ISO/IEC JTC 1/AG 7 **N 66**

REPLACES: ISO/IEC JTC 1/AG 7 N 55

ISO/IEC JTC 1/AG 7
Trustworthiness
E-mail of Secretary: volker.jacumeit@din.de
Secretariat: DIN

JTC 1 AG 7 – Trustworthiness – Inventory and heatmap

Date of document 2019-10-14

Expected action Info

Inventory of Trustworthiness in JTC 1 and other SDOs

14th Oct 2019

Introduction

This report provides an update inventory of trustworthiness and trust terms gathered by AG 7 – Trustworthiness as well as a "heatmap" of Trustworthiness characteristics. The characteristics used to build the heatmap are taken from revised report by the trustworthiness Rapporteur (AG 7 N64) and include the characteristic "Accuracy".

The Trustworthiness inventory prepared for the JTC 1 meeting in November 2019 has been updated to f to include additional responses. A table including the previous results has been formatted for this report.

Both files are maintained in a spreadsheet format and can easily be updated as new data becomes available.

Trustworthiness characteristics heatmap

The heatmap should show in which JTC 1 SCs as well as other relevant ISO and IEC TCs, Trustworthiness characteristics are considered to important to the SC for their scope. Unfortunately, data from only a few JTC 1 SCs and one ISO TC was either gathered directly or inferred by reviewing the SC scope as well as the scope of some of the most relevant deliverables. It should be noted this is an incomplete analysis at this time, SCs were not able to respond to enquiries without consulting their membership. However initial analysis does show some interesting trends.

Table 1 shows the raw heatmap data, rows being the order Trustworthiness characteristic appears in AG 7 N64 Trustworthiness Vocabulary Rapporteur v1.4 presentation and the columns being the sorted list first of the JTC 1 SCs followed by TC 292.

Table 1 - Heatmap of Trustworthiness characteristics

Characteristic	SC 6	SC 7	SC 17	SC 27	SC 31	SC 37	SC 38	SC 40	SC 41	SC 42	TC 292
Reliability			5						5	3	5
Availability			5	5			5				4
Resilience			4						4		4
Security			5	5			5		4		5
Privacy			5	5			5			2	3
Safety									3		5
Accountability							5			5	5
Transparency										5	3

Integrity			5			4		5		5
Authenticity			3			5				5
Quality		5							4	5
Usability		4	3			5			4	4
Accuracy										

Table 2 shows the same data sorted by the occurrence of the high priority Trustworthiness chrematistics. This shows where these characteristics are already considered important r or are already being considered in deliverables by the SC.

Unsurprisingly, the characteristic Security is considered most often, followed by Availability, Integrity and Privacy, whereas Safety, Transparency and Resilience is only considered in few SCs to lesser extent. The characteristic Accuracy has not been considered yet as it was added after the initial lists of characteristic was created.

Table 2 Sorted trustworthiness heatmap sorted by occurrence of characteristics for each SC

Charateristic	SC 6	SC 7	SC 17	SC 27	SC 31	SC 37	SC 38	SC 40	SC 41	SC 42	TC 292
Security			5	5			5		4		5
Availability			5	5			5				4
Integrity				5			4		5		5
Privacy			5	5			5			2	3
Reliability			5						5	3	5
Accountability							5			5	5
Authenticity				3			5				5
Usability			4	3			5			4	4
Quality			5							4	5
Safety									3		5
Transparency										5	3
Resilience			4	4					4		4
Accuracy											

Again, it should be noted that this is based on preliminary and gathered data rather than responses from the SCs. Should the work of AG 7 continue, it would be worth maintaining and updating the Trustworthiness heatmap to be able to continue to monitor if SCs are considering Trustworthiness across all its characteristics in their deliverables.

Definitions of trustworthiness terms

Table 3 is a list of definitions for trust and trustworthiness and some related terms. The table has been updated to according to the item 5 of SG 5 N4. However, as the columns Sector, Type of document and Context contain no data they are not shown below.

Table 3 - List of trustworthiness definitions in JTC 1/SCs and other SDOs

SDO	TC/SC	Term	Definition	Document name	Reference

ISO/IEC JTC 1	SC 27	trust	3.13: trust: relationship between two entities and/or elements, consisting of a set of activities and a security policy in which element x trusts element y if and only if x has confidence that y will behave in a well-defined way (with respect to the activities) that does not violate the given security policy; [SOURCE: ISO/IEC 13888−1:2009, 3.59, modified]	27036 - Information security for supplier relationships	SC 27
ISO/IEC JTC 1	SC 27	trustworthiness assessment	techniques, mechanisms, and approaches used to evaluate trustworthiness of a system, environment, organization, technology or products. The approaches include, but are not limited to risk analysis, SDL (Secure Development Lifecycle), governance, deterministic testing, and other.		
ISO/IEC JTC 1	SC 27	trustworthiness	demonstrable likelihood that the system performs according to designed behaviour under a typical set of conditions as evidenced by its characteristics, such as safety, security, privacy, reliability and resilience (from NIST CPS Framework v1.0).	SC 27/WG 3 Study Period Report - Guidelines for ICT Trustworthiness Assessment Framework	SC 27
ISO/IEC JTC 1	SC 31		Crypto suite specification which deals with over the air security between RFID tags and readers.	20248 - Automatic identification and data capture techniques -- Data structures -- Digital signature meta structure	SC 31
ISO/IEC JTC 1	SC 31		Digital signature data structures for automated identification. This specification provides a method for data obtained from an AutoID carrier to be verified in the absence of access to a central system and in any place in the chain between the detection and the use of the data. This verification includes data structure ownership, data structure, data ownership and data verification.	29167 - Information technology -- Automatic identification and data capture techniques	SC 31

ISO/IEC JTC 1	SC 38	trust	3.7 degree to which a user or other stakeholder has confidence that a product or system will behave as intended [SOURCE: ISO/IEC 25010:2011, 4.1.3.2] ---------- Note that there are 5 elements of Trust in the Framework for trusted cloud processing of multi-sourced data of the TR 23186. - Data use obligations and controls - Data provenance records, quality and integrity - Chain of custody - Security and privacy - Immutable proof of compliance ISO/IEC 23751 (WD1) - Data Sharing Agreement (DSA) Framework also follows the elements of ISO/IEC TR 23186.	TR 23186 - Information technology — Cloud computing — Framework of trust for processing of multi-sourced data	SC 38
ISO/IEC	SC 40	Governance of Trust	ISO/IEC 38500 defines 3 activities all relevant to apply in order to obtain state of and control of trustworthiness: Evaluate (current state of Trust by stakeholders), Direct (what level of Trust is acceptable?) and Monitor (if the requested level of trust has been achieved).	ISO/IEC 38500	
ISO/IEC	SC 40	Governance of Trust	ISO/IEC 38500 states 6 principles relevant to apply in the context of assessing and obtaining Trustworthiness objectives: Principle 1 is Responsibility. How is trustworthiness anchored in the organisation in terms of roles and responsbilities?	ISO/IEC 38500	
ISO/IEC	SC 40	Governance of Trust	ISO/IEC 38500 states 6 principles relevant to apply in the context of assessing and obtraining Trustworthiness objectives: Principle 2 is Strategy. How is the terms and relevance of trustworthiness included in any strategy considerations?	ISO/IEC 38500	

ISO/IEC	SC 40	Governance of Trust	ISO/IEC 38500 states 6 principles relevant to apply in the context of assessing and obtraining Trustworthiness objectives: Principle 3 is Acquisition. How is due diligence of new vendors and other acquisition decisions supporting that trustworthiness throughout the supply chain has been addressed?	ISO/IEC 38500
ISO/IEC	SC 40	Governance of Trust	ISO/IEC 38500 states 6 principles relevant to apply in the context of assessing and obtraining Trustworthiness objectives: Principle 4 is Performance. Which KPI's are addressing trustworthiness objectivies and how often do we monitor performance?	ISO/IEC 38500
ISO/IEC	SC 40	Governance of Trust	ISO/IEC 38500 states 6 principles relevant to apply in the context of assessing and obtraining Trustworthiness objectives: Principle 5 is Conformance. How trustworthy are the adherence to external and internal compliance requirements?	ISO/IEC 38500
ISO/IEC	SC 40	Governance of Trust	ISO/IEC 38500 states 6 principles relevant to apply in the context of assessing and obtraining Trustworthiness objectives: Principle 6 is Human Behaviour. How are human behaviour and organizational culture supporting the trustworthiness objective? (or the opposite!)	ISO/IEC 38500
ISO/IEC	SC 40	Governance of Security	ISO/IEC 27014 Governance of cyber Security. Security being one of the definitions of trustworthiness this standard should be part of the assessing current standardization activities.	ISO/IEC 27014
ISO/IEC	SC 40	Implementation of trust governance	ISO/IEC 38501, 38502 addresses the implementation of governance activities and principles in the context of any organization. These two standards may be applied with the purpose of addressing trustworthiness objectives.	ISO/IEC 38501, ISO/IEC 38502

ISO/IEC	SC 40	Assessing governance against Trustworthiness	ISO/IEC 38503 Assessing IT governance is a standard that is addressing the expected outcomes of good governance and the methodology may be applied towards the expected outcome of trust.	ISO/IEC 38503
ISO/IEC	SC 40	Investing in trustworthiness	ISO/IEC 38506 Application of 38500 to the IT-enabled investments is a standard that addresses due diligence, technical debt and other investment topics that may impact the trustworthiness objective in either direction.	ISO/IEC 38506
ISO/IEC	SC 40	Governance of Trust	ISO/IEC 38505 - Part 1: Application of ISO/IEC 38500 to the governance of data, - assuring stakeholders that, if the principles and practices proposed by this document are followed, they can have confidence (=trust?) in the organization's governance of data - informing and guiding governing bodies in the use and protection of data in their organization.	ISO/IEC 38505 - Part 1
ISO/IEC	SC 40	Governance of Trust	ISO/IEC 38505 - Part 2: implications of ISO/IEC 38505-1 for data management. It assumes understanding of the principles of ISO/IEC 38500 and familiarization with the data accountability map and associated matrix of considerations, as presented in ISO/IEC 38505-1. Trustworthy data and/or data trustworthiness may very well be identified objectives for data management.	ISO/IEC 38505 - Part 2
ISO/IEC JTC 1	SC 41	Trustworthiness	deserving of trust or confidence	

ISO/IEC JTC 1	SC 41	IT system Trustworthiness	deserving trust within the entire lifecycle of an IT system to ensure security, privacy, safety, reliability and resiliency Note to the entry 1: ITT can be expressed with a Level of Trust (1.6). Note to the entry 2: Trustworthiness includes attributes describing Security (information integrity, device/system integrity, information availability, device/system availability, information confidentiality, and device/system confidentiality), Privacy (privacy frameworks, and Law & Regulations), Safety (environmental safe, living entity safety, and operational safety), Reliability and Resiliency.	
ISO/IEC JTC 1	SC 41	IoT system Trustworthiness	deserving trust within the entire lifecycle of an IoT system to ensure security, privacy, safety, reliability and resiliency Note to the entry 1: IoTT can be expressed with a Level of Trust (1.6). Note to the entry 2: Trustworthiness includes attributes describing Security (information integrity, device/system integrity, information availability, device/system availability, information confidentiality, and device/system confidentiality), Privacy (privacy frameworks, and Law & Regulations), Safety (environmental safe, living entity safety, and operational safety), Reliability and Resiliency. (ISO/IEC 30149)	ISO/IEC 30149 Internet of things (IoT) -- Trustworthiness framework

ISO/IEC JTC 1	SC 41	Level of Trust	list of Trustworthiness controls (1.7) that have to be implemented and verified Note to the entry 1: IT system Level of Trust is only valid for the IT system environment in which it was identified, including its Business sector contexts, Regulatory contexts and Technological contexts where an IT system will be used and/or are operated, and also taking in account the IT system's specifications. Note to the entry 2: The verification-measurement process included within each Trustworthiness control will produces expected evidences that this controls was correctly implemented and is mitigating related risks as expected.	ISO/IEC 30149 Internet of things (IoT) -- Trustworthiness framework	
ISO/IEC JTC 1	SC 41	trustworthiness	7.2 IoT system trustworthiness characteristics 7.2.2 Availability 7.2.3 Confidentiality 7.2.4 Integrity 7.2.5 Protection of personally identifiable information 7.2.6 Reliability 7.2.7 Resilience 7.2.8 Safety	ISO/IEC 30141 Internet of Things (IoT) – Reference architecture	SC 41
ISO/IEC JTC 1	SC 41	trustworthiness	degree of confidence a stakeholder has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disruptions, human errors, system faults and attacks	ISO/IEC 20924 Internet of Things (IoT) - Vocabulary	SC 41
ISO/IEC JTC 1	SC 41	trustworthiness	deserving of trust or confidence	Internet of Things (IoT) – Methodology for implementing and maintaining trustworthiness of IoT systems and services	SC 41
ISO/IEC JTC 1	SC 41	trustworthiness	deserving of trust or confidence	ISO/IEC SC 41 AHG 8	SC 41

				Trustworthiness Report	
ISO/IEC JTC 1	SC 41	IoT trustworthiness	deserving trust within the entire lifecycle of an IoT implementation to ensure security, privacy, safety, reliability and resiliency	ISO/IEC SC 41 AHG 8 Trustworthiness Report	SC 41
ISO/IEC JTC 1	SC 41	Trustworthiness Control	data structure containing a precise enumeration and description of a trustworthiness activity and its associated verification measurement to be performed at a specific point in an IoT system's life cycle (See Figure 1) (ISO/IEC 30149)	Internet of things (IoT) -- Trustworthiness framework	
ISO/IEC JTC 1	SC 42	trustworthiness	The degree to which a user or other stakeholder has confidence that a product or system will behave as intended, This definition can be applied across the broad range of AI systems, technologies, and application domains.	ISO/IEC 24028:2019 Overview of trustworthiness in artificial intelligence	SC 42
ISO/IEC JTC 1	SC 7	trustworthy data	data and related information that is accurate, complete, relevant, readily understood by and available to those authorised users who need it to complete a task	19970 - Information technology -- IT asset management -- Part 1: IT asset management systems	SC 7
ISO	TC 171	trustworthiness	quality [of a TTPR] of being dependable and reliable	17068 - Information and documentation -- Trusted third party repository for digital records	TC 171
ISO	TC 171	trustworthy	ability to demonstrate authenticity, integrity and availability of ESI over time	TR 15801:2017 - Document management -- Electronically stored information -- Recommendations for trustworthiness and reliability	TC 171
ISO	TC 171	trustworthy	stored electronically in an accurate, reliable and usable/readable manner, ensuring integrity over time	18829 - Document management -- Assessing ECM/EDRM implementations	TC 171

				-- Trustworthiness	
ISO	TC 20	trustworthy digital repository	a mission to provide reliable, long-term access to managed digital resources to its Designated Community, now and into the future	Space data and information transfer systems -- Audit and certification of trustworthy digital repositories	TC 20/SC 13
IIC		trustworthiness	degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disturbances, human errors, system faults and attacks	The Industrial Internet of Things, Volume G8: Vocabulary	IIC:PUB:G8:V2.1:PB:20180822
IIC		trust boundary	separation of different application or system domains in which different levels of trust are required	The Industrial Internet of Things, Volume G8: Vocabulary	
ILNAS		trust	Trust is one of the fundamental constructs to any interaction in our society and relates to the presumption about the dependability of, reliability of, and/or confidence in a person, process, system or other entity.	Digital Trust for Smart ICT	
ILNAS		trust	Mayer et al. define trust as: “the willingness of a party [trustor] to be vulnerable to the actions of another party [trustee] based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party”.	Digital Trust for Smart ICT	
ILNAS			Trust comprises three fundamental elements that relate to expectations, beliefs, and the risk appetite of trustor and trustee. Huang and Nicol describe it as follows: 1) expectancy – the trustor anticipates a specific behavior from the trustee; 2) belief – the trustor has confidence that the expected behavior occurs, based on the evidence of the trustee’s competence, goodwill, and	Digital Trust for Smart ICT	

		integrity; 3) willingness to take risk – the trustor is prepared to take a risk for that belief.	
ILNAS	digital trust	Digital Trust for Smart ICT indicates a positive and verifiable belief about the perceived reliability of a digital information source, product or service, leading to an intention to use.	Digital Trust for Smart ICT
ILNAS	digital trust	Building and maintaining Digital Trust involves more aspects than in a world without electronic communications, because digital communications rely not only on human beings and their relationships, but also on digital components. In Digital Trust, not only the classical social trust concept is involved, but also technological trust from the different parties in an IT system as depicted by Giustiniano and Bolici.	Digital Trust for Smart ICT
ILNAS	digital trust	Accenture also defines Digital Trust as “the confidence placed in an organization to collect, store, and use the digital information of others in a manner that benefits and protects those to whom the information pertains”. They identified four key areas to Digital Trust: 1) accountability, 2) security, 3) privacy, and 4) consumer benefit and value, each of which must be satisfied to gain and maintain trust with a specific brand.	Digital Trust for Smart ICT

ILNAS	digital trust	Digital Trust is fundamental for ensuring the further development and success of IoT. For devices, or “things” that are permanently connected, whose purpose is the monitoring of activities and data collection and that send these data through the Internet, two major Digital Trust requirements have to be addressed: security and privacy. These two broad requirements include authentication and authorization within the IoT network, data confidentiality, privacy and trust among users and things, and the enforcement of security and privacy policies. Sicari et al. argue that conventional security measures and privacy enforcement cannot be applied to IoT technologies due to their limited computing power. In addition, the huge number of interconnected devices will cause scalability issues. Nevertheless, to guarantee Digital Trust in IoT environments, the interconnected devices have to process and handle the data in compliance with user rights and needs. Borgia discusses the most significant IoT requirements that include one category specifically allocated to trust, security and privacy. Further requirements relate to efficiency, flexibility and quality, among others.	Digital Trust for Smart ICT

ILNAS	digital trust	In the field of Cloud Computing, there are still complex and important Digital Trust challenges to be tackled. From the perspective of the consumer, these range from technical to commercial and strategic aspects: • Data security concerns • Reliability of service and business continuity • Integration and interoperability with on-premises systems • Weak contracts, SLAs and consequences for non-performance • Limited transparency • Loss of control • Immaturity of vendors • Vendor lock-in and data portability • Long-term costs and total cost of ownership (TCO) uncertainties • Legal and regulatory compliance	Digital Trust for Smart ICT

ILNAS	digital trust	Accenture focuses on four key areas to build and maintain Digital Trust: accountability, security, privacy, and consumer benefit and value. To build Digital Trust, consumers need confidence in each of these areas. - Accountability: At all times, companies must be accountable for the protection of consumers' digital information. Companies should establish a transparent model that specifies what and how data is sourced and from whom. Monitoring what data is accessed, when and by whom is a critical aspect of maintaining trust. Furthermore, companies are accountable for misuse of and incorrect information about customers and they must promptly take corrective actions. Selecting the right business partners that enhance consumer trust is another vital ingredient to further increase customers' Digital Trust. - Security: Access control mechanisms should be more sophisticated and no longer be based on a username / password combination as more user-friendly and secure technologies are necessary to improve the user experience. Examples are biometric authentication methods using human finger prints, irises, and voice recognition to replace the numerous PIN or password-protected sources. - Privacy: User confidence in the security of personal information must be enhanced. Transparency and control are crucial elements to meet consumer privacy needs. They require the ability to opt in (instead of to opt out) for activities related to sharing information, ads, recommendations and offers based	Digital Trust for Smart ICT

		on location. If consumers do not recall giving their permission, they will probably consider this as a privacy violation. For companies to build Digital Trust, they have to create guidelines on data used to administer these activities and communicate this to consumers. This allows users to have at least some control over who uses their personal information and how. - Consumer benefit and value: Two-thirds of all consumers worldwide are willing to share their personal information in exchange for some perceived value, such as discounts or services that they value. However, companies must offer real value in exchange for personal information that the consumers provide and the data in question are clearly necessary to the services that are provided.At the same time, both consumers and companies must treat the exchange of consumers' personal information as a monetary transaction. This will ease the struggle between privacy on the one hand, and providing tailored services for each consumer's specific interest on the other.	
NIST	trustworthiness	Trustworthiness includes attributes such as security, privacy, reliability, safety, availability, and performance, to name a few.	NIST SP 800-183
NIST	trustworthiness	Trust in some NoT (=Network of Things) A, at some snapshot X, is a function of NoT A's assets ϵ {sensors (s), aggregator(s), communication channel(s), eUtility(s), decision trigger(s)} with respect to the members ϵ {geographic location, owner, environment, cost, Device_IDs, snapshot} when applicable.	NIST SP 800-183

NIST	Internet of Things (IoT) Trust Concerns	Here, trust is the probability that the intended behavior and the actual behavior are 126 equivalent, given a fixed context, fixed environment, and fixed point in time. Trust is viewed as a 127 level of confidence. In this publication, trust is considered at two levels: (1) can a 'thing' or 128 device trust the data it receives, and (2) can a human trust the 'things', services, data, or 129 complete IoT offerings that it uses.	NIST Draft NISTIR 8222	
NIST	trust	A characteristic of an entity that indicates its ability to perform certain functions or services correctly, fairly and impartially, along with assurance that the entity and its identifier are genuine.	Glossary - CSRC	NIST SP 800-152
NIST	trust	The confidence one element has in another, that the second element will behave as expected.	Glossary - CSRC	NIST SP 800-161, NISTIR 7622
NIST	trust	The willingness to take actions expecting beneficial outcomes, based on assertions by other parties.	Glossary - CSRC	NIST SP 800-95
NIST	trust	An ISCM capability that ensures that untrustworthy persons are prevented from being trusted with network access (to prevent insider attacks).	Glossary - CSRC	NISTIR 8011 Vol. 1 under Capability, Trust Management
NIST	trust	See Capability, Trust Management.	Glossary - CSRC	NISTIR 8011 Vol. 1