International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Technical Report

(19 July 2019)

ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities

Technical Report D4.3

Overview of technical enablers for trusted data

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for the establishment of focus groups are defined in Recommendation ITU-T A.7. ITU-T Study Group 20 set up the ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities (FG-DPM) at its meeting in March 2017. ITU-T Study Group 20 is the parent group of FG-DPM.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

Technical Report D4.3

Overview of technical enablers for trusted data

Summary

This Technical Report addresses the following issues:

- description of trusted data;
- perspectives on trusted data;
- specific considerations for technical enablers to ensure data trustworthiness from existing standards, specifications and use cases;
- stakeholder’s interests and concerns on technical enablers to ensure data trustworthiness for Internet of Things and Smart Cities and Communities;
- characteristics and quality characteristics of trusted data across domains for Internet of Things and Smart Cities and Communities;
- an integrated requirements framework for technical enablers to ensure trusted data for Internet of Things and Smart Cities and Communities;
- generic considerations for trusted data.

Acknowledgements

This Technical Report was researched and principally authored by Xiaomi An (Renmin University of China), Xiaoshuang Jia (Renmin University of China), Ilyoung Chong (Hankuk Univeristy of Foreign Studies), Nathalie Feingold (NPBA), Robert Lewis-Lettington (UN-HABITAT) and Wei Wei (Renmin University of China) under the chairmanship of Gyu Myoung Lee (Korea, Rep.of).

Additional information and materials relating to this Technical Report can be found at: www.itu.int/go/tfgdpm. If you would like to provide any additional information, please contact Denis Andreev (TSB) at tsbfgdpm@itu.int.

Keywords

Trusted data; technical enablers; data processing and management.

Technical Report D4.3

Overview of technical enablers for trusted data

CONTENTS

Technical Report D4.3

Overview of technical enablers for trusted data

1. Scope

This Technical Report provides an overview of technical enablers for trusted data.

The scope of this Technical Report includes:

- Characteristics and supporting enablers of trusted data, as well as the process of enabling trusted data from a recordkeeping and from a data quality management perspective;
- Special concerns about technical enablers to ensure trusted data;
- An integrated requirements framework for technical enablers to promote trusted data.

2. References

[ISO15489-1] ISO15489-1:2016 *Information and documentation-Records management-Part 1: Concepts and principles.*

[ISO 16091] ISO 16091:2018, *Space systems — Integrated logistic support*.

[ISO/TR18128] ISO/TR 18128:2014 Information and documentation — Risk assessment for records *processes and systems*.

[ISO 30300] ISO 30300:2011, *Information and documentation—Management systems for records — Fundamentals and vocabulary.*

[ISO 30301] ISO 30301:2019 *Information and documentation — Management systems for records — Requirements.*

[ITU-T Y.3051] ITU-T Recommendation Y.3051 (2017), *The basic principles of trusted environment in ICT infrastructure.*

[ITU-T Y.3052] ITU-T Recommendation Y.3052 (2017), *Overview of Trust Provisioning in ICT Infrastructures and Services.*

[ITU-T Y.3053] ITU-T Recommendation Y.3053 (2018), "*Framework of trustworthy networking with trust-centric network domains*".

[FG-DPM TS D0.1] Draft Technical Specifications D0.1 "*Data Processing and Management for IoT and Smart Cities and Communities: Vocabulary*".

[FG-DPM TR D4.1] Draft Technical Report D4.1, "*Framework for Security, Privacy and Governance in DPM*".

3. Terms and definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 ecosystem [FG-DPM TS D0.1]: A set of organisations forming a distributed system with both technical and non-technical properties.

NOTE — in DPM, ecosystem refers to a data ecosystem, which is comprised of the technical and non-technical factors and mechanisms which directly or indirectly impact DPM activities in an ecosystem, based on various degrees of interoperability. Factors and mechanisms include: but are not limited to data laws, regulations and policies, data standards, data skills, data research and development programs, data entrepreneurship, data economy financial incentives, data platforms.

3.1.2 trust [ITU-T X.1252]: The reliability and truth of information or the ability and disposition of an entity to act appropriately, within a specified context.

3.1.3 data [ISO 16091:2018]: Information represented in a manner suitable for automatic processing.

3.1.4 trusted environment (in ICT infrastructure) [ITU-T Y.3051]**:** An information and communication technology-enabled environment providing a set of technical and regulatory conditions sufficient for establishing trust between interacting entities.

NOTE – from a broader perspective, the trusted environment can be perceived as a multidimensional concept with technological and societal implications.

3.2 Terms defined in this Technical Report

This Technical Report defines the following term:

3.2.1 authority control: Operations to ensure standardized allocation of creating, capturing, storing, sharing, implementing and assessing points to trusted data in a trusted data ecosystem.

4. Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

ICT	Information and Communication Technology
I/O	input/output
MSS	Management System Standards

5. Conceptual framework for trusted data

5.1 Characteristics and supporting enablers of trusted data

The concept of trust is a complicated notion with different meanings. According to [ITU-T Y.3052], from the perspective of trust provisioning, there are physical, cyber and social worlds. In such a trust relationship model, cyber and virtual objects are linked with physical things and social entities.

Figure 1 shows the characteristics of trusted data and its lifecycle enabling processes and external supporting enablers. Table 1 and Table 2 show attributes and quality indicators of trusted data from [ITU-T Y.3051].

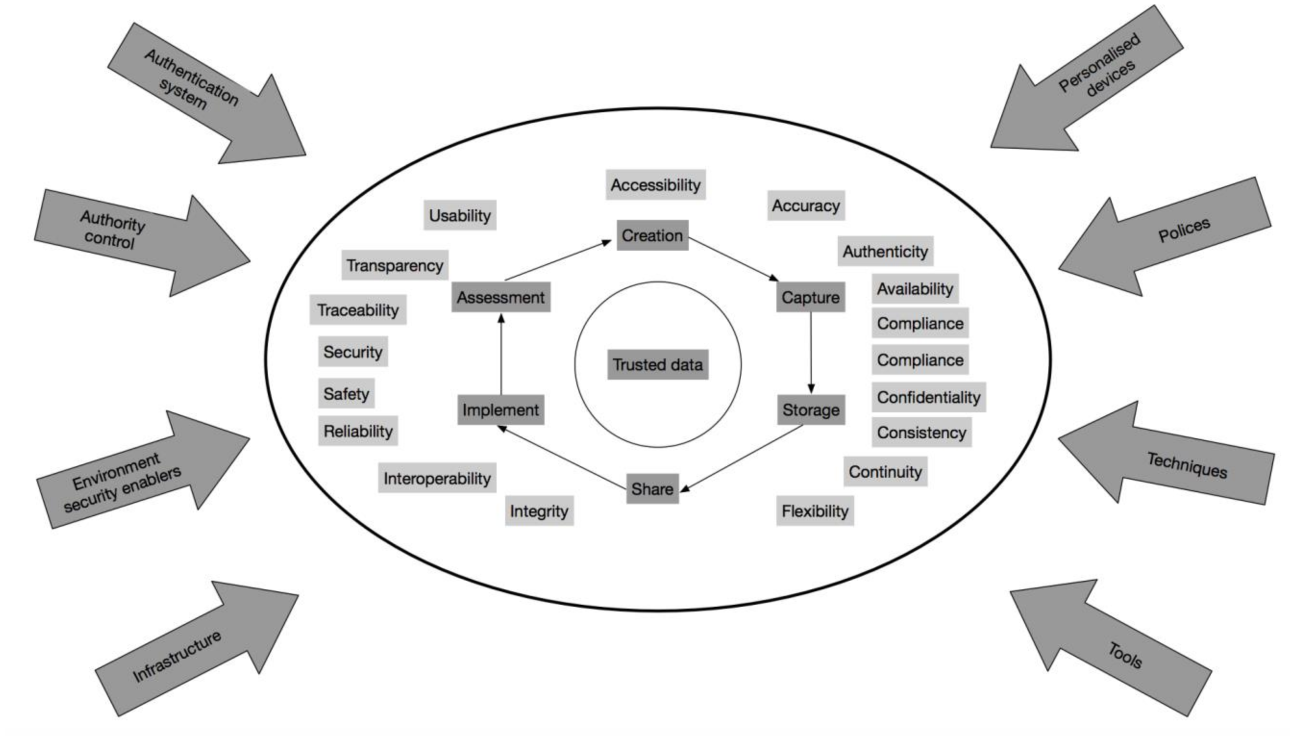

Figure 1 - Characteristics of trusted data and the supporting enablers

Table 1 - Provisioning attributes of trusted data [ITU-T Y.3051]

Provision of trusted data	Attributes description
ability/capability	stability, reliability, scalability, safety, robustness, safety
integrity/honesty	accuracy/correctness, consistency, certainty, recency
benevolence/cooperation	assurance, credibility, relevance, availability, cooperation

Table 2 - Quality indicators of trusted data

Dimension	Description	Measure	Related dimension
completeness	The proportion of stored data against the potential of "100% complete".	The measure of completeness is concerned with the percentage of existing non-empty fields.	validity and accuracy
uniqueness	Not a thing will be recorded more than once based upon how that thing is identified.	The data value can be compared with all other values in a data set to ensure that a data value is not repeated. A comparison is made between the realistic calculated data set and the recorded data set.	consistency
timeliness	The degree to which data represent reality from the required point in time.	Time variance can be compared to the time of the actual event occurrence.	accuracy
validity	Data is valid if it conforms to the syntax (format, type, range etc.) of its definition.	Data gathered can be compared to a metadata that specifies the format such as the number of figures, type such as string or decimal and range	accuracy, completeness consistency and uniqueness

Dimension	Description	Measure	Related dimension
		such as the minimum value and the greatest value permitted	
accuracy	The degree to which data correctly describes the "real world" object or event being described.	Data collected can be compared to the features of the object it's denoting to measure resemblance. Comparisons of gathered data can be made to a set of data that is derived from trusted sources.	validity (Data need to be valid for it to be accurate)
consistency	The absence of difference, when comparing two or more representations of a thing against a definition.	An examination of the value occurrences of a data in several datasets can be performed to ensure no differences are present.	validity, accuracy and uniqueness

5.2 Enabling trusted data and recordkeeping

A well-defined trust enabling process can promote trusted data. For this purpose, Figure 2 proposes a trusted data enabling process model in compliance with the requirements of [ISO 15489-1:2016] and [ISO 30301:2019] (see Appendix A normative, operational requirements for records processes, control and systems) as follows:

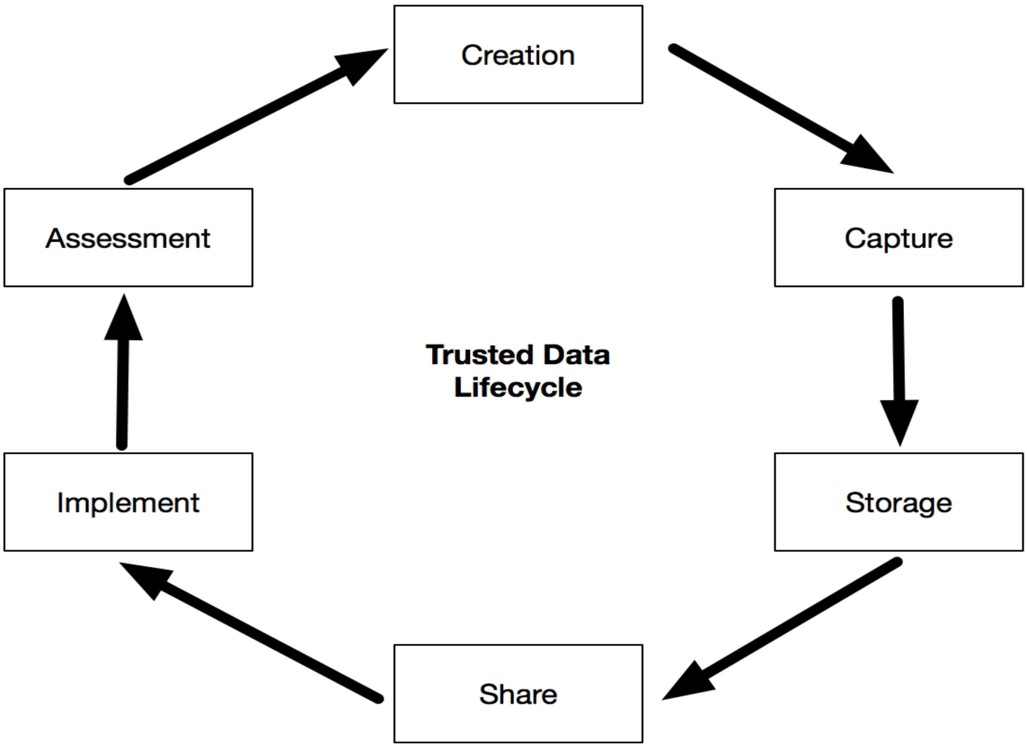

Figure 2 - Trusted data lifecycle process model

- **Create.** In the trusted data creation phase, creation control is critical to decide whether documented information or records can be regarded as trusted.
- **Capture.** There are several ways to obtain trusted data. One is where the data creator deposits data directly in the system, another is through retrieval. Technologies such as data key and blockchain can be used to ensure the trustworthiness of the data transmission process and the results.

- **Storage.** In the storage phase of trusted data, data curation should be strengthened to maintain the integrity of trusted data in both content and technology, so as to meet future use requirements.
- **Share.** The realization of trusted data sharing usually requires the support of infrastructure and third-party organizations. During the sharing process, collaboration and contractual cooperation among multiple stakeholders should be strengthened.
- **Implement.** In the implementation phase of trusted data, security tags, encryption algorithms, personalized I/O devices and other technical tools can provide strong support for the maintenance of trusted data's authenticity and integrity.
- **Assessment.** The assessment phase can focus on the evaluation of all aspects of the trusted data lifecycle. This process is of great significance for the continuous improvement of trusted data.

5.3 Process of enabling trusted data from a data quality management perspective

Table 3 shows a process to ensure trusted data through a data development cycle, which includes processes of data collection, organization, data preservation, data application.

Table 3 - Attributes for a data development cycle

Quality	Attributes	Remarks
collection quality	accuracy	The data values stored for an object have correct values and are represented in a consistent and unambiguous form.
	objectivity	Data collection always produces the same result, regardless of who collects the data.
	trustworthiness of the collector	The degree that the gatherer is honest and truthful and does not fabricate.
	completeness	Every value of data that includes all relevant elements for the process in question to be collected is actually collected.
	clarity	The degree that data holds no ambiguous observations. This point also relates to visual (and metadata) labels.
organization quality	reliability of data clerks	Data clerks should enter data values in a manner that consistently meets all attributes.
	consistency	A database with dissimilar data will be reasonably compatible.
	storage efficiency	The ability to store and manage data that consumes the least amount of space with the least impact on performance and in a lower total operational cost.
	retrieval efficiency	A search to located specific information would be efficient.
	navigability	A person can navigate through the correlated information intuitively.
presentation quality	semantic stability	Identical data possess only one meaning at different times and locations.
	faithfulness	The degree that the offered data matches the original in sense and exactness.
	neutrality	The data chosen for presentation are not biased for any specific view or purpose.
	interpretability	Data is actually described in terms of clarity, precision and ease of use.
	formality	Data is offered in a concise and reliable way
application	ease of manipulation	A measurement on the ease of analyzing data (e.g., indexing).

Quality	Attributes	Remarks
quality	timeliness	The degree to which data is current and adequately updated for a task.
	privacy	The degree to which data is accessible or personally identifiable only according to need.
	security	The degree that a task has admission to the data secured according to pre-determined criteria.
	relevancy	The degree that data are appropriate and beneficial for a certain theory or process.
	appropriate amount of data	The degree to which the quantity of information is suitable for a certain theory or process.

6. Special concerns about technical enablers to promote trusted data

6.1 Concerns about technical enablers to promote trusted data from literature

Figure 3 shows the concerns in ensuring trusted data under a multi-dimensional and layered perspective from the macro level to the micro level, as drawn from the literature. The infrastructure layer is the central part of the demand hierarchy map. The strategic level includes framework construction and methodological guidance, mainly related to the policies, the top decision-making, environmental factors, technology factors and the specific methods about "how to make data trusted". The infrastructure layer includes system construction, device production, operation and maintenance as well as cyberspace security update equipment as enablers. The operational level includes the business integration layer and the application layer. The application layer relates to data storage, data warehouse, data identification, data integration and other data services. The business integration layer is the central part of the demand analysis, i.e. it is essential to know data, people, activities and procedures (process). The essential elements of data are data quality and data security considerations. The key to the people element of business integration lies in clearing rights and in the interests of stakeholders, with activities focusing on various types of data behaviours. The essential aspects of procedures lie in inter-organizational and cross departmental cooperation and business collaboration.

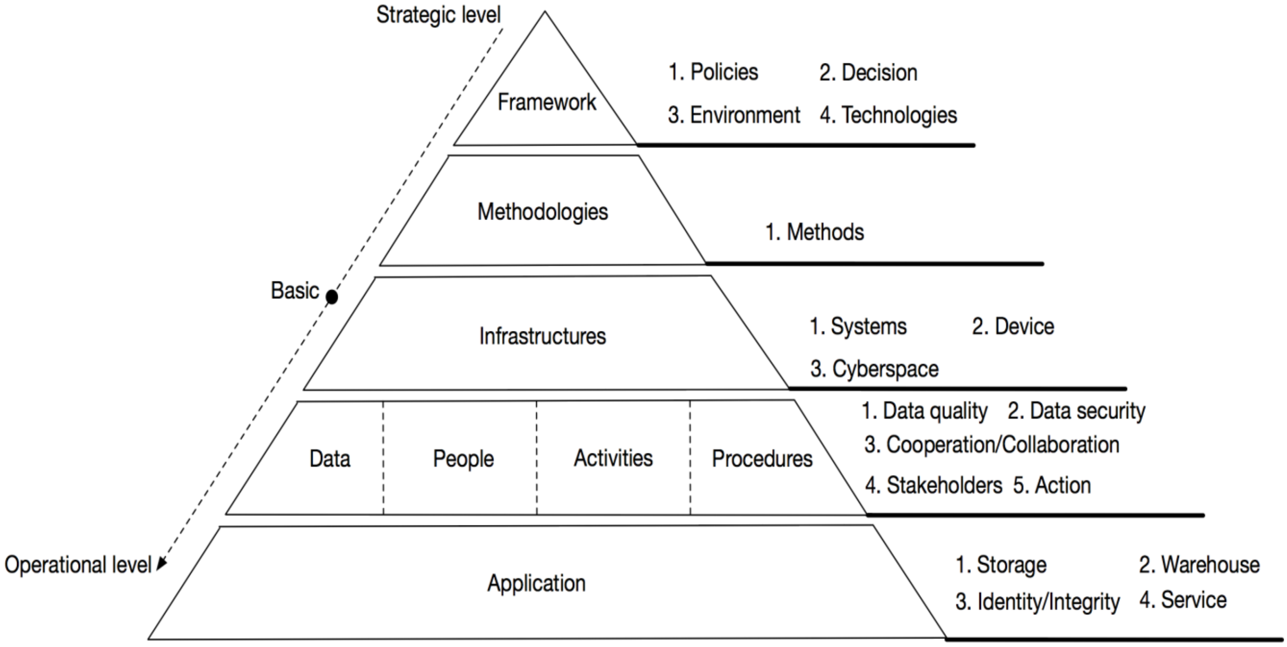

Figure 3 - Concerns about technical enablers to ensure trusted data from literature

6.2 Requirements and considerations about technical enablers to promote trusted data from ISO standards and the work of the ITU-T FG-DPM

Four publications from ISO/TC46/SC11 are identified as relevant to discussion here: [ISO 15489-1:2016], [ISO/TR 18128:2014], [ISO 30300:2011] and [ISO 30301:2019] (see Appendix B and Appendix C). Figure 4 describes the requirements and considerations in promoting trusted data based on these four ISO standards.

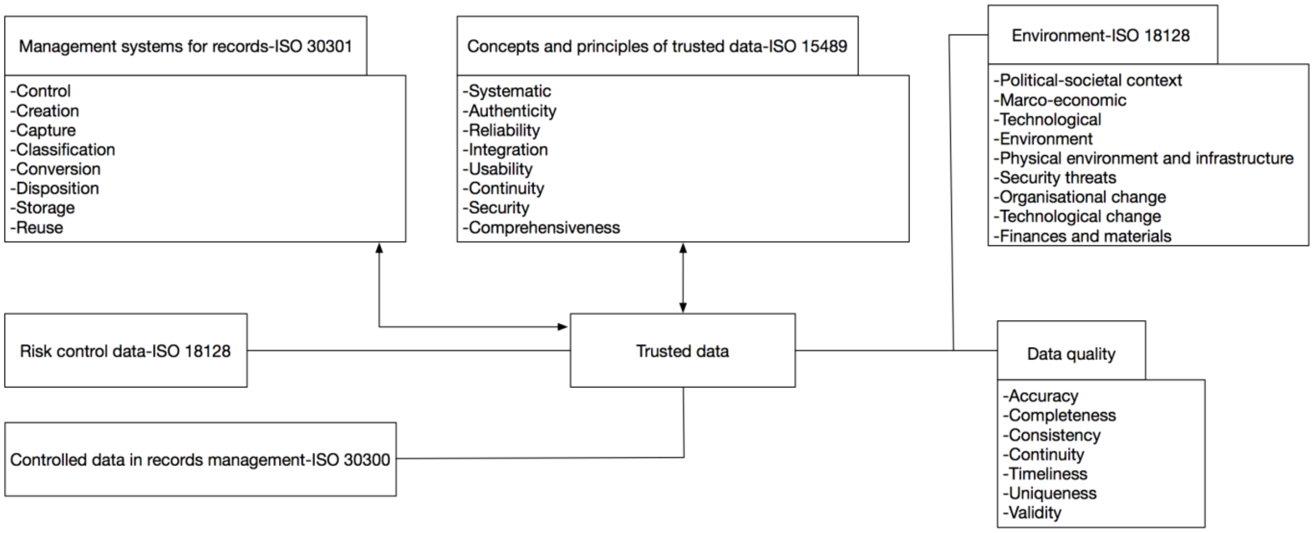

Figure 4 - Requirements and considerations for technical enablers to promote trusted data from ISO/TC46/SC11 publications

[ISO 15489-1:2016] establishes the core concepts and principles for the creation, capture and management of records to enable trusted data. Records control, processes and systems are to support technical enablers to maintain trusted data in conformity with the following requirements:

- Systematic
- Authenticity
- Reliability
- Integration
- Usability
- Continuity
- Security
- Comprehensiveness

[ISO/TR 18128:2014] is intended to help records professionals and people who have responsibility for records in their organization to assess the risks related to records processes and systems. This is distinct from the task of identifying and assessing the organization's business risks related to creating and keeping adequate records at a strategic level. The decisions to create or not create records in response to general business risk are business decisions which should be informed by the analysis of the organization's records requirements undertaken by records professionals together with business managers. The premise of this Technical Report is that the organization has created records of its business activities to meet operational and other purposes and has established at least minimal mechanisms for the systematic management and control of the records as trusted data.

The consequence of risk events to records processes and systems is the loss of, or damage to, records that are consequently no longer usable, reliable, authentic, complete or unaltered and, therefore, can fail to meet the organization’s purposes. So the probable areas of risk may also be relevant to the risks to trusted data. Similarly, the technical enablers for trusted data should also satisfy the requirements of risk control, which is discussed in [ISO/TR 18128:2014]. The key domains of risk control are listed here:

- Political-societal context
- Macro-economic
- Technological
- Environment
- Physical environment and infrastructure
- Security threats
- Organizational change
- Technological change
- Finances and materials

According to [ISO 30300:2011], the creation and management of records are integral to any organization’s activities, processes and systems. Records enable business efficiency, accountability, risk management and business continuity. They also enable organizations to capitalize on the value of their information resources as business, commercial and knowledge assets and to contribute to the preservation of collective memory, in response to the challenges of the global and digital environment. Management System Standards (MSS) provide tools for top management to implement a systematic and verifiable approach to organizational control in an environment that encourages good business practices. Although [ISO 30300: 2011] focuses on records management in organizational activities, the record is documented information, which is also a form of trusted data, so the following guidelines of [ISO 30300:2011] are also applicable to trusted data:

- Defined roles and responsibilities;
- Systematic processes;
- Measurement and evaluation;
- Review and improvement.

[ISO 30301: 2019] specifies requirements to be met by a ‘management system for records’ to support an organization in the achievement of its mandate, mission, strategy and goals. It addresses the development and implementation of a records policy and objectives and gives information on measuring and monitoring performance. A management system for records can be established by an organization or across organizations that share business activities. Throughout this International Standard, the term “organization” is not limited to one organization but also includes other organizational structures. Process control in [ISO 30301:2019] is fundamental to the construction of functional requirements for technical enablers to promote trusted data:

- Control
- Creation
- Capture
- Classification
- Storage

- Use and reuse
- Migration and conversion
- Disposition

Data quality can be specified as the degree to which the characteristics of the data satisfy stated and implied needs when used under specified conditions. Several dimensions can define the quality of data, including:

- Accuracy
- Completeness
- Consistency
- Continuity
- Timeliness
- Uniqueness
- Validity

6.3 Common concerns about technical enablers to promote trusted data

Based on the analysis of 6.1 and 6.2, a comprehensive framework of technical enablers to ensure trusted data is recommended. Figure 5 shows different aspects of technical enablers which can promote the core attributes of trusted data.

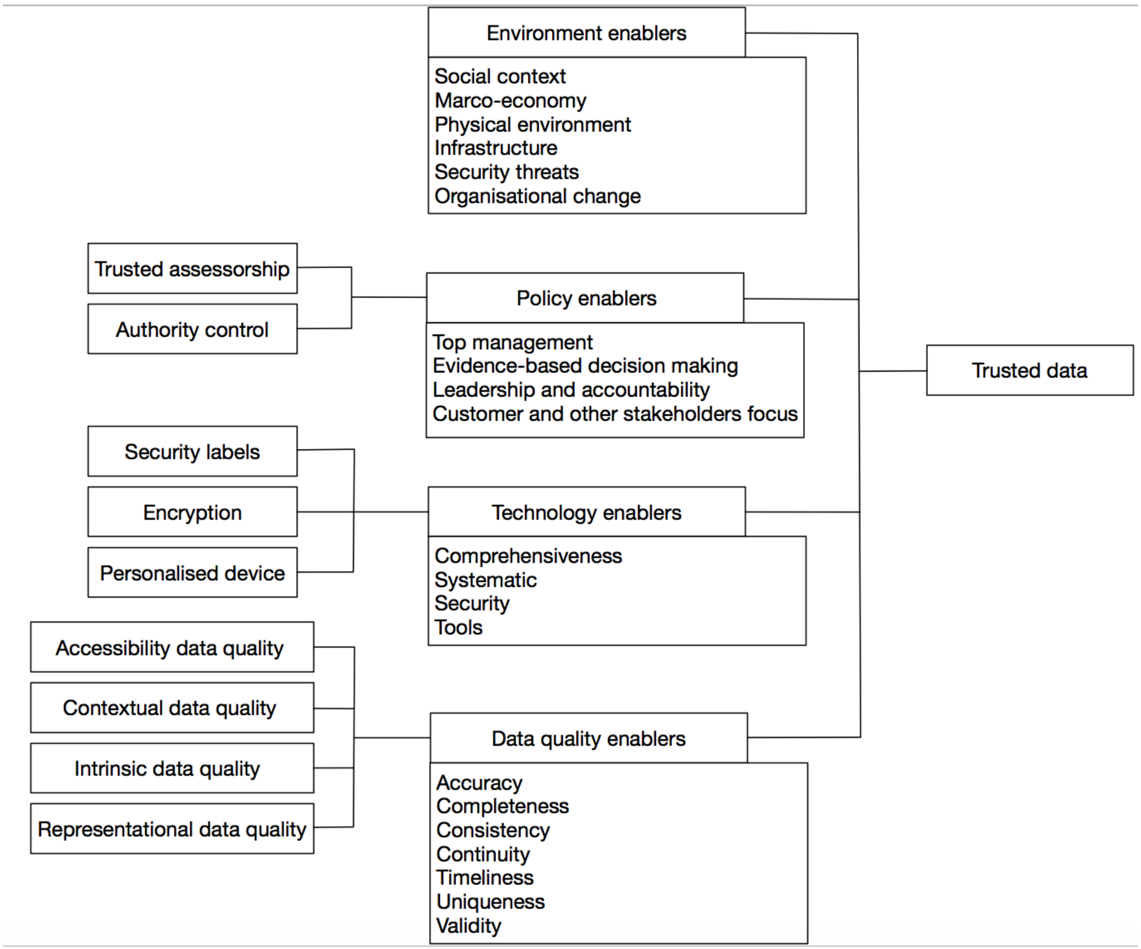

Figure 5 - Framework of technical enablers to promote trusted data

The technical enablers of trusted data may be categorised into four groups: environment, policy, technology and data quality. The security and macro policy factors in the external environment provide the development background and direction for the technical enablers. Technology is important to provide technical support, while data quality is indispensable. The source of metadata and its important attributes are a critical determinant of data quality.

– Environment enabler. The external environment has some basic properties, such as social context, macro-economy, physical environment, infrastructure, security threats and organizational change (these attributes are arranged according to their logical sequence).

– Policy enabler. According to ISO international standards, macro policies include top management, evidence-based decision making, leadership and accountability and customer and other stakeholders' focus. In this part, trusted assessorship and authority control of technology are recommended.

– Technology enabler. Technology includes three aspects, which are security labels, encryption and personalized I/O device. In this part, the comprehensiveness, systematic use and security of the technology is recommended.

– Data quality enabler. Data quality includes traceable actions and appropriate metadata to promote the accuracy, completeness, consistency, continuity, timeliness, uniqueness and validity of data to make it trustworthy. In this part, accessibility data quality, contextual data quality, intrinsic data quality and representational data quality of technology is recommended.

7. An integrated requirements framework for technical enablers to promote trusted data

An integrated requirements framework is recommended for technical enablers to promote trusted data. Such a framework consists of three parts producing a complementary whole: i) strategy requirements, ii) infrastructure requirements, and iii) process requirements. Figure 6 describes the key components of an integrated framework and their relationships. The integrated framework brings the major concerns discussed in section 6.3, above, together as organic whole to promote the working of technical enablers in a consistent, coherent and interconnected way that enables trusted data.

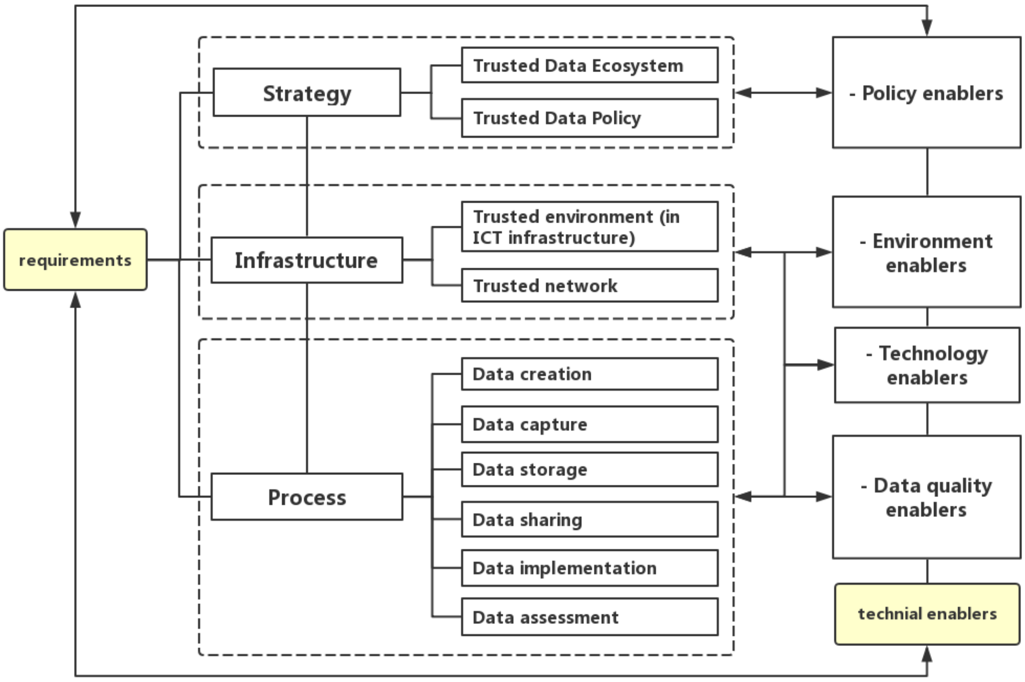

Figure 6 – An integrated requirements framework for technical enablers to promote trusted data

7.1 Strategy requirements for technical enablers that promote trusted data

7.1.1 Trusted data ecosystem

A data ecosystem is a collection of all other value adding peripheral and non-specific factors comprised of data laws, regulations and policies, data standards, data skills, data research and development programs, data entrepreneurship, data economy financial incentives, data platforms. It is a multi-layered system that attempts to include a variety of data sources in the cyber world.

It is recommended to:

- Build a more complete system of data laws, regulations or policies to enhance trust for data.
- Build a commonly agreed standards to enable collaboration and cooperation among different stakeholders and allow them to adopt a unified language and provide various shortcuts for trusted data.
- Take a lot of action items to enhance data skills of actors such as providing workplace and professional training programs.
- Set up good data research and development programs to address particular challenges and to help build data skills and knowledge for the long term.
- Encourage data entrepreneurship and provide a rich environment conducive to innovation.
- Build a financial incentive to promote monetary benefit to motivate or encourage trust behaviours or actions of actors.
- Build data platforms to provide connectivity and capabilities by architecting and implementing trusted data related to ICT infrastructure, solutions and services.

7.1.2 Trusted data policy

A trusted data ecosystem requires authority control, which means operations to ensure standardized allocation of creating, capturing, storing, sharing, implementing and assessing points to trusted data in a trusted data ecosystem. Authority control is recommended to ensure the trusted data ecosystem run in a systematic, planned and managed way.

It is recommended to:

- Develop a data governance policy to outline the data governance framework that covers the responsibilities, accountabilities and interests relating to the data process.
- Develop a digital continuity policy for trusted data to outline how to embed digital continuity in data management, IT strategy and environment, and change management.

NOTE – A data governance policy and a digital continuity policy can be merged into one provided that the specific need for continuity is not lost.

7.2 Infrastructure requirements for technical enablers to promote trusted data

The infrastructure requirements for technical enablers to ensure trusted data consist of a trusted environment and a trusted network in ICT infrastructure.

7.2.1 Trusted environment

Creating a trusted environment in the ICT infrastructure is necessary for technical enablers to promote trusted data. A trusted environment in the ICT infrastructure must meet the requirements of predictability, information security, interoperability and the availability of administrative services. A trusted environment within ICT infrastructure should meet the following requirements:

- **Predictability.** All participants within a trusted environment are required to be equipped with the capability to predict the outcome of their interactions in order to reduce the risks of negative consequences caused by the inappropriate behaviour of any participant(s). To achieve this, the

ICT infrastructure used to create a trusted environment is required to meet a certain level of quality. The provision of intuitive user interfaces and systems of access to a trusted environment is recommended for participants to improve predictability, by using comfortable and familiar methods of interaction each time.

- **Information security.** Where relevant, the confidentiality, integrity and the availability of information, as well as the absence of misinformation, should be guaranteed for all participants interacting within a trusted environment. Minimum security requirements for an end-to-end trusted environment in an ICT infrastructure are required to be developed for all security dimensions with the goal of providing electronic exchange of information in a trusted environment at the same level of trust as in a non-electronic interaction.
- **Interoperability.** All participants should be able to exchange information with any other participant within a trusted environment in an ICT infrastructure. A trusted environment in an ICT infrastructure is required to support internetwork connections to provide uniform interaction capabilities to each participant, independent of the technical infrastructure (core networks) each uses. Predictability, information security and availability of administrative services requirements are required to be supported for internetwork connections.
- **Availability of administrative services.** The provision of continuous customer support is required for all interacting participants within a trusted environment in an ICT infrastructure, as well as prompt compensation if service provision fails. A trusted environment in an ICT infrastructure is required to maintain the capacity to enroll new participants, enabling them to rapidly integrate and start operating within the trusted environment in the ICT.

NOTE - For more details, see [ITU-T Y.3051], the basic principles of trusted environment in ICT infrastructure.

7.2.2 Trusted network

A ‘trusted network’ is a set of methods that provides reliable and secured communications among any pair of network elements that have trust relationships. The building of trustworthy networking within trust-centric network domains is recommended.

High-level requirements for trustworthy networking within trust-centric network domains include:

- The network elements should be managed by identifiers and locators;
- The evaluation of the trustworthiness of all the network elements within the trust-centric network domains;
- The provision of an interface for communicating outside of the trust-centric network domain;
- Supporting trust management to maintain the trust-centric network domain;
- The provision of a trustworthy communication link which satisfies the proper trust levels.

The functional requirements for trustworthy networking within trust-centric network domains include:

- Trust management is required to i) evaluate the trust levels of network elements or domains by aggregating their trust-related information, ii) validate the trust levels of network elements or domains after a trust evaluation process, and iii) support the lifecycle management of the trust information including planning, creation, allocation, modification and deletion.
- Administration. A trust-centric network domain is required to i) provide mapping between IDs and locators for access and delivery control, ii) manage the membership of the network elements during registration, identification and policy enforcement, and iii) settle domain policies (e.g., the trust level of domain membership and security configuration of the domain).

– Access and delivery control. A trust-centric network domain should include checks and control of the communication link with any actor outside of the trust-centric network domain. This should be managed according to trust levels and provides data delivery control to enable data forwarding and routing to control incoming and outgoing data packets and to make decisions on the routing paths of packets according to the trust-centric network domain management policy.

NOTE – Deliverable [ITU-T Y.3053] provides more analysis on this topic.

7.3 Process requirements for technical enablers to promote trusted data

Based on the trusted data enabling process model described in section 5.2, above, the process requirements for technical enablers to ensure trusted data include 6 parts, from data creation through to data assessment.

7.3.1 Data creation

In the trusted data creation phase, data creation should be regulated by corresponding policies, regulations and subject to authority control. Trusted data can be created by the data creator directly in the system as well as be collected or gathered by the data creator from outside components.

Documented information should be created at the time of the transaction or event to which they relate by an individual with direct knowledge of the facts or by instruments routinely used by the organization to conduct the transaction. The form and structure of the information required as trusted data for each work process should be identified and documented [ISO 30301:2019].

7.3.2 Data capture

In the trusted data capture phase, the device and platform used to capture data are required to have enough precision to identify and prioritise relevant data at acceptable expense to extract relevant trust information from the system or things in question. Privacy mechanisms are an important component in the data capture process. The use of technologies such as data key, gateway and blockchain are recommended to ensure the trustworthiness of the data transmission process. Contextual information about the trusted data being transmitted should be added at the point of capture. At the time of capture, a unique identifier should be attached wherever work processes may require evidence of capture. When a record supersedes an existing one (updating), the new version shall indicate the obsolete one and the changes made [ISO 30301:2019].

7.3.3 Data storage

In the trusted data storage phase, the data should be effectively curated to meet the digital continuity requirements of completeness and availability. The means of maintaining and storing records should meet the relevant standards for the medium and technology used, in order to ensure they remain useable for as long as required [ISO 30301:2019].

NOTE - Digital continuity is the ability to use data and information, in a way adapted to the need in question, for as long as may be needed. This promotes the accountable, legal, effective and efficient maintenance of documented information.

7.3.4 Data sharing

Data sharing refers to the transfer of data between components within an internal system as well as to transfers between internal systems and external systems. Collaboration and contractual cooperation among multiple stakeholders should be strengthened in the trusted data sharing phase. The support of infrastructure and third-party organizations such as archival institutions are recommended. Trusted data should remain accessible and useable over time. Actions on trusted data to be recorded in metadata should be defined and implemented [ISO 30301:2019]. Rules to access trusted systems in order to undertake system administration tasks should be established, documented and maintained [ISO 30301:2019].

7.3.5 Data implementation

In the trusted data implementation phase, the use of technologies such as security tags, encryption algorithms, personalized I/O devices and other technical tools to maintain the authenticity and integrity of data is recommended to make that data trustworthy. Actions on trusted data to be recorded in metadata should be defined and implemented. [ISO30301:2019]. Decisions about the transfer, removal or destruction of trusted data should be authorized and documented. [ISO30301:2019]. Technologies for creating and capturing trusted data should be selected for work processes. The selection and technological changes should be documented [ISO 30301:2019].

7.3.6 Data assessment

The assessment of data quality and risk is recommended for all aspects of the trusted data lifecycle to maintain the properties of trusted data identified in 5.3, above. The quality of high value data should be monitored on a regular basis and should be involve everyone within a given ecosystem.

NOTE 1- For more information and process about data risk management. See section 6 ‘Risk management in DPM’ in “Framework for security, privacy, and governance in DPM” [FG-DPM TR D4.1].

NOTE 2 - Data quality rules and policies should be implemented and continuously improved. For further detail, see section 6.3 ‘Guidance for organisations and ecosystem in “Framework for security, privacy, and governance in DPM” [FG-DPM TR D4.1].

Control information (registration, identification and metadata) about the trusted data which has been destroyed shall be retained where relevant to the nature and complexity of the business or required by formal accountability standards. [ISO 30301:2019]. Descriptive and control information required to create and control the trusted data for each work process should be identified and documented and the decisions about metadata required to identify, manage and control trusted data should be documented and implemented [ISO 30301:2019]. Retention and disposition schedules and actions should be authorized and documented [ISO 30301:2019].

Regulator monitoring of the performance of a trusted data system against business requirements and trust objectives should be implemented and documented [ISO 30301:2019].

Trusted data should remain accessible and useable over time. Actions on trusted data to be recorded in metadata should be defined and implemented [ISO 30301:2019]. Rules to access trusted systems in order to undertake system administration tasks should be established, documented and maintained [ISO 30301:2019].

Appendix A
Features of trusted data from ISO standards

ISO standard	Attributes of trusted data	Characteristics	Enablers

[ISO 15489-1:2016]	Systematic;
	Authenticity;
	Reliability;
	Integration Usability;
	Continuity;
	Security;
	Comprehensiveness;
		Evidence for business activity	Business purpose;
			Efficient and systematic control of records

[ISO/TR 18128:2014]	1.Context, systems, and processes 2.Political-societal context， Macro-economic and technological environment, Physical environment and infrastructure, security threats 3.Organizational change, Technological change， Technological change, Finances and materials 4.Sustainability and Continuity		Against what can happen or what situations can exist that could affect the capacity of records to support the needs of the organization.
[ISO 30300:2011]	1.For future reference or for recovery purposes in case the original data is damaged or lost. 2.Find, manage, control, understand or preserve. 3.Authenticity, integrity, reliability and usability (from one hardware or software configuration to another, or from one generation of technology to another) 4.Systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities	Enduring value, as evidence	Business purpose
[ISO 30301: 2019]	1.Records which are reliable, authentic, have integrity and are useable. 2.Records which are reliable, secure, compliant, comprehensive and systematic.	1.Integral to any organization's activities, processes and systems. 2.Enable business efficiency, accountability, risk management and business continuity. 3.Enable organizations to capitalize on the	It addresses the development and implementation of a records policy and objectives and gives information on measuring and monitoring performance.

ISO standard	Attributes of trusted data	Characteristics	Enablers
		value of their information resources 4.Contribute to the preservation of collective memory, in response to the challenges of the global and digital environment	

Appendix B
Functional requirements for promoting trusted data from ISO/TC46/SC11 publications

ISO standard	Stakeholders	Process	Techniques	Tools
[ISO 15489-1:2016]	Organization; Individual	Creating and capturing records; Creating, receiving and maintaining; Creation, receipt, maintenance, use and disposition of records Storing records	Metadata	Records system; Access control; Monitoring; Agent validation; Authorized destruction; Information security; Business continuity
[ISO/TR 18128:2014]		Processes for capturing; maintenance procedures; migration; Security procedures; Processes to sustain the records' reliability and authenticity; Management procedures; Outsourcing, off-shoring, cloud arrangements , migrate, disposition or retention, regular monitoring	Security policy	Faced with the challenge of changing mentioned in page11/12/13(many clues here, need excavating)
[ISO 30300:2011]	A person, family or organisation, public or private	Records management; Transfer; Export; Aggregations; Migration; Created or received	1.Policy, procedures, people and other agents, and assigned responsibilities. 2.Principles of provenance, original order and collective control	Confirmed export of digital records and associated metadata
[ISO 30301: 2019]	1.Top management who make decisions regarding the establishment and implementation of management systems within their organization; 2.People responsible for implementation of a management system for	Creating records; Capturing records; Records classification and indexing; Storing records; Use and reuse; Migrating and converting records; Disposition		

records, such as professionals in the areas of risk management, auditing, records, information technology and information security.

Appendix C
Core concepts relating to trusted data from ISO standards

Key words	Definition1: [ISO 15489-1:2016]	Definition2: [ISO/TR 18128: 2014]	Definition3: [ISO 30300:2011]	Defintion4: [ISO 30301:2019]
Systematic	X	X	X	V
Authenticity	V	V	V	V
Reliability	V	V	V	V
Integration	V	X	V	V
Usability	V	X	V	V
Continuity	V	V	X	V
Security	V	V	X	V
Comprehensiveness	X	X	X	V
Evidence	X	X	V	X
Control	V	V	V	X
Capture	V	V	V	V
Creation	V	X	V	V
Classification	X	X	X	V
Reuse	X	X	X	V
Conversion	X	X	X	V
Disposition	V	V	V	V
Storage	V	X	X	V
Environment	X	V	X	V
Data quality	X	X	X	X
technology	X	X	V	V

Note:(V=Yes it has, X=No, it has not)