, 2nd in March 2019, 3rd release published on 3rd of May 2020
- **HLA / High Level Architecture** Marco Carugi (Huawei), Omar Elloumi (Nokia) R4, published in June 2018, R5 ongoing (2020)
 - **IoT Reference Architecture** and its mapping with existing IoT Reference Architectures
 - **IoT identifiers** Juergen Heiles (Siemens), Henri Barthel (GS) 1st release published Feb'18
- **SemIoP IoT Semantic Interoperability** Martin Bauer (NEC lab), Laura Daniele (TNO) two JWP on semantic interoperability published in October 2019
- **IoT Privacy** (with WG04) Arthur van der Wees (Arthurs Legal) Nuance of Trust event, Series of GDPR-Centric AIOTI webinars,
 - IoT Platform, experimentation, LSPs recommendations on concrete standard framework & references to enable "IoT Trust" and IoT "Privacy by design" + STF 547
- **IoT Security** (with WG04) Arthur van der Wees (Arthurs Legal), Jacques Kruse-Brandao (SGS), Harm Arendshorst (ilabs)
 - IoT Security Architecture for Trusted IoT Devices; Baseline Requirements for Security & Privacy up to segment requirements; experimentation, LSPs recommendations on concrete standard framework & references to enable "IoT Trust" based on IoT "Security by design" + STF 547
 - Series of IoT Webinars on Application-Centric (IoT Verticals meet IoT Horizontals); The central themes of the webinars are: Personal Wearables (H2x): Health, Living, Consumer, Public Space, and other verticals, Moving Sensors (M2x): Farm2Fork, Mobility, Consumer, Cities, and other verticals + Long Term Fixed IoT Applications (F2x): Industry 4.0, Cities, Consumer, Water Management, Energy, Construction, Living, and other verticals

Outline

- AIOTI Overview
- AIOTI WG03 IoT Standardisation Overview
- AIOTI WG03 Gap Analysis
- Challenges in Green Airports

Gap Analysis and recommendations

- [High Priority IoT Standardisation Gaps and Relevant SDOs - Release 1.0 – May 2018](#)
 - Summary of gaps from ETSI STF505
 - CREATE-IoT: Large-Scale Pilots perceived Major gaps
 - Preliminary analysis for gap resolution
- [Release 2.0 - Published January 2020](#)
 - Update Release 1.0 of the report
 - Main focus: update the analysis of resolution of High Priority IoT Standardisation Gaps by relevant SDOs
 - But also:
 - ✓ Insert new gaps in the list when relevant
 - ✓ Identify tools to maintain an up-to-date overview of standardisation activities and specifications related to IoT (SDO databases)
- Methodology
 - Analyse each of the gaps individually:
 - For each gap, provide keywords that would help searching for potentially available standards in the SDO databases
 - Prepare a short summary of the status of the gap and recent actions since Release 1.0 of report



6.4 Safety

Short description: Safety.
Domain: Deployment
Keywords: Provisional IoT safety, European legislation, Harmonized standards, Machinery directive

Possible approaches identified to resolve this gap:

AIOTI WG03: Consolidated list of gaps in the report

Nb	Short name of gap	Nature of the gap	Domain
1	Connectivity interoperability	Competing communications and networking technologies.	Connectivity
2	Semantic interoperability	Standards to interpret and process the sensor data in an identical manner across heterogeneous platforms. Need of a global and neutral data model.	Service and applications
3	Enabling Applications to Span Multiple Ecosystems	APIs that decouple applications from the details of specific IoT ecosystems as a means to enable open markets of services.	Service and applications
4	Safety	Safety.	Deployment
5	Solution deployment and maintenance tools	Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms.	Deployment
6	Software deployment	Standardized methods to distribute software components to devices across a network	Deployment
7	Scalable device deployment	Unified model/tools for deployment and management of large-scale distributed networks of devices.	Deployment/ Device-sensor technology
8	Usability	Easy accessibility and usage to a large non-technical public.	Applications Management
9	Harmonized identification	Harmonized reference for unique and secured naming mechanisms.	Applications Management
10	Platform interoperability	Multiplicity and fragmentation of IoT HLAs, platforms and discovery mechanisms.	Integration / Interoperability IoT Architecture
11	Device certification	Certification mechanisms defining “classes of devices” and ensuring quality of the devices.	Device-sensor technology
12	Data management	Data rights management: ownership, storage, sharing, selling, liability, etc.	Security & Privacy
13	(Cyber-)Security	Risk Management Framework and Methodology.	Security & Privacy
14	Green technologies	Green technologies.	IoT Architecture
15	Ethics and trustworthiness	Ethics. Transparency and choice for citizens.	Service and applications / Security & Privacy / Societal
16	Open Markets of Digital Services	Standards needed to enable open markets of services.	Business



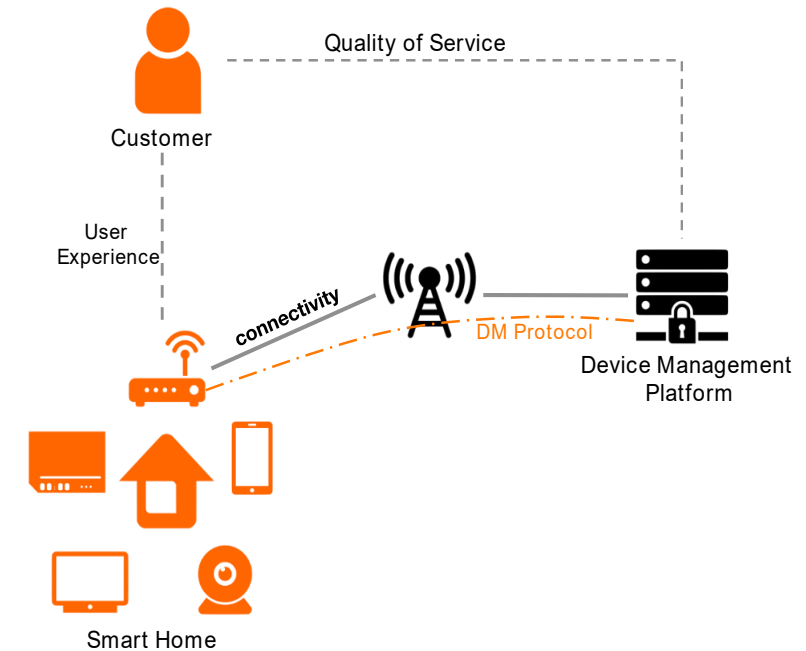
AIOTI WG03: Consolidated list of gaps in the report

Nb	Short name of gap	Nature of the gap	Domain
1	Connectivity interoperability	Competing communications and networking technologies.	Connectivity
2	Semantic interoperability	Standards to interpret and process the sensor data in an identical manner across heterogeneous platforms. Need of a global and neutral data model.	Service and applications
3	Enabling Applications to Span Multiple Ecosystems	APIs that decouple applications from the details of specific IoT ecosystems as a means to enable open markets of services.	Service and applications
4	Safety	Safety	Deployment
5	Solution deployment and maintenance tools	Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms.	Deployment
6	Software deployment	Standardized methods to distribute software components to devices across a network	Deployment
7	Scalable device deployment	Unified model/tools for deployment and management of large-scale distributed networks of devices.	Deployment/ Device-sensor technology
8	Usability	Easy accessibility and usage to a large non-technical public.	Applications Management
9	Harmonized identification	Harmonized reference for unique and secured naming mechanisms.	Applications Management
10	Platform interoperability	Multiplicity and fragmentation of IoT HLAs, platforms and discovery mechanisms.	Integration / Interoperability IoT Architecture
11	Device certification	Certification mechanisms defining “classes of devices” and ensuring quality of the devices.	Device-sensor technology
12	Data management	Data rights management: ownership, storage, sharing, selling, liability, etc.	Security & Privacy
13	(Cyber-)Security	Risk Management Framework and Methodology.	Security & Privacy
14	Green technologies	Green technologies.	IoT Architecture
15	Ethics and trustworthiness	Ethics. Transparency and choice for citizens.	Service and applications / Security & Privacy / Societal
16	Open Markets of Digital Services	Standards needed to enable open markets of services.	Business



Example: Solution and software deployment and maintenance tools

- Short description:
 - Tools to enable ease of deployment: installation, configuration, maintenance, operation of devices, technologies, and platforms, e.g. **airport terminal, airport transport**
 - Standardized methods to distribute software components to devices across a network
- Analysis:
 - Legacy device management : set of operations remotely executed on connected devices in a secure environment: provisioning, configuration, firmware updates, and diagnostics
 - IoT challenges: heterogeneity of devices, diversity of usages, security, confidentiality, and availability
 - Current standards initiatives: Broadband Forum (BBF), Open Mobile Alliance (OMA), IETF, oneM2M and OSGi Alliance
- Conclusion:
 - Standards needed for:
 - ✓ capacity to scale up,
 - ✓ capacity to hide and abstract the heterogeneous ecosystems of devices to manage (device abstraction layer with semantic descriptions),
 - ✓ capacity to take the context of users/customers and of their devices into account whilst guaranteeing their privacy protection



AIOTI WG03 - Open Issues - Impact


Nb	Short name	Nature of the standardization gap	Domain
1	Applications to Span Multiple Ecosystems	APIs that decouple applications from the details of specific IoT ecosystems as a means to enable open markets of services.	Service and applications
2	Safety	Safety.	Deployment
3	(Cyber-)Security	Risk Management Framework and Methodology.	Security / Privacy
4	Data management	Data rights management: ownership, storage, sharing, selling, liability, etc.	Security / Privacy
5	Harmonized identification	Harmonized reference for unique and secured naming mechanisms.	Applications Management
6	Semantic interoperability	Standards to interpret and process the sensor data in an identical manner across heterogeneous platforms. Need of a global and neutral data model.	Service and applications
7	Platform interoperability	Multiplicity and fragmentation of IoT HLAs, platforms and discovery mechanisms.	Integration / Interoperability IoT Architecture
8	Connectivity interoperability	Competing communications and networking technologies.	Connectivity
9	Ethics and trustworthiness	Ethics. Transparency and choice for citizens.	Service and applications Security / Privacy Societal
10	Open Markets of Digital Services	Standards needed to enable open markets of services.	Business
11	Device certification	Certification mechanisms defining “classes of devices” and ensuring quality of the devices.	Device-sensor technology
12	Solution deployment and maintenance tools	Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms. Standardized methods to distribute software components to devices across a network	Deployment
13	Scalable device deployment	Unified model/tools for deployment and management of large-scale distributed networks of devices.	Deployment/ Device-sensor technology
14	Green technologies	Green technologies.	IoT Architecture / Societal
15	Usability	Easy accessibility and usage to a large non-technical public.	Applications Management

- Technical topics are well understood
- Interoperability is making its way
- Data security & privacy well understood, but more work needed
- IoT and Edge Computing convergence as an open Issue
- Deployment and societal topics need further focus in standardisation



AIOTI WG03 – Security & Privacy

- Example Contextual State of the Art Privacy and Security: Overview of 50+ Security in IoT Principles (From 2016 & 2017 EC /AIOTI Reports Only). Referred to by European governments, such as UK DCMS (Consumer IoT Security).

1. USER/HUMAN FACTOR	2. DATA	3. SERVICES	Sustainability
Human-centric approach	Data segmentation and classification	Life time protection	Assurance
Privacy by design	Privacy by design	End of support	Certification
Privacy by default	'As-if' by design		Trusted IoT label
Decoupling multiple identities	Data minimisation	4. SOFTWARE/APPLICATION	Defined functions
Identity protection by design	De-identification	Security by default	Secure interface points
Metrics	Data control	Secure updates	
Independent privacy and security audits	Data access	Frequency of updates	6. AUTHENTICATION
Transparency of data processing	Data ownership	Accountability & Liability	Authentication of identities among themselves
Transparency of privacy policy	Data management	Third-party libraries	
Transparent roles	Data isolation	Information exchange	7. INFRASTRUCTURE/NETWORK
Indication of purpose	Security of personal data		Harmonised industry approach
Single point of contact	Encryption by default	5. HARDWARE	Reduce impact of national regulations
Consent	Encryption at the application layer	High-level baseline	Interoperability
Non-discriminatory practices	Standardisation	Separate safety and security	Taxonomy
Manufacturer-implemented parametrisation	Accountability	Security rationale	Continuous monitoring
Accountability	Risk impact assessment by design	Security evaluation	
		Security levels	

Digital & Data are Now Highly Regulated Domains



State of Play October 2020

Security & Privacy By Design By Default needed and required for complete data cycle, e.g. generation, collecting, storage, access, sharing, retention, strong deletion and other processing

PSD2: 13 January 2018

NIS: 9 May 2018 (under review)

GDPR: 25 May 2018

eIDAS: 23 July 2014 (under review)

Free Flow of Data Regulation: 29 April 2019

Cyber Security Act & Certification Scheme: 27 June 2019

Proposed e-Privacy Regulation

Proposal Regulation for European Cybersecurity Industrial, Technology and Research



All rights reserved, Arthur's Legal B.V.



Outline

- AIOTI Overview
- AIOTI WG03 IoT Standardisation Overview
- AIOTI WG03 Gap Analysis and recommendations
- Challenges in Green Airports

- IoT, edge computing and connectivity solutions and standardization support for Green airports
 - European Green Deal: “transport should become drastically less polluting”, highlighting in particular the urgent need to reduce greenhouse gas emissions (GHG) in aviation and waterborne transport. In aviation, traffic volumes are expected to increase significantly by 2050 and the sector is already generating 14% of the EU GHG emissions from transport
 - Airport Transport, including data security & privacy support:
 - ✓ access and multimodal connections to the airport (e.g. from cities or other nodes);
 - ✓ from the airport terminal to the aircraft (airside);
 - ✓ at the airport landside (logistics, ground handlings and operations, as well as green energy production/supply of sustainable alternative fuels or electricity);
 - ✓ promoting intermodal smart mobility, including efficient rail interconnection and public transport solutions and as well innovative train-airport station concepts;
 - Airport Terminal, including data security & privacy support:
 - ✓ integration of new solutions with operations, green and smart logistics and infrastructures;
 - ✓ improving the energy efficiency of buildings; optimising services such as lighting, heating, natural ventilation and air conditioning, taking into account strict public health criteria, water/energy usage and efficiency;
 - Cross-cutting aspects, including data security & privacy support:
 - ✓ use of ICT and other solutions to effectively manage resources and assets, including management of information and production of knowledge, taking into account all the related safety and security aspects of the solutions developed and proposed;





Contact
Details

Thank You



Huawei Technologies Dusseldorf GmbH



Georgios Karagiannis



georgios.karagiannis@huawei.com



The project CHARIOT has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780075