



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 of Trust-based Media Services

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

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/had not] 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/>.

© ITU 2018

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Contents

1	Scope.....	3
2	References.....	3
3	Definitions	3
3.1	Terms defined elsewhere	3
3.2	Terms defined in this draft Recommendation	4
4	Abbreviations and acronyms	4
5	Conventions	4
6	Overview of trust-based media services	4
6.1	Risks in media services	4
6.2	Necessity of trust-based media services	5
7	Requirements for trust-based media services	6
7.1	Requirements for trust data collection.....	6
7.2	Requirements for trust analysis	6
7.3	Requirements for applying trust to trust-based media services.....	7
7.4	Requirements for operating and managing trust-based media services	7
8	Architectures for trust-based media services	7
8.1	Trust Agent (TA).....	8
8.2	Trust Information and Management System (TIMS).....	9
8.3	Trust Service Enabler (TSE)	10
9	Trust analysis and service provisioning for trust-based media services.....	10
9.1	Trust analysis mechanism for trust-based media services.....	10
9.2	Service provisioning for trust-based media services	11
10	Security Consideration.....	11
	Appendix I – Use cases of trust-based media services	13
	Appendix II – Calculating trust index for trust-based content consumption services	19
	Bibliography.....	22

Draft Recommendation ITU-T Y.3054 (Y.trustworthy-media)

Framework of 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 at restraining untrustworthy users from conducting malicious behaviours as well as being robust to unexpected executions and failures with certain predictability and reliability. Thus, this draft Recommendation provides a framework of trust-based media services. The scope of this draft 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 Recommendation contains provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations 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 draft Recommendation uses the following terms defined elsewhere:

3.1.1 Trust [ITU-T Y.3052]: Trust is the measureable belief and/or confidence which represent accumulated value from history and the expecting value for future.

NOTE – Trust is quantitatively and/or qualitatively calculated and measured, which 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 for presenting of information.

3.2 Terms defined in this draft Recommendation

This draft Recommendation defines the following terms:

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 draft Recommendation uses the following abbreviations and acronyms:

ID	Identification
TA	Trust Agent
TIMS	Trust Information Management System
TSE	Trust Service Enabler
API	Application Programming Interface
idM	identification Manager
PID	Pseudo Identity
SNS	Social Networking Service
UI	User Interface
URL	Uniform Resource Locator
OAM	Operations, Administration, and Management

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 number of content is enormously increasing, and users are participating in multiple media services (e.g., mail, contents delivery services, social networking service (SNS), etc.). Basically, media service environment consists of four major entities (i.e., media service itself, content, sender, and receiver) as shown in Figure 6-1.

When a sender and a receiver have interactions of using content in 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 behaviours of the user, etc.

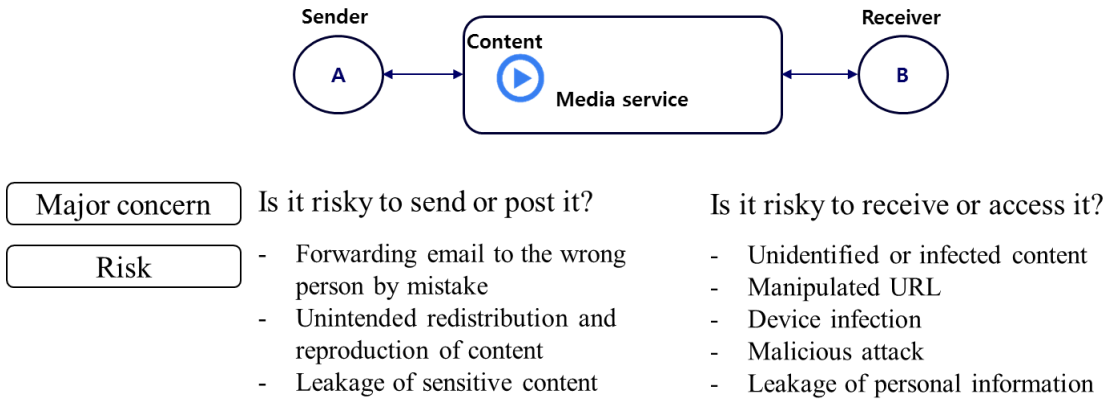


Figure 6-1. Inherent risks in media services

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

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

6.2 Necessity of trust-based media services

Although it is critical for media service providers to build reliable and secured content usage environment, they relied on limited capabilities providing rating information and comments on content. However, these capabilities are not enough to identify potential risks due to insufficient measurements and analysis.

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

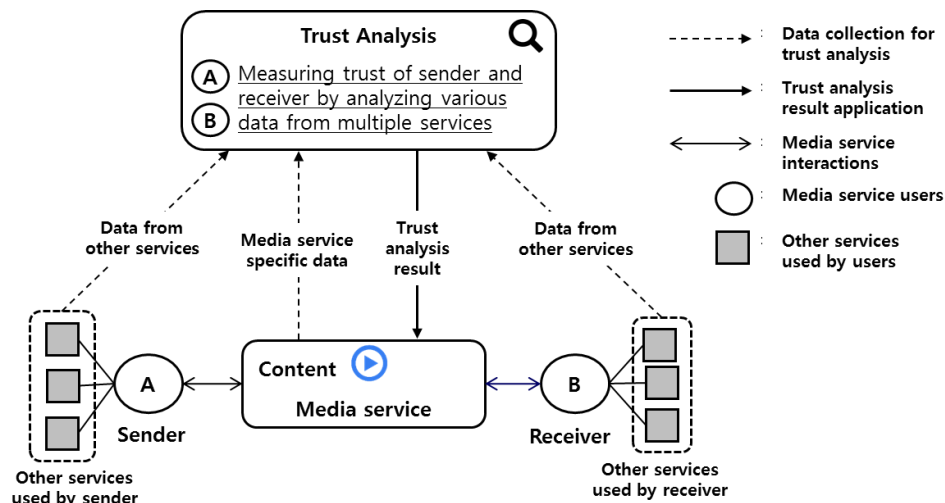


Figure 6-2. A conceptual approach of trust-based media services

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: It is required to collect 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.).
- Pre-processing of collected data: It is recommended that the collected data is refined, filtered for pre-processing.
- Transferring collected data: It is required to transfer collected data into components for analyzing trust in secured ways.

7.2 Requirements for trust analysis

- Trust evaluation: It is required to evaluate trust by analyzing data with various methods.
- Quantization of trust: It is required for trust-based media services to calculate various trust information into a specific value (i.e., a real number).
- Analysis of heterogeneous data: It is required to process and analyze heterogeneous data because collected data varies on properties.
- Data repository: It is recommended to store trust information in a repository to keep track of trust over time.
- Interface for trust information: It is required to provide an interface (i.e., Application Programming Interface (API), etc.) between service/application and trust information analysis entities to exchange trust information.
- Maintenance of trust-relevant information: It is required to monitor and modify trust information seamlessly because trust information is valid only in a specific time period and can be changed as time goes on.