International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3054

(05/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Future networks

Framework for trust-based media services

Recommendation ITU-T Y.3054

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
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	
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	
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
Network control architectures and protocols	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.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
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.3054

Framework for trust-based media services

Summary

Content is produced, shared, exchanged and consumed through various media services. However, media services are associated with many inherent risks. In order to minimize unexpected risks and to maximize the survivability of media services, trust can be used to evaluate and verify that entities involved in media services are working in expected ways. Trust-based media services aim to restrain untrustworthy users from behaving maliciously, as well as being robust to unexpected executions and failures with a certain level of predictability and reliability.

Thus, Recommendation ITU-T Y.3054 provides a framework for trust-based media services. Recommendation ITU-T Y.3054 identifies inherent risks in existing media services and describes the necessity for trust-based media services. After identifying functional requirements, the Recommendation describes components and a functional architecture for trust-based media services. Finally, trust-based content consumption and sharing services are introduced along with a trust analysis mechanism for trust-based media services.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3054	2018-05-29	13	11.1002/1000/13609

Keywords

Functional architecture, media service, requirements, trust.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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 received notice of intellectual property, protected by patents, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3054

Framework for trust-based media services

1 Scope

In order to minimize unexpected risks and to maximize the survivability of media services, trust can be used to evaluate and verify that entities involved in media services are working in expected ways. Trust-based media services aim to restrain untrustworthy users from behaving maliciously, as well as being robust to unexpected executions and failures with a certain level of predictability and reliability. Thus, this Recommendation provides a framework for trust-based media services. The scope of this Recommendation includes:

– identifying risks of media services and the necessity of trust-based media services;

– functional requirements for trust-based media services;

– components and a functional architecture for trust-based media services;

– trust analysis mechanism, trust-based content consumption and sharing services.

Detailed use cases for trust-based media services are described in Appendix I and calculating trust index is described in Appendix II.

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 terms defined elsewhere:

3.1.1 trust [ITU-T Y.3052]: The measureable 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.

3.1.2 content [b-ITU-T H.780]: A combination of audio, still image, graphic, video, or data.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 media service: A service providing the electronic communication tools that are used to store, aggregate, share, discuss and deliver various types of content.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

ID Identifier

idM identification Manager

OAM Operations, Administration and Management

PID Pseudo-Identity

SNS Social Networking Service

TA Trust Agent

TIMS Trust Information Management System

TSE Trust Service Enabler

UI User Interface

URL Uniform Resource Locator

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 of trust-based media services

6.1 Risks in media services

Media services store, aggregate, share, discuss and deliver various types of content. Recently, the volume of content has been enormously increasing and users participate in multiple media services (e.g., mail, contents delivery services or social networking services (SNSs)). Basically, the media service environment consists of four major entities (i.e., the media service itself, content, sender and receiver) as shown in Figure 6-1.

When a sender and a receiver have content use interactions on the media service, there are various inherent risks associated with each entity.

– Risks of media service: malicious attack, device infection, etc.

– Risks of content: leakage of sensitive content, unidentified content, infected content, manipulated content address, etc.

– Risks of users (i.e., sender and receiver): privacy leakage, unintended redistribution, reproduction of content, malicious comments on contents, other malicious behaviour by the user, etc.

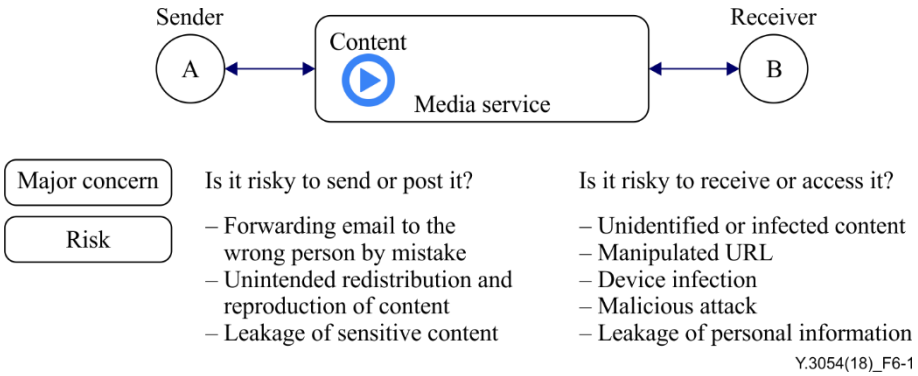

Figure 6-1 – Inherent risks in media services

Since these inherent risks cause various problems, mitigating them is one of the most urgent and significant challenges in the media services environment. However, it is hard to mitigate risks of a sender and a receiver when they have content interactions (e.g., using text, images, short clips, movies and advertisements) on the media service because they do not have enough information about each other.

Although those risks significantly threaten the media service environment, conventional media service providers have not addressed these problems adequately. While several feasible solutions can mitigate the risks, current approaches are limited. A new approach is to apply the concept of trust defined in [ITU-T Y.3052] to minimize risks to media services.

6.2 Necessity for trust-based media services

Although it is critical for media service providers to build a reliable and secure content usage environment, to date they rely on limited capabilities providing rating information and comments on content. However, these capabilities are insufficient to identify potential risks due to inadequate measurements and analysis.

To overcome those limitations, this Recommendation describes trust-based media services that evaluate and utilize trust by modelling, collecting and analysing user data from multiple services. Figure 6-2 presents a conceptual approach to trust-based media services.

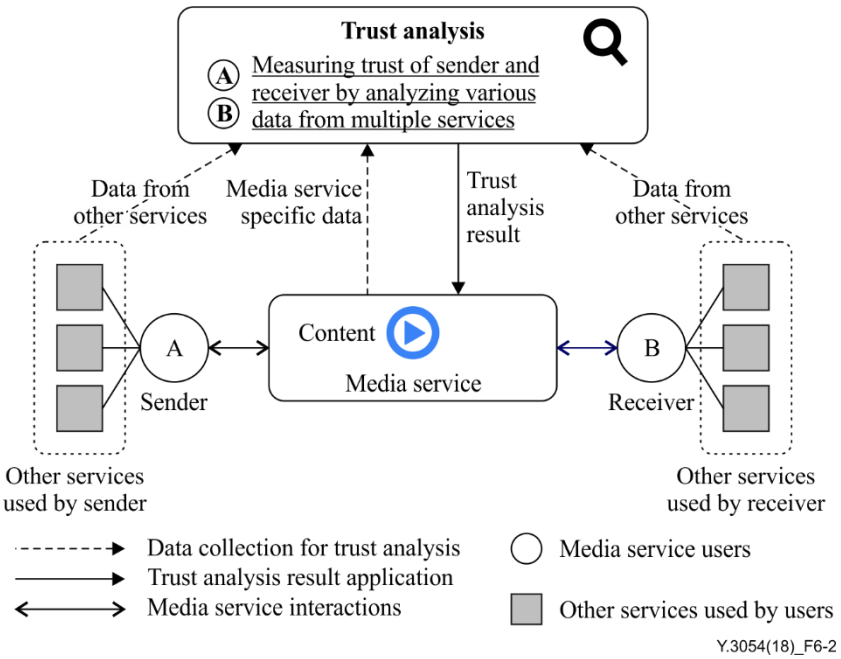

Figure 6-2 – A conceptual approach to trust-based media services

7 Requirements for trust-based media services

This clause identifies functional requirements for trust-related capabilities in order to support trust-based media services.

7.1 Requirements for trust data collection

– Collecting data in multiple services: Collection of internal data (e.g., media usage) from the media service as well as external data (e.g., social activities) from various services (i.e., SNS, etc.) is required.

– Pre-processing of collected data: It is recommended that the collected data be refined and filtered for pre-processing.

– Transferring collected data: Transfer of collected data into components for analysing trust in secured ways is required.

7.2 Requirements for trust analysis

– Trust evaluation: Evaluation of trust by analysing data by various methods is required.

– Quantization of trust: For trust-based media services, calculation of a specific value from various trust information sources (i.e., a real number) is required.

– Analysis of heterogeneous data: Processing and analysis of heterogeneous data, because the data collected varies in properties, is required.

– Data repository: It is recommended that trust information be stored in a repository to keep track of trust over time.

– Interface for trust information: Provision of an interface (i.e., an application programming interface (API), etc.) between service or application and trust information analysis entities to exchange trust information is required.

– Maintenance of trust-relevant information: Monitoring and modification of trust information seamlessly, because trust information is valid only for a specific time period and can change as time goes on, is required.

7.3 Requirements for applying trust to trust-based media services

– Applying analysed trust to content: The granting by a media service provider to users of appropriate rights of access, downloading and reacting to content in accordance with trust is required.

– Dynamic authentication: A media service provider is required to apply dynamic authentication based on evaluated trust, which varies with time.

– Initiating media usage right: It is recommended that initial trust be granted for media content usage rights to a new user by a media service provider.

7.4 Requirements for operating and managing trust-based media services

– Identifier (ID) management: Trust-based media services are required to issue and manage unique IDs to identify users and respond to requests for trust.

– Operations, administration and management (OAM) of trust information: A service provider is required to operate and maintain entities and related information involved in trust-based media services.

– User-friendly user interface (UI): Support of a user-friendly UI efficiently to handle complicated interactions between users and services can be optionally needed.

8 Architectures for trust-based media services

In order to provide trust-based media services, a legacy media service provider needs to be connected to a trust information management platform consisting of: 1) a trust information management system (TIMS); 2) a trust agent (TA); and 3) a trust service enabler (TSE). Trust-relevant functionalities can be added to traditional media services by connecting the media service to a trust information management platform. Figure 8-1 illustrates the components of trust-based media services.

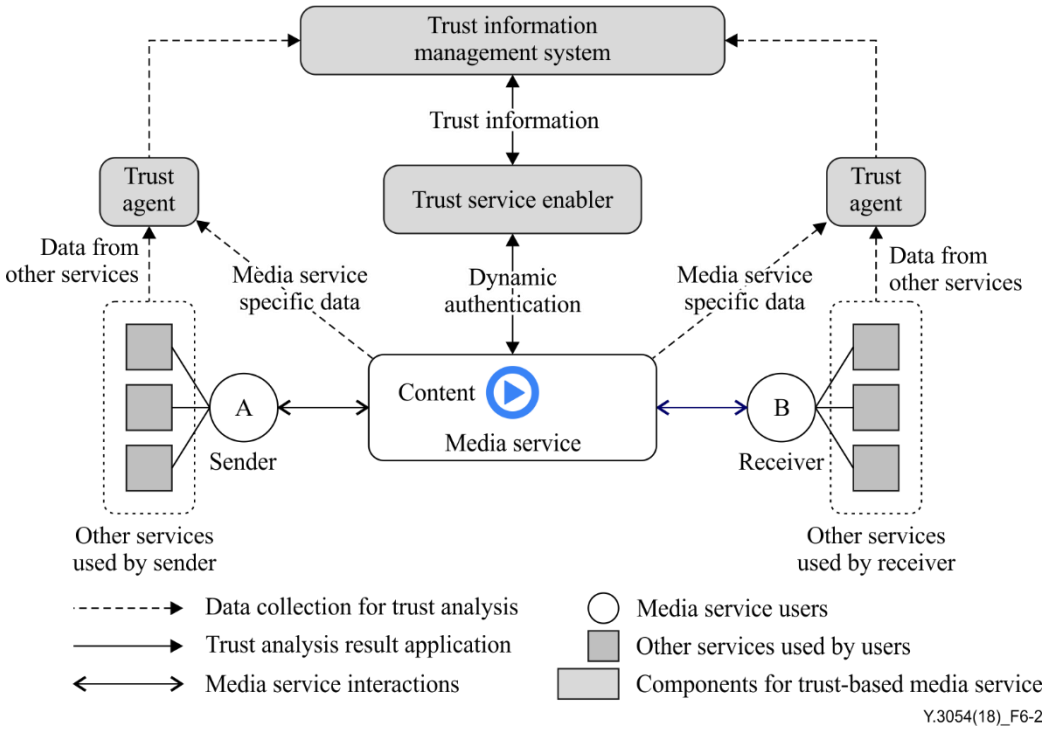

Figure 8-1 – Components of trust-based media services

– A **TIMS** is responsible for modelling and evaluating trust by collecting data from TAs. Based on analysis of heterogeneous data from TAs, a TIMS measures trust and represents it as an explicit value.

  NOTE – A TIMS can utilize multiple trust analysis methodologies, e.g., calculation, machine learning and natural language processing. A media service provider can select the most appropriate analysis method for its purpose.

– **TAs** collect various internal and external data from the media service itself and other services. Because users use multiple services, it is beneficial to gain abundant data to analyse user trust accurately. For efficient trust analysis, TAs conduct pre-treatment processing of data, and then deliver the data into a TIMS in a secure way.

– A **TSE** provides trust-adapting capabilities to media servers. A TSE also provides various APIs for TAs and TIMS to call functions. In this manner, legacy media service providers request a TIMS to analyse trust through a TSE.

A functional architecture for trust-based media services is presented in Figure 8-2. Each component of a TA, TIMS and TSE provides functional modules aligning with specified requirements. This architecture is developed by referring to [b-CG-Trust-TR].

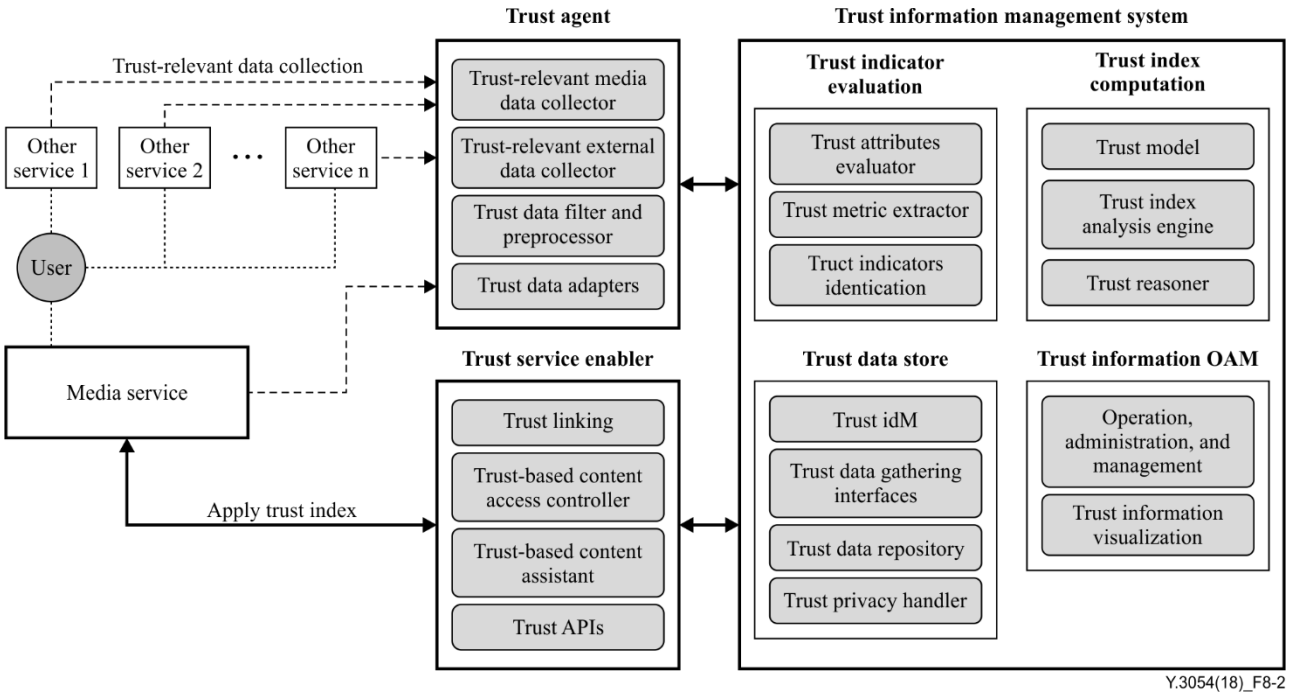

Figure 8-2 – Functional architecture of trust-based media services

8.1 Trust agent

A TA is responsible for collecting trust-related data from multiple services by the following modules.

– **Trust-relevant media data collector**: This is responsible for gathering media specific data required for measuring trust attributes from the media service.

– **Trust-relevant external data collector**: This is responsible for gathering external data from other services for measuring trust attributes.

– **Trust data filtering and pre-processor**: This is used to refine trust data sets without including other data that can be repetitive, irrelevant or even sensitive for trust evaluation.

– **Trust data adapter**: This is responsible for linking collected data to a TIMS, as an internal interface. It conducts a data synchronization process to establish consistency among data flowing from a TA toward a TIMS.

NOTE – Because raw data from various services have different data characteristics, a trust data adapter adjusts collected data for a TIMS.

8.2 Trust information and management system

A TIMS consists of four components of trust indicator evaluation, trust data store, trust index computation and trust information OAM. Each component consists of different modules to satisfy functional requirements.

1) Trust indicator evaluation

– **Trust attributes evaluator**: This is used to evaluate trust attributes defined in a trust model.

NOTE 1 – Trust attributes are used as gradients to generate trust indicators, such as ability, benevolence and integrity (Refer to [ITU-T Y.3052]).

– **Trust metric extractor**: It recognizes trust characteristics, accounts for factors influencing trust and determines proper trust metrics for the trust modelling and reasoning by analysing the metadata or semantic ontologies.

– **Trust indicators identification**: This is used for identifying trust indicators by referring to trust metric extractor.

2) Trust data store

– **Trust identification manager (idM)**: This is used to protect and identify users. It generates a pseudo-identity (PID) for each user and identifies the PID when identification is required to collect and analyse trust data by collaborating with a trust privacy handler.

– **Trust data gathering interface**: This is used to interact with a trust data adapter by transforming data collected from a trust data adapter into a trust data repository.

– **Trust data repository**: This is responsible for storing raw data and analysed trust value.

– **Trust privacy handler**: This is used to encrypt and decrypt user data to protect private data stored in a trust data repository at the request of an idM.

NOTE 2 – To evaluate trust, the necessary data is loaded from this repository and is transferred to a trust indicator evaluation module.

3) Trust index computation

– **Trust model**: This is used to specify, annotate and build trust relationships between users for the purpose of calculating trust data.

– **Trust index analysis engine**: This is used to calculate a trust index and set rules based on a trust model. It cooperates and communicates with the trust data repository.

– **Trust reasoner**: This is used to infer a level of trust by means of a trust index based on a trust model.

NOTE 3 – Because a trust index can change with time and circumstantial context, a trust reasoning method must be able to handle such dynamics of trust. Trust computation happens when the state of a user is changed or an interaction occurs between users.

4) Trust information OAM

– **Operations, administration and management**: This is used to operate, administer and manage TIMS for both media service providers and trust information providers.

– **Trust information visualization**: This is used to visualize trust information on a UI to correspond to various requests from media services.

8.3 Trust service enabler

A TSE is responsible for granting a user appropriate rights to content depending on the trust evaluated. A TSE directly controls a user's rights to accessing, sharing, protecting and reacting rights on specific content.

– **Trust linking**: This is a module capable of identifying an encrypted ID in collaboration with a trust idM.

– **Trust-based content access controller**: This is used to grant a user appropriate rights to content in accordance with a combination of information about the content creator's rules, the service provider's trust policies and an evaluated trust index.

– **Trust-based content assistant**: This is used to attach a trustworthy tag to content and to display trust information about content.

– **Trust APIs**: This is used to respond to various requests from media service providers and users. APIs allow service operators to utilize trust information for specific purposes.

9 Trust analysis and service provisioning for trust-based media services

9.1 Trust analysis mechanism for trust-based media services

While trustworthiness and trust have been treated as subjective concepts, trust-based media services utilize objectified trust, which is determined by a set of trust indicators computed by collected data, as described in [ITU-T Y.3052].

Figure 9-1 shows the objectified trust evaluation and utilization process. When users make a decision (e.g., user A – sending content; user B – clicking a uniform resource locator (URL)) about content in a media service, a trust-based media service grants a user (trustee) appropriate rights (access, distribution, reaction and tagging) to content with a trustee's objectified trust (user A). Simultaneously, a trustor can refer to the objectified trust to make a decision.

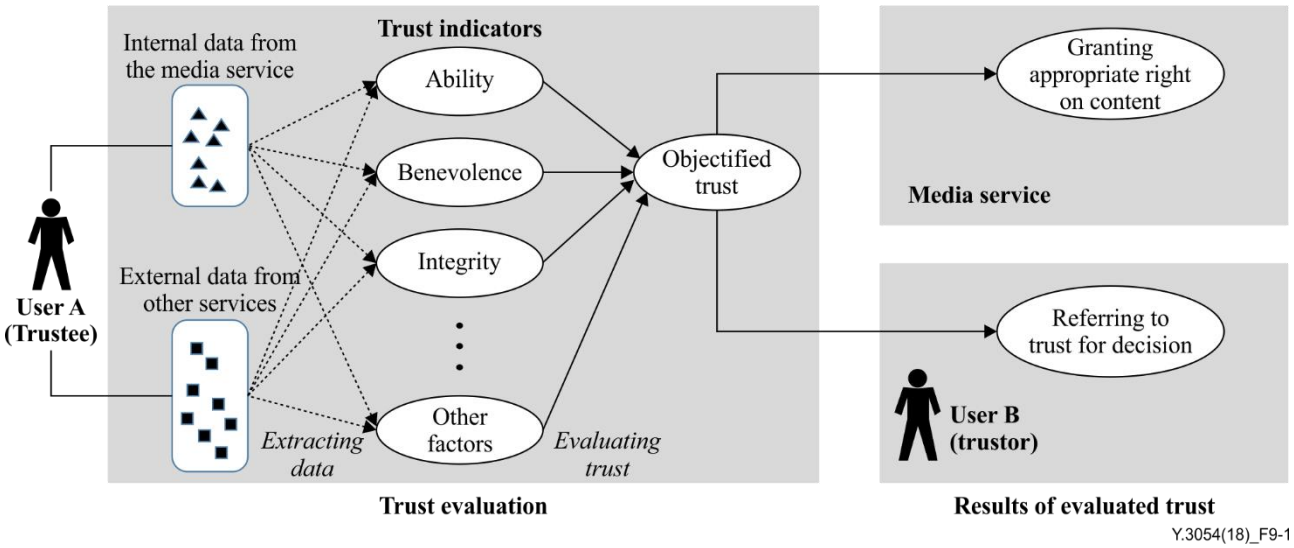

Figure 9-1 – Objectified trust evaluation and utilization process

NOTE – A detailed explanation of the trust computation process is given in Appendix II.

9.2 Service provisioning for trust-based media services

In general, there are two types of media services – closed and open.

– Closed media service: a content creator (sender) specifies receivers (e.g., email). After receiving permission to enter a closed media service, there are relatively low restrictions on content usage rights. Thus, potential risks exist in a closed media service.

– Open media service: content is open to anyone in an open media service (e.g., a blog). Because content in an open media service is not restricted, content involves some level of risk.

9.2.1 Trust-based content consumption service

The service covers a closed media service. For a content sender (trustor), the rights of a receiver (trustee) to content can be adjusted by trust as follows.

– **Access right**: Even though a content creator (trustor) sends content to multiple users (trustees), only trustworthy receivers can access the content. If the content is forwarded to another user (trustee) regardless of the sender's intention, only trustworthy users can access the content based on the trust of the original sender (trustor) towards the forwarded user.

For a content receiver (trustor), the right of a sender (trustee) to content can be adjusted by trust as follows.

– **Trustworthy tag**: The service automatically provides trust information by attaching a "trustworthy" tag to the content representing the level of trust in the sender (trustee). Before accessing content, a receiver can refer to trust information.

– **Distribution right**: The content distribution right of an untrustworthy sender is restricted when an untrustworthy sender distributes content continuously.

9.2.2 Trust-based content-sharing service

The service covers an open media service. For a content creator (trustor), the rights of a content consumer (trustee) to content can be adjusted by trust as follows:

– **Reaction right**: Content reaction rights depend on evaluated trust. An untrustworthy consumer (trustee) can neither add and reply to comments nor redistribute the content. However, trust does not influence the access right to the content. Even untrustworthy consumers can access the content on an open media service.

For a content consumer (trustor), the rights of a content creator (trustee) to content can be adjusted by trust as follows:

– **Trustworthy tag**: The service automatically provides trust information by attaching a "trustworthy" tag to content representing the level of trust in the sender (trustee). By referring to this information, users can access content selectively.

– **Distribution right**: The content distribution right of an untrustworthy content creator is restricted when that creator tries to share content continuously.

NOTE – Detailed use cases of services are described in Appendix I.

10 Security considerations

Trust-based media services aim to restrain untrustworthy users from behaving maliciously, as well as being robust to unexpected executions and failures with a certain level of predictability and reliability. To satisfy trust for media services, the media service provider should deliver security for building, managing and operating trust-based media services. Detailed security requirements and mechanisms can be based on [b-ITU-T Y.2701] and [b-ITU-T X.509]. In addition, privacy protection for user data should be guaranteed because trust-based media services collect and utilize privacy-sensitive data to analyse trust.

Appendix I

Use cases of trust-based media services

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

I.1 Trust-based content consumption services

I.1.1 Motivation

As content sharing has emerged as a popular application; users can easily share content with others. However, the increasing number of untrustworthy users reduces the credibility of shared content. Also, malicious users can distribute original content (e.g., private photos, videos or documents) without the permission of creators, and it sometimes causes problems. Utilizing trusted information is an effective solution to problems, by protecting content from being recklessly distributed and abused.

I.1.2 Overview

Figure I.1 is an overview of trust-based content consumption services. As a TIMS is a cloud computing service, it can be easily applied to various existing media services.

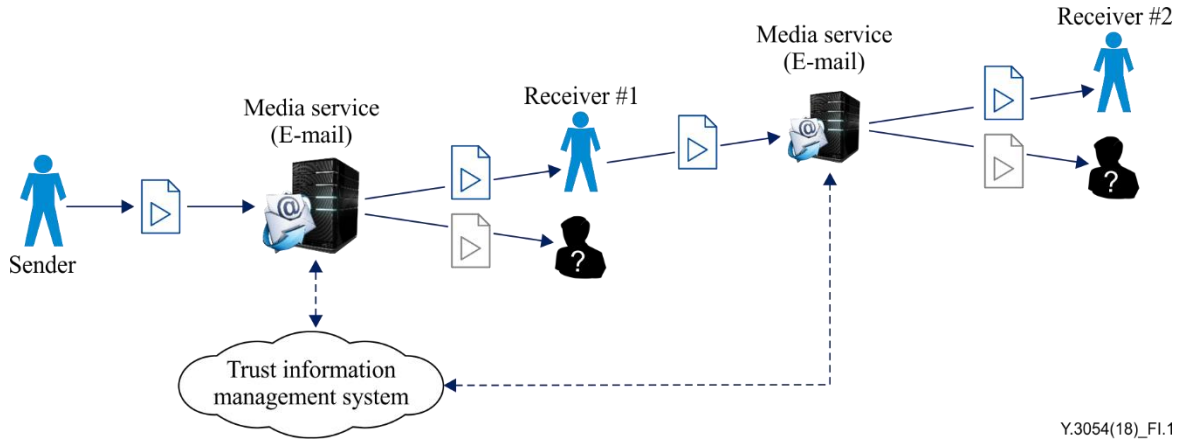

Figure I.1 – Overview of trust-based content consumption services

In closed media service, a sender can send an e-mail with various content types (e.g., text, image, video clip or URL) to any designated receiver. All receivers can open the e-mail and share the content it contains. If one receiver forwards the e-mail to others with attached content, then they are also able to share and redistribute content created by the original sender without the original sender's permission.

From the sender's perspective, trust in a receiver can be analysed by a TIMS from e-mail, SNSs and other services. Then, trust is utilized to determine whether to grant permission to access content. Except for the e-mail service described in the previous paragraph, various applications related to open media service (e.g., chatting or messenger services and peer-to-peer file sharing) are described in clause I.2 as trust-based content-sharing services.

I.1.3 Information flow

Figure I.2 depicts information flow in a trust-based content consumption service for a sender usingan e-mail application as an example. Specifically, a trust-based content consumption service analyses trust in the receiver by the sender. Because receivers can forward content to other users regardless of the sender's intention, the service grants access rights to content to receivers based on their trust, which is analysed by a TIMS.

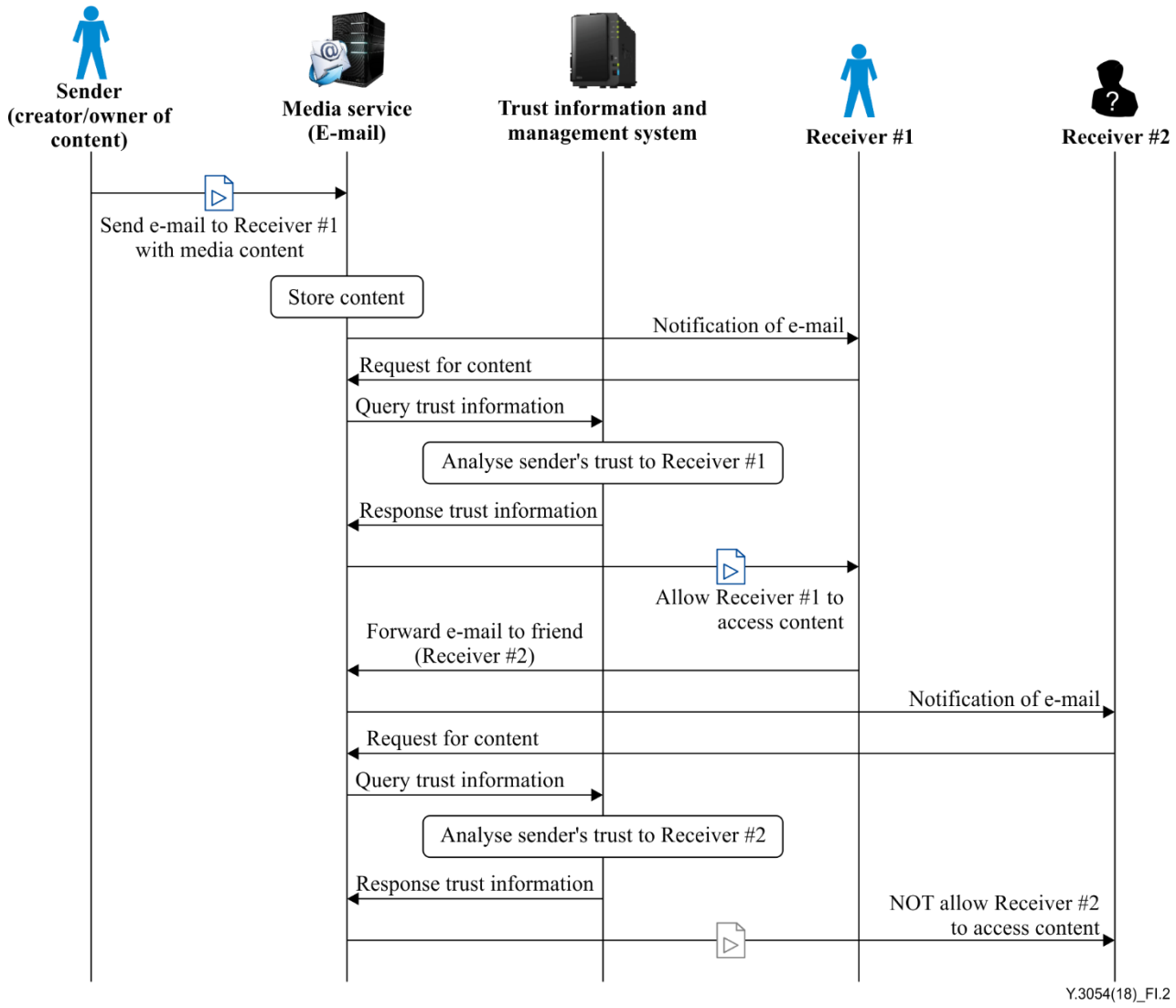

Figure I.2 – Information flow in a trust-based content consumption service for senders

The interaction shown in Figure I.2 can be described as follows:

1) a sender sends content to receiver #1 (No. 1);
2) a media service (e-mail service) stores the attached content and informs receiver #1 about the receipt of the e-mail;
3) receiver #1 requests to download content, and the media service requests trust information about receiver #1 (i.e., sender's trust toward receiver #1) to a TIMS;
4) the TIMS responds to the request for media service by providing trust information that is analysed by data and information collected from various data sources (i.e., e-mail, SNSs, etc.);
5) if measured trust in receiver #1 is greater than the criterion level, the media service allows receiver #1 to access content based on the response from the TIMS;
6) receiver #1 forwards content to receiver #2 to share the contained content, and the media service informs receiver #2 about the receipt of the content;
7) on receiving the e-mail, receiver #2 requests content, and the media service requests trust information about receiver #2 (i.e., trust of the sender in receiver #2) to the TIMS;
8) a TIMS analyses the trust information about receiver #2 and responds to the media service request;

9) if measured trust in receiver #2 is greater than the criterion level, the media service allows receiver #2 to access the content – if not, media service is denied.

On the other hand, from the receiver's perspective, it is risky to access content from a suspicious or unknown sender. Figure I.3 depicts an information flow in a trust-based content consumption service for the receiver using an e-mail application as an example. Specifically, a trust-based content consumption service analyses trust in a sender by a receiver. Based on the analysis of trust in the sender, the content is tagged by "trustworthy". Even though trust in the sender is less than the criterion level, receivers can still access content. As such, the media service intends to minimize intervention in content flow because the service provides users with an option to access received content from an untrustworthy sender.

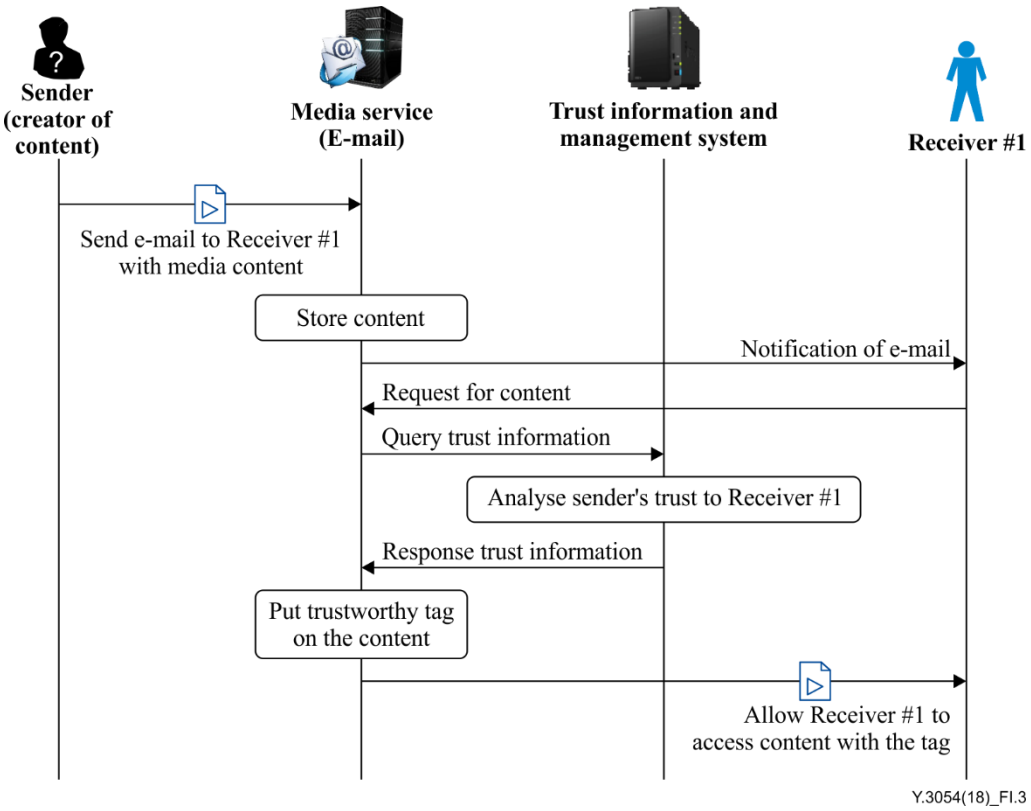

Figure I.3 – Information flow in a trust-based content consumption service for receivers

The interaction shown in Figure I.3 can be described as follows:

1) a sender sends content;
2) the media service requests information about trust in the sender in response to a receiver request;
3) a TIMS gathers data required to analyse trust from various services and analyses trust information;
4) the TIMS responds to a request from the media service by providing measured trust information about the sender;
5) based on the trust information, the media service attaches a trustworthy tag to the content;
6) a receiver can access the content with the tag.

I.2 Trust-based content-sharing services

I.2.1 Motivation

In trust-based content-sharing services, anyone can access content as long as a content creator does not impose restrictions. Even though content is open to anyone, the concept of trust is still required because content contains a certain level of risk.

Accordingly, it is critical not to impose unnecessary restrictions on open media services because they are developed to share content with anyone. In this context, a trust-based content-sharing media service aims to minimize intervention determined by trust.

From the perspective of a receiver (content consumer), contaminated, manipulated or illegal contents are major concerns. From the perspective of a sender (content producer), reputation attack, rating distortion and malicious threads are major concerns.

I.2.2 Overview

Figure I.4 is an overview of trust-based content-sharing services. From the content consumer perspective, content with a trustworthy tag can be useful. While any user can upload or post content in an open media service, it is beneficial to consumers if they can refer to trust information to avoid accessing infected, contaminated, manipulated or illegal contents. For this purpose, trust-based content-sharing services provide content producer trust information so that the media service can add a trustworthy tag to content. Based on trust indicated by the tag, consumers can access trustworthy content and avoid inherent risks in content consumption. If consumers want to see only trustworthy content, trust information about content producers is analysed and presented by interaction between the media service and a TIMS.

From the content producer perspective, this media service prevents untrustworthy users from reacting to the content, since their major concerns are reputation attack, rating distortion and malicious threads. Reacting includes replying, rating and re-distributing. The media service prevents untrustworthy consumers reacting to the content. However, even untrustworthy consumers are still able to access the content (i.e., to watch or read it).

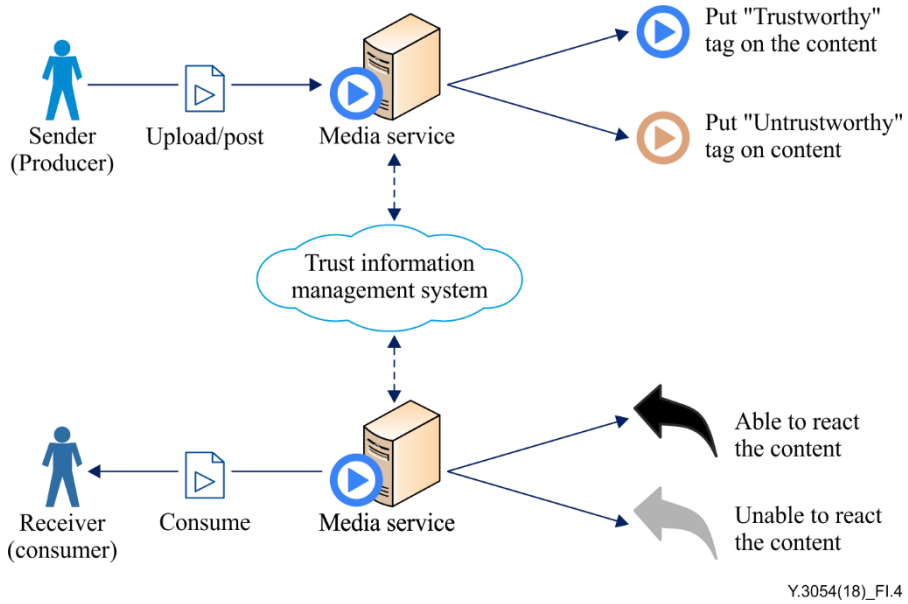

Figure I.4 – Overview of trust-based content-sharing services

I.2.3 Information flow

Figure I.5 depicts information flow in a trust-based content-sharing service for content consumers, while Figure I.6 illustrates such flow for content producers.

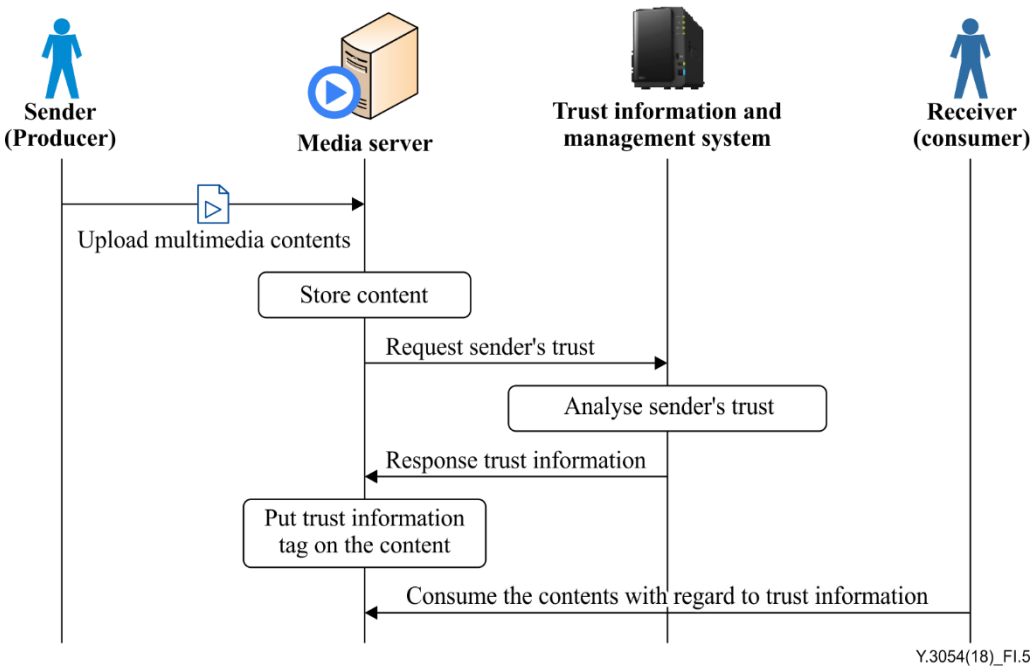

Figure I.5 – Information flow in a trust-based content-sharing service for content consumers

The interaction shown in Figure I.5 can be described as follows:

1) the producer uploads content to a media service, and the media service stores content;
2) the media server requests trust information about the producer trust from a TIMS;
3) the TIMS gathers relevant data from various services (e.g., media services or SNSs) and analyses trust information;
4) the TIMS responds to the request from the media service by providing measured trust information about the content producer;
5) based on the trust information, the media service attaches a trustworthy tag to the content;
6) consumers can refer to the tagged trust information when they consume content.

NOTE – The media service has multiple options to utilize trust information. For example, the media service can prohibit untrustworthy producers for uploading content if the media service applies a strict regulation.

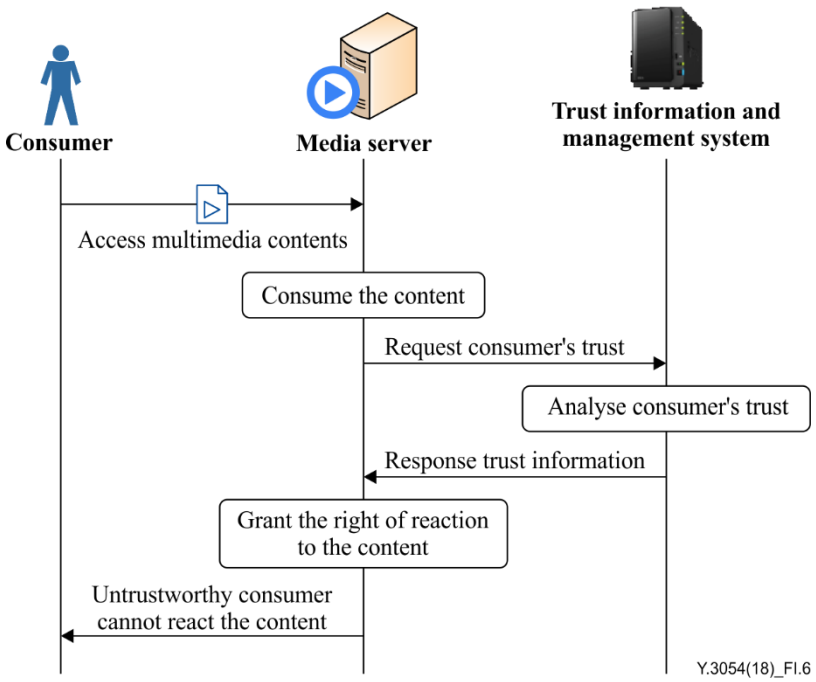

Figure I.6 – Information flow in a trust-based content-sharing service for content producers

The interaction shown in Figure I.6 can be described as follows:

1) a content consumer accesses the content;
2) the media service requests consumer trust information when the consumer wants to react to the content;
3) the TIMS gathers the data required to analyse trust from various services and analyses trust information;
4) the TIMS responds to the request from the media service by providing measured trust information about the content consumer;
5) based on the trust information, the media service grants the consumer right of reaction to the content;
6) only consumers to whom the reaction right has been granted can react to content.

Appendix II

Calculating a trust index for trust-based content consumption services

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

II.1 The concept of a trust index for trust-based media services

This appendix introduces an example of applying a trust index to closed media services. Although various methods of measuring trust exist, this appendix introduces a computational trust analysis method. Assuming that a trustor, user *i*, want to determine whether it is safe to send an important e-mail to a trustee, user *j*. In this situation, user *i* can request a TIMS to analyse trust in user *j*.

In a trust-based media consumption service, *Trust index* (*i, j, t*) indicates the trust of user *i* in user *j* at time *t*. *Trust index* (*i, j, t*) is calculated by 1) *trustworthiness* (*j*), and 2) *relationship* (*j*→*i*) between *j* and *i*. It should be noted that the relationship (*j*→*i*) is considered because the reverse relationship (*i*→*j*) is already identified by user *i*. *Trustworthiness* can be evaluated by four trust indicators: *Ability*, *Integrity*, *Benevolence* and *Sincerity*. Table II.1 shows definition and measurements for each trust indicator.

Table II.1 – Definition and measurement for each trust indicators

Trust indicator	Definition	Example of trust attributes and data source
Ability	The potential of a group of skills, competencies and characteristics that enable a party to have influence in media services [b-Mayer] [b-Colquitt]	– Number of received content a day – Number of friends on an SNS – Number of likes a day on an SNS
Benevolence	The degree to which a trustee is believed to want to do good to the trustor, aside from an egocentric profit motive in media services [b-Mayer] [b-Colquitt]	– Number of postings of malicious URLs on the medium itself – Number of postings of malicious URLs on an SNS
Integrity	The degree to which the trustee adheres to a set of principles prescribed by media services [b-Mayer] [b-Colquitt]	– Reported number of disagreed behaviour incidents on the medium itself – Reported number of disagreed behaviour incidents on an SNS

For trust-based media consumption services, *relationship* (*j*→*i*) is measured by three factors: *similarity, relationship period* and *closeness*. Similarity is an indictor measuring how much trustor and trustee share the same network in a given network. The more they share the same users in the network, the more user *j* trusts user *i*. In a similar vein, the longer their relationship period is, the more user *j* trusts in user *i*. If user *j* comparably sends more e-mails to user *i*, it is clear that *j* has a close relationship with user *i*. Figure II.1 represents a computational trust reasoning method for trust-based media services.

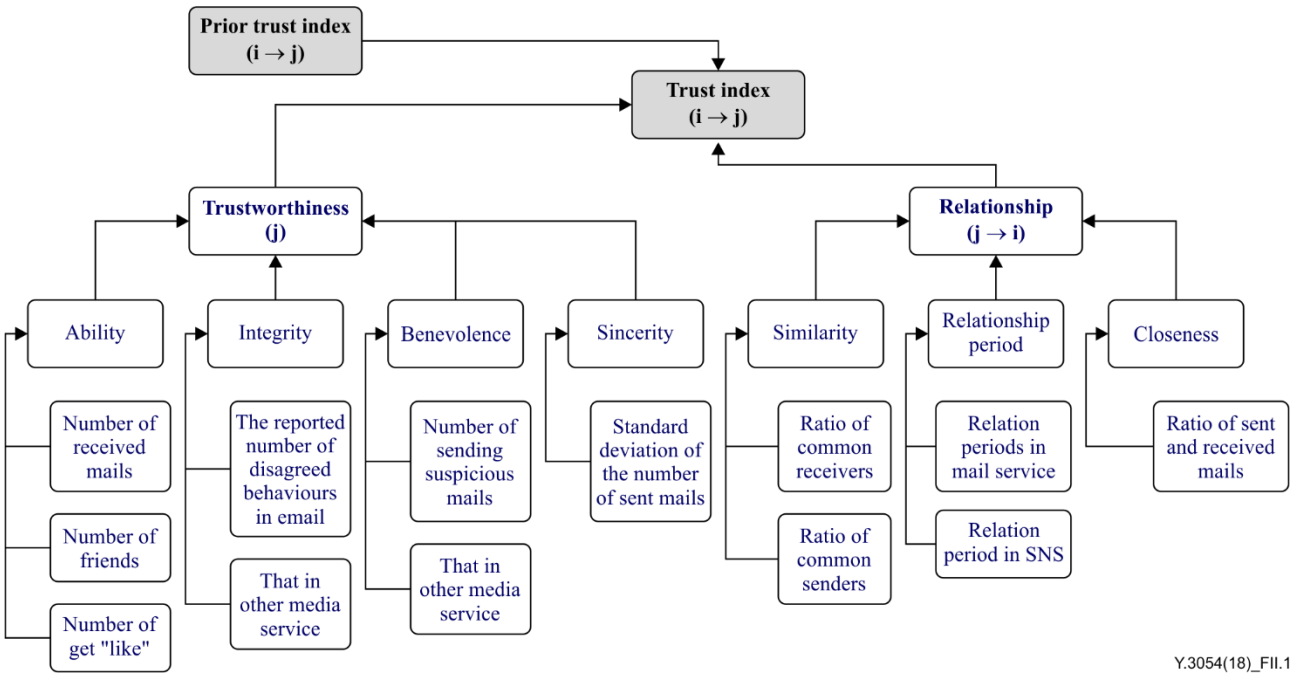

Figure II.1 – Method of evaluating trust for trust-based content consumption services

II.2 Calculation of trust index

Equation II-1 represents the method of measuring the trust index *T (i, j, t)*.

$$T(i,j,t) = \alpha \cdot Trustworthiness\,(j,t) + \beta \cdot Relationship\,(j,i,t) \quad \text{(II-1)}$$

$$Trustworthiness\,(j,t) = \sigma \cdot Ability\,(j,t) + \tau \cdot Integrity\,(j,t) + \varphi \cdot Benevolence\,(j,t) + \Phi \cdot Sincerity\,(j,t) \quad \text{(II-2)}$$

$$Relationship\,(j,i,t) = \gamma \cdot Similarity\,(j,i,t) + \delta \cdot Relationship\ period\,(j,i,t) + \varepsilon \cdot Closeness\,(j,i,t) \quad \text{(II-3)}$$

In Equations II-1 to II-3, α, β, σ, τ, φ, Φ, γ, δ, ε indicate weights for each factor.

To evaluate *trustworthiness (j, t)*, three indicators of *Ability*, *Integrity* and *Sincerity* should be calculated by Equations II-4 to II-6. *Ability* (*j*, *t*) can be measured by Equation II-4:

$$Ability\,(j,t) = \frac{Number\ of\ received\ mail_j}{Number\ of\ received\ mail_j + 1} + \frac{Number\ of\ friends_j}{Number\ of\ frinds_j + 1} + \frac{Number\ of\ get\ "like"_j}{Number\ of\ get\ "like"_j + 1} \quad \text{(II – 4)}$$

If *j* has a strong ability, others may send e-mails for requests.

Integrity (*j*, *t*) can be measured by Equation II-5, as [b-Lee] suggests:

$$Integrity\,(j,t) = \mathrm{M} - \frac{1}{h}\sum_{k=1}^{h} n_k \quad \text{(II-5)}$$

In Equation II-5, M indicates initial value, n_k denotes the reported number of disagreed behaviours. For example, n_1 is the number of reported incidences of to swearing on the media service and n_2 is the number of violated behaviour incidents on an SNS. A large value of *j* indicates a high incidence of violating pre-described rules, while a lowevalue of *j* means trustworthy.

Benevolence (*j*, *t*) can be measured by Equation II-6:

$$Benevolence\,(j,t) = \mathrm{N} - \frac{1}{h}\sum_{O=1}^{h} n_O \quad \text{(II-6)}$$

In Equation II-6, N indicates initial value, n_O denotes the number of incidences of sending and posting malicious content in media service n_o. The more *j* conducts doubtable behaviours, the less *j* means trustworthy.

Sincerity (j, t) can be measured by Equation II-7, as [b-Song] suggests:

$$Sincerity\ (j,t) = \left(1 - \frac{1}{\overline{n}_t}\right) \cdot \frac{1}{STD^M} \quad \text{(II-7)}$$

In Equation II-7, $\overline{n}_j$ indicates the average number of sent mails, and STD^M refers to the standard deviation of the number of sent mails. Sincerity measures user *j*'s consistent usage in media services.

To measure *relationship (j→i)*, three factors of *Similarity*, *Relationship period* and *Closeness* are considered, as represented by Equations II-8 and II-9.

Similarity (*j*, *i*, *t*) can be measured by Equation II-8:

$$Similarity\ (j,i,t) = \left(\frac{send\ mail\ (i) \cap send\ mail\ (j)}{send\ mail\ (i) \cup send\ mail\ (j)} + \frac{receive\ mail\ (i) \cap receive\ mail(j)}{receive\ mail(i) \cup receive\ mail(j)}\right) \quad \text{(II-8)}$$

Both *i* and *j* send mails to the same other user, *send mail(i)*$\cap$ *send mail(j)* will increase. In addition, both *i* and *j* receive e-mail from the same user, again the value of this intersection will increase.

Relationship period (*j*, *i*, *t*) can be measured by Equation II-9:

$$Relationship\ period\ (j,i,t) = \left(\frac{First\ mail\ (j,i)}{stat\ mail(j)}\right) \quad \text{(II-9)}$$

In Equation II-9, *start mail (j)* denotes the date when *j* starts to use e-mail, and *First mail (j, i)* indicates the first date on which *j* sent an e-mail to *i*.

Closeness (*j*, *i*, *t*) is measured by Equation II-10:

$$Closeness\ (j,i,t) = \left(\frac{send\ (j \rightarrow i)}{send\ (j \rightarrow i) + send(i \rightarrow j)}\right) \quad \text{(II-10)}$$

The measured value of *Closeness (j, i, t)* increases when *j* sends more e-mails to *i* than user *i* does to user *j*.

Based on data gathered from media services, a trust-based media service provides trust information (i.e., a trust index) so that users can refer to the analysed trust index or the e-mail service via a TSE and can make a decision about whether to allow content download . For example, it is possible to build and operate a policy that someone whose trust index is less than 0.3 is not allowed to download attached content.

Bibliography

[b-ITU-T H.780] Recommendation ITU-T H.780 (2012), *Digital signage: Service requirements and IPTV-based architecture*.

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2016) | ISO/IEC 9594-8:2017, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

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

[b-Colquitt] Colquitt, A., Brent A. Scott, B.A, LePine, J.A, (2007), *Trust, Trustworthiness, and Trust Propensity: A Meta-Analytic Test of Their Unique Relationships With Risk Taking and Job Performance*, Journal of Applied Psychology, **92**, No. 4, pp. 909~927.

[b-Lee] Lee, C.H., Jang, Y.M., Jung, J.W., Won, D.H. (2013). *Dynamic user reliability evaluation scheme for social network service*. Journal of the Korea Institute of Information Security and Cryptology, **23**(2), pp. 157-168.

[b-Mayer] Mayer, R.C., Davis, J.H., Schoorman, F.D. (1995). *An integrative model of organizational trust*. Academy of Management Review, **20**, pp. 709-734.

[b-Song] Song, H.S. (2013). *Prediction method for implicit interpersonal trust between Facebook users* [in Korean]. Journal of Information Technology Applications and Management, **20**(2), pp. 177-191.

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

Printed in Switzerland
Geneva, 2018