

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.741.1

(06/2012)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

IPTV multimedia services and applications for IPTV –
IPTV application event handling

IPTV application event handling: Audience measurement operations for IPTV services

Recommendation ITU-T H.741.1



International
Telecommunication
Union
Documents

Document Sharing Hub

ITU-T H-SERIES RECOMMENDATIONS
AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779
Digital Signage	H.780–H.789

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

Recommendation ITU-T H.741.1

IPTV application event handling: Audience measurement operations for IPTV services

Summary

The ITU-T H.741.x series of Recommendations defines a foundational platform for audience measurement (AM) of IPTV services. They focus on the interface between terminal devices and an audience measurement aggregation function.

The AM platform integrates a method for end users to report personal information, and is designed to easily add time-shifted and interactive services, and non-terminal device measurement points. While the ITU-T H.741.x series allows the implementation of audience measurement for IPTV services, its mechanism may be equally applicable to non-IPTV services.

The design philosophy in the ITU-T H.741.x series is focused on scalability, minimizing the use of resources, security, flexibility to support a variety of service provider deployments, and rich privacy support to meet emerging regulations and legislation.

Recommendation ITU-T H.741.1 specifies the operations of AM, including procedures prior to configuration of terminals, configuration of terminals, reporting by terminals, security mechanisms, and recovery from abnormal situations. Informative Appendices I-VII discuss discovery metadata, implementation considerations, examples, permission levels, vendor considerations, alternative privacy schemes, and discuss capabilities and profiles.

Amendment 1 to Recommendation ITU-T H.741.1 (integrated into this edition) includes XML schema on audience measurement service discovery in Appendix VIII and XML schema instances for TD-AMF configurations, reports and permits in Appendix IX.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T H.741.1	2012-06-29	16
1.1	ITU-T H.741.1 (2012) Amd. 1	2013-01-25	16

Keywords

Audience measurement, audience rating service, audience viewership, configuration, contents rating, discovery metadata, distributed content service, end-user permission, engagement metrics, examples, implementation guidelines, interactive services, IPTV application event handling, IPTV service, linear TV, monitoring, personalized service, privacy protection, reporting, service discovery XML schema.

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, 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 2013

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

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	4
4 Abbreviations and acronyms	5
5 Conventions	6
6 Preconfiguration	6
7 Effective configuration of TD-AMFs.....	10
7.1 Configuration package.....	10
7.2 End-user permits.....	19
8 Specific aspects of reporting.....	20
8.1 Reporting of services which start or end outside measurement periods	20
8.2 Reporting surrounding restricted content	20
8.3 Reporting of user presence	21
8.4 Reporting changes due to effective permit changes	21
8.5 Reporting of storage congestion.....	21
8.6 Nothing to report	21
9 Security, privacy and permission mechanisms.....	21
9.1 Security and privacy of AM messages	21
9.2 End-user permission operation modes.....	28
10 Abnormal situations and potential recovery actions.....	31
Appendix I – Discovery of audience measurement services by terminal devices	35
Appendix II – Considerations on implementation	40
II.1 Considerations on whether to implement AM.....	40
II.2 Considerations for end-user permission method selection.....	41
II.3 Considerations on using content filtering in configuration packages	45
II.4 Considerations on using different measurement triggers	46
II.5 Considerations for using AM message acknowledgements	47
II.6 Considerations for configuration mode selection.....	47
II.7 Considerations regarding methods of obtaining end-user permits	49
II.8 Considerations for using multicast sub-addressing mechanisms	50
II.9 Considerations for requesting error message responses to multicast messages	52
II.10 Considerations for delivery mode selection	53
II.11 Considerations on using end-user information to filter measurement requests	54



	Page
Appendix III – Examples of TD-AMF configurations, reports and permits	56
III.1 Example of use of configuration package data structure for service- common measurements	56
III.2 Example of measurement reports associated with configuration example of Figure III.1	58
III.3 Examples using end-user information for filtering configuration packages ..	65
III.4 Example of UserPermit	67
Appendix IV – Considerations of end-user permission levels.....	69
Appendix V – Considerations regarding the unlinkability property	71
Appendix VI – Considerations for AM vendors	74
Appendix VII – Audience measurement capabilities and profiles	75
Appendix VIII – XML schema on the data structures for audience measurement service discovery	76
Appendix IX – XML schema instances for TD-AMF configurations, reports and permits	79
IX.1 Instance based on clause III.1.....	79
IX.2 Instances based on clause III.2	81
IX.3 Instances based on Appendix III.3	86
IX.4 Instance based on Appendix III.4.....	87
Bibliography.....	88

Recommendation ITU-T H.741.1

IPTV application event handling: Audience measurement operations for IPTV services

1 Scope

This Recommendation describes the operational aspects of audience measurement for IPTV services. It specifies the discovery, configuration, reporting, error handling, and security aspects for IPTV audience measurement.

Audience measurements are constrained to the communications interface(s) between terminal device audience measurement functions and measurement aggregation functions. Subsequent Recommendations are anticipated to address communications interface(s) with audience measurement functions located within other functions of the IPTV architecture see [ITU-T H.741.0].

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 H.741.0] Recommendation ITU-T H.741.0 (2012), *IPTV application event handling: Overall aspects of audience measurement for IPTV services*.
- [ITU-T H.741.2] Recommendation ITU-T H.741.2 (2012), *IPTV application event handling: Data structures of audience measurement for IPTV services*.
- [ITU-T H.741.3] Recommendation ITU-T H.741.3 (2012), *IPTV application event handling: Audience measurement for IPTV distributed content services*.
- [ITU-T H.741.4] Recommendation ITU-T H.741.4 (2012), *IPTV application event handling: Transport mechanisms for audience measurement*.
- [ITU-T X.1191] Recommendation ITU-T X.1191 (2009), *Functional requirements and architecture for IPTV security aspects*.
- [IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 aggregation function [ITU-T H.741.0]: The function that configures audience measurement functions (AMFs), then receives processed events, sample values and end-user information from AMFs. It may participate in the communication of end-user permissions.

3.1.2 application [b-ITU-T Y.101]: A structured set of capabilities, which provide value-added functionality supported by one or more services.

3.1.3 application event [b-ITU-T H.740]: An application event is every end-user interaction or occurrence related to multimedia contents in IPTV applications. It includes an emergency event from event notification services.

3.1.4 audience information [ITU-T H.741.0]: The overall information about end-user behaviour, and the related end-user information, during the time IPTV audience measurement is inactive.

3.1.5 audience measurement [ITU-T H.741.0]: The measurement of people's engagement with IPTV services.

3.1.6 audience measurement data [ITU-T H.741.0]: End-user behaviour data which is related to a service and content consumption, combined or not with end-user information.

3.1.7 audience measurement function (AMF) [ITU-T H.741.0]: The function that, if given permission, measures the end-user behaviour by processing events or samples from IPTV services. AMFs may request and collect end-user information. AMFs transfer processed events, samples and end-user information to aggregation functions.

3.1.8 audience measurement service provider [ITU-T H.741.0]: A service provider providing audience measurement services. An audience measurement service provider configures an audience measurement system to control what audience information the system collects.

3.1.9 audience measurement system [ITU-T H.741.0]: The system which, with end-user permission, measures end-user behaviour by detecting application events within the IPTV service and collecting their data within the IPTV service.

3.1.10 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.11 configuration package [ITU-T H.741.0]: A configuration package is the data structure which specifies the target services to be measured, content filtering, measurement schedule, events and samples to be measured, and measurement report delivery.

3.1.12 content (object) [b-ITU-T T.174]: Encoded generic value, media or non-media data

3.1.13 content consumption [ITU-T H.741.0]: A series of valid operation actions to complete selecting an IPTV service and consuming the relate content based on the procedure flow within the IPTV system.

3.1.14 content rating [ITU-T H.741.0]: Actively asserted opinions evaluating aspects of content, using a position assigned on a defined scale, to communicate those aspects to others. Scales may be industry standard, or not. Example scales include, among others, the Motion Picture Association of America (MPAA), a number of stars, and thumbs up or down.

NOTE – Examples of use include the indicating of suitability for audience segments, censorship, and levels of entertainment, quality, or popularity; content optimization and targeting across audience segments, and content recommendation.

3.1.15 controlled information [ITU-T H.741.0]: A classification of end-user information that can be used alone or easily in combination with other information to uniquely identify, contact, or locate an end user or subscriber, in line with Annex A of [ITU-T X.1191].

3.1.16 digital destinations [ITU-T H.741.0]: The result of navigation across services, including channels, applications, or portals.

3.1.17 directive(s) [ITU-T H.741.0]: Instructions that are input as part of an order from stakeholders to the AM system regarding target audiences, what and how to measure, and what to report back to stakeholders.

3.1.18 electronic programme guide (EPG) [b-ITU-T H.721]: A service navigation application which is used especially for scheduled linear programmes.

NOTE – in some traditional broadcast services, EPG is defined as an on-screen guide used to display information on scheduled live broadcast television programmes, allowing a viewer to navigate, select, and discover programmes by time, title, channel, and genre. This traditional definition does not cover "catalogues" for on-demand and download services (sometimes called electronic content guide or broadband content guide) and bi-directional interactive service (sometimes called interactive programme guide) for end-user interaction with a server or head-end.

3.1.19 end user [b-ITU-T Y.1910]: The actual user of the products or services.

NOTE – The end user consumes the product or service. An end user can optionally be a subscriber.

3.1.20 end-user behavioural information [ITU-T H.741.0]: A part of audience measurement information which includes "application events" and/or "end-user context". An "application event" is information reflecting the behaviour of an IPTV service end user. "End-user context" is information relating to the situation when an "application event" was generated.

3.1.21 end-user information [ITU-T H.741.0]: "End-user info" is information about an IPTV service end user. It includes "identifying end-user information" and "non-identifying generic user information".

3.2.22 engagement metric [ITU-T H.741.0]: A measure of the level of involvement, interaction, sentiment and promotion that an end user has with content. It provides a more holistic view of end users than audience ratings. Examples of involvement metrics include time spent or frequent watcher. Examples of involvement metrics include replay and requests for information. Examples of sentiment metrics include associated amount of chat and words used. Examples of promotion metrics include forwarding to friends or posting to a blog.

NOTE – Example uses include focus on acquisition of evangelists, finer granularity audience targeting, and emerging uses.

3.1.23 integrity [b-IEC/ISO 27001] and [b-IEC/ISO 27002]: Safeguarding the accuracy and completeness of information and processing methods.

3.1.24 Internet Protocol Television (IPTV) [b-ITU-T Y.1901]: Multimedia services such as television/video/audio/text/graphics/data delivered over IP-based networks managed to support the required level of QoS/QoE, security, interactivity and reliability.

3.1.25 IPTV terminal device [b-ITU-T Y.1901]: A terminal device which has IPTV terminal function (ITF) functionality, e.g., an STB.

3.1.26 IPTV terminal function (ITF) [b-ITU-T Y.1901]: The end-user function(s) associated with a) receiving and responding to network control channel messages regarding session set-up, maintenance, and tear-down, and b) receiving the content of an IP transport from the network and rendering.

3.1.27 linear TV [b-ITU-T Y.1901]: A television service in which a continuous stream flows in real time from the service provider to the terminal device and where the end user cannot control the temporal order in which contents are viewed.

3.1.28 metadata [b-ITU-T Y.1901]: Structured, encoded data that describe characteristics of information-bearing entities to aid in the identification, discovery, assessment, and management of the described entities.

NOTE – EPG metadata have many applications and may vary in depth from merely identifying the content package title or information to populate an EPG, to providing a complete index of different scenes in a movie or providing business rules detailing how the content package may be displayed, copied, or sold.

3.1.29 measurement report [ITU-T H.741.0]: The data that the audience measurement function (AMF) generates from an end-user behaviour event or sample.

3.1.30 privacy [b-ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

3.1.31 repudiation [b-ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.1.32 sample [ITU-T H.741.0]: A sample is a periodic action occurring on a configurable schedule time interval, during a service period, which captures specified information values.

3.1.33 sample set [ITU-T H.741.1]: A sample set contains one or more information fields, captured at a specific instance of periodic action occurring on a configurable schedule time interval, during a service period.

3.1.34 sample time [ITU-T H.741.0]: A sample time is when an instance of the periodic action occurs on a configurable schedule time interval, which captures specified information values, during a service period.

3.1.35 sample value [ITU-T H.741.0]: The content of an information field, captured at a specific instance of periodic action occurring on a configurable schedule time interval, during a service period.

3.1.36 service [b-ITU-T Y.101]: A structure set of capabilities intended to support applications.

3.1.37 service common [ITU-T H.741.1]: Qualifier of measurements such as events and elements, and reports to indicate that these measurements and reports are commonly applicable to two or more distributed content or interactive services.

3.1.38 service navigation [b-ITU-T H.720]: A process of presenting information that allows the end user to discover, select and consume services.

3.1.39 service provider [b-ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other end users either on a tariff or contract basis. A service provider may or may not operate a network. A service provider may or may not be a customer of another service provider.

3.1.40 set-top box (STB) [b-ITU-T J.183]: A hardware box that contains a digital signal demodulator, de-multiplexer, MPEG-2 decoder, and other functionalities and interfaces related to digital signal reception and presentation of the distributed programme at the subscriber's site.

3.1.41 subscriber [b-ITU-T M.3050.1]: The subscriber is responsible for concluding contracts for the services subscribed to and for paying for these services.

3.1.42 terminal device (TD) [b-ITU-T Y.1901]: An end-user device which typically presents and/or processes the content; such as a personal computer, a computer peripheral, a mobile device, a TV set, a monitor, a VoIP terminal or an audio-visual media player.

3.1.43 video-on-demand (VoD) [b-ITU-T Y.1901]: A service in which the end user can, on demand, select and view a video content and where the end user can control the temporal order in which the video content is viewed (e.g., the ability to start the viewing, pause, fast forward, rewind, etc.).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 broadcast (based on [b-ITU-T M.60]): One-way transmission of TV signals from one point to two or more other points.

3.2.2 effective measurement period: An effective measurement period is the time duration when one or more concatenated measurement periods, and a service period overlap.

3.2.3 effective permit: An effective permit is the end-user permit which is in force at a particular time.

3.2.4 multicast sub-addressing: The use of elements in a multicast message to determine if the message is intended for the receiving terminal device audience measurement function (TD-AMF).

3.2.5 sender anonymity: A sender's anonymity is beyond suspicion if, though the attacker can see evidence of a sent message, the sender appears no more likely to be the originator of that message than any other potential sender in the system.

3.2.6 unlinkability: Unlinkability of two or more items of interest (e.g., subjects, messages, actions, etc.) means that within a particular set of information, the attacker cannot distinguish whether these items of interests are related or not (with a high enough degree of probability to be useful).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ack	Acknowledge
AES	Advanced Encryption Standard
AGF	Aggregation Function
AM	Audience Measurement
AMF	Audience Measurement Function
EPG	Electronic Programme Guide
HMAC	Hash-based Message Authentication Code
HTTP	HyperText Transfer Protocol
ID	IDentifier
MAC	Media Access Control
nPVR	network Personal Video Recorder
OTP	One-Time Password
PC	Personal Computer
PVR	Personal Video Recorder
QoE	Quality of Experience
QoS	Quality of Service
P2P	Peer-to-Peer
RSA	Rivest Shamir Adleman public-key encryption
SHA	Secure Hash Algorithm
SP	Service Provider
SRP	Secure Remote Protocol
TD-AMF	Terminal Device Audience Measurement Function
TLS	Transport Layer Security
TLS-SRP	Transport Layer Security – Secure Remote Password
URL	Uniform Resource Locator

VoD	Video-on-Demand
XML	eXtensible Markup Language

5 Conventions

In this Recommendation, the following conventions apply.

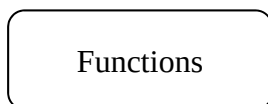
The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

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.

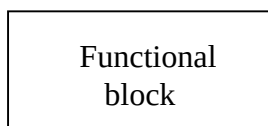
The keywords "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is 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.

The keyword "functions" is defined as a collection of functionalities. It is represented by the following symbol in the context of IPTV architecture:



The keywords "functional block" are defined as a group of functionalities that has not been further subdivided at the level of detail described in this Recommendation. It is represented by the following symbol in the context of IPTV architecture:



NOTE – In the future, other groups or other Recommendations may possibly further subdivide these functional blocks.

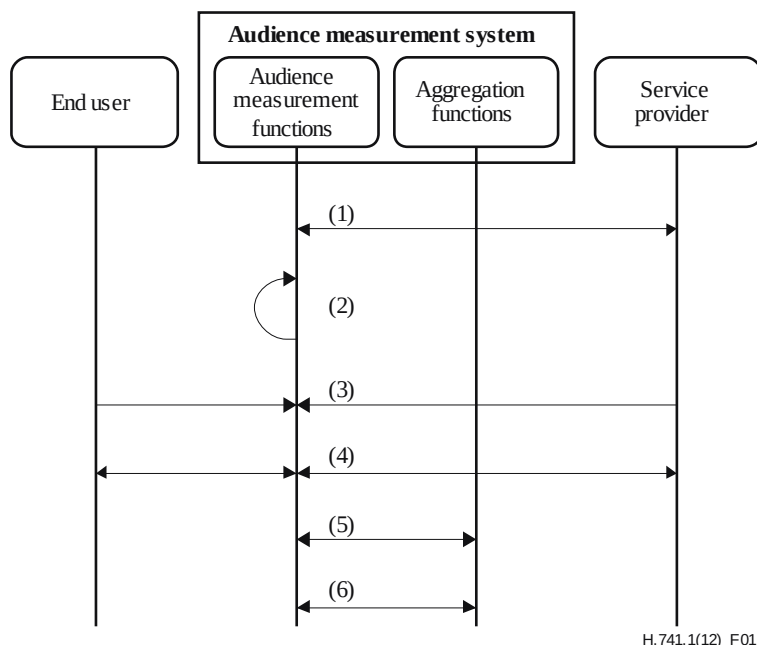
6 Preconfiguration

Prior to a terminal device audience measurement function (TD-AMF) being configured to run audience measurement functions, it first discovers, selects and connects to an IPTV service provider. The discovery of service providers and their services are described in [b-ITU-T H.770]. Aggregation functions may obtain information about terminal devices online from other IPTV services. A TD-AMF discovers and selects an audience measurement service; it is then configured for audience measurement before starting measurement of IPTV services. The audience measurement service may be provided: by the connected IPTV service provider, by a different IPTV service provider, or by an independent audience measurement service provider (see Appendix I of [ITU-T H.741.0]). Multiple audience measurement services may be able to measure the services of the connected IPTV service provider; in which case an end user may be given the choice to select which audience measurement service is to be used.

This Recommendation specifies:

- 1) Inputs required from discovery process
- 2) Optional inputs of permission information
- 3) AM messages.

This clause specifies how the AM system operates from start-up until configuration from the perspective of the TD-AMF.



- (1) – AM service and attribute discovery
- (2) – Determine compatible AM providers
- (3) – Optional AM service selection
- (4) – Optional input of permission information
- (5) – Authentication
- (6) – AM configuration messages

Figure 1 – Preconfiguration sequence

Figure 1 shows the sequence of operations leading to configuration of audience measurement functions by aggregation functions following discovery, selection, registration and connection to an IPTV service provider for the first time.

- 1) The TD-AMF discovers which AM providers are available for this IPTV service provider. Attributes of the AM provider are discovered, including:
 - a) Permission mode (internal, external, or hybrid) – available and preferred (mandatory). Defined in clause 7.2.
 - b) Address – one of the addresses described in points (i), (ii) or (iii) below is mandatory; multiple are possible:
 - (i) Address to which all TD-AMF AM configuration request messages are to be sent.
 1. Optional address for errors to be sent to, otherwise use address of (i).
 - (ii) Multicast address/port/source address to which the TD-AMF listens for a multicast configuration request response message.
 - (iii) Multicast address/port/source address to which the TD-AMF listens for a multicast configuration message.

- (iv) Optional addresses for responses to multicast messages.
 - 1. Optional address for errors to be sent to, otherwise no error reporting.
 - 2. Optional address for multicast configuration message acknowledgments to be sent to, otherwise use address of (iv-1) or no ack reporting.
- c) Configuration push, pull or pull and push (hybrid) mode – available and preferred, for each mode available and preferred transport protocols. Defined in [ITU-T H.741.0] and below.
- d) Available transport protocols for measurement reporting – available and preferred.
- e) Available cryptographic protocols for each of configuration and reporting – available and preferred.
- 2) The TD-AMF determines which of the AM providers matches its audience measurement capability profile. See [ITU-T H.741.2].
- 3) The end user optionally selects from among compatible AM providers.
- 4) Optional permission messages are received by the TD-AMF:
 - a) If internal permission mode, then directly from an end user.
 - b) If hybrid permission mode, then from a service provider (SP).
- 5) Authentication between TD-AMF and AGF occurs (see clause 9.1.1).
- 6) The TD-AMF becomes ready for the initial AM message:
 - a) If configuration pull, or configuration pull and push (hybrid) mode, then send a "configuration request message". The TD-AMF shall not wait for a response for more than three seconds after the "configuration request message" is sent.
 - b) If configuration push mode, then listen to multicast address.

During initial configuration, TD-AMFs are provided with all the information not already obtained from discovery, to participate in audience measurement. For both the configuration pull and the configuration pull and push (hybrid) modes, a configuration package check delay is defined, which triggers subsequent checks for availability of a new configuration package. Following activation of the first configuration package (see clause 7.1), a timer counts down the "configuration package check delay" in days.

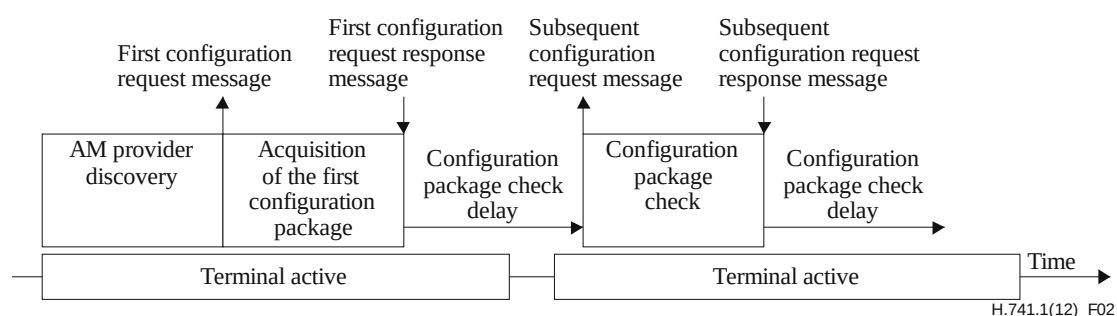


Figure 2 – Acquisition of the initial configuration package and configuration package checks

For the configuration pull mode. When the timer expires, there are two possible situations:

Situation 1: The terminal device is active; the TD-AMF then issues a configuration request message. Situation 1 is shown in Figure 2.

Situation 2: The terminal device is not active when the configuration package check delay expires, so it discovers this only after it is switched on again and gets connected to the same IPTV service provider. The TD-AMF then issues a configuration request message. Situation 2 is shown in Figure 3.

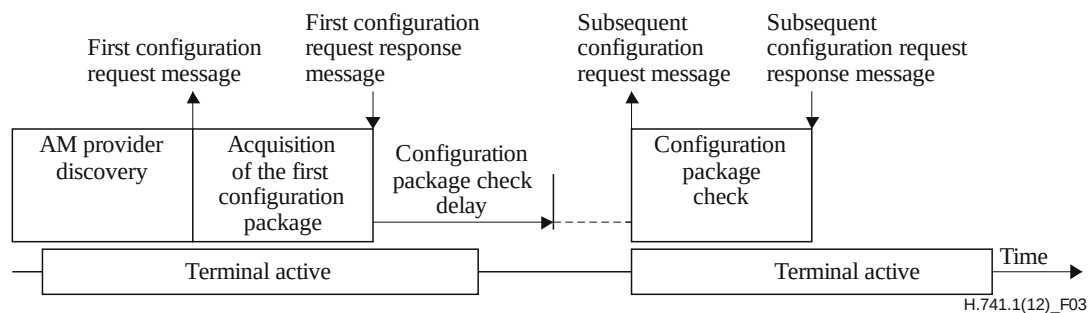


Figure 3 – Acquisition of the subsequent configuration package after delayed switch-on

The time of the initial configuration package acquisition is randomized because it is the time at which the end user connects to the IPTV service provider for the first time. To keep the configuration package check-time randomized, the time for the next configuration package check occurs on a multiple of the configuration package check delay subsequent to the initial configuration package acquisition, as illustrated in Figure 4.

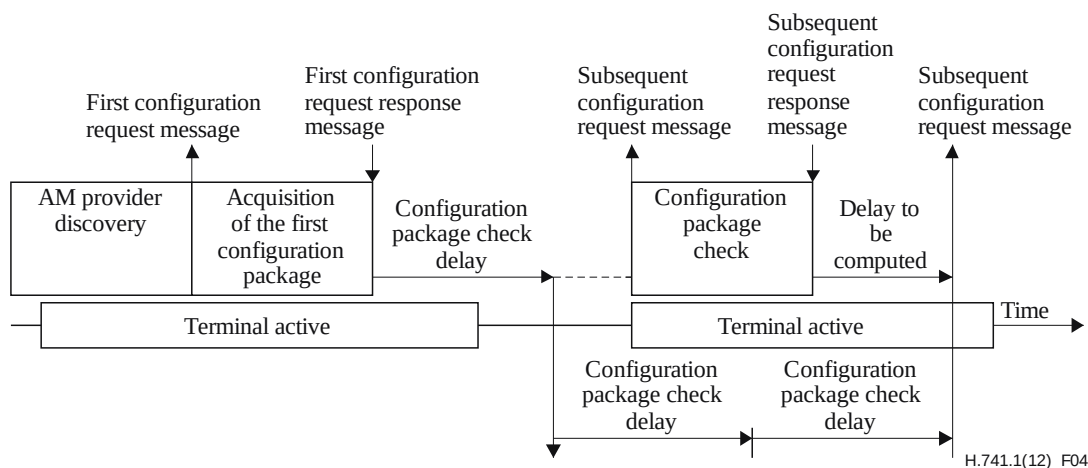


Figure 4 – Use of multiples of configuration package check delay

For pull and push (hybrid) configuration mode, a TD-AMF initially and subsequently requests configuration per the pull mode and receives pushed configuration from aggregation functions. In this mode, when a configuration push occurs the TD-AMF defers the configuration package check time until the next multiple of configuration package check delay. TD-AMF configuration requests do not occur as long as configuration messages are pushed to a TD-AMF. For pull and push (hybrid) configuration mode, the aggregation functions initially responds with a configuration request response message which uses one of the transport protocols supported in the configuration request message. If a unicast configuration request response message is used, then it must use the same transport protocol as the configuration request message.

For (unicast or multicast) push mode configuration mode, the TD-AMF listens only, and does not request configuration. Multicast configuration messages may be sent in one or more multicast-supporting transport protocols.

See [ITU-T H.741.2] for metadata elements of configuration package request response, including configuration package check delay.

7 Effective configuration of TD-AMFs

Configuration of TD-AMFs is accomplished by aggregation functions using the configuration message or configuration request response message. Effective configuration is the result of constraining the received configuration package(s) with an effective end-user permit if present in a TD-AMF. This clause specifies the configuration package and end-user permits.

7.1 Configuration package

This clause specifies the configuration of the TD-AMF. Data elements and structures are specified in [ITU-T H.741.2] and examples are provided in Appendix III. Default values are used to reduce the size of the configuration package.

Configuration packages apply to the whole configuration of the audience measurement functions. Partial updates are not directly supported and any configuration change must be made by transmitting a complete configuration package.

It is not required that the configuration values within the configuration package be validated by audience measurement functions. It is recommended that the aggregation functions validate the values, e.g., bounds checking and self-consistency, which have been placed into configuration packages before transmission.

Identical configuration packages may be sent to multiple TD-AMFs.

The configuration package consists of:

- Package header – package info.
- Measurement requests – including services to be measured, measurement schedule, events and sample values to be measured, and measurement report message delivery schedule.

7.1.1 Configuration package headers

Information related to the configuration package is distributed in multiple data structures, at the start of:

- the configuration package
- unicast and multicast XML transport of configuration messages
- unicast and multicast XML transport of configuration request response messages
- multicast binary transport of configuration and configuration request response messages.

Certain configuration capabilities are common while others have transport dependencies as follows.

7.1.1.1 Transport independent capabilities

A header indicates a message-expiration time, after which the message is not accepted. This is recommended to be set to ten minutes after message-transmission time. The message-expiration time is a security feature to minimize the impact of replay attacks.

Versioning of the AM message protocol is configurable to support its evolution. Interoperability between versions is indicated by versioning.

The compression/decompression algorithm applied to the XML payload is indicated in AM message headers.

Using an identifier, AM management tracks configuration packages. The aggregation functions generate an identifier as an AM service provider unique identifier. Versioning of the package identifier is additionally supported.

Configuration packages are sent to TD-AMFs for immediate use, or they are sent in advance and scheduled for use when they become effective. When an immediate package is received, or when the effective time arrives, the new configuration becomes effective. Any and all prior stored

measurements are reported immediately. Two configuration packages may be sent to a TD-AMF at a time, one for immediate use, the other for future use. TD-AMFs are required to handle a maximum of one immediate and one future configuration package at any one time.

A header may indicate that there is no immediate configuration package, in which case any and all prior stored measurements are reported immediately and audience measurement stops.

A configuration package check delay may be configured, which triggers subsequent checks for availability of a new configuration package.

See [ITU-T H.741.2] for metadata elements used in the configuration package header. See [ITU-T H.741.4] for metadata elements used in the delivery of unicast and multicast configuration and configuration request response messages

7.1.1.2 Multicast dependent capabilities

AM multicast messages provide four filtering capabilities to define targeted subsets of TD-AMFs which are to process the associated configuration packages.

- 1) For configuration push mode, a threshold configuration may adjust the subset size of the responding TD-AMFs. This configuration may be helpful for network congestion avoidance as the number of TD-AMFs grows. The threshold is implemented by the TD-AMF generating a random number between 0 and 10000 once at (re)-boot time, and the value is used upon receipt of every configuration message containing a threshold element.

If the generated random number is between the configured lower and upper thresholds (i.e., the threshold range), the TD-AMF configures its operation mode with the received immediate configuration package depending on end-user permissions and starts audience measurement as soon as an IPTV service is activated. If a future configuration package is also present in the received configuration message, then it is stored until the effective time.

If the random number is outside the threshold range, then the TD-AMF ignores the configuration message.

Multiple configuration messages with different threshold ranges can optionally be used to configure multiple TD-AMF subsets. The threshold ranges may be used to "address" each TD-AMF subset.

- 2) The configuration message header may be configured to specify the TD-AMF device type(s) which are to process the associated configuration package.
- 3) The configuration message header may be configured to specify the MAC addresses of the TD-AMFs which are to process the associated configuration package.
- 4) The configuration message header may be configured to specify a match to information provided by the end user to specify the target TD-AMFs which are to process the associated configuration package. The configuration also specifies whether to ignore the matching rule when the specified end-user data is not available, when the reason for not being available may be due to the end user not providing the information or to a permission restriction.

When multiples of the above sub-addressing filters are used concurrently, they must all be matched for a TD-AMF to process the associated configuration package.

Multicast headers include message integrity checks and signatures for authentication.

The configuration message header may be configured to enable optional acknowledgement messages to the multicast configuration message for operational management.

The configuration message header may be configured to enable optional error messages to the multicast configuration and multicast request response messages for operational management.

See [ITU-T H.741.4] for metadata elements of multicast headers.

7.1.2 Measurement requests

Measurement requests contain services to be measured, measurement schedules, events and sample values to be measured, and measurement report message delivery schedules.

A configuration package may contain multiple measurement requests. Some identical values may be used in multiple measurement requests. So to reduce the size of a configuration package, configuration may set values used by multiple measurement requests in a special common structure. Multiple common structures which each relate to a set of measurement requests may be configured.

A configuration may specify measurement requests which are to be conditionally processed by a TD-AMF dependent upon a match to element values associated with that TD-AMF. The elements used to qualify measurement requests may include generic (uncontrolled) information and/or identifying (controlled) end-user information. Use of this measurement request filtering capability requires that the TD-AMF be associated with a minimum end-user permission level 2 or 3 respectively. The configuration also specifies whether to ignore the matching rule where the specified end-user data is not available, when the reason for not being available may be due to the end user not providing the information or to a permission restriction. When multiple end-user information matching rules are used concurrently, they must all be matched for a TD-AMF to process the associated measurement request(s). Measurement request filtering may be used separately or in conjunction with multicast sub-addressing, including using information provided by end users (see clause 7.1.1.2).

AM management tracks measurement requests (and associated reports) using an identifier, which is to be generated by aggregation functions as an AM service provider unique identifier.

See [ITU-T H.741.2] for metadata elements used to configure sets of measurement requests.

7.1.2.1 Configuration of services to be measured

Each measurement request may be configured to indicate which specific services are to be measured (Figure 5).

A service period for each measured service is defined as the period between a service start event and a service end event. These events correspond to service-specific events such as "channel start" in linear TV or "play" in VoD.

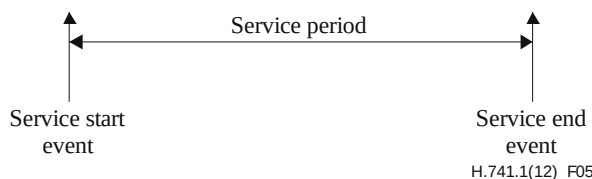


Figure 5 – Service period definition

A session is defined as a period of time for linear TV, VoD and nPVR, in which an end user is connected to a service provider (between end-user log in and log out), see Figure 6. Figure 6 shows how these relate to service periods, using linear TV as an example.

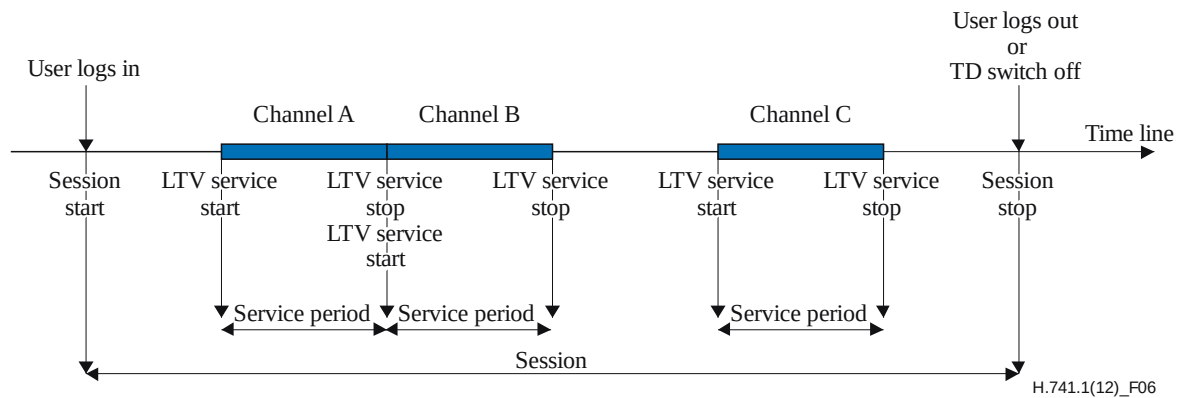


Figure 6 – Session definition

See [ITU-T H.741.2] for metadata elements used to configure the services to be measured.

7.1.2.2 Configuration of content classes to be filtered

Each measurement request may be configured to indicate whether to filter measurements across services based upon specified content classes.

Examples of content class types are (1) genres as defined by different organizations which may indicate children's TV, adult TV, religious and political programmes, etc., (2) originating studio IDs as defined by different organizations, series, or any other content classification scheme as defined by different organizations.

If content filtering is configured but a TD-AMF is unable to determine content-class information about particular content, then measurements associated with that content may occur with constraints. Measurements associated with the unclassified content shall be reported with the constraints of permission Level 1, and shall not be batched with other reports for delivery.

See [ITU-T H.741.2] for metadata elements used to configure content classes to be filtered.

7.1.2.3 Configuration of measurement schedule

Each measurement request includes one or more measurement schedules. A measurement schedule specifies when and how a requested service is to be measured. It specifies measurement periods and how generation of a measurement report will be triggered, either periodically and/or on specific events.

A measurement period is the duration of time during which measurements may occur, as illustrated in Figure 7.

Each measurement schedule may include multiple measurement periods, as illustrated in Figure 8.

Each measurement period may specify on which days of the week and at what start-and-end time measurements may occur. Each measurement period may fall within a day, or cross the boundaries of a single day. A measurement period may not be specified, in which case it is defined by the default which is "always". The number, position and duration of measurement periods per day are independent.

Measurement periods may cross day boundaries, as illustrated in Figure 9.

If a measurement period is specified to extend into a day which is not configured as a day to start measurement, the measurement period ends at the configured end time.

See [ITU-T H.741.2] for metadata elements used to configure measurement schedules.

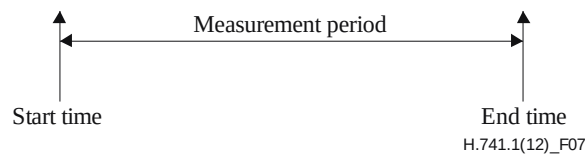


Figure 7 – Measurement period definition

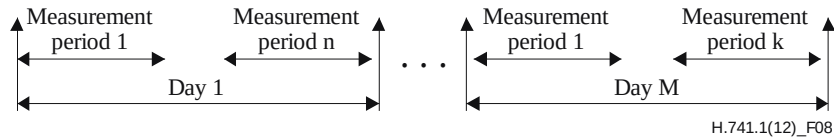


Figure 8 – Measurement schedule definition

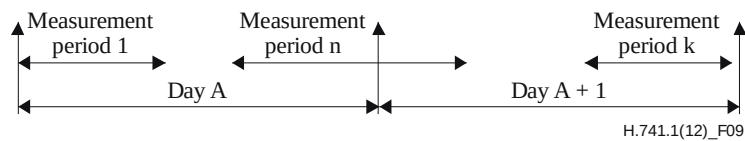


Figure 9 – Cross-day measurement period

7.1.2.4 Configuration of elements to be measured

Each measurement request is configured to indicate which events and sample values are to be measured.

The events and sample values to be measured are classified into two categories: service-common and service specific:

- "Service-common" events and samples are defined for two or more specific services. They are defined in [ITU-T H.741.2].
- "Service-specific" events and samples apply to one specific service. They are defined in [ITU-T H.741.3].

"Service-common" events and samples in a measurement request are applied to the specific services configured in that measurement request. In the case where no specific services are configured in that measurement request, then the "service-common" events and samples apply to specific services configured in any measurement request.

There are three measurement methods which may be used separately or in combination. These methods use a measurement trigger of one of the following:

- 1) An event. One of several defined end-user initiated events. The elements to be measured are specified for each event.
- 2) A scheduled sample time. Measurement by scheduled sampling is defined by a sequence of sample times with configurable periodicity, where periodicity indicates the regular periods between which measurements are to be captured during the measurement period. The elements to be measured are specified by referring to sets of elements.
- 3) A service start. Measurement by scheduling qualified service start times is defined by a configurable interval, where an interval is the period when measurements are triggered at the first service start of a day. The elements to be measured are specified by referring to sets of elements.

The basic measurement time definitions are illustrated in Figures 10 to 13.

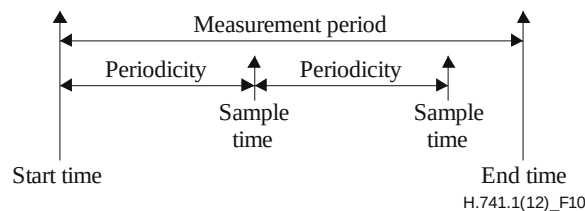


Figure 10 – Scheduled sample times

The effective measurement period is defined to be when both the measurement period and service period overlap, as illustrated in Figures 11 to 13.

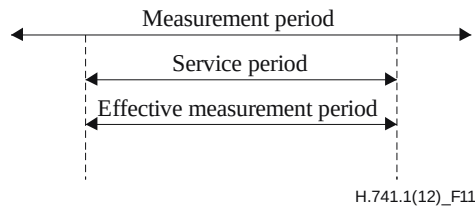


Figure 11 – Effective measurement period definition (1)

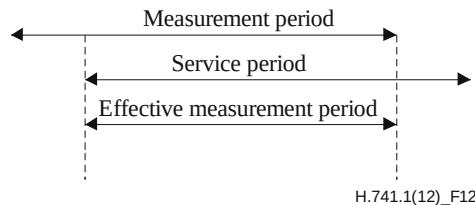


Figure 12 – Effective measurement period definition (2)

An effective measurement period may span many concatenated measurement periods, supporting measurement requests configured differently for each measurement period. In Figure 13, for example, two different sets of measurements (measurement profiles) occur during an effective measurement period.

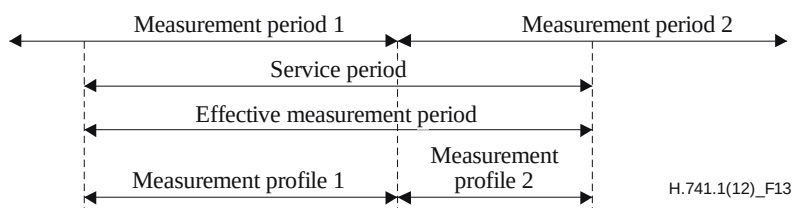


Figure 13 – Effective measurement period definition (3)

Within the effective measurement period, events and sample values are measured, as depicted in Figure 14.

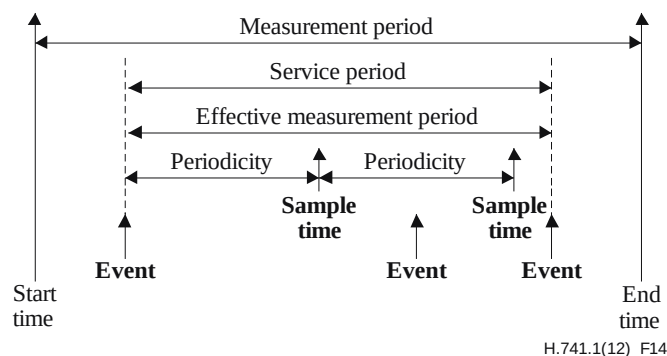


Figure 14 – Sample values and events are measured within the effective measurement period

Both service-common and service-specific events and samples are measured only during effective measurement periods.

Service specific measurements occur only during their respective specific service periods. Whereas, service-common measurements occur during the service period associated with any specific service.

Measurement requests may be configured to include either service-common only measurements, service specific only measurements, or both service-common measurements and service specific measurements.

Measurement of events and sample values may be configured following declaration of service-common and/or service specific measurements. Events and sample values may be qualified by a configured parameter. When an event or sample occurs that matches those configured for measurement, it triggers generation of a measurement report.

Most events need to be configured in a measurement request. However there is one common event which does not require configuration. This "focus" event may occur when the focus of an end user or IPTV platform changes among multiple concurrent targeted IPTV services such that the audio of a particular service is presented.

Certain service specific events and/or samples may not need to be, or be allowed to be, explicitly configured. Declaring a specific service in a measurement request may lead to certain events and/or samples being set as a default. When multiple measurement requests generate similar reports for these events (having only a difference in MeasurementRequestID), then only one report is included in a report package. The report having the lowest MeasurementRequestID is to be reported. Service specific events and samples are defined in [ITU-T H.741.3].

Service start measurements are provided for the measurement of slowly changing information. The interval may be configured to generate a measurement every M integer number of days, see Figure 15. If not configured, the default is to measure at each service start as shown in Figure 16.

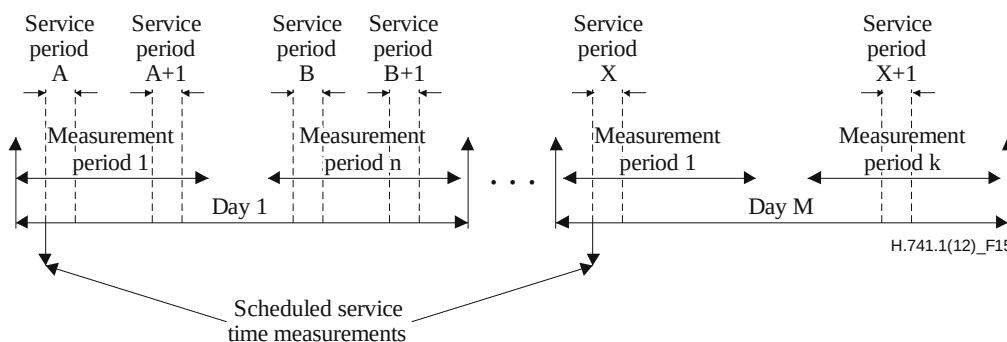


Figure 15 – Service start measurements with interval M days

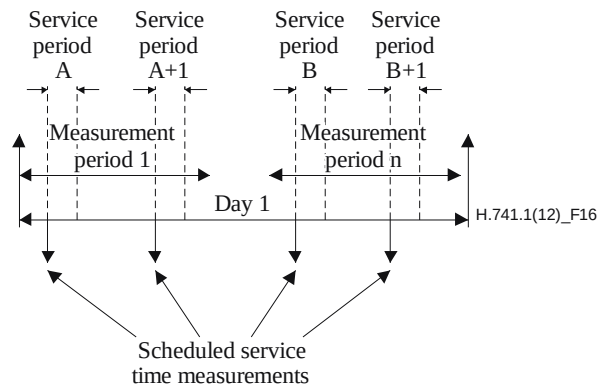


Figure 16 – Service start measurements with no interval

The service context of the service start measurement configuration determines which services are used as reporting triggers. When configured with a specific service, the first occurrence of that specific service triggers a measurement every M days, if it occurs during a measurement period. When configured within a service-common context, the first occurrence of any service triggers a measurement every M days, if it occurs during a measurement period.

Service start measurements may be configured to trigger measurements at multiple service starts within a day. The service context determines which service start trigger measurements. A specific service context causes measurements to be made at each service start of that service. (This includes channel changes for the linear TV service). A service-common context causes measurements to be made at the start of any service.

When internal or hybrid permission modes are used, the configuration may specify that if an end-user permit constrains the configured measurements due to permission level, device type or service, then that constraint will be reported. If configured, this report may be sent for any permission level, including permission level 0.

Configuration of recovery actions due to lack of storage of measurements is specified. Storage priority for events and sample values are configurable. In the case of storage congestion, the priority levels of existing stored measurements and new measurement are compared to decide whether to store the new measurement.

A storage congestion policy may be configured to either immediately push the oldest measurement reports to free up sufficient storage, or to drop enough of the lowest priority events and/or sample values to free space for new higher priority events and/or sample values. For dropping, the age of lowest priority events and/or sample values is to be used as a tie-breaking criterion. If the immediate push fails, then all measurement reports are considered for dropping. This policy may be configured to apply to multiple or to individual measurement requests.

See [ITU-T H.741.2] for metadata elements used to configure the events and sample values to be measured.

7.1.2.5 Configuration of filtering and summarization

Each measurement request may be configured to use TD-AMF filtering and summarization processing, which may filter reporting of specified events or sample values, and/or additionally report the summarized information. Filtering and summarization may apply to service-common or service-specific events and sample values.

In the cases of both service-common and service-specific time sampling.

When a sample value is found to be effectively the same as the previous sample value (a duplicate), configuration determines the reporting action to be taken. The duplicate sample value may either be ignored and not reported, reported as empty, or reported normally. When a sample set consists of

multiple elements and some of the sample values of these elements change, then the TD-AMF reports the subsequent time samples of all elements (including the unchanged ones).

Reporting of sampled geographic location is considered to be effectively the same if sample values indicate that a subsequent location is within the configured reporting distance threshold. All other timesampled values are effectively the same when their sample values are equal.

To obtain a count of events without event details, a list of events may be configured. The event counting period is delimited by either configured time periodicity or events which indicate that the user no longer views the same service. Either will terminate the current event count and start a new event count.

See [ITU-T H.741.2] for metadata used to configure reporting of geographic location and event counts. See [ITU-T H.741.2] for configuration of policy regarding duplicate sample values. See [ITU-T H.741.3] for filtering and summarization of linear TV measurement reports.

7.1.2.6 Configuration of delivery schedule

Each measurement request may include a delivery schedule which may have multiple delivery windows scheduled by time of day. One of four types of delivery modes is configured:

- 1) **Immediate Push Mode:** When a measurement is made, it is optionally grouped with a number of other measurements within a period of time, before being sent in a measurement report package message.
- 2) **Delayed Push Mode:** Measurements are stored until a TD-AMF randomly picked time during the configured delivery window is reached. At that time the TD-AMF groups measurement reports and sends them in a measurement report package message.

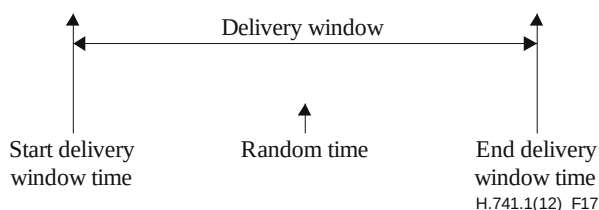


Figure 17 – Delivery window

- 3) **Pull Mode:** Measurements are stored until a measurement report request message is received from the aggregation functions. This message causes selected measurements to be grouped before being sent in a measurement report package message. A configured policy indicates what the TD-AMF does in the eventuality of storage congestion.
- 4) **Delayed Push and Pull Mode:** Measurements are stored until either a report request message is received from the aggregation function, or a TD-AMF time picked at random during the configured delivery window is reached. Whichever trigger is sooner causes measurements to be grouped before being sent in a measurement report package message.

The following are configurable for all delivery modes:

- **Delivery address(es)** – Zero or more URLs used by a TD-AMF to send measurement reports to. The value of an URL may provide an indication of the security and/or transport protocol to be used for each address. The TD-AMF will select one URL to send all measurement reports to. When not specified in a delivery schedule, an address is obtained from the special common structure or else from discovery.
- **Retransmit number** – The number of TD-AMF transmission retries when a measurement report message is not acknowledged (at the transport layer) by the aggregation functions.

When a delivery schedule is not configured, the following default is used:

- Immediate push mode.
- Delivery address URL to be used to send measurement reports from the TD-AMF as specified in the AM aggregation function discovery process or as configured in the special common structure.
- Retransmit number is configured in the special common structure.
- The storage congestion policy default applies: this is to drop enough of the lowest priority events and/or sample values to free space for new higher priority events and/or sample values. The age of the lowest priority events and/or sample values is to be used as a tie-breaking criterion.

See [ITU-T H.741.2] for metadata elements used to configure delivery schedules.

7.2 End-user permits

End-user privacy policies may be expressed within end-user permits in AM.

Permits are per end user or multiple end users in a subscription.

An end-user permit may contain an expiration date, a default permission level, and a default content restriction list. An anonymous UserID may be included if there is a permission level in the permit with a value of less than 3. The identifying UserID may be included if there is a permission level in this permit with a value of more than 2. One or more user permission sets may be specified which allow a permission level to be associated with combinations of services, terminal device types and content restrictions.

User permissions impact audience measurements depending upon one of three modes used:

- **External permission mode** – relies upon end-user permissions being managed outside of AM. No end-user permits are used at the TD-AMFs.
- **Internal permission mode** – relies on AM to manage permissions. Permits are created at TD-AMFs and may be made available to other TD-AMFs. They are delivered to the TD-AMF separately from the configuration package and configuration package request response messages.
- **Hybrid permission mode** – relies on a combination of AM and external entities to manage permissions. Permits are delivered to the TD-AMF separately from the configuration package and configuration package request response messages. They are delivered to the TD-AMF from the IPTV SP.

The TD-AMF learns of which permission mode to use from the discovery process.

Regarding multiple devices for the internal permission mode, it is not specified how permits are made available to the other devices of the same end user. For the hybrid permission mode, permits for each end-user device are made available when an end user logs in.

An effective permit is the end-user permit which is in force at a particular time. AM obtains the effective permit from functions outside of AM, which are responsible for associating end users with permits.

The effectiveness of measurement requests may be reduced when end-user permits are used. If internal or hybrid permission modes are used, then measurement reports may be limited by permission levels of the effective permit. Measurement reports may be disallowed by device type and/or service and/or content.

In internal and hybrid modes, when the TD-AMF obtains a new permit, it must apply that permit immediately to new measurements. Previously stored measurement reports may be sent without application of the new permit. Receipt of a new permit triggers the TD-AMF to send a configuration request message to aggregation functions.

If content filtering is included in the effective permit, but a TD-AMF is unable to determine content class information about particular content, then measurements associated with that content may occur with constraints. Measurements associated with the unclassified content shall be reported with the constraints of permission level 1, and shall not be batched with other reports for delivery.

User permits are optionally included in a configuration request, a configuration request response and configuration messages to support the management of permits, the details of which are out of the scope of AM.

See clause 9.2 for more details regarding permission modes.

See [ITU-T H.741.2] for the metadata elements of user permits.

8 Specific aspects of reporting

8.1 Reporting of services which start or end outside measurement periods

A ServiceInstanceID is generated when a service starts, so it may be generated outside of a measurement period. When this service is still being consumed at the start of a measurement period, then a service start event report will be generated with the time of the start of the measurement period, unless the same service start report had previously been generated. When a service end event occurs after a measurement period, then a service end event report will be generated with the time of the end of the previous measurement period.

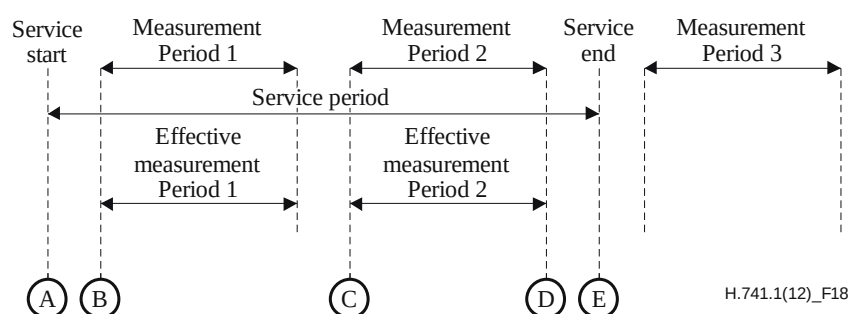


Figure 18 – Reporting of services which start or end outside measurement periods

In Figure 18, a service start event occurs at A so a ServiceInstanceID is allocated and a report is generated. If or when a measurement period starts which is configured to measure that service, then the start time B of that measurement period is associated with the service start event. The service start event is reported per the associated measurement request. If the service period continues through the time of a subsequent measurement period C, then the service start event is not reported again. If the associated service end event occurs outside a measurement period at time E, then it is associated with the time of the end of the previous measurement period D. The service end event is reported per the associated measurement request.

8.2 Reporting surrounding restricted content

Changes in genres are monitored by a TD-AMF, when restricted content starts to be played at time A in Figure 19 below, then measurements stop, and a service stop event report shall be generated. When un-restricted content starts to be played after restricted content, then

measurements may start. A service start event report shall indicate the start time B, of the unrestricted content.

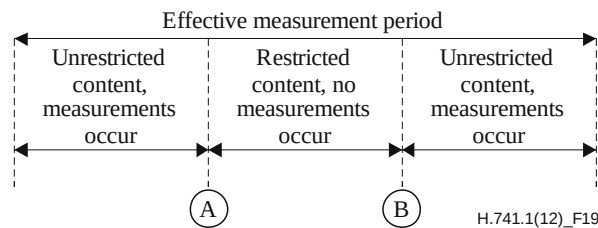


Figure 19 – Reporting surrounding restricted content

8.3 Reporting of user presence

The detected presence of end users may only be reported when the effective permit (if provided) grants permission level of 1-3.

8.4 Reporting changes due to effective permit changes

Measurement permissions may be available to the TD-AMF expressed in an effective permit. When the effective permit changes, reflecting a change in permissions granted, then measurements and reports shall immediately reflect those permission changes.

8.5 Reporting of storage congestion

In the case where event information and/or sample information has been dropped due to storage congestion and priority in a TD-AMF, indication of the services impacted is reported within the measurement report message.

8.6 Nothing to report

In the case where pull mode is used and the aggregation functions request measurement reports from a TD-AMF which has nothing to report, then no measurement report is returned by that TD-AMF.

9 Security, privacy and permission mechanisms

9.1 Security and privacy of AM messages

AM messages, if left unprotected, unverified, and unauthenticated will allow an adversary to compromise the very intention of audience measurement.

The entities of the AM architecture need to adhere to the AM security requirements in order to achieve audience measurement that is verifiably correct, unadulterated, and preserves end-user privacy – an important aspect which determines the willingness of end users to share their AM data. An algorithm or a set of algorithms can be used to provide security for AM information. The following clauses elaborate implementation considerations for each of the security requirements in the AM architecture, while leaving it to the implementer to implement them in isolation or in combination through a single algorithm/mechanism or a set of algorithms/mechanisms. In the following clauses, multiple algorithm/mechanisms are specified. For interoperability, AGFs and TD-AMFs must use the same algorithm/mechanisms. The methods of communications of choices between the entities are specified.

9.1.1 Authentication

In order to guarantee that the TD-AMF is interacting with the intended AGF, and vice versa, the TD-AMF and AGF are required to authenticate each other directly or indirectly via a third-party. This clause describes direct authentication. Indirect authentication is out of the scope of this Recommendation.

The absence of authentication would allow TD-AMFs to be configured by a rogue entity, or an aggregation function to be fed with modified/stale/garbage AM reports on behalf of TD-AMFs.

It is recommended to implement an authentication mechanism consisting of two sub-mechanisms: primary and secondary. The primary authentication mechanism must be able to perform authentication on its own. The secondary authentication mechanism is optional. An authentication mechanism requires a TD-AMF or an AGF entity to be authenticated to provide a proof of possession of credentials, e.g., password or digital certificate. Primary authentication mechanisms involve the use of actual credentials in proof generation, whereas secondary authentication mechanisms use pseudo-credentials in proof generation. An authenticator issues pseudo-credentials upon successful primary authentication. Secondary authentication mechanism can be employed for authenticating all successive communications that follow the first successfully authenticated communication.

In direct authentication mode, a TD-AMF or an AGF entity presents proof of possession of its credentials directly to the other. In indirect authentication mode, a trusted third party is involved which performs entity authentication and issues a token that in turn can be used as proof of possession of credentials. AM may support either or both authentication modes.

Depending on the use of push, pull, or pull and push (hybrid) message sequences of communication, the role of the authenticator is determined by the TD-AMF or AGF that initiates the message sequence. For example, prior to a configuration push message, the AGF must authenticate itself to the TD-AMFs, or prior to a push report message TD-AMFs must authenticate themselves to the AGF.

The first instance of authentication between a TD-AMF and an AGF takes place after service discovery but before TD-AMF configuration (see Figure 1). All successive message sequences between previously authenticated entities also need to be authenticated. Secondary authentication may be employed for such successive message sequences. The choices of cryptographic protocols for authentication are indicated in the capabilities profile (see [ITU-T H.741.2]) and in the discovery data structure (see Appendix I).

Configuration pull message sequence – Prior to the configuration request message, the TD-AMF authenticates the AGF using transport layer security (TLS) [IETF RFC 5246] which makes use of ITU-T X.509v3 [ITU-T X.509] digital certificates. TD-AMFs do not accept configuration packages from an AGF without this type of authentication. This requires the AGF to have a valid digital certificate issued by a Certification Authority (CA). TD-AMFs need to authenticate themselves before sending configuration response error messages. TD-AMFs use their digital certificates to authenticate themselves with the AGFs. In the absence of digital certificates issued to TD-AMFs, TD-AMFs must use their respective UserID and corresponding password issued at the time of registration with IPTV SP. A TD-AMF may obtain a token from its IPTV SP, which can be used as a credential for authentication with the AGF. The AGF trusts the IPTV SP in such a type of indirect authentication. To minimize the cost of authentication for successive AM communications between the TD-AMF and AGF, a secondary authentication mechanism one-time password (OTP) [ITU-T X.1153] or hash-based message authentication code (HMAC) [FIPS PUB 198-1] may be communicated outside of AM and used.

Configuration push message sequence – Prior to the configuration message, the AGF authenticates itself to TD-AMFs using transport layer security (TLS) as above. Prior to sending a configuration acknowledgement or configuration error message, TD-AMFs need to authenticate themselves to the AGF as above.

Configuration pull and push message sequence – This requires the authentication combination of the pull message sequences, and may require authentication of the push message sequences, depending upon whether the pull message sequence authentication has expired.

Measurement report pull sequence – If the previous primary authentication has expired, then prior to the measurement report request message, the AGF needs to authenticate itself to the TD-AMFs again using primary mechanism. If the previous primary authentication has not expired, then a measurement report request message can continue to use the secondary authentication mechanism. Prior to sending a measurement report message or measurement report request error message, a TD-AMF needs to authenticate itself to an AGF as above. The measurement report error message may not need separate authentication, depending upon the transport mechanism.

Measurement report push sequence – If the previous primary authentication has not expired, then a measurement report message can continue to use the secondary authentication mechanism. If the previous authentication has expired, then prior to sending a measurement report message, a TD-AMF needs to authenticate itself to an AGF as above. If the previous primary authentication has expired, then prior to responding with a measurement report error message, the AGF needs to authenticate itself. Depending upon the transport mechanism, the measurement report error message may not need separate authentication.

AM messages that are not authenticated are not accepted.

All measurement report message sequence authentications must expire at the end of a delivery period. Optionally, implementers can choose an expiration period smaller than the delivery period specified in a configuration package by an AGF. All configuration message sequence authentication must expire at the end of a configuration message sequence.

A change in internal and hybrid permissions on a TD-AMF will cause the expiration of all on-going communications and reinitiate authentication with an AGF.

9.1.2 Confidentiality

In order to safeguard end-user privacy, it is required that all unicast AM messages be encrypted. It is recommended that all multicast AM messages be encrypted. For unicast and multicast messages see [ITU-T H.741.4].

The absence of confidentiality would allow an unauthorized entity to understand AM messages. This could lead to theft of information, uncovering of personal end-user information which could contribute to identity theft, etc. In addition, it would make it easier to conduct attacks on the AM system.

The choices of cryptographic protocols for confidentiality are indicated in the capabilities profile and in the discovery data structure.

Confidentiality is usually achieved with the help of cryptographic protocols that support encryption/decryption. The TLS protocol [IETF RFC 5246] supports an array of negotiable encryption/decryption methods that require cryptographic keys to perform the encryption or decryption operations on the data. Cryptographic keys are generated and shared between a TD-AMF and an AGF at the end of successful authentication. In the case of digital certificates not being issued to TD-AMFs, it is recommended that the TLS-SRP [b-IETF RFC 5054] protocol be used to establish the cryptographic keys. The choices are indicated in the capabilities profile and in the discovery data structure.

For TD-AMFs that do not make use of the TLS protocol for key agreement and key distribution, (e.g., smart-card-based TD-AMFs that have pre-shared keys), it is recommended to use AES [b-FIPS PUB 197].

In Figure 20, authentication and confidentiality are shown for the configuration pull message sequence.

In Figure 21, authentication and confidentiality are shown for the configuration push message sequence. If the previous primary authentication has expired, an AGF must authenticate itself before sending a configuration message.

For configuration of pull and push (hybrid mode), authentication and confidentiality occur as in Figure 20, followed by Figure 21.

In Figure 22, authentication and confidentiality are shown for the measurement report pull message sequence.

In Figure 23, authentication and confidentiality are shown for the measurement report push message sequence.

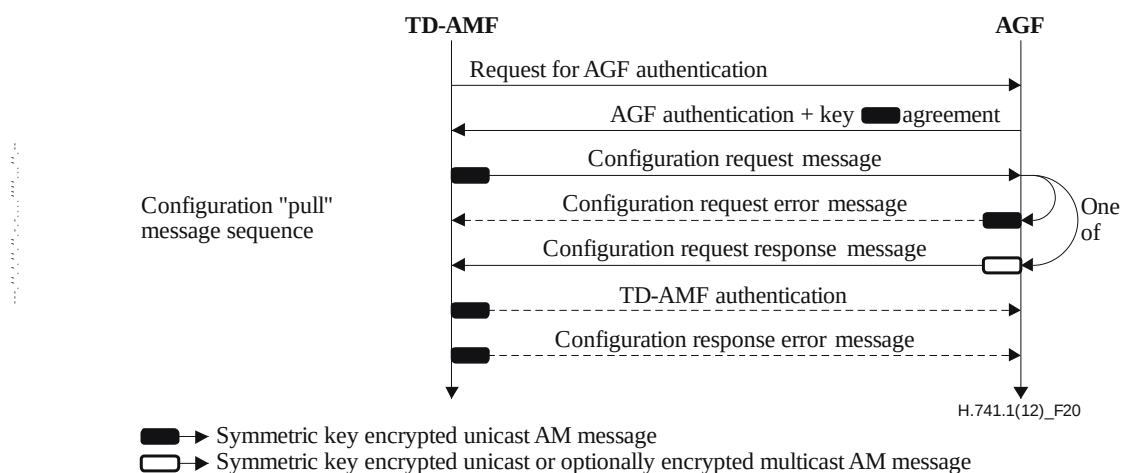


Figure 20 – Security in the configuration "pull" message sequence

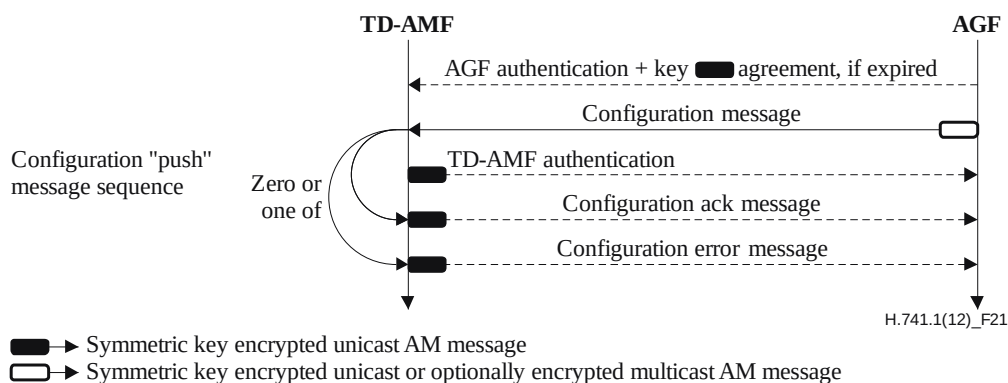


Figure 21 – Security in the configuration "push" message sequence