ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.3058 (09/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Future networks

Functional architecture for trust enabled service provisioning

ITU-T Y-SERIES RECOMMENDATIONS

Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
General	Y.100-Y.199
Services, applications and middleware	Y.200-Y.299
Network aspects	Y.300-Y.399
Interfaces and protocols	Y.400-Y.499
Numbering, addressing and naming	Y.500-Y.599
Operation, administration and maintenance	Y.600-Y.699
Security	Y.700-Y.799
Performances	Y.800-Y.899
INTERNET PROTOCOL ASPECTS	Y.1000-Y.1999
General	Y.1000-Y.1099
Services and applications	Y.1100-Y.1199
Architecture, access, network capabilities and resource management	Y.1200-Y.1299
Transport	Y.1300-Y.1399
Interworking	Y.1400-Y.1499
Quality of service and network performance	Y.1500-Y.1599
Signalling	Y.1600-Y.1699
Operation, administration and maintenance	Y.1700-Y.1799
Charging	Y.1800-Y.1899
IPTV over NGN	Y.1900-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
Frameworks and functional architecture models	Y.2000-Y.2099
Quality of Service and performance	Y.2100-Y.2199
Service aspects: Service capabilities and service architecture	Y.2200-Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250-Y.2299
Enhancements to NGN	Y.2300-Y.2399
Network management	Y.2400-Y.2499
Computing power networks	Y.2500-Y.2599
Packet-based Networks	Y.2600-Y.2699
Security	Y.2700-Y.2799
Generalized mobility	Y.2800-Y.2899
Carrier grade open environment	Y.2900-Y.2999
FUTURE NETWORKS	**Y.3000-Y.3499**
CLOUD COMPUTING	Y.3500-Y.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800-Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999
General	Y.4000-Y.4049
Definitions and terminologies	Y.4050-Y.4099
Requirements and use cases	Y.4100-Y.4249
Infrastructure, connectivity and networks	Y.4250-Y.4399
Frameworks, architectures and protocols	Y.4400-Y.4549
Services, applications, computation and data processing	Y.4550-Y.4699
Management, control and performance	Y.4700-Y.4799
Identification and security	Y.4800-Y.4899
Evaluation and assessment	Y.4900-Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3058

Functional architecture for trust enabled service provisioning

Summary

A trust enabled service is a reliable service which satisfies service and trust requirements by applying additional functions for trust provisioning capabilities to conventional information and communication technology (ICT) service entities (including resources, stakeholders and users), and that is able to develop a better quality of services and experience. In order to provide trust enabled features to existing ICT services, relevant architectures with key components are required. Therefore, Recommendation ITU-T Y.3058 provides a functional architecture for trust enabled service provisioning. It describes the concept and requirements and specifies related functional blocks, reference points and trust enabled service provisioning procedures between related functional blocks to support trust provisioning processes.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3058	2023-09-29	13	11.1002/1000/15637

Keywords

Functional architecture, trust, trust enabled service provisioning, trust provisioning.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

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 World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3058

Functional architecture for trust enabled service provisioning

1 Scope

This Recommendation provides a functional architecture for trust enabled service provisioning to specify detailed functions and their relationships. The scope of this Recommendation includes:

– Concept of trust enabled service provisioning;

– General and functional requirements for trust enabled service provisioning;

– Functional architecture that specifies the associated functional blocks and interfaces;

– Trust enabled service provisioning procedures that specifies the flows between related functional blocks.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3052] Recommendation ITU-T Y.3052 (2017), *Overview of trust provisioning for information and communication technology infrastructures and services*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 trust [ITU-T Y.3052]: The measurable belief and/or confidence which represents accumulated value from history and the expecting value for the future.

NOTE – Trust is quantitatively and/or qualitatively calculated and measured. Trust is used to evaluate values of entities, value-chains among multiple stakeholders, and human behaviours, including decision making.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 trust enabled service: A reliable service which satisfies service and trust requirements by applying additional functions for trust provisioning capabilities to conventional ICT service entities (including resources, stakeholders and users) and that is able to develop better quality of services and experience.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AC-FE Admission Control Functional Entity

API Application Programming Interface

DPF	Discovery and Provisioning Function
ICT	Information and Communication Technology
PII	Personal Identifiable Information
TA	Trust Agent
TAI-FE	Trust Agent Interface Functional Entity
TAMF	Trust Analysis and Management Function
TDC-FE	Trust Data Collection Functional Entity
TDFP-FE	Trust Data Filtering and Pre-processing Functional Entity
TDGI-FE	Trust Data Gathering Interface Functional Entity
TDR-FE	Trust Data Repository Functional Entity
TECM-FE	Trust Enabled Contract Management Functional Entity
TER-FE	Trust Enabled Recommendation Functional Entity
TLA	Trust Level Agreement
TMEF	Trust Modelling and Evaluation Function
TME-FE	Trust Metric Extraction Functional Entity
TM-FE	Trust Model Functional Entity
TRE-FE	Trust Reasoning and Evaluation Functional Entity
TRGF	Trust Repository and Gathering Function

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview

The concept of trust implies belief and confidence that the functional entities in information and communication technology (ICT) infrastructures and services will behave in expected ways. As ICT-based applications and services underpin other industrial domains and involve multiple stakeholders, trust evaluation of the corresponding value chains of business as well as of the system and component levels in a holistic manner can enable users to have confidence in their services and applications. Therefore, trust provisioning is one of the most important functional capabilities in ICT infrastructures and services [ITU-T Y.3052].

Trust provisioning in ICT infrastructures and services consists of a set of processes that include gathering data from entities and the producing trust information by evaluating all aspects of trust to support the decision-making of entities in establishing trust relationships with other entities [ITU-T Y.3052].

The ultimate goal for trust provisioning in ICT infrastructure is to develop a trust infrastructure that cooperates with ICT applications and services to assess and compute all aspects of trust among any entities in future ICT environments; in order to support these applications and services for better quality of services and experience. Therefore, the existing ICT applications and services need a way to provide trust provisioning processes to provide trustworthy ICT services.

A trust enabled service is a reliable service which satisfies service and trust requirements, by applying additional functions for trust provisioning capabilities to conventional ICT service entities (including resources, stakeholders and users), and that is able to develop better quality of services and experience. A trust enabled service is bidirectional and bilateral. This means that a trust relationship in telecommunications applications and environments works in both directions. For example, when an end device attempts to connect to a network for telecommunications services, the network can make an assessment of how much it trusts the end device and the end device can make an assessment of how much it trusts the network to which it is connecting. The end device, and the network, can assume the roles of both trustors and trustees [ITU-T Y.3052].

The trust provisioning process consists of data collection, data management, trust information analysis, trust information dissemination and trust information lifecycle management. Furthermore, in order to provide the trust service, trust components and platform architecture are described in clause 7.3 of [b-CG-Trust-TR]. Therefore, this Recommendation specifies functional architecture for trust enabled service provisioning, which includes related functional blocks, reference points and procedures to support trust provisioning processes.

Figure 1 shows the concept of trust enabled services, that includes trust enabled service provisioning flow based on relative functions by comparing with conventional services. The conventional services do not consider the trust information. An additional process is required to consider trust, a new value for ICT infrastructure and services.

A trust enabled service consists of trust-related data collection, trust analysis, trust provisioning and service provisioning phases through the trust provisioning functions that are developed based on the trust components in [b-CG-Trust-TR]. The trust provisioning functions consist of trust agent, trust analysis and management and trust enablement.

Trust Agents collect trust-related information needed for trust provisioning from each service domain. The collected information is sent to the trust analysis and management and applied to the trust model for trust analysis of the target. The trust model is bidirectional, adaptive to changes in the network or application and accounts for flexible trust and reputation calculations. It is possible for different services or applications to have different trust models. For example, the trust model for adding an IoT device to a broader network may be very different from the trust model that supports access to a specific platform (e.g., a video sharing service).

Trust enablement provides trust requirement analysis and trust attribute extraction, and requests trust information needed by trust analysis and management to satisfy the trust requirements of target service providers.

The requested trust analysis and management derives the target's trust index according to the trust requirements. The trust enablement provides the results of the trust consideration (i.e., trustworthy search or recommendation results) to the service provider. The service provider that acquires the target's trust index can provide service through trust-based decision-making.

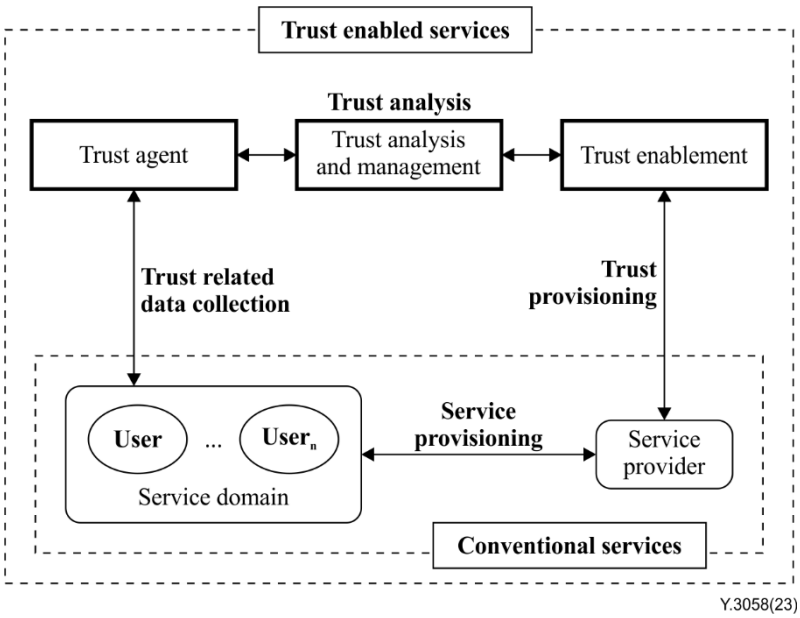

Figure 1 – The concept of trust enabled service provisioning

7 Requirements for trust enabled service provisioning

The requirements for trust enabled service provisioning are specified in clauses 7.1, 7.2, 7.3 and 7.4, respectively. Data collection for trust enabled service provisioning shall be subject to local, regional and national regulation that governs the security, privacy and confidentiality of data collected. Since the regulatory environment for data collection is not harmonized globally, there can be no global standard for data collection regarding trust enabled service provisioning.

In order to perform trust analysis and management, the trust enabled service requires a base of data on which to carry out trust evaluations. In the case of end devices connecting to networks, this base of data potentially combines information from a variety of sources – possibly greater in scope that traditional telecommunication metadata collected by conventional ICT services.

7.1 Requirements of trust-related data collection for trust enabled service provisioning

- It is required to collect trust-related data about resources and stakeholders from the target service domain as well as other service domains in which the resources and stakeholders are used and work.
- It is required to collect profile and status data of resources and stakeholders to manage resource availability.
- It is required that PII information is not requested and not stored.
- It is required to provide data filtering and/or pre-processing for refining trust data sets.
- It is required to provide transformation of heterogeneous data collected from different service domains.

7.2 Requirements of trust analysis for trust enabled service provisioning

- It is recommended to provide bidirectional relationship, meaning that any stakeholder may be in the role of trustor and/or trustee.
- It is required to process trust-related data representing different service domains, resources and stakeholders including their relationships. It is understood that it is possible to use multiple trust models depending on the service domain, application or stakeholder.

- It is required to process trust information taking into account different characteristics of trust attributes (e.g., subjectivity, dynamicity)

  NOTE – [b-CG-Trust-TR] and [ITU-T Y.3052] describe different characteristics of trust.
- It is recommended to reflect the changes of the network or application characteristics between service domains.
- It is required to follow various conformance of service domains to gain access for trust analysis and management.
- It is recommended to consider usage data of resources and stakeholders for trust analysis.
- It is recommended to provide scalability to include additional information required for trust analysis.
- It is required to provide trust evaluation by analysing data with different methods.
- It is recommended to provide trust quantization to calculate various trust information into a specific value (i.e., a real number).
- It is required to store trust calculations and intermediate trust processing information, for the use of future trust calculations.

7.3 Requirements of trust provisioning for trust enabled service provisioning

- It is required to accumulate trust value usage feedback from trustors and trustees to improve the trust value calculation in the future.
- It is required to provide trust requirement analysis and trust attribute extraction.
- It is required to provide a resource and service discovery based on trust requirement.
- It is recommended to provide a recommendation based on trust requirements for selecting a suitable resource and service.
- It is required to provide trust-based decision-making for selecting resources or stakeholders according to the result of trust-based discovery or recommendation.
- It is required to provide a contract management between trustor and trustee which updates contract terms and usage information.
- It is required to provide a usage control of target resources according to contract terms between trustors and trustees.
- It is required to provide permission control and admission control of target resources according to trust decision between trustors and trustees.

7.4 Security and resilience requirements for trust enabled service provisioning

- It is required to suspend the provision of resources to the user when the trust value of the service does not meet the users' requirements.
- It is recommended to create a list containing several services that meet the historical requirements and sort them according to the trust value.
- It is required to change another service for the user if the current service does not meet the trust requirement.
- It is recommended to evaluate each user's trust index if multiple users need to obtain a specific trust-based service resource at the same time.
- It is recommended to ask users whether or not they can wait if no suitable service can be provided at the current time.

8 Functional architecture

Based on the concept of ICT trust provisioning and the architectural framework and requirements of existing documents [b-CG-Trust-TR], [ITU-T Y.3052], [b-ITU-T Y.3054], a functional architecture for trust enabled service provisioning is presented in Figure 2.

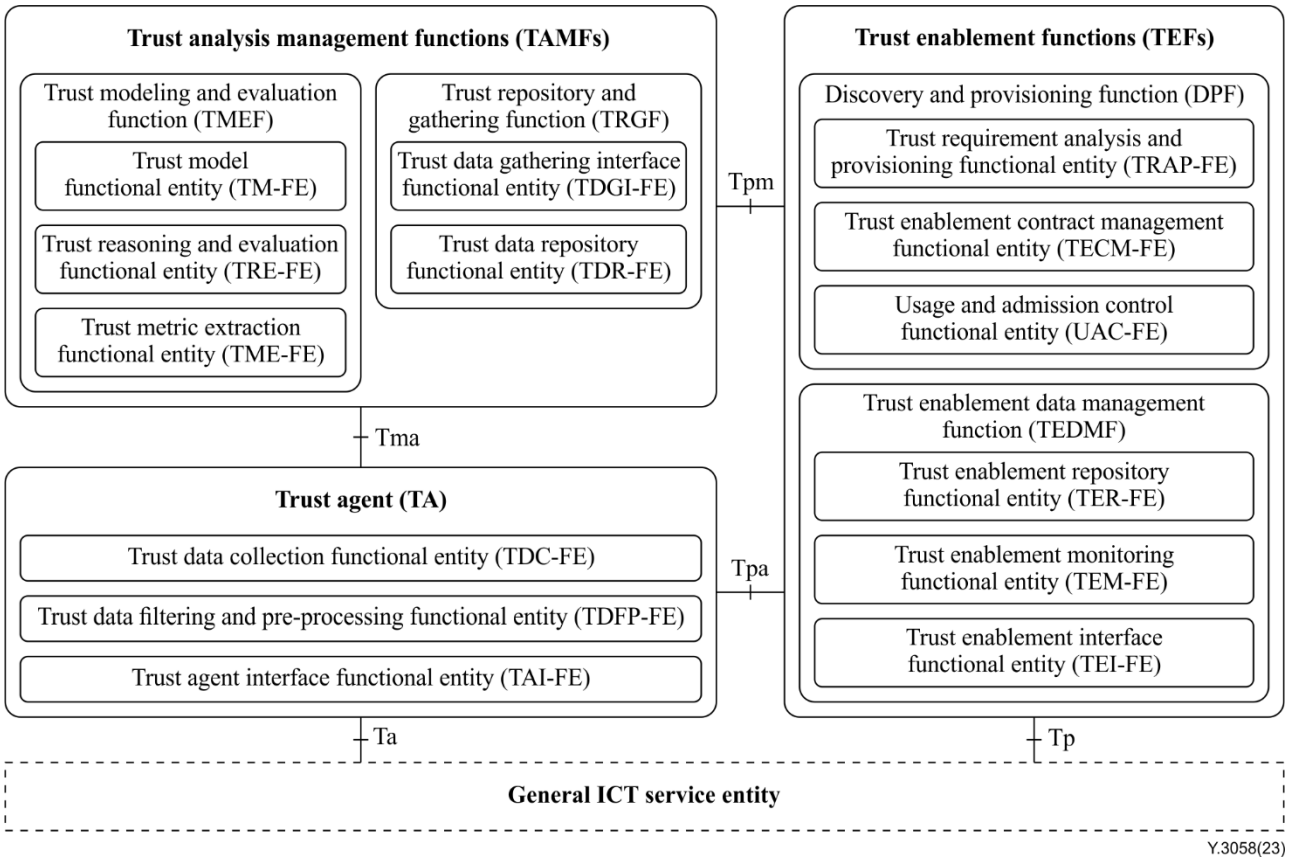

Figure 2 – Functional architecture of trust enabled service provisioning

8.1 Trust agent (TA)

TA is used to collect trust-related data from the general ICT service entity with trust agent interface, trust data collection, and trust data filtering and pre-processing.

- The trust agent interface functional entity (TAI-FE) provides connectivity to various types of objects to collect trust-related data. It also needs to connect to existing platforms and devices to extract the required data.
- The trust data collection functional entity (TDC-FE) is responsible for gathering the data required to evaluate a trust level of an object. It is also responsible for gathering the general and domain-specific data for evaluating a trust level of an object in a domain-specific perspective.
- The trust data filtering and pre-processing functional entity (TDFP-FE) is used to refine trust data sets without including other data that can be repetitive, irrelevant or even sensitive for trust evaluation.

8.2 Trust analysis and management functions (TAMFs)

TAMFs is used to model, reason and manage trust data collected from TAs to verify that objects meet certain trust criteria and to identify the required trust metrics for the object. TAMFs consists of trust modelling and evaluation function (TMEF) and trust repository and gathering function (TRGF).

– TMEF: This function provides trust analysis of the target entity, managing the trust-related data as a trust model, and extracts appropriate trust metrics for trust evaluation and reasoning. This function includes three functional entities as follows:
  - The trust model functional entity (TM-FE) is used to specify, annotate and build trust relationships between objects for the purpose of reasoning trust data. Trust modelling is social-cyber-physical and service domain-specific, and there are social, cyber and physical trust models to define a trust model for each domain in the ICT infrastructure.
  - The trust reasoning and evaluation functional entity (TRE-FE) is used to analyse and assess trust levels based on the trust model. There are various types of reasoning methods, depending on the service domains, and an appropriate reasoning method for the specific object.
  - The trust metric extraction functional entity (TME-FE) recognizes trust characteristics, considers for factors that influence trust and determines appropriate trust metrics for the trust modelling and reasoning.
– TRGF: This function manages the collected data as a repository. This function includes two functional entities as follows:
  - The trust data gathering interface functional entity (TDGI-FE) provides a connection with appropriate trust agents and trust enablement functions which is located in target service domains for gathering trust-related data regarding on an object's trust aspects.
  - The trust data repository functional entity (TDR-FE) manages the trust data including the operations of objects and the history of interactions among objects.

8.3 Trust enablement functions (TEFs)

TEFs are used for discovery and provisioning of trust resources and trust enabled service. TEFs also manage the repository for contract, usage and satisfaction data of trust enabled service and provide a brokering service to share and disseminate domain-specific trust knowledge across service domains. TEFs consist of a discovery and provisioning function (DPF) and a trust enablement data management function (TEDMF).

– DPF: This function provides a suitable trusted resource according to trust requirements. The DPF includes a trust requirement analysis and provisioning functional entity (TRAP-FE), a trust enablement contract management functional entity (TECM-FE) and a usage and admission control functional entity (UAC-FE).
  - The trust requirement analysis and provisioning functional entity (TRAP-FE) provides trust requirement analysis, trust-based discovery and recommendation. TRAP-FE analyses trust requirements form the service environment (e.g., user and service provider) and extract appropriate trust attributes for trust analysis. For trust-based discovery, TRAP-FE provides available lists of suitable resources or services which have the required level of trust. TRAP-FE provides a recommendation for selecting a suitable object that is similar to level of trust previously used.
  - The trust enablement contract management functional entity (TECM-FE) manages contracts between trust enabled service participants. The contract information is stored by the TEDMF.
  - The usage and admission control functional entity (UAC-FE) provides usage and admission control. Admission control manages trust enabled service users and existing service providers who access through the trust enablement interface functional entity (TEI-FE). Usage control grants permission to use an entity according to the TLA. The TLA defines the permitted operation, usage scope and usage time of a particular resource for an authorized user.

– TEDMF: This function stores and manages the trust contract, usage and satisfaction information through the trust enablement repository functional entity (TER-FE), the trust enablement monitoring functional entity (TEM-FE) and the trust enablement interface functional entity (TEI-FE).
  - The trust enablement repository functional entity (TER-FE) stores trust enablement data such as trust enablement contract information, usage information and satisfaction information. The trust enablement contract information contains the participant information and the target service information trust level agreement (TLA) that uses every target service resource. Usage information includes historical information such as creation time, access time and modification time, transaction type and a user who used the resource. The satisfaction information is a feedback data from trustors and trustees about service experience.
  - The trust enablement monitoring functional entity (TEM-FE) collects trust enablement contract, usage and satisfaction information and stores it at the trust enablement repository functional entity (TER-FE).
  - The trust enablement interface functional entity (TEI-FE) provides an application programming interface (API) between TEFs and general ICT service entities to operate TEFs. TEI-FE provides trust enablement information to TAMFs for subsequent trust evaluation of participants and trust enabled service. It also creates a trust link between authorized trust enabled service participants (trustor and trustee).

9 Reference point

9.1 Reference point Ta

The reference point Ta is located between the TA and the general ICT service entity. It allows the TA to collect general and trust-related data of trust enabled service entities (i.e., trustor and trustee) from the general ICT service entity.

The TA collects trust-related data and status data from the reference point Ta to monitor the status of entities.

The TA collects general and trust-related data from the reference point Ta to register a new entity.

9.2 Reference point Tp

The reference point Tp allows the communication between TEFs and the general ICT service entity. It allows the TEFs to receive the trust enabled service request from the user. Also, the TEFs can notify the result which includes the trust enabled service list and trust contract information.

The trust enabled service user sends the service request through the reference point Tp to TEFs for discovering the trust enabled service entity which satisfies certain trust criteria.

The TEFs can provide the response to the trust enabled service user by the reference point Tp. This response includes the trust enabled service list, trust contract information and usage information.

The trust enabled service user can notify the selecting result of the service list to TEFs by the reference point Tp to announce the beginning of the task.

The trust enabled service user can report the completion of the task with satisfaction data about the selected service or resource to TEFs through the reference point Tp to update usage and trust information.

9.3 Reference point Tma

The reference point Tma allows the TAMFs to receive data collected by the TA.

The TA constantly monitors the status of the trust enabled service entity and sends the collected information to the TAMFs to update the trust model and evaluate the trust of the target entity.

When a trust evaluation result of a particular target entity is required, the TA can obtain the evaluation result from the TAMFs though the reference point Tma.

9.4 Reference point Tpm

Tpm is a reference point which enables the communication between TAMFs and TEFs.

TEFs send trust-related data to TAMFs through reference point Tpm to create trust model (i.e., specify, annotate and establish trust relationship) and evaluate the trust level of newly registered entity.

TEFs can receive the trust evaluation result from TAMFs by reference point Tpm for entity discovery and recommendation.

According to the status of the entity, TEFs send renewed trust-related data to TAMFs through reference point Tpm which includes usage information for updating the trust model.

9.5 Reference point Tpa

Tpa is a reference point which enables the communication between TA and TEFs.

TEFs receives trust-related and profile data from TA through reference point Tpa to register a new entity.

TECM-FE of TEFs creates a trust contract and usage model for the newly registered entity.

10 Procedures

This clause provides procedures for trust enabled service provisioning between functional blocks. It includes registration, request, monitoring, discovery and recommendation of the trust enable entity.

10.1 Trust enabled entity registration procedure

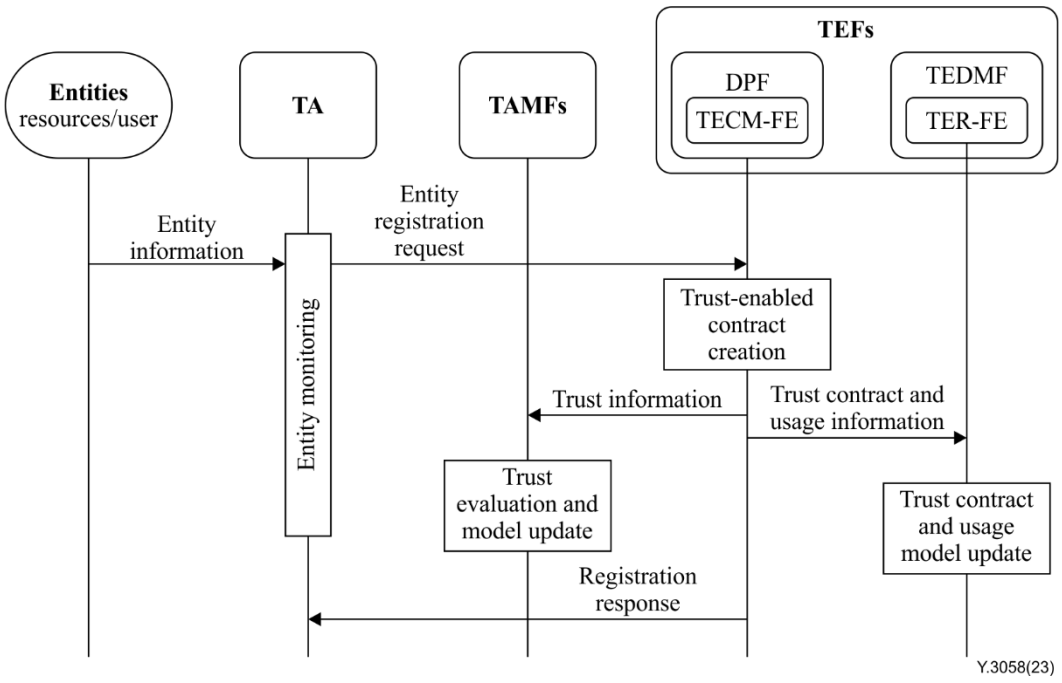

Figure 3 – Trust enabled entity registration procedure

All entities must first be registered for trust enabled service provisioning. As shown in Figure 3, the trust enabled entity registration procedures are described below:

1) When the TA discovers new entity through the entity monitoring, the TA sends the entity registration request to the TECM-FE of the TEFs. This request contains general and trust-related data about a new entity which is aggregated by TA.

2) TECM-FE creates a trust contract which describes a scope of authority such as ownership, permitted operation, permitted time, usage history and permitted target.

3) TECM-FE sends trust-related data to TAMFs for trust model update and trust evaluation about the newly registered entity.

4) TECM-FE sends usage data to TER-FE for trust contract and usage model update for the newly registered entity.

5) When the registration is completed, the TECM-FE sends the registration response to notify the registration result to TA.

10.2 Trust enabled entity request and monitoring procedure

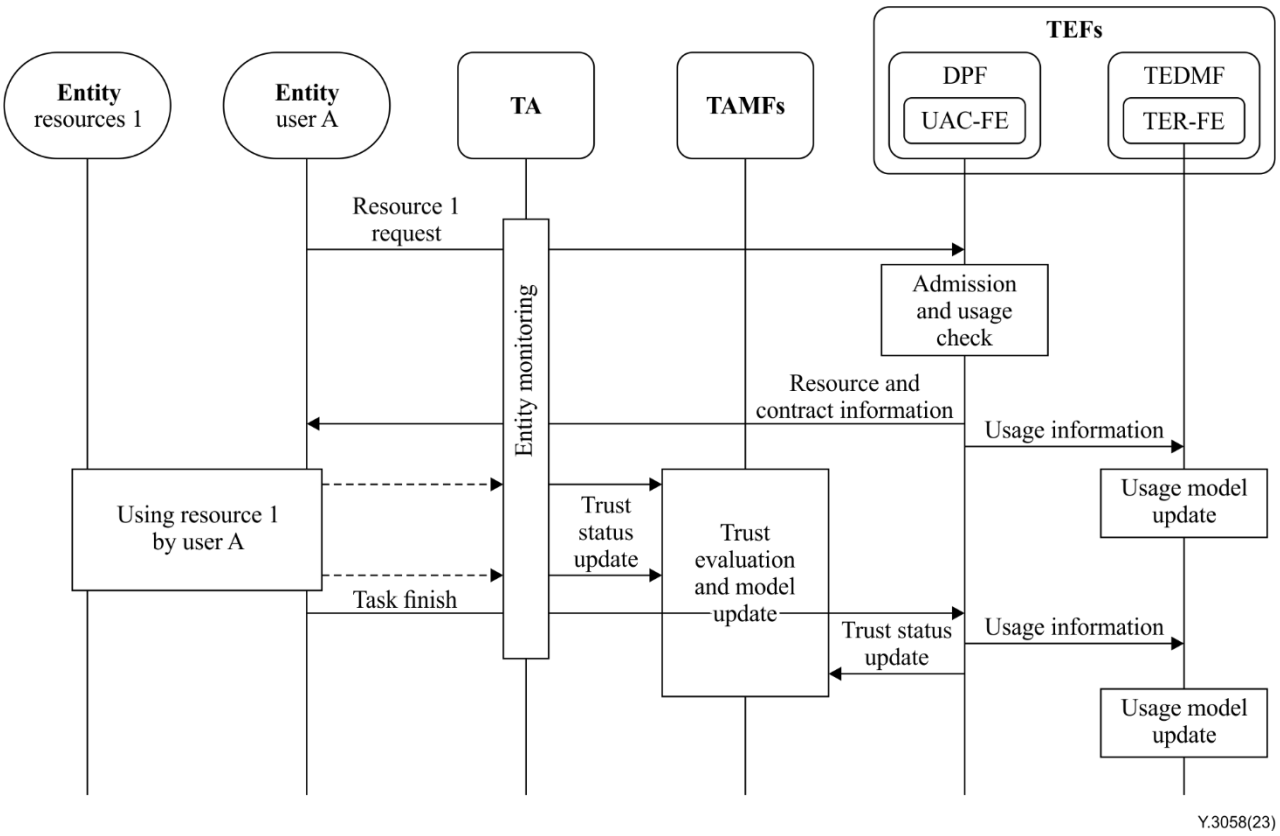

Figure 4 – Trust enabled entity request and monitoring procedure

In order to use a particular entity, the status and trust level of the target must be updated when the status of the entity is changed. As shown in Figure 4, the trust enabled entity request and monitoring procedures are as follows:

1) To provide entity monitoring, TA constantly monitors the status of entities in its scope.

2) User A sends a request message to UAC-FE of TEFs to use specific entity (Resource 1).

3) UAC-FE of TEFs checks the permission and usage of the requested entity.

4) If User A is allowed, UAC-FE sends the resource and contract information to User A. It includes the access point and usage profile of the requested resource. User A then starts a task with Resource 1.

5) UAC-FE sends usage information about Resource A to the TER-FE to update the usage model.

6) If the state of an entity (Resource 1) has changed, the TA sends the trust status update message to the TAMFs for trust evaluation and trust model update.

7) When the task is completed, User A notifies the completion of the task with satisfaction data about the entity (Resource 1) to UAC-FE. And the UAC-FE updates the usage model again.

8) The UAC-FE sends the satisfaction data to the TAMFs for trust evaluation and trust model update about this task.

10.3 Trust enabled entity discovery procedure

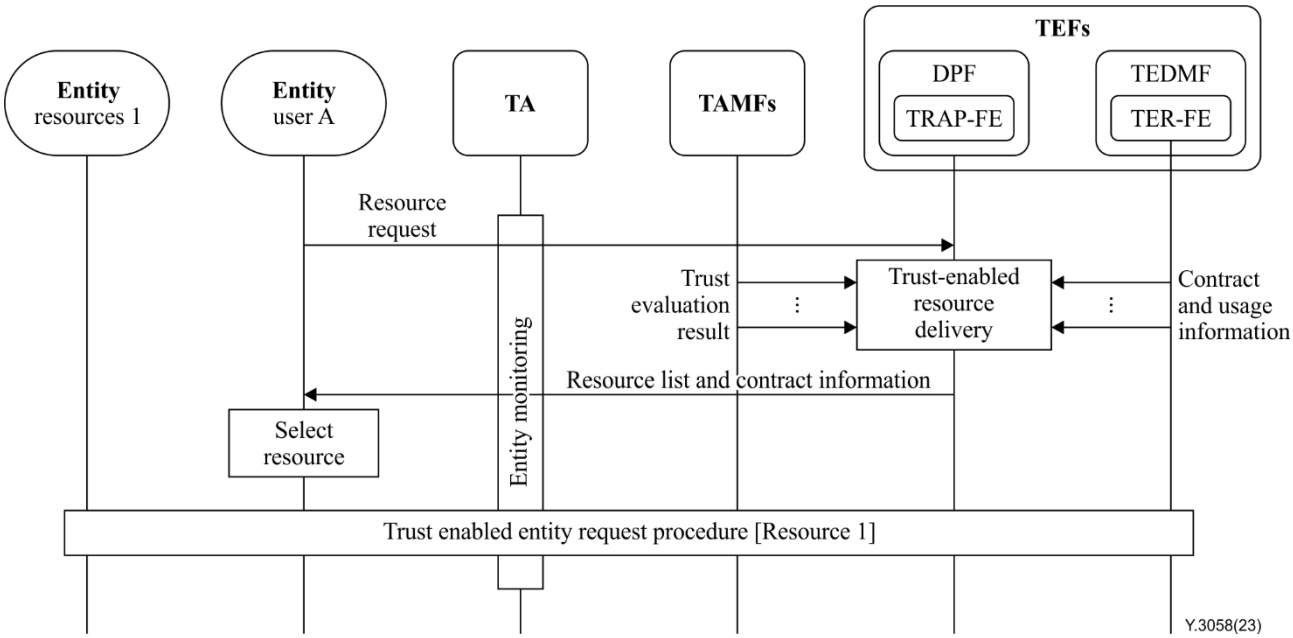

Figure 5 – Trust enabled entity discovery procedure

Users can request a search to use entities that meet their target trust profile. As shown in Figure 5, the trust enabled entity discovery procedures are as follows:

1) User A sends a request message to TRAP-FE of TEFs to search for entities that satisfy their target trust profile. The trust profile describes requirements such as entity type, trust level and scope of use.

2) TRAP-FE aggregates trust evaluation information from TAMFs and trust contract and usage information from TER-FE about relevant entities. Based on the aggregated trust-related information, TRAP-FE sends a list of entities which meet the required trust profile.

3) User A selects an entity from the list and the trust enabled entity request procedure which is described in clause 10.2 is performed.

10.4 Trust enabled entity recommendation procedure

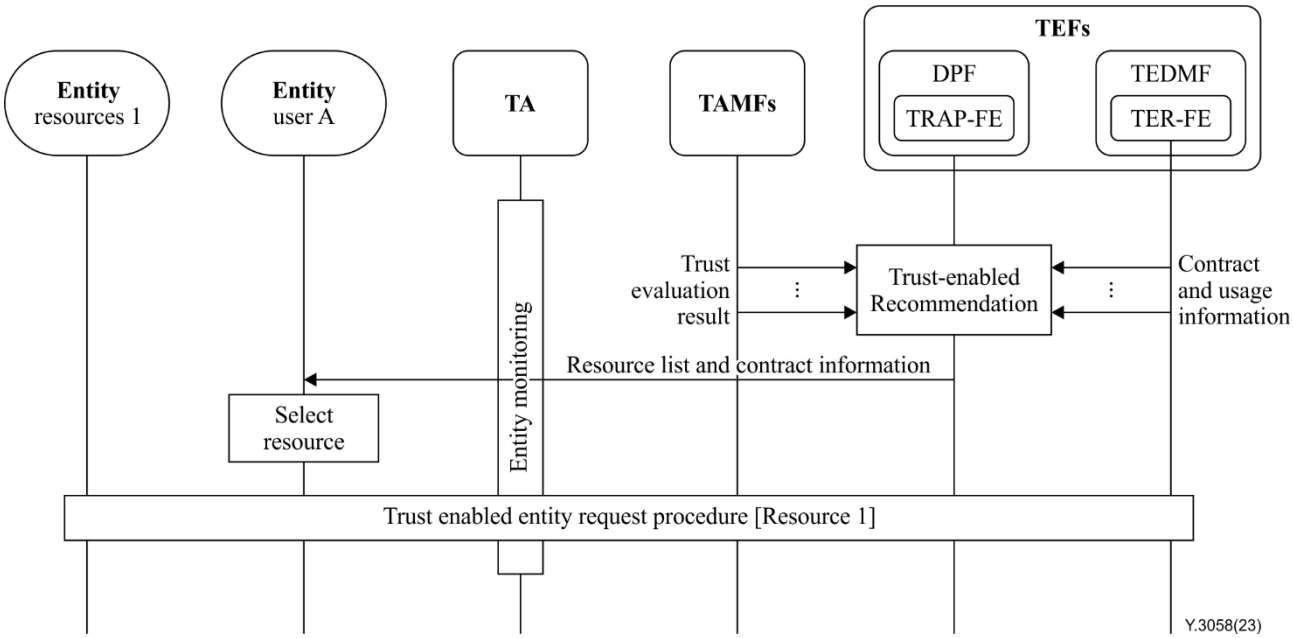

Figure 6 – Trust enabled entity recommendation procedure

TEFs can recommend an entity (resource or service) that meets a particular user's requirement. For this purpose, TRAP-FE collects data of historical requirements (e.g., previously used or requested information by the user) to entity recommendation. As shown in Figure 6, the trust enabled entity recommendation procedures are described below:

1) For entity recommendation, TRAP-FE continuously aggregates trust contract and usage information and their trust level information.

2) Based on the aggregated trust-related information, TRAP-FE makes a recommendation list of entities which satisfy the historical requirements and TRAP-FE sends the recommendation list to the target user.

3) User A selects an entity from the recommendation list and the trust enabled entity request procedure which is described in clause 10.2 is performed.

11 Security considerations

To support a reliable service that satisfies trust requirements, a secure environment should be provided for interacting with service entities (including resources, stakeholders and users) for trust provisioning. In addition, the privacy of user data should be ensured, because there is a possibility that privacy-sensitive data may be collected and used to analyse the trust of the service entity. It is required that PII information is not requested and not stored.

Appendix I

Comparison of trust provisioning relative functions

(This appendix does not form an integral part of this Recommendation.)

This appendix provides a comparison table (Table I.1) of trust provisioning relative functions which are defined in relevant Recommendations and draft Recommendations. The functions located in the same row are classified as the same category.

Table I.1 – Comparison of trust provisioning related functions

TR, trust provisioning		**ITU-T Y.3053 (Trustworthy networking) [b-ITU-T Y.3053]**	**ITU-T Y.3054 (Trust-based media service) [b-ITU-T Y.3054]**	**ITU-T Y.3055（Trust-based personal data management) [b-ITU-T Y.3055]**	**Trust-arch**	
TA (trust agent)	TA interface		Trust data adapters		TA (arust agent)	TA interface
	Trust data collection	Trust verification support FE	Trust relevant media data collector, trust relevant external data collector			Trust data collection
	Trust data filtering and pre-processing		Trust data filter and preprocessor			Trust data filtering and pre-processing
TAMP (Trust Analysis and Management Platform)	Trust models		Trust models	Trust modelling function	TAMFs (Trust analysis and management functions)	Trust models
	Trust reasoner and evaluator	Trust level validation FE	Trust reasoner, trust attributers' evaluator	Trust information analysis function		Trust reasoning and evaluation
	Data analytics					
	Cloud computing					
	Trust metric extractor		Trust metric extractor, Trust index analysis engine, trust indicators identification			Trust metric extraction
	Trust knowledge gathering Interface		Trust data gathering interface	Trust attributes monitoring function		Trust data gathering interface
	Trust data repository		Trust data repository			Trust data repository
		Trust information lifecycle management FE	Trust information OAM	Trust information lifecycle management function	TEFs (Trust enablement functions)	Usage and admission control
TSE (Trust service enabler)	Trust linker		Trust linking			
	Trust idM	ID-locator mapping support FE	Trust idM			
	Trust-based recommendation					

Table I.1 – Comparison of trust provisioning related functions

TR, trust provisioning		ITU-T Y.3053 (Trustworthy networking) [b-ITU-T Y.3053]	ITU-T Y.3054 (Trust-based media service) [b-ITU-T Y.3054]	ITU-T Y.3055 (Trust-based personal data management) [b-ITU-T Y.3055]	Trust-arch	
			Trust APIs			Trust enablement interface
TSB (Trust service broker)						Trust requirement analysis and provisioning
						Trust enablement contract management
						Trust enablement repository
						Trust enablement monitoring
Domain-specific optional functions		Domain membership management FE, domain policy management FE, accessing / peering control support FE, data transport and processing FE, ID-based routeing support FE	Trust-based content access controller, trust-based content assistant, Trust privacy handler	Privacy compliance management functions, personal data evaluation functions, personal data transaction management functions		

Bibliography

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

[b-ITU-T Y.3054] Recommendation ITU-T Y.3054 (2018), *Framework for trust-based media services.*

[b-ITU-T Y.3055] Recommendation ITU-T Y.3055 (2020), *Framework for trust-based personal data management.*

[b-CG-Trust-TR] Technical Report CG-Trust (2016), *Trust provisioning for future ICT infrastructures and services*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023