DTF Strategy Overview

Table of Contents

Introduction

The Digital Trust[1] Forum (DTF) is a global, open and independent initiative with a focus on enabling trusted digital solutions for connected, intelligent, physical products, utilizing AI and the Internet of Things (collectively referred to as AIoT in this context). DTF is inspired by the EU initiatives on AI and trust.

The inaugural DTF was held in May 2019 in Berlin, hosted by Bosch group-CDO Michael Bolle and EU Commissioner Mariya Gabriel. Participating organizations included BDI, DIGITALEUROPE, Eclipse Foundation, Enisa, ETSI, IEEE, Industrial Internet Consortium, ISO/IEC JTC 1/SC 42, Platform Industrie 4.0 and Trusted IoT Alliance.

This paper[2] outlines the DTF vision, implementation strategy, and call for participation.

Figure 1: DTF at Bosch ConnectedWorld 2019

Motivation

Technology is evolving at – sometimes breathtakingly – high speed. Especially the rapid advancements in Artificial Intelligence (AI) and the Internet of Things (IoT), and their massive utilization (AIoT), are causing not only enthusiastic responses, but also many concerns. These concerns are not only related to security and data privacy, but sometimes relate to dystopic visions of failing civil infrastructure, criminally abused IT systems, or even out-of-control autonomous systems. In order to ensure that the many opportunities presented by these new technologies continue to find high level of customer acceptance, trust between all related stakeholders have to be established. A trustworthy behavior of technical systems and all related stakeholders which meets end-users' expectations must be ensured on many levels.

The Digital Trust Forum is bringing together representatives from the relevant stakeholder groups in order to help ensure that end-users develop an ongoing high level of trust in AI and IoT-based solutions. Only within such a trustworthy environment will new solutions be able to continue to attract new customers and users. DTF will help its partners and supporters to take a proactive role in setting and managing expectations regarding trust in such digital solutions by making trust policies explicit and transparent, and building the required trust management mechanism directly into digital solutions.

---

1 In this document, the terms "trust", "trustworthy" and "trustworthiness" are used interchangeably. In reality, these terms have different meanings. Trust is a relationship between two systems, while trustworthiness is a characteristic of a system that is a precondition for enabling trust between systems. These terms will be formally defined in subsequent stages of the DTF project.

2 Participating organizations contributed content to this paper.

Call for Participation

The initiators of the DTF invite all stakeholders to join the DTF efforts and work together in a number of areas:

- Requirements: DTF relies on continued interaction with a diverse set of trust stakeholders, and the derivation of relevant and realistic requirements.
- Solution design: Based on the requirements, DTF aims to create a high level of solution design, and to work with SDOs and industry alliance and private standardization organizations to refine and standardize aspects related to design.
- Solution implementation: DTF aims to create a market for DTF-compliant AIoT trust management solutions. Engage with DTF, if you are in this market!
- Policy creation: DTF aims to establish an active community to work on creating and maintaining the DTF AIoT trust policy library.
- Industry validation: DTF will work with organizations from different verticals and industries to implement and validate the DTF solutions already in the early stages of creation.
- Certification: A medium- to long-term goal is to engage with relevant organizations to work on a DTF certification scheme and a DTF cybersecurity certification scheme, supported by a trust mark and related to the standardization process.

If any of these activities are of relevance, contact DTF via our LinkedIn group[3] to get engaged!

DTF Vision

DTF acknowledges the need for well-defined responsibilities and governance as a foundation for trust in AIoT. A key question addressed by DTF is how to enable trust in AIoT-enabled systems by defining quality parameters, fulfilling regulatory and other requirements, defining, maintaining and observing policies, and monitoring compliance. Figure 2 shows how the DTF scope fits accordingly into the digital trust supply chain.

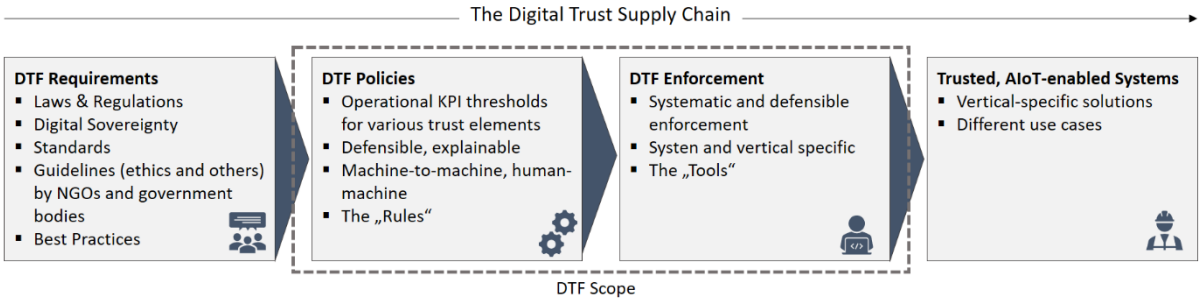

Figure 2: Digital Trust Supply Chain

DTF aims to support the establishment of a broad range of trust-related policies. Figure 3 provides an overview of the initially planned trust policy categories. The first category will include policies related to security and self-trust. This is especially important in an AIoT system, in which assets in the field are not only subject to potential software attacks; while a lesser concern due to the indirect relation between the AIoT and the beneficiary, hardware tampering emerges as an additionally important a concern. Building on these, the next category will include policies related to sharing personal as well as non-personal data, including aspects related to data privacy and data sharing. This will include user data, as well as data coming from the assets in the AIoT, which include operational data, metadata and the like. The third level may include policies related to how the data

[3] https://www.linkedin.com/groups/8896185/

in the AIoT is used for instance on the functional level, behavioral level, etc., especially as it relates to AI.

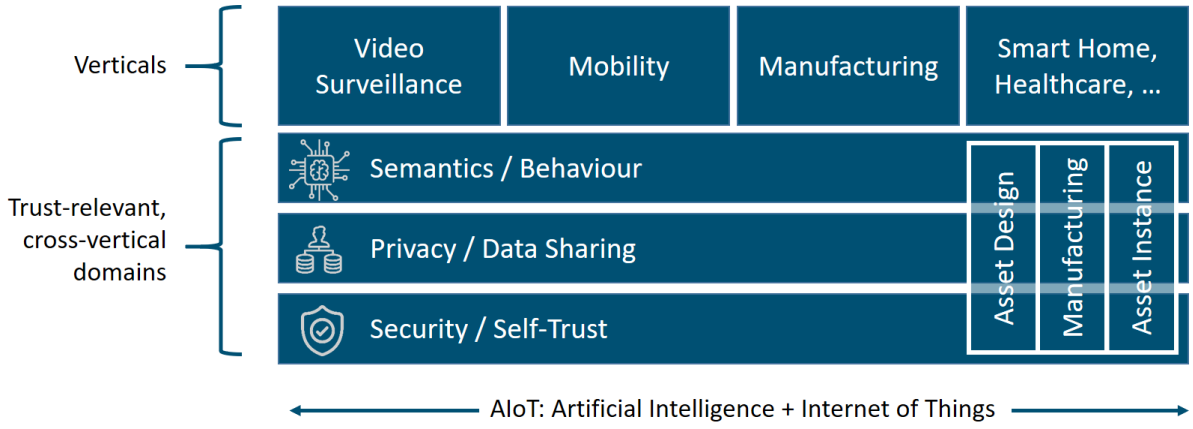

Figure 3: DTF Trust Policy Categories

Technically, DTF will help establish trust by supporting a process that is based on two pillars, as shown in Figure 4: Firstly, formalized AIoT trust policies that reflect regulatory requirements, managed by a Trust Policy Management system. Secondly, trust anchors and an execution environment that allows trusted execution and self-monitoring with regard to the trust policies.

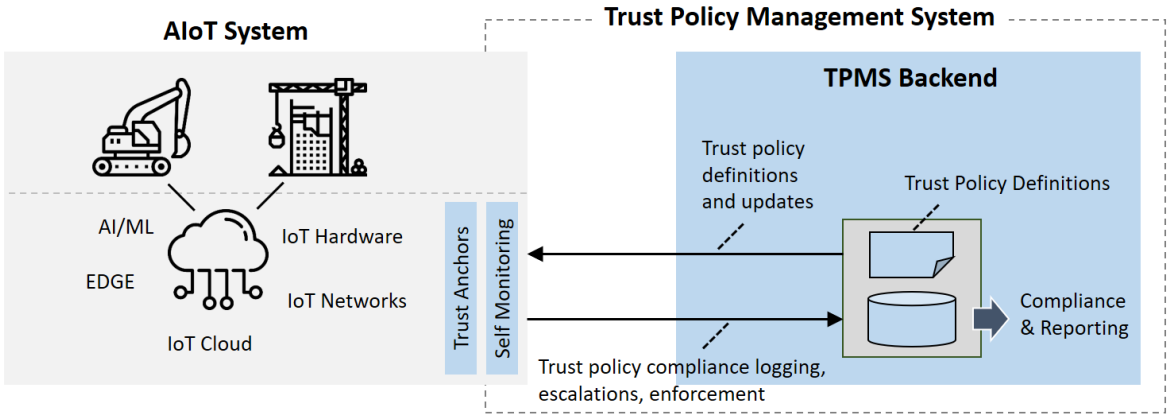

Figure 4: Vision – Establish Trustworthiness for AIoT with Trust Policy Management System (Icons: Flaticon.com)

The underlying idea is that trust is a relationship between two entities with respect to a specific task that requires entitlement, competence and compliance to certain pre-defined de-jure and de-facto standards and principles. The identity, and thus the authority, of the entities can be established by certificates. If required, additional safeguard mechanisms (e.g. HW trust anchors) can be put in place. Entitlement and competence can be managed by formalizing Trust Policies for AIoT Systems in a manner than can be consumed directly by these systems in the field and enforced within them. By making all policies transparent, jurisdiction-aware and defensible, the system can access the currently applicable and validated policy definitions remotely in real-time. Compliance of an entity with the policies, thereby taking information about all internal processing and execution layers into account, will be performed by a self-monitoring engine on the AIoT system. This process can be utilized for external control of system compliance and performance. The overall system behaviour from a trustworthiness perspective can be logged and published, and trust can be efficiently enforced by managing system exceptions and escalations.

DTF Framework Overview: Towards a "Trust Escrow"

DTF will be defining a framework for managing how expectations can be met and responsibility and governance is organized in an AIoT environment, by utilizing formalized trust policies and a framework to implement them and apply them on an AIoT device. This needs to reflect three (defensible) governance maturity milestones:

1) Formalized, organization-approved and published DT policies;
2) Systematized processes and methods for compliance with these policies; and
3) Established track record of adherence with the DT policies.

An overview of the DTF framework is provided in Figure 5.

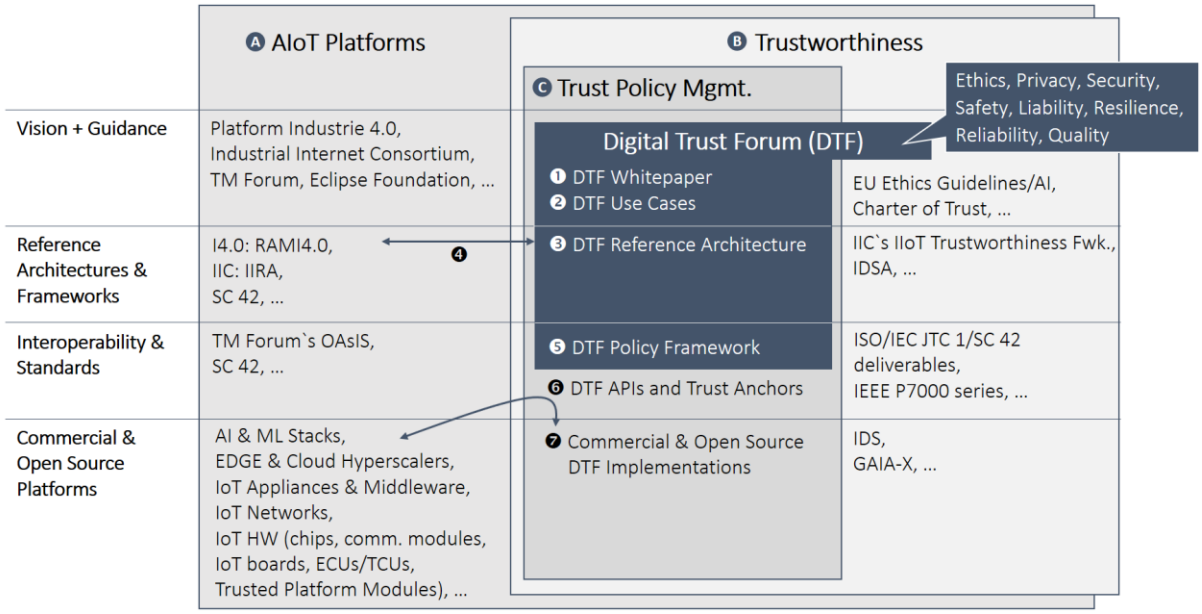

Figure 5: DTF Framework

The DTF framework seeks to represent and address key elements of trustworthiness, which need to address topics like ethics, privacy, security, safety, liability, resilience, reliability and quality of AIoT-based solutions. DTF is following a holistic approach by defining stakeholder expectations for system behavior, robustness, safety, security, defensibility and explainability and by providing mechanisms to verify compliance.

AIoT Platforms

All of these topics have to be seen in the context of AIoT platforms, which are the foundation for utilizing the disruptive potential of AI and IoT, and their convergence. The DTF framework includes different levels of abstraction through which AIoT platforms can be looked at, including vision and guidance, reference architectures, interoperability and standards, and finally commercial platforms.

Various NGOs and alliances are providing guidance and vision for AIoT platforms, including Platform Industrie 4.0, the Industrial Internet Consortium (IIC), TM Forum and the Eclipse Foundation, to name but a few. Most of these organizations have also defined reference architectures, which are addressing key elements of an AIoT platform. Some organizations have gone down one level and started specifying standards and concrete APIs in this context, such as TM Forum's OAsIS project. And finally, there are commercial and open source solutions available, which support the different aspects of an AIoT platform, including Cloud Hyperscalers, EDGE Infrastructure, IoT Appliances &

Middleware, IoT Networks and IoT Hardware (chips, communication modules, IoT boards, ECUs/TCUs, Trusted Platform Modules).

Trustworthiness

Closely related to these generic AIoT platform elements are the trustworthiness aspects. A number of organizations have stepped up to provide vision and guidance in this area, including the EU Ethics Guidelines for Trustworthy AI, or the Charter of Trust for Cyber-Physical Systems.

On the level of reference architectures related to trustworthiness, IIC's IIoT Trustworthiness framework is building onto existing AIoT reference architectures, while the International Data Spaces Association (IDSA) is proposing a new reference architecture with a focus on secure data sharing, which is one important element of trustworthy AIoT.

ISO and IEC are developing international standards on AI through a joint committee. ISO/IEC JTC 1/SC 42 is developing international standards for the entire AI ecosystem. One aspect of the committee's work program is AI Trustworthiness, where the committee is developing standards for:

- An overview of the topic;
- AI Trustworthiness specific aspects such as unintended bias and robustness of neural networks; and
- An AI risk management framework that builds on the generic ISO 31000 risk management standard for AI to address trustworthiness issues.

In addition, SC 42 is considering ethical and societal concerns: (a) across its entire work programme (e.g. use cases collected incorporate ethical and societal concerns) and (b) specifically within its trustworthiness work programme via a project that lists ethical and societal requirements, such as emerging regulatory aspects, and mapping them to the technical SC 42 trustworthiness deliverables the committee is developing.

SC 42's work programme is also considering foundational aspects such as terminology, framework for AI using ML, lifecycle, computational methods, governance implications of AI, use cases and applications of AI. SC 42 is also studying AI Systems Engineering issues and is in the process of developing a justification study for a Management Systems Standard that, if approved, would tie the work programme together and contain AI-specific process requirements that would allow for assessment of conformance.

Another important aspect is represented by the Engineering Methodologies for Ethical Life-Cycle Concerns Working Group, developed as part of the IEEE P7000 series. The standard establishes a process model by which engineers and technologists can address ethical considerations throughout the various stages of system initiation, analysis and design. Expected process requirements include management and engineering view of new IT product development, computer ethics and IT system design, value-sensitive design, and stakeholder involvement in ethical IT system design.

IEEE SA is completing the first phase of its programme focused on defining critical certification criteria relating to accountability, transparency and reduction of algorithmic bias for autonomous and intelligent systems.

Finally, initiatives like IDSA and GAIA-X are looking at launching concrete initiatives, which would address key elements of trustworthy AIoT on the platform level.

Trust Policy Management System

In this context, DTF proposes to establish a framework for Trust Policy Management Systems (TPMS). DTF will be working on different elements of a TPMS as follows:

(1) DTF Whitepaper: Requirements and Vision.
(2) DTF Use Cases: A set of concrete use cases to further validate the original requirements.
(3) DTF Reference Architecture: Describes the key layers and components of a TPMS for AIoT, Including interaction with trust anchor and self-monitoring system.
(4) Mapping to existing AIoT Reference Architectures: Described the mapping of TPMS to existing reference architectures.
(5) DTF Trust Policy Framework: Describes the different trust policy categories and proposes a way to formalize and standardize trust policy definitions that can be consumed directly by AIoT systems and enforced within them.

Based on this work, DTF will work together with standardization organizations and commercial vendors to establish:

(6) TPMS APIs: Application Programming Interfaces required to integrate a TPMS with an AIoT platform; and
(7) Commercial TPMS Implementations: Concrete implementations and commercial products which comply with the DTF framework.

(1) DTF Whitepaper

The DTF Whitepaper will outline the overall TPMS vision in detail. DTF will work with key stakeholders to develop a vision of how a TPMS market should ultimately work. We will start with identifying where responsibility for Trust lies (generally at the Board of Directors of a large corporation, or some other stakeholder group), and then consider how this group should most appropriately discharge their fiduciary duties, given that many of those accountable will not themselves be technical experts.

It is likely that to be effectively implemented in the 'real world' any TPMS system will need to incorporate entities such as TPMS solution vendors, trusted third parties, providers of certification of compliance, TPMS auditors, lawyers, and insurers, all underpinned by a regulatory and standards-based regime.

Next, the DTF whitepaper will define a set of concrete requirements. The goal is to derive requirements from both industry and government, as well as directly from the citizens.

Based on these detailed requirements, the DTF vision will be refined. For example, requirements can be directly mapped to use cases and digital trust policy categories, which will be included in the whitepaper.

Another important aspect addressed by the whitepaper will be the lifecycle perspective: How can trust be built into digital solutions already during the conception and design phase?

Finally, the identification of the key DTF stakeholders, and the roles they can/should play in the context of TPMS instances in different domains and industries, will be important.

The DTF whitepaper will be a key instrument to clearly communicate the DTF vision and how it will be operationalized.

(2) DTF Use Cases

The DTF Use Cases will help to make the requirements as clear as possible, and also to distinguish requirements from non-requirements. Each use case should provide concrete examples for trust policies that would support it. The initial list of proposed use cases is shown in the table below.

Industry/Domain	DTF Use Case	Description
Mobility	OTA (Over-the-Air Updates)	Describes a set of desirable trust policy definitions related to OTA updates with direct or potential impact on vehicle performance, e.g. for Electric Vehicles or Autonomous Driving functions.
Smart Building / Smart City	Video Surveillance	Covers examples for trust policy definitions and observing the adherence of the camera device related to the use of video surveillance technology in public areas, such as commercial buildings and on the street level
Manufacturing	Digital Twin	Covers examples for trust policy definitions and processing instructions related to use cases where data from multiple machine components from potentially multiple suppliers are collected and analysed, and results are distributed back to multiple stakeholders, utilizing digital twin technology.

Figure 6: Candidates for Digital Trust Use Cases

Initially, the use cases will be defined in a single document. Medium-term, they will be maintained using an online repository.

(3) DTF Reference Architecture

The DTF reference architecture will define the general structure and key components of a Trust Policy Management System (TPMS) for AIoT. These can include, for example:

- TPMS repository for creating and maintaining Trust Policy Definitions;
- Description of trust anchor and self-monitoring mechanism and their interactions with the TPMS backend;
- Real-time APIs for accessing trust policy definitions from the AIoT solution;
- TPMS component for trust policy enforcement; and
- TPMS component for reporting and compliance checks.

Note that the TPMS reference architecture will not replicate the elements typically found in a generic AIoT reference architecture. Instead, a clear mapping will be provided (see below).

In the case of newly emerging initiatives such as GAIA-X, it should be examined in the early development stages what a possible alignment would look like. From the perspective of the DTF, this is particularly important since the strengthening of open and competitive markets for AIoT infrastructure (including cloud and edge data management platforms) will help ensure freedom of choice and transparency. These are two important prerequisites for achieving trustworthiness in AIoT.

(4) Mapping DTF to existing AIoT Architectures and Infrastructures

DTF will work with interested industry organizations which are active in the field of AIoT reference architectures, in order to provide clean mappings between the key elements of the TPMS architecture on the one hand, and the AIoT architectures on the other.

Interoperability between the implementation of a TPMS system on the one hand, and a solution based on an AIoT platform on the other will be a key success factor for DTF. The mapping points identified here will be a key input for the TPMS APIs described in section (6).

(4.1) RAMI4.0 and IIRA

Two of the most widely recognized reference architectures for the IIoT are RAMI4.0 and IIRA. RAMI4.0 is the reference architecture defined by Platform Industrie 4.0, which focuses on manufacturing systems and their value chains. IIRA is the reference architecture of the Industrial Internet Consortium (IIC), which is designed to support IIoT application in different industrial domains, including manufacturing but also energy, transportation, mining, healthcare, and so on. DTF aims for work with Platform Industrie 4.0 and IIC to ensure that the DTF Reference Architecture supports both, RAMI4.0 and IIRA.

(4.2) GAIA-X

GAIA-X[4] is a major project initiated by the German Federal Ministry for Economic Affairs and Energy to enable a trusted data infrastructure via a federation mechanism, effectively creating a virtual cloud hyper-scaler. GAIA-X is currently designed around two main components: GAIA-X Registry and GAIA-X Identity Management. The Trust Policy Management created by DTF could effectively be used by GAIA-X as its third pillar. While DTF aims to be an independent initiative, such a possible collaboration with GAIA-X should be further evaluated.

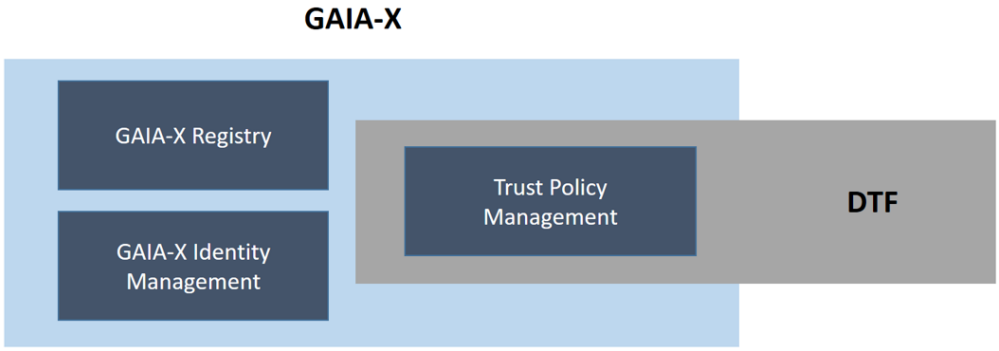

Figure 7: DTF and Gaia-X

(4.3) Electronic Identification, Authentication and Trust Services

Electronic Identification, Authentication and Trust Services such as eIDAS regulate electronic signatures and electronic transactions, as well as the involved bodies and their embedding processes, to provide a safe way for users to conduct business online. Figure 8 provides an overview of a potential mapping.

[4] https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.html

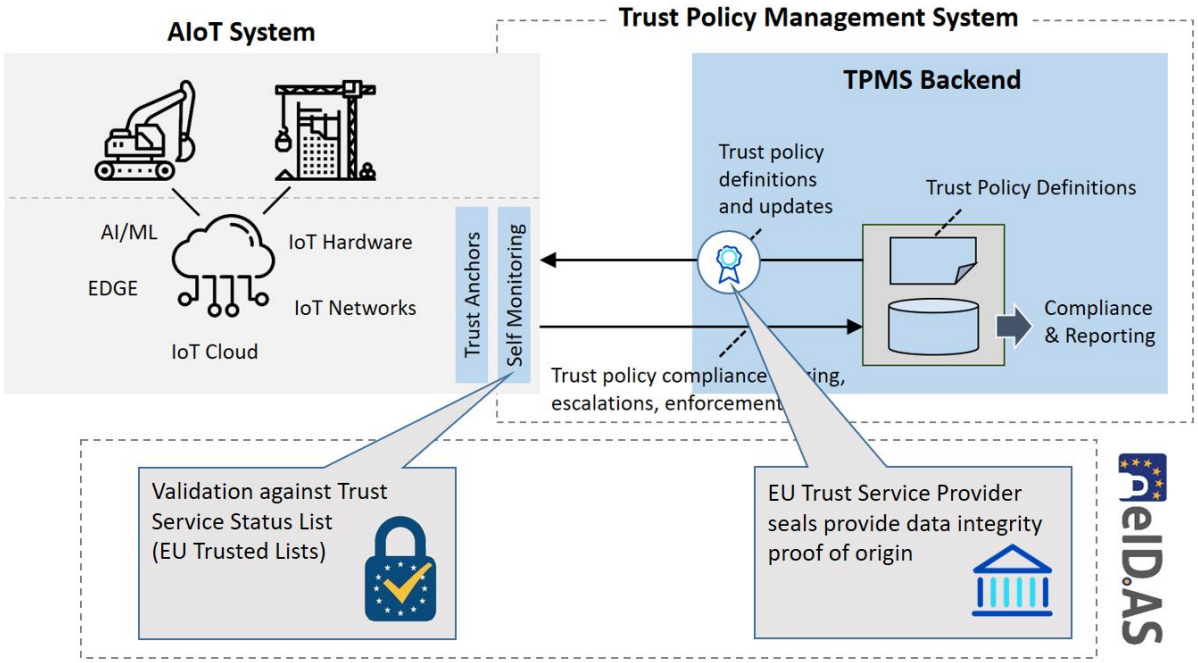

Figure 8: Mapping between DTF Architecture and eIDAS

(4.4) Open Source

Open source provides a very complementary philosophy to DTF, and potentially also existing implementations which could be leveraged for DTF. For example, the recently launched project Alvarium defines a set of trust insertion technologies which could be utilized for DTF. Figure 9 provides an overview of a potential mapping.

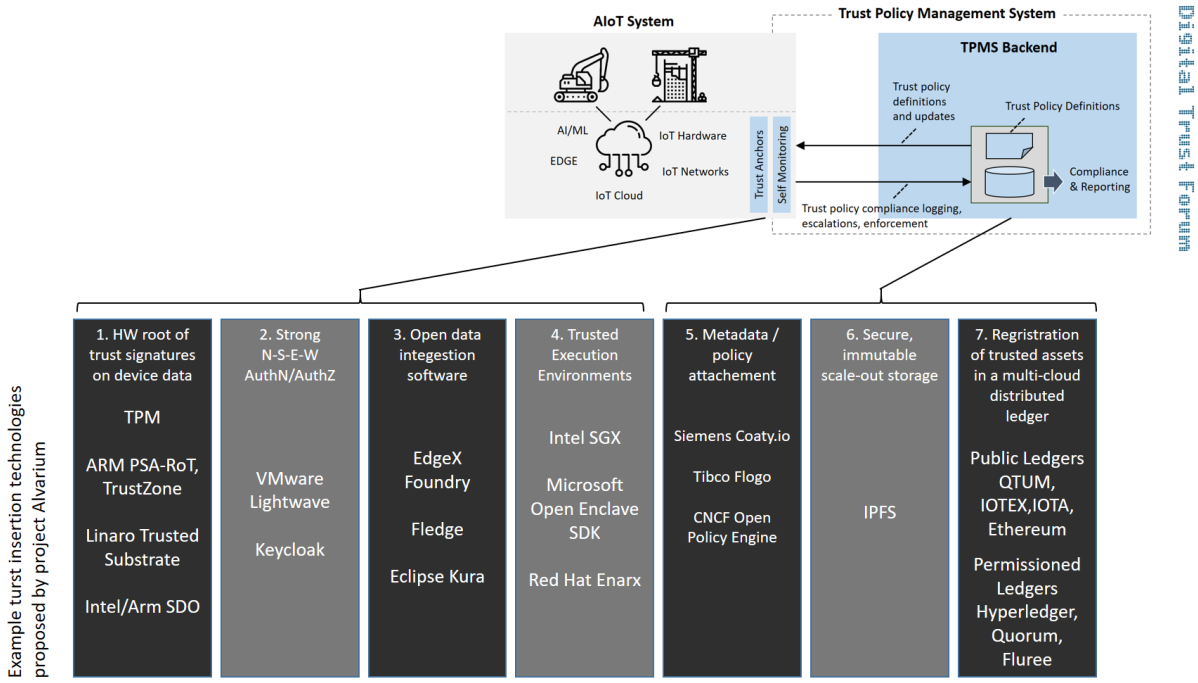

Figure 9: Mapping between DTF Architecture and Project Alvarium

(5) DTF Policy Framework

DTF will aim to define a holistic policy framework to address all key aspects of digital trust in AIoT-based solutions. This framework will include:

- A set of AIoT Trust Policy Categories;
- A data schema to manage instances of AIoT Trust Policy Definitions, with jurisdiction-specific variations and version control;
- A catalogue of events (and their data schema) that can trigger policy enforcement actions within the AIoT System;
- A catalogue of jurisdictions where the AIoT System (or components of) may be deployed; and
- A catalogue of reference definitions for AIoT Trust Policies, based on said schema.

The last point can be further broken down into industry-, domain-, and use case-specific policy definitions. The use cases described in section (2) will help guide this work.

(6) DTF APIs and Trust Anchors

In order to ensure interoperability between the AIoT solutions on the one hand, and the TPMS platform on the other, it will be critical to define a set of Application Programming Interfaces (APIs) which can be used to facilitate the required data exchange and service interactions.

The AIoT system will embed “Trust Anchors” in order to provide the means for establishing identity and authority of a device. The self-monitoring component provides the required local logic. Trust Anchors can communicate with the TPMS via the TPMS APIs.

DTF aims to work with leading industry organizations in this field in order to define a standardized set of APIs for this purpose. One potentially interesting set of APIs is defined by TM Forum as part of their OAsIS APIs. Another interesting approach could be the Online Trustworthiness Exchange Protocol (OTEP) proposed by Platform Industrie 4.0.

(7) Commercial and Open Source Implementations

Finally, DTF will help create a market for TPMS implementations, by working together with key stakeholders in governments, end-users and industry analysts. This should be an incentive for commercial (and potentially open source) software vendors to develop and supply AIoT Trust Management solutions according to the architectures and specifications initiated by DTF.

Together with its partners and supporters, DTF will help ensure that the disruptive potential of AIoT can be utilized within well managed levels of trustworthiness.

Governance

Finally, the proposed DTF governance structure and conformity assessment will be discussed in this section.

DTF Governance Structure

The Digital Trust Forum is being set up as a global, open and independent initiative with a strong focus on ensuring that DTF concepts are validated and adopted by industrial users of AIoT in different verticals. In order to ensure openness and independence, DTF will adopt from the early stages a democratic and inclusive governance structure. In order to ensure industry relevance, DTF

will focus on industry partnerships and initiate and manage a portfolio of DTF-related co-innovation projects.

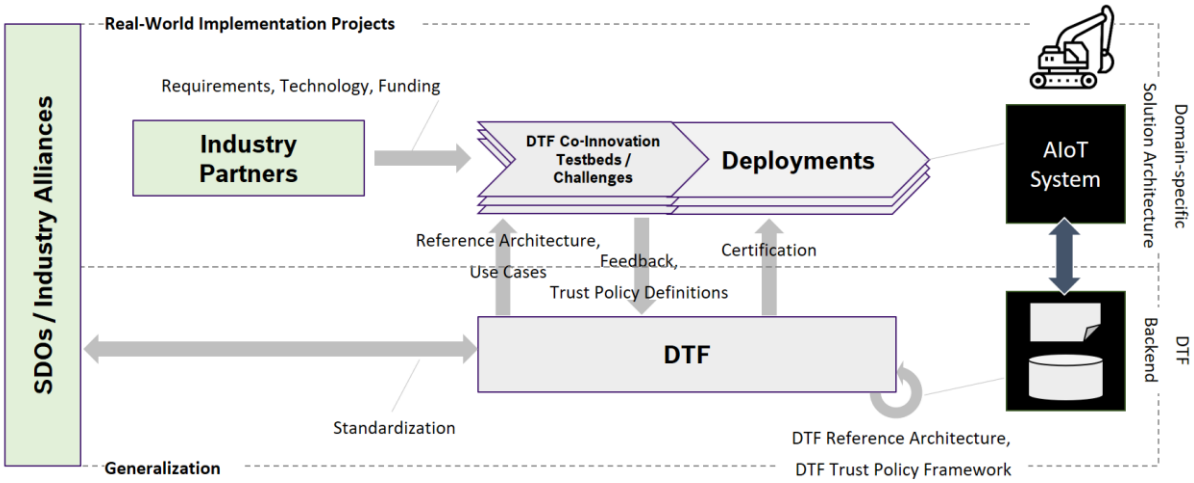

Figure 10: DTF Governance Structure

Figure 10 shows the proposed DTF governance structure. The DTF organization will initially be lightweight, open to new members who are willing to contribute to the DTF cause, and steered by pragmatic and democratic governance rules.

DTF co-innovation vehicles will include testbeds and challenges, executed in close collaboration with supporting SDOs. Testbeds provide a controlled experimentation environment in a defined ecosystem. Challenges are adding the dimension of a competition for finding the best suitable solution.

DTF Conformity Assessment

An explicit goal of the DTF is to establish a DTF conformity assessment mechanism, in order to help promote the adoption of the tools delivered by DTF for ensuring trust in AIoT systems. A range of options are available here, including certified trust labels, trust labels, and self-assessments.

Certification can be two-pronged, addressing functional aspects as well as cybersecurity aspects, within the framework provided by the EU Cybersecurity Act. Dedicated certification schemes will support trust-related decisions that beneficiaries and users of the AIoT will make. Subject to successful conformity assessment, a dedicated trust seal can be issued.

Self-assessments by AIoT solution providers according to DTF guidelines could provide a more lightweight alternative to formal 3rd party certifications. A good balance must be found between the thoroughness of the conformity assessment on the one hand, and the often agile and lean nature of AIoT development projects on the other.