International Telecommunication Union

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

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.

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/.

Table of Contents

Page

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.

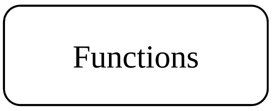
The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

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.

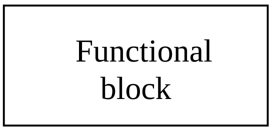
The keywords "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.

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.

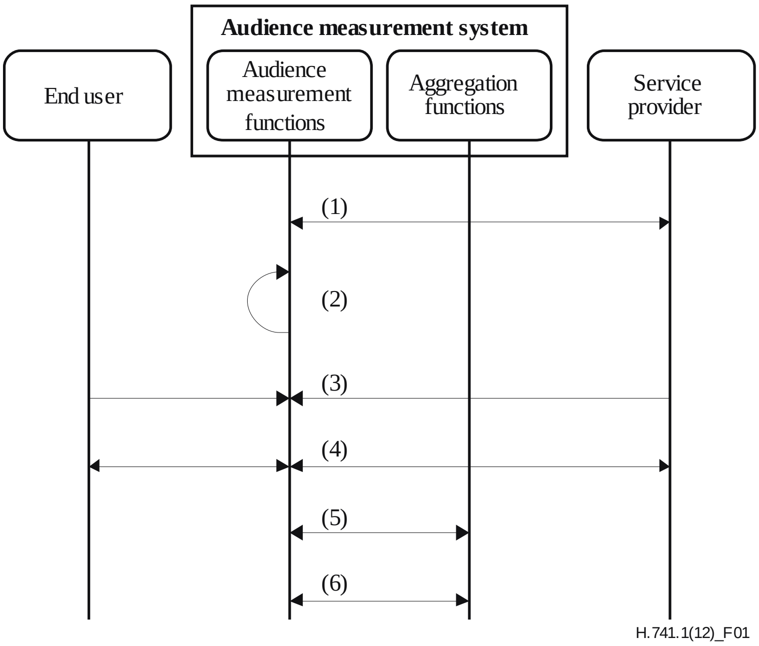
This Recommendation specifies:

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.

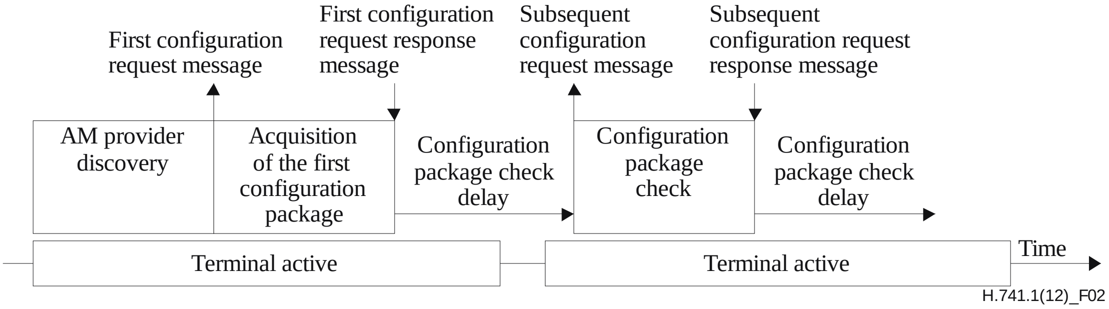

First configuration request message
First configuration request response message
Subsequent configuration request message
Subsequent configuration request response message
AM provider discovery
Acquisition of the first configuration package
Configuration package check delay
Configuration package check
Configuration package check delay
Terminal active
Terminal active
Time
H.741.1(12)_F02

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.

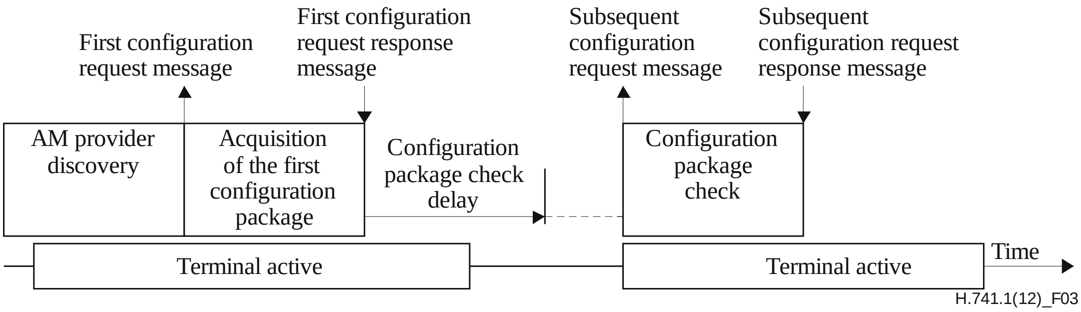

First configuration request message
First configuration request response message
Subsequent configuration request message
Subsequent configuration request response message
AM provider discovery
Acquisition of the first configuration package
Configuration package check delay
Configuration package check
Terminal active
Terminal active
Time
H.741.1(12)_F03

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.

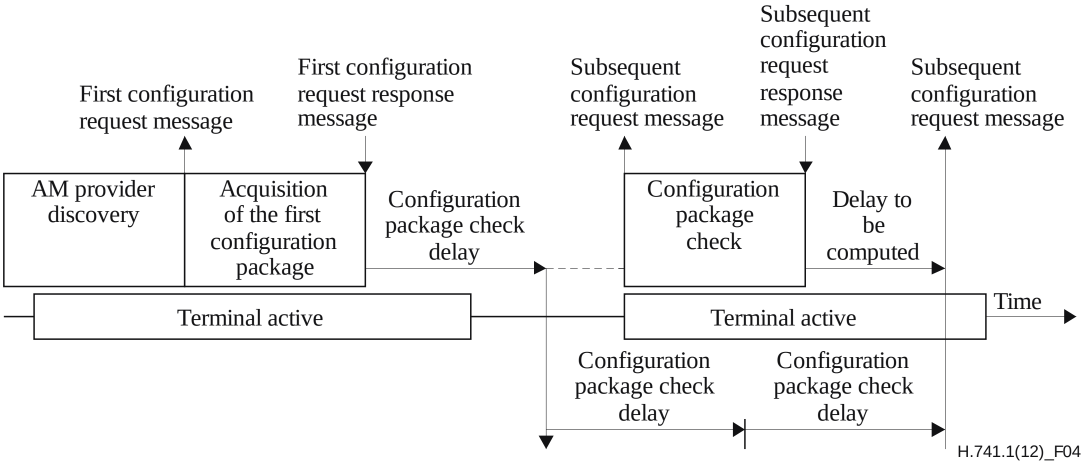

First configuration request message
First configuration request response message
Subsequent configuration request message
Subsequent configuration request response message
Subsequent configuration request message
AM provider discovery
Acquisition of the first configuration package
Configuration package check delay
Configuration package check
Delay to be computed
Terminal active
Terminal active
Time
Configuration package check delay
Configuration package check delay
H.741.1(12)_F04

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.

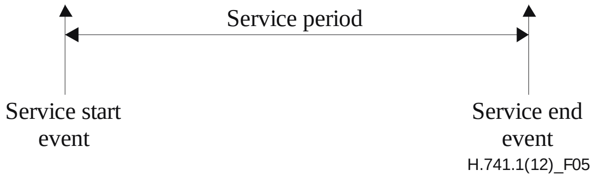


Figure 5 – Service period definition

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.

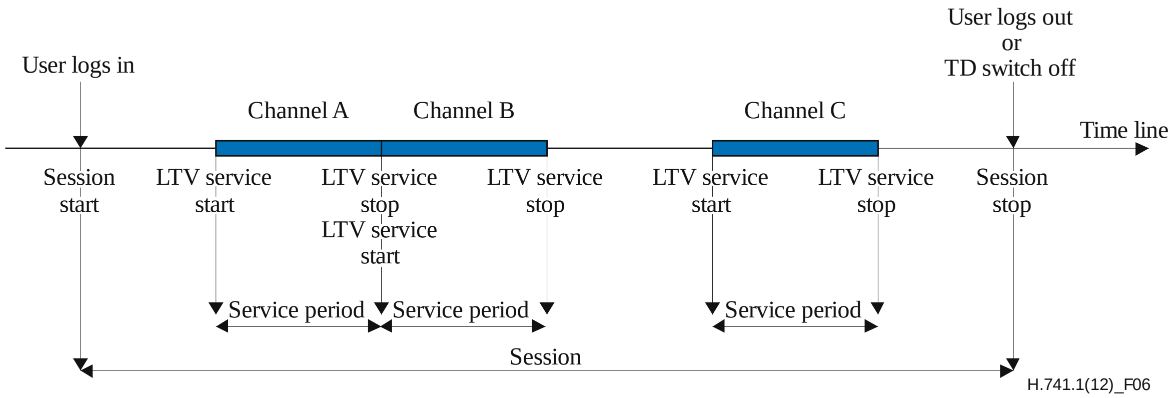


Figure 6 – Session definition

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.

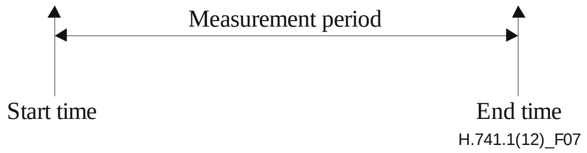


Figure 7 – Measurement period definition

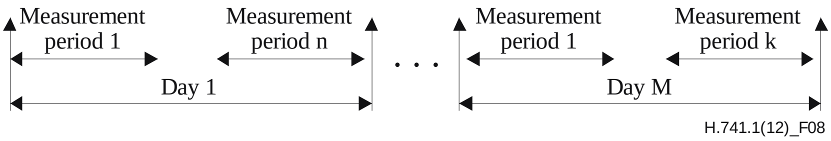


Figure 8 – Measurement schedule definition

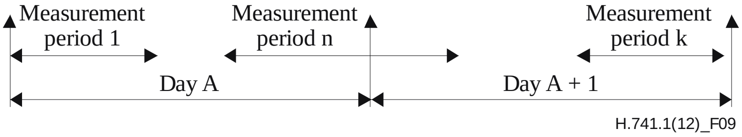


Figure 9 – Cross-day measurement period

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.

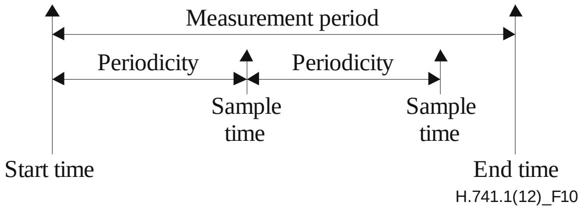


Figure 10 – Scheduled sample times

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

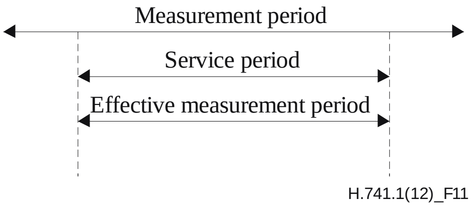


Figure 11 – Effective measurement period definition (1)

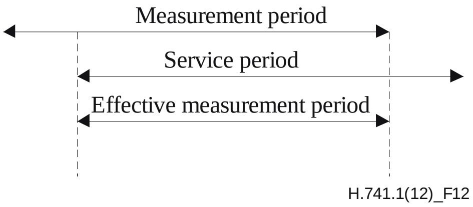


Figure 12 – Effective measurement period definition (2)

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.

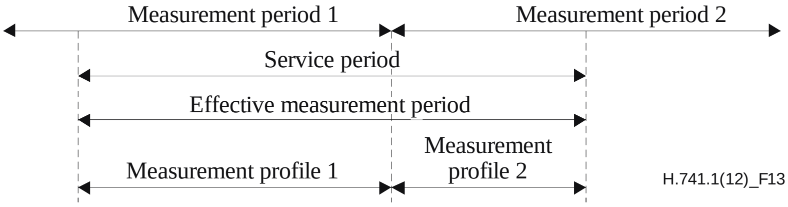


Figure 13 – Effective measurement period definition (3)

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

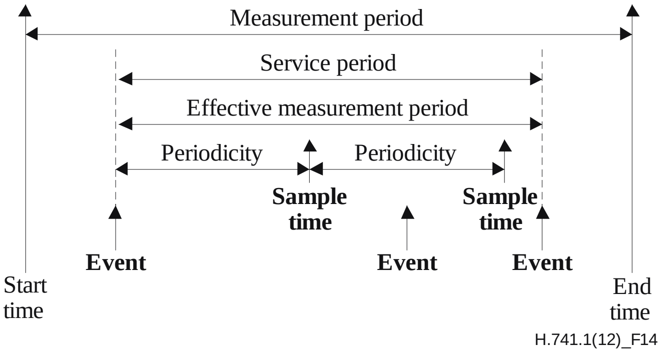


Figure 14 – Sample values and events are measured within the effective measurement period

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.

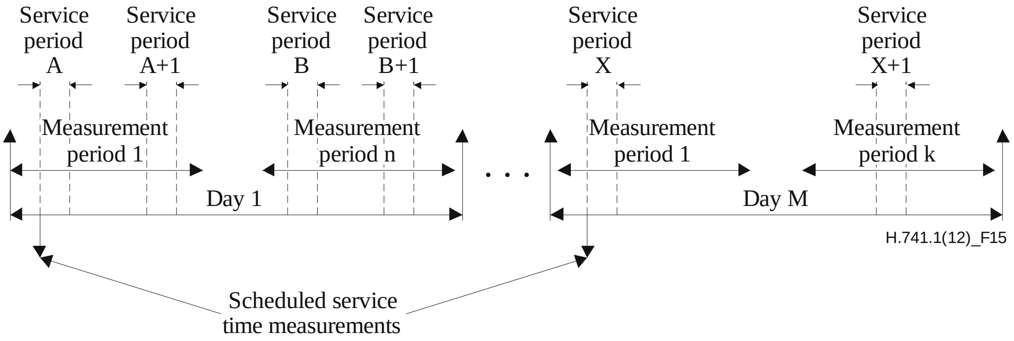


Figure 15 – Service start measurements with interval M days

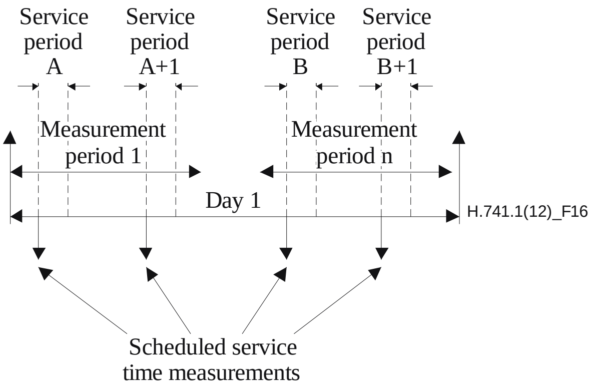


Figure 16 – Service start measurements with no interval

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.

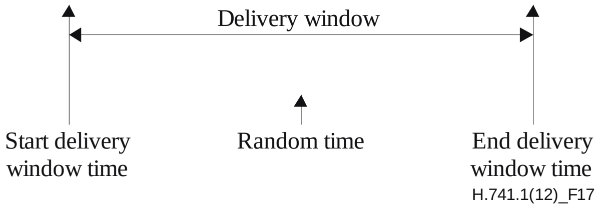


Figure 17 – Delivery window

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.

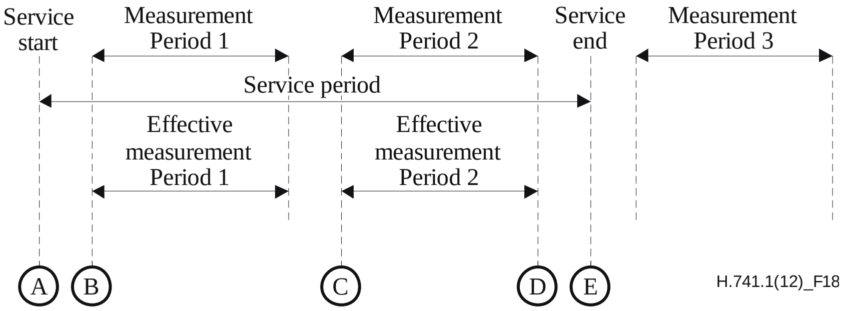


Figure 18 – Reporting of services which start or end outside measurement periods

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 un-restricted content.

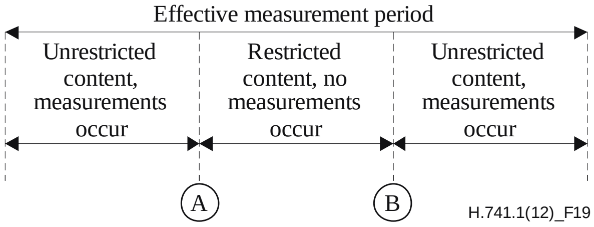

Effective measurement period
Unrestricted content, measurements occur
Restricted content, no measurements occur
Unrestricted content, measurements occur
A
B
H.741.1(12)_F19

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.

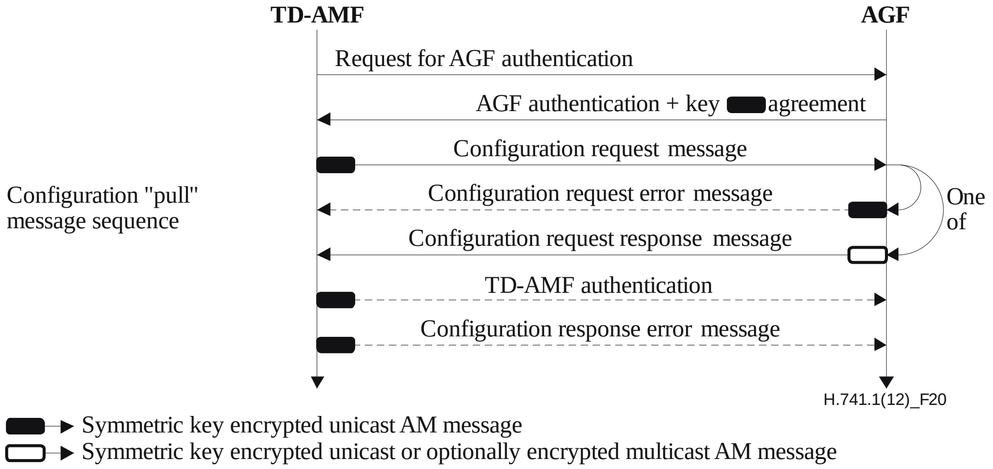

TD-AMF
AGF
Request for AGF authentication
AGF authentication + key agreement
Configuration request message
Configuration "pull" message sequence
Configuration request error message
One of
Configuration request response message
TD-AMF authentication
Configuration response error message
H.741.1(12)_F20
Symmetric key encrypted unicast AM message
Symmetric key encrypted unicast or optionally encrypted multicast AM message

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

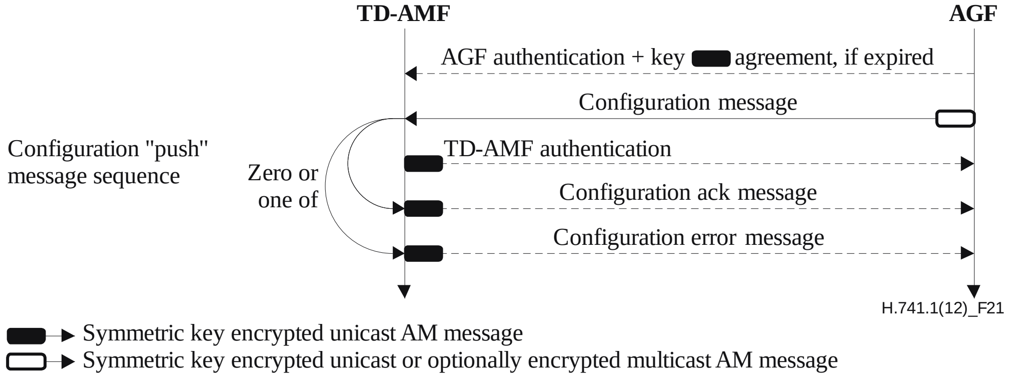

TD-AMF
AGF
AGF authentication + key agreement, if expired
Configuration message
Configuration "push" message sequence
Zero or one of
TD-AMF authentication
Configuration ack message
Configuration error message
H.741.1(12)_F21
Symmetric key encrypted unicast AM message
Symmetric key encrypted unicast or optionally encrypted multicast AM message

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

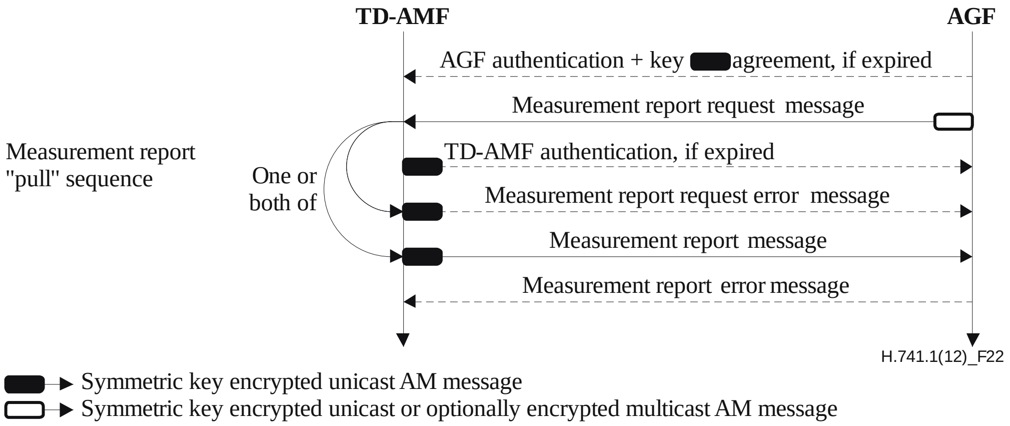

TD-AMF
AGF
AGF authentication + key agreement, if expired
Measurement report request message
TD-AMF authentication, if expired
Measurement report request error message
Measurement report message
Measurement report error message
Measurement report
"pull" sequence
One or
both of
H.741.1(12)_F22
Symmetric key encrypted unicast AM message
Symmetric key encrypted unicast or optionally encrypted multicast AM message

Figure 22 – Security in measurement report "pull" sequence

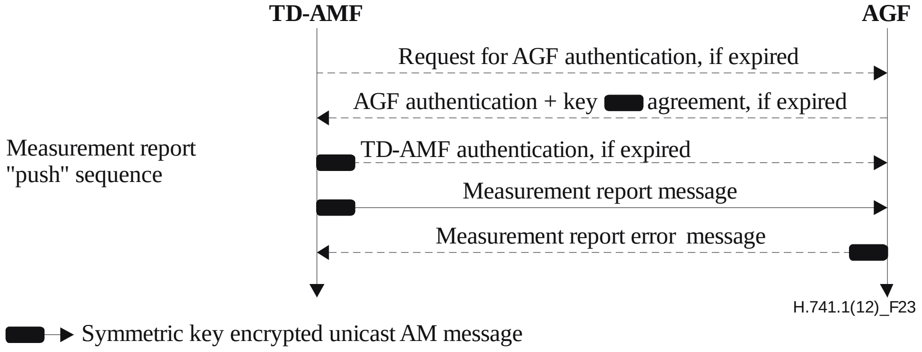

TD-AMF
AGF
Request for AGF authentication, if expired
AGF authentication + key agreement, if expired
TD-AMF authentication, if expired
Measurement report message
Measurement report error message
Measurement report
"push" sequence
H.741.1(12)_F23
Symmetric key encrypted unicast AM message

Figure 23 – Security in measurement report "push" sequence

9.1.3 Integrity

In order to ensure that the AM messages are not modified by an attacker, it is required that all AM messages include a proof to ensure that their data is unmodified. In order to ensure that the AM messages are not used in a replay attack, it is required that all AM messages are valid in time. Receivers discard messages for which modification checks or valid time checks fail.

The absence of modification and valid time indicators will allow attackers to misconfigure TD-AMFs, and to falsely trigger abnormal situation responses.

Every AM message has its own expiration time. Every multicast message also has its own cryptographic digest (SHA-256) and a digital signature (RSA-1024).

9.1.4 Non-repudiation (see [b-ITU-T X.800])

In order to ensure the authenticity of AM information, it is required to guarantee the authenticity of data received.

The absence of non-repudiation will allow an authenticated malicious entity to deny its actions.

The AM messages for which non-repudiation is most important are the measurement reports which are expected to be audited to certify the output of AM. The inclusion of signatures provides non-repudiation for AM reports.

9.1.5 Privacy

In order to support privacy, it is recommended that the protection of end-user information and identity, and AM message unlinkability, be supported.

In the absence of protection over end-user information and identity, an end-user's privacy policy cannot be met. This would effectively restrict the information that the AM system could support due to a lack of end-user trust, e.g., voluntary end-user controlled information.

The AM system supports mechanisms to protect end-user information and identification within the AM data structures. End-user information elements are classified as "controlled" or "uncontrolled", which supports differentiated handling. End-user permission levels (see [ITU-T H.741.0]) are used to control the reporting by TD-AMFs of end-user information and to choose to use either AnonID vs. UserID (see [ITU-T H.741.2]) for identity control.

In order to achieve unlinkability between a sender and its AM report, it is recommended to provide sender-anonymity.

In the absence of unlinkability, a receiver can correlate the sender of the AM report message with other information previously or subsequently obtained. For example, an AGF may use the IP address of a TD-AMF to correlate anonymous AM report messages with stored information to de-anonymize the TD-AMF.

The AM system relies upon the AGF to remove unintentional linkability information before providing information to higher functions. The details of such filtering are out of the scope of this Recommendation. Further considerations regarding unlinkability are discussed in Appendix V.

9.1.6 Summary of security methods and corresponding algorithms

The security methods and corresponding algorithms used for downstream and upstream AM messages are summarized in Table 1.

Table 1 – Security methods and corresponding algorithms

Security capabilities	**Security methods and corresponding algorithms**							
	Downstream AM messages				**Upstream AM messages**			
	AGF →		**TD-AMF**		**TD-AMF →**		**AGF**	
	Method	**Algorithm**	**Method**	**Algorithm**	**Method**	**Algorithm**	**Method**	**Algorithm**
Authentication	Digital certificate	RSA-1024	Digital certificate verification	RSA-1024	Digital certificate or password	RSA-1024 or TLS-SRP	Digital certificate or password verification	RSA-1024 or TLS-SRP
Confidentiality	(preceded by authentication for key agreement) Symmetric key encryption	AES-256	Symmetric key decryption	AES-256	(preceded by authentication for key agreement) Symmetric key encryption	AES-256	Symmetric key decryption	AES-256
Integrity	Hash generation + optional digital signature (for multicast)	SHA-256 + RSA-1024	Hash verification + optional digital signature verification (for multicast)	SHA-256 + RSA-1024	–	–	–	–

9.2 End-user permission operation modes

This Recommendation includes three modes to support the requesting, receipt, and storing of an end-user response and to ensure that measurement happens with end-user permission. A summary description of these modes is provided in the following clauses.

Deployment considerations of end-user permission modes are discussed in Appendix II.

9.2.1 External permission mode

In external permission mode, an IPTV SP is responsible for obtaining permits and is responsible for using those permits.

The request and receipt of end-user permissions occur within the IPTV SP system. In this mode, AM end-user permissions are part of the end-user information stored by the IPTV service provider. The IPTV SP provides the tool to allow the end users to set their AM end-user permissions for the different services it offers, e.g., telephone, web page or linear TV customer-care channel. The details of the tool are out of the scope of this Recommendation.

When an IPTV SP obtains end-user permissions, an IPTV SP function may combine one or more end-user permits into an effective permit. The effective permit is used to constrain configuration directives which are inputs to the aggregation functions. The details of configuration directives are out of the scope of this Recommendation. The aggregation functions configure the TD-AMFs with configurations for sets of end users that have given similar permissions.

In this mode, a TD-AMF does not have access to end-user permits. Figure 24 illustrates the different steps of the IPTV system operation with a focus on the use of the external permission mode. The configuration pull mode message sequence is shown in the figure, however the permission mode is independent of the configuration mode, so either the configuration push mode or the configuration hybrid mode could be used.

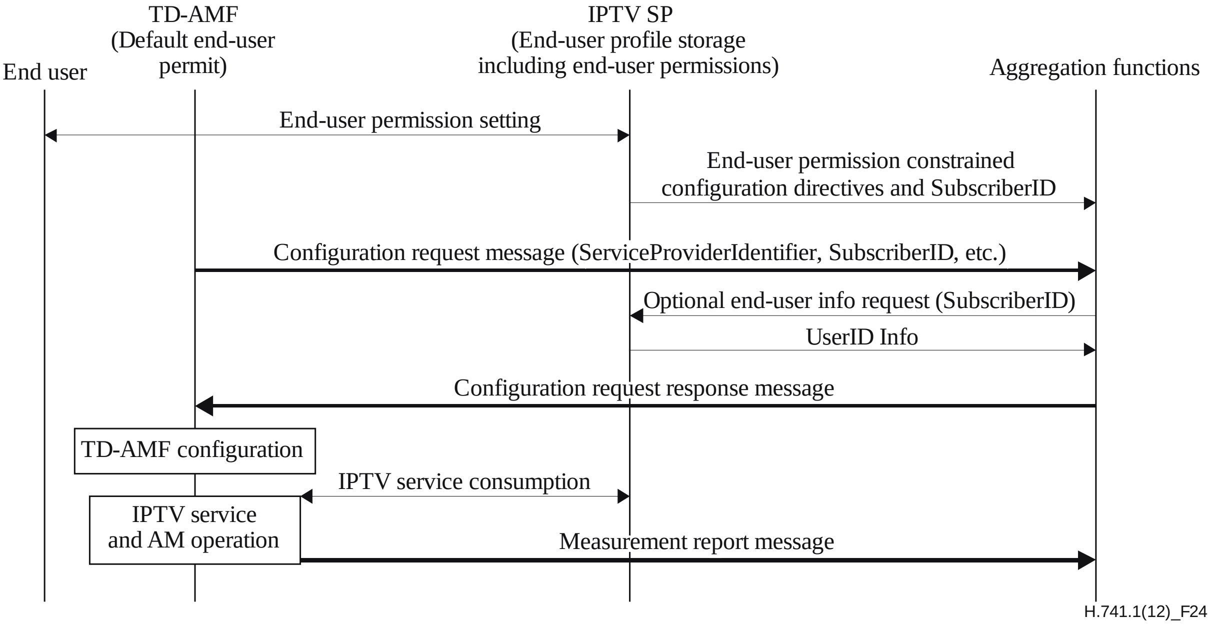

TD-AMF
(Default end-user
permit)
IPTV SP
(End-user profile storage
including end-user permissions)
End user
Aggregation functions
End-user permission setting
End-user permission constrained
configuration directives and SubscriberID
Configuration request message (ServiceProviderIdentifier, SubscriberID, etc.)
Optional end-user info request (SubscriberID)
UserID Info
Configuration request response message
TD-AMF configuration
IPTV service consumption
IPTV service
and AM operation
Measurement report message
H.741.1(12)_F24

Figure 24 – Permission flows in external permission mode

NOTE 1 – The "SubscriberID" is an identifier generated by the IPTV SP. Multiple end-users may be represented by the single SubscriberID and the associated end-user permit.

NOTE 2 – End-user permission setting is optional before the first connection to the IPTV service provider. The default "AM user permission level" is "no AM permitted".

NOTE 3 – After connection to the IPTV service provider, the end user may modify its AM end-user permissions at any time, like the other elements of its end-user information stored by the IPTV service provider. When the modification of the end-user permit may have an impact on the previously delivered configuration package, the IPTV SP issues a revised configuration directive.

Use of the external permission mode may constrain the use of multicast sub-addressing (see clause II.3.1).

9.2.2 Internal permission mode

In internal permission mode, an AM SP is responsible for obtaining permits and is responsible for using those permits.

In this mode, the request and receipt of end-user permission occurs within the AM system. TD-AMFs support the ability to ask for an end user's permission, and store responses. They are capable of autonomously re-asking for an end user's permission just prior to expiration of previously granted permission. The details of the interaction between the end user and the TD-AMF, e.g., interactive pop-up or EPG, are out of the scope of this Recommendation.

Specific measurements in the received configuration package may be disallowed by the TD-AMF depending upon the end-user permissions. Using this mode, AM enables or disables measurements across multiple-federated (federated opt-in, where end-user consent for audience measurements on one device in a home is extended to cover multiple devices in that home) audience measurement devices via messages relayed by the aggregation functions. Note that messages to support federation of permits between aggregation functions and TD-AMFs are out of the scope of this Recommendation.

In this mode, the configuration process does not need to know about end-user permissions. Figure 25 illustrates the different steps of the IPTV system operation with a focus on the use of internal permission mode. The configuration pull mode message sequence is shown in Figure 25. However, permission mode is independent of configuration mode, so either configuration push mode or configuration hybrid mode could be used.

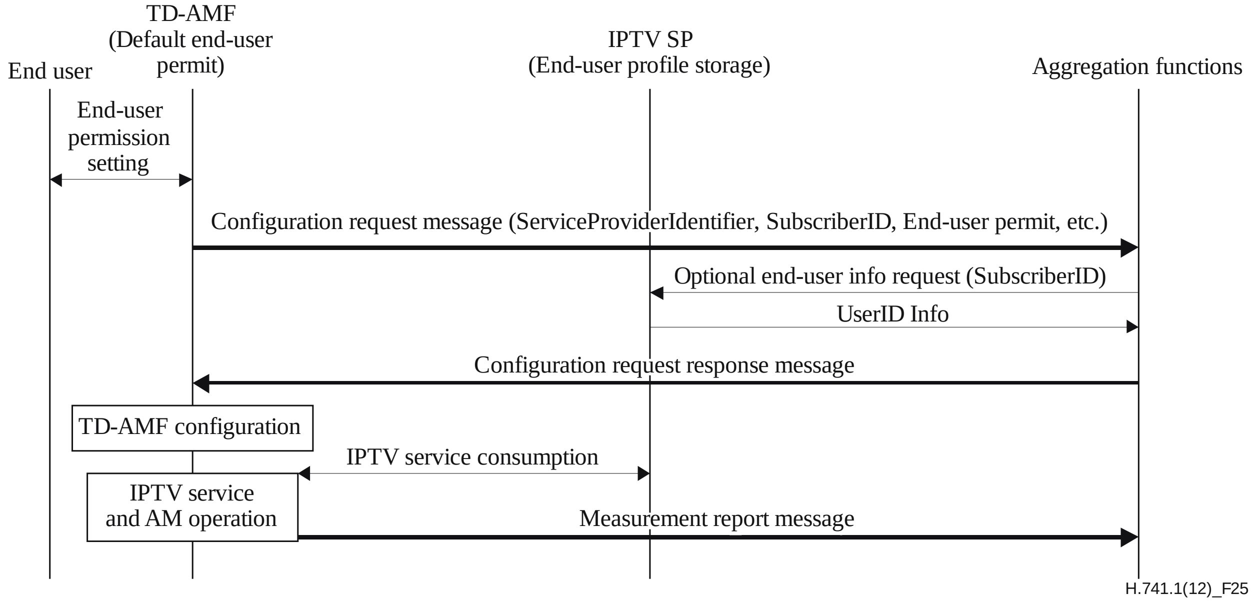

End user
TD-AMF
(Default end-user permit)
IPTV SP
(End-user profile storage)
Aggregation functions
End-user permission setting
Configuration request message (ServiceProviderIdentifier, SubscriberID, End-user permit, etc.)
Optional end-user info request (SubscriberID)
UserID Info
Configuration request response message
TD-AMF configuration
IPTV service consumption
IPTV service and AM operation
Measurement report message
H.741.1(12)_F25

Figure 25 – Permission flows in internal permission mode

NOTE 1 – The "SubscriberID" is an identifier generated by the IPTV SP. Multiple end-users may be represented by the single SubscriberID and the associated end-user permit.

NOTE 2 – End-user permission setting is optional before the first connection to the IPTV service provider. The default "AM user permission level" is "no AM permitted".

NOTE 3 – The end user may modify its AM end-user permissions at any time. Any impact on measurements is immediate.

9.2.3 Hybrid permission mode

In hybrid permission mode, an IPTV SP is responsible for obtaining permits and an AM service provider is responsible for using those permits.

The request and receipt of end-user permissions occur within the IPTV SP system. In this mode, AM end-user permissions are part of the end-user information stored by the IPTV service provider. The IPTV SP provides the tool to allow the end users to set their AM end-user permissions for the different services it offers.

The TD-AMF gets the permit from the IPTV SP system, and may use the permit for local filtering, or send it to the aggregation functions to filter configuration packages. The messages to support distribution of permits from the IPTV SP to TD-AMFs are out of the scope of this Recommendation.

The TD-AMF supports the ability to access and use end-user permits to:

– get permits from the IPTV service provider.

– send permits to the aggregation functions.

– locally filter audience measurement requested by the AM service provider depending upon these permits.

– report audience measurement with all the elements or part of the elements requested by the AM service provider, depending upon these permits.

Figure 26 illustrates the different steps of the IPTV system operation with a focus on the use of hybrid permission mode. The configuration pull mode message sequence is shown in the figure. However, permission mode is independent of configuration mode, so either configuration push mode or configuration hybrid mode could be used.

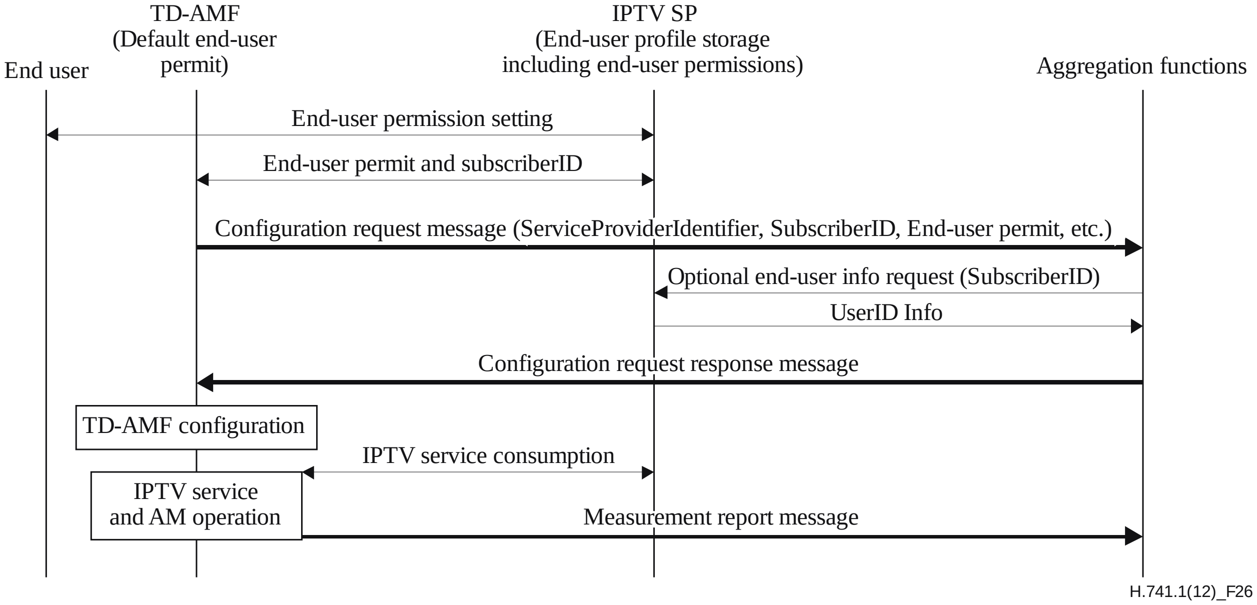

End user
TD-AMF
(Default end-user
permit)
IPTV SP
(End-user profile storage
including end-user permissions)
Aggregation functions
End-user permission setting
End-user permit and subscriberID
Configuration request message (ServiceProviderIdentifier, SubscriberID, End-user permit, etc.)
Optional end-user info request (SubscriberID)
UserID Info
Configuration request response message
TD-AMF configuration
IPTV service consumption
IPTV service
and AM operation
Measurement report message
H.741.1(12)_F26

Figure 26 – Permission flows in hybrid permission mode

NOTE 1 – The "SubscriberID" is an identifier generated by the IPTV SP. Multiple end-users may be represented by the single SubscriberID and the associated end-user permit.

NOTE 2 – End-user permission setting is optional before the first connection to the IPTV service provider. The default "AM user permission level" is "no AM permitted".

NOTE 3 – After connection to the IPTV service provider, the end user may modify its AM end-user permissions at any time, like the other elements of its end-user information stored by the IPTV service provider. The distribution of the modified end user permit is out of scope of this Recommendation. When the modification of the end-user permit may have an impact on the configuration package it received, then the TD-AMF sends a configuration request message.

10 Abnormal situations and potential recovery actions

Abnormal situations happen during the procedures of discovery, configuration, storing, and reporting AM data. Abnormal situations occurring during discovery are beyond the scope of this Recommendation. Abnormal situation types related to configuration, storing and reporting AM data are defined in Table 2, with associated potential recovery actions.

Table 2 – Abnormal situations and potential recovery actions

Abnormal situation name	Abnormal situation description	Potential recovery action
Message high-level error	A received AM message has high-level errors	TD-AMF or aggregation functions responds to the message sender with an error message, and ErrorCode defined by HighLevelErrorCode in Table 8 of [ITU-T H.741.2], e.g., not well-formed XML message (syntax error), or invalid XML message (not compliant with the schema). Upon receipt of an error message for push sequence messages, and pull sequence request messages; the message sender may rebuild and resend the message if different. After receipt of an error message for pull sequence response messages, if the message sender receives the same request it is not recommended to issue the same response. If high level errored messages from a TD-AMF persist following an error response, then aggregation functions may either ignore messages, and/or attempt to re-configure the TD-AMF to correct the problem or turn off AM.
Configuration message or configuration request response message error	A TD-AMF detects an error in a received configuration request response message or a configuration message (Note)	TD-AMF responds to aggregation functions with an error message with ErrorCode defined in ConfigPackageErrorInfo in Table 8 of [ITU-T H.741.2], e.g., element not supported, element information not available, element not permitted, event not supported. Upon receipt of the configuration error message, aggregation functions analyses the error message and may rebuild a subset or all of the configuration message and re-sends if different. After receipt of a configuration response error message, the aggregation functions are not recommended to issue the same configuration request response to a subsequently received configuration request message.

Table 2 – Abnormal situations and potential recovery actions

Abnormal situation name	Abnormal situation description	Potential recovery action
		When TD-AMF receives an errored configuration package in either message, it may accept and act upon the non-erroneous part of the configuration package and indicates its behaviour in the error message.
Configuration request message error	Aggregation functions detect an error in a configuration request message	Aggregation functions may respond to the TD-AMF with an error message and Error code defined in ConfigRequestError in Table 8 of [ITU-T H.741.2]. Or if the aggregation functions can safely continue despite the error then aggregation functions may send a configuration request response message. Upon receipt of the error message, a TD-AMF may rebuild a subset or all of the message and re-send if different. If the error persists then aggregation functions may either ignore the configuration request messages from that TD-AMF, send an error message, or send a configuration request response message to turn off AM.
Measurement report request message error	A TD-AMF detects an error in a measurement report request message (Note)	In unicast, and if error reporting is requested in multicast, a TD-AMF responds to the aggregation functions with an error message and ErrorCode defined in ReportRequestError in Table 8 of [ITU-T H.741.2]. If there are reports for non-errored requested MeasurementRequestIDs then the TD-AMF responds in a measurement report message. Upon receipt of the error message, aggregation functions may ignore the error message, or analyse the error message and may rebuild a subset and re-send, or rebuild all of the measurement report request message and re-send if different.
Measurement report message error	Aggregation functions detect an error in a measurement report message	Aggregation functions respond to the TD-AMF with an error message and ErrorCode defined in ReportError in Table 8 of [ITU-T H.741.2]. Upon receipt of the error message, a TD-AMF may stop sending any subsequent reports, or keep sending reports except for the errored elements of individual measurement reports, or ignore the error messages and keep sending reports if different. If the error persists then aggregation functions may either ignore the measurement

Table 2 – Abnormal situations and potential recovery actions

Abnormal situation name	Abnormal situation description	Potential recovery action
		report message messages from that TD-AMF, or not send report request message to that TD-AMF, or send a configuration message to turn off AM. Additionally, for cases where configuration push is not supported, then following an error and a subsequent configuration request message the aggregation function may send a configuration request response to turn off AM.
Storage overrun	TD-AMF has no available storage space for a new measurement report to be stored	TD-AMF action depends upon StorageCongestionPolicy defined in Table 12 of [ITU-T H.741.2], and measurement trigger Priority defined in Table 11 of [ITU-T H.741.2]. TD-AMF indicates the dropping of events and/or sample measurement in a measurement report message. Aggregation functions may take no action, or increase the frequency of measurement report request messages, or reconfigure the TD-AMF to either reduce the amount of data to be stored or to increase the frequency of reporting or both.
No measurement report message transport ack	TD-AMF does not receive a transport protocol acknowledgement from the aggregation functions following transmission of a measurement report message.	TD-AMF retries transmission of up to N duplicate measurement report messages. Where N is the RetransmitNumber defined in Table 12 of [ITU-T H.741.2]. If no transport protocol acknowledgement is received after the N retries, then either: a) the measurement reports of the measurement report message may be deleted depending upon available storage, StorageCongestionPolicy defined in Table 12 of [ITU-T H.741.2]and measurement trigger Priority defined in Table 11 of [ITU-T H.741.2], or b) the measurement report message is kept for later retransmission.
Delayed push report missed	TD-AMF misses the randomly picked reporting time in delayed push mode or delayed push and pull mode. This situation is detected when the TD-AMF resumes operation following a period of terminal inactivity or loss of network connectivity to aggregation functions.	The TD-AMF picks another random time within the delivery window when it will push the stored audience measurement reports or waits for the next delivery window.

Table 2 – Abnormal situations and potential recovery actions

Abnormal situation name	Abnormal situation description	Potential recovery action
Content filtering error	Content genre information is unavailable to support content filtering per configuration or permit.	A TD-AMF that makes measurements associated with the un-classified content shall send reports with the constraints of permission level 1, and shall not be batched with other reports for delivery.
TD-AMF sends inappropriate but valid AM messages	A – repetition of a valid AM message (following no error response) B – transmission of a valid AM message outside a valid message sequence C – transmission of a valid report message outside of valid configured reporting period.	Aggregation functions may either ignore messages, and/or attempt to re-configure the TD-AMF to correct the problem or turn off AM.
NOTE – Error message responses to unicast messages are mandatory when an error is detected. Error message responses to multicast messages are configurable.		

When a capability is not supported by a TD-AMF but the configuration message contains directives regarding that capability then the TD-AMF ignores those directives. An error message may be sent.

Appendix I

Discovery of audience measurement services by terminal devices

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

There are several possible operational options of the aggregation functions which need to be understood by TD-AMFs. It is therefore necessary for the aggregation functions to declare the available and preferred options they support, to allow the terminal devices to check at the AM service discovery time if they are able to operate with them or not, and how best to operate.

Table I.1 contains the elements to be included in [b-ITU-T H.770] for the discovery of AM services.

The notation is used in the following table to facilitate the specification of the corresponding schema:

– *Support:* 1 = mandatory (one instance), 0-1 = optional (max one instance), 0-* = (optional and multiple instances possible), 1-* = mandatory and multiple instances possible).

– *Type*: string, integer, float, etc.

– *Container:* elements are defined to group associated elements.

An alternative representation is shown in Figure I.1 which illustrates the data structure. In case of discrepancy between the alternative representation and the table, the correct information is to be found in the table.

Table I.1 – Elements to be included in [b-ITU-T H.770] for the declaration of AM services

Element	Description	Support/type	Notes or Value domain
PermissionOperation Modes	Specifies which end-user permission modes are available and preferred by aggregation functions	1-* xs:string enumeration	Values: 'External', 'Internal', 'Hybrid'
Preferred	Attribute of PermissionOperationModes The end-user permission mode is preferred	0-1 xs:boolean Default: False	NOTE – When multiple modes are available, at least one mode is not marked as preferred
Addresses	Container specifying which addresses the TD-AMF uses	1	
Unicast	Element of Addresses Container specifying which addresses the TD-AMF uses to send messages which are part of message sequences including only unicast messages	0-1	
ConfigRequest Address	Element of Unicast Address to which all TD-AMF AM configuration request messages are to be sent	0-1 URL Note 1	NOTE – For configuration pull or hybrid mode

Table I.1 – Elements to be included in [b-ITU-T H.770] for the declaration of AM services

Element	Description	Support/type	Notes or Value domain
ErrorAddress	Element of Unicast Address to which all TD-AMF configuration response error messages and configuration error messages are to be sent	0-1 URL Default: ConfigRequest Address	NOTE – For configuration pull, or hybrid, or push mode
Multicast	Element of Addresses Container specifying which addresses the TD-AMF uses to receive and send messages for message sequences including a multicast transport message	0-1	
MulticastHybrid Address	Element of Multicast This element contains the multicast address to listen to for the multicast configuration request response message	0-1 gt:ipAddressType Note 1	NOTE – For configuration pull and multicast push (hybrid) mode
MulticastHybrid AddressPort	Attribute of MulticastHybridAddress This element contains the multicast port to listen to for the multicast configuration request response message	1 xs:unsignedShort	
MulticastHybrid SourceAddress	Element of MulticastHybridAddress This element contains the multicast source address for the multicast configuration request response message	1 gt:ipAddressType	
MulticastPush Address	Element of Multicast This element contains the multicast address to listen to for the multicast configuration message	0-1 gt:ipAddressType Note 1	NOTE – For multicast configuration push mode
MulticastPush AddressPort	Attribute of MulticastPushAddress This element contains the multicast port to listen to for the multicast configuration message	1 xs:unsignedShort	
MulticastPush SourceAddress	Element of MulticastPushAddress This element contains the multicast source address for the multicast configuration message	1 gt:ipAddressType	
ErrorAddress	Element of Multicast Address to which all TD-AMF configuration response error messages and configuration error messages are to be sent	0-1 URL Default: No error reporting	NOTE – For error response following multicast configuration response or multicast configuration message

Table I.1 – Elements to be included in [b-ITU-T H.770] for the declaration of AM services

Element	Description	Support/type	Notes or Value domain
AckAddress	Element of Multicast Address to which all TD-AMF configuration acknowledge messages are to be sent	0-1 URL Default: ErrorAddress	NOTES – – For acknowledgements response following multicast configuration messages – if neither AckAddress nor ErrorAddress is present then there will be no ACK responses
ConfigurationModes	Container specifying which configuration modes are available and preferred by aggregation functions, and for each mode the available and preferred transport protocols	1	
Push	Element of ConfigurationModes Configuration push mode is available	0-1 Note 2	
Preferred	Attribute of Push Configuration push mode is preferred	0-1 xs:boolean Default: False	
TransportProtocols	Element of Push Indicates the transport protocol available	1-* xs:string enumeration	Values are out of the scope of AM
Preferred	Attribute of TransportProtocols Indicates that the transport protocol indicated by the value is preferred	0-1 xs:boolean Default: False	
Pull	Element of ConfigurationModes Internal permission mode is available	0-1 Note 2	
Preferred	Attribute of Pull Configuration push mode is preferred	0-1 xs:boolean Default: False	
TransportProtocols	Element of Pull Indicates the transport protocol available	1-* xs:string enumeration	Values are out of the scope of AM
Preferred	Attribute of TransportProtocols Indicates that the transport protocol indicated by the value is preferred	0-1 xs:boolean Default: False	
Hybrid	Element of ConfigurationModes Configuration pull and push (hybrid) mode is available	0-1 Note 2	

Table I.1 – Elements to be included in [b-ITU-T H.770] for the declaration of AM services

Element	Description	Support/type	Notes or Value domain
Preferred	Attribute of Hybrid Configuration pull and push (hybrid) mode is preferred	0-1 xs:boolean Default: False	
TransportProtocols	Element of Hybrid Indicates the transport protocol available	1-* xs:string enumeration	Values are out of the scope of AM
Preferred	Attribute of TransportProtocol Indicates that the transport protocol indicated by the value is preferred	0-1 xs:boolean Default: False	
MeasurementReport TransportProtocol	Container specifying which transport protocols for measurement reporting are available and preferred by aggregation functions	1-* xs:string enumeration	Values are out of the scope of AM
Preferred	Attribute of MeasurementReportTransport Protocol The transport protocol is preferred	0-1 xs:boolean Default: False	
Cryptographic Protocol	Specifies which cryptographic protocols for reporting are available and preferred by aggregation functions	1-* xs:string enumeration Note 3	Values: 'TLS', 'TLS-SRP', 'OTP', 'HMAC' NOTE – 'TLS' is TLS 1.2 [IETF RFC 5246], 'TLS-SRP' is TLS-SRP [b-IETF RFC 5054], 'OTP' is [b-ITU-T X.1153], 'HMAC' is [b-FIPS PUB 198-1].
Preferred	Attribute of CryptoReport This cryptographic protocol is preferred	0-1 xs:boolean Default: False	
Compression	Specifies which compression/decompression algorithms are available and preferred by aggregation functions for XML payloads	0-* xs:string enumeration Default 'EXI'	Values: 'None', 'BiM', 'ZLIB', 'Infoset', or 'EXI'. See Note 4.

Table I.1 – Elements to be included in [b-ITU-T H.770] for the declaration of AM services

Element	Description	Support/type	Notes or Value domain
Preferred	Attribute of Compression This compression algorithm is preferred	0-1 xs:boolean Default: False	
NOTE 1 – One or more of these must be present. NOTE 2 – One or more of these must be present. NOTE 3 – 'TLS' or 'TLS-SRP' is required to be present. NOTE 4 – For BiM see [b-ISO/IEC 23001-1], for ZLIB (including GZIP) see [b-ETSI TS 102 472], for (Fast) Infoset see [b-ITU-T X.891], and for EXI see [b-W3C EXI]. NOTE 5 – For xs: data types, see [b-W3C XMLSchemaP2]; for the URL data types, see [b-IETF RFC 3986]; for gt: data types, see [b-ATIS 0800026].			

```
PermissionOperationModes (1-*) [Preferred (0-1)]
Addresses (1)
| Unicast (0-1)
| | ConfigRequestAddress (0-1) Note 1
| | ErrorAddress (0-1)
| Multicast (0-1)
| | MulticastHybridAddress (0-1) [MulticastHybridAddressPort (1)] Note 1
| | | MulticastHybridSourceAddress (1)
| | MulticastPushAddress (0-1) [MulticastPushAddressPort (1)] Note 1
| | | MulticastPushSourceAddress (1)
| | ErrorAddress (0-1)
| | AckAddress (0-1)
ConfigurationModes (1)
| Push (0-1) [Preferred (0-1)] Note 2
| | TransportProtocols (1-*) [Preferred (0-1)]
| Pull (0-1) [Preferred (0-1)] Note 2
| | TransportProtocols (1-*) [Preferred (0-1)]
| Hybrid (0-1) [Preferred (0-1)] Note 2
| | TransportProtocols (1-*) [Preferred (0-1)]
MeasurementReportTransportProtocol (1-*) [Preferred (0-1)]
CryptographicProtocol (1-*) [Preferred (0-1)]
Compression (0-*) [Preferred (0-1)]
```

Figure I.1 – Alternative representation of [b-ITU-T H.770] AM data structure

The XML schema that can be exchanged for audience measurement service discovery is in Appendix VIII.

Appendix II

Considerations on implementation

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

This appendix provides guidance for SPs on whether and how to deploy audience measurement.

II.1 Considerations on whether to implement AM

Deploying audience measurement functions as part of the IPTV architecture provides benefits over traditional audience measurement which uses carefully selected panels to provide end-user information and media engagement measurements.

Benefits of AM as part of IPTV architecture in comparison to traditional methods include:

1) A larger audience sample – Many AM uses depend upon the statistical extrapolation of a sample:

   a) Given the fragmentation of digital destinations, the number of panel members that visit the long tail may be small or zero. A larger sample increases the statistical likelihood of meaningful measurement of more digital destinations.

   b) Local market characteristics are more likely to be detected.

   c) More stable measurement of small groups of interest.

   d) AM aggregated across service providers amplifies the benefit.

2) More detailed engagement measurements – Since AM has direct access to IPTV systems, it is able to measure IPTV engagement events, which are otherwise inaccessible, with greater time accuracy.

3) Opportunity for combination with other IPTV services – Since AM has direct access to IPTV systems, it may be used to enhance other systems; for example:

   a) Impact of service degradation – how many viewers leave channels because of a high error rate.

   b) Improve content/advert recommendation services – making recommendations and correlating subsequent choices and engagements.

4) Passive data collection – some traditional methods rely upon viewers who may suffer from fatigue or bias to record information. No active action by end users is needed using AM.

AM limitations in comparison to ideal methods include:

1) AM does not measure all end-user engagements on end-user devices which support IPTV services – End users engage substantially with non-IPTV services depending upon device type.

   a) TV – services provided via alternative input (e.g., game console content and games).

   b) Mobile device – phone, text, navigation, music, web, photography, etc.

   c) PC – web, chat, local programs/apps, etc.

2) AM is for IPTV "TV" only, it does not include over-the-air TV, analogue STBs, or uni-directional broadcasts, which additionally may be predominately used by particular audiences.

3) The AM audience sample may not be representative of the total viewing population which may be a problem for extrapolation. Optionally provided end-user information could be used to build a representative audience sample.

4) AM TV viewing measurements may be misleading without presence detection to indicate how many viewers are currently engaged.

5) AM TV viewing measurements may not be associated with the identity and attributes of those viewers currently engaged.

6) TV measurements may be overstated when the TV is powered off and a STB in powered on.

7) The measurement analytics and offering/delivery mechanisms to stakeholders are not standardized.

8) Integrated measurement of the audience and the quality of experience is not provided; the outputs of these separate systems can be manually combined.

In comparison to emerging technology, multi-function mobile devices used as remote controls are typically more powerful modern devices than some TV STBs, and so may have advantages as a measurement point.

II.2 Considerations for end-user permission method selection

There are three recommended methods to support the requesting, receipt, and storing of end-user responses and to ensure that measurement takes place with end-user permission, summarized in clauses 9.2.1, 9.2.2 and 9.2.3. The following are considerations of the situations for which each method is best suited.

II.2.1 External permission mode

In this method, the request and receipt of end-user permission occurs outside of the AM system, such as in the situation illustrated in Figure II.1.

Conditions that may lead to this method being selected include:

1) The deployment of a broad customer communications system, which lends itself to integration of end-user permission functions such as directly asking for an end-user's permission, storing responses, reporting on end-user permission status, and aggregating end users into segments based upon permission status.

2) A preference to communicate with end users through either a customer-care channel, or a non-resident downloadable application.

3) A desire to de-couple the permission system software from the audience measurement software. This may be important if frequent revisions or multiple versions (such as language or legislative zones) are expected.

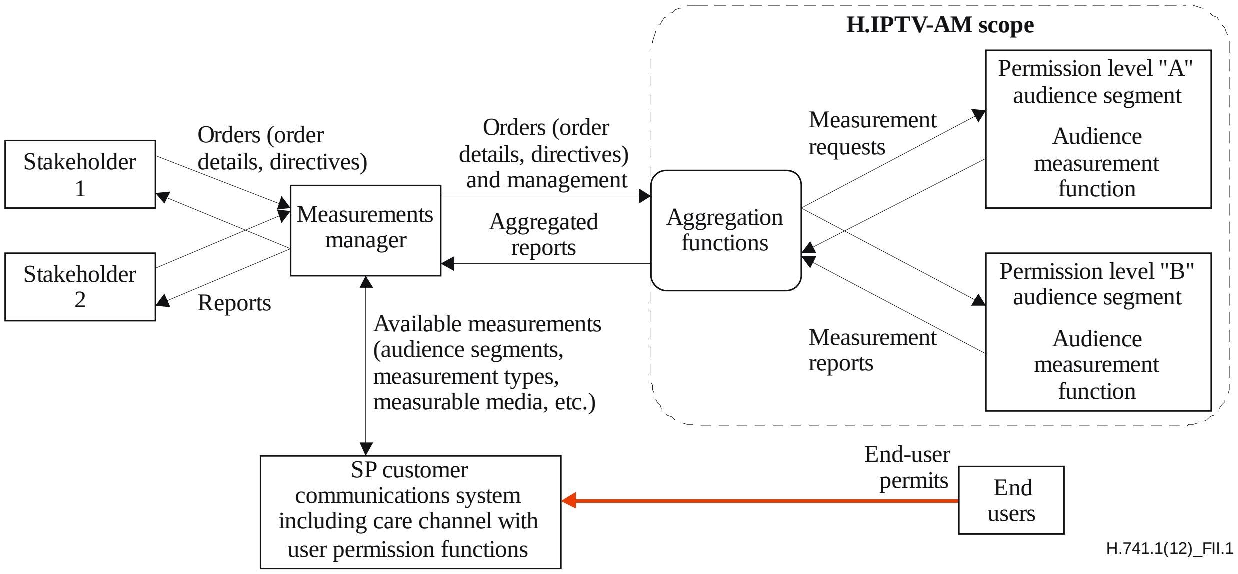

H.IPTV-AM scope
Stakeholder 1
Stakeholder 2
Orders (order details, directives)
Reports
Measurements manager
Orders (order details, directives) and management
Aggregated reports
Aggregation functions
Measurement requests
Measurement reports
Permission level "A" audience segment
Audience measurement function
Permission level "B" audience segment
Audience measurement function
Available measurements (audience segments, measurement types, measurable media, etc.)
SP customer communications system including care channel with user permission functions
End-user permits
End users
H.741.1(12)_FII.1

Figure II.1 – Example of external permission mode

In external permission mode, TD-AMFs do not know the details of permits. Consider that all TD-AMFs might have the same permission level, or that subsets of TD-AMFs might have different permission levels. There are four multicast sub-addressing mechanisms: threshold ranges, device type, device address and end user info.

– Threshold ranges mechanism – is independent of the permission level; a configuration sent to a random set of TD-AMFs must make an assumption about the permission levels assigned to the TD-AMFs. Consider that all have a single permission level (either 1, 2 or 3) – then a single configuration can be sent according to that permission level. Consider a population of TD-AMFs having different permission levels (1 and 2, 2 and 3, 1 and 3, or 1 and 2 and 3) – then a single configuration appropriate to the lowest permission level present, e.g., permission level 1, would be sent. If the population of TD-AMFs includes permission level 0, then the permission level 0 factor is ignored. For example, in the case of a population having different permission levels of 0, 1, 2 and 3, then a single configuration appropriate to permission level 1 would be sent.

– Device Type mechanism – the considerations are similar as for the threshold ranges mechanism.

– Device addresses mechanism – addresses of the target TD-AMF subsets may be determined by awareness of permission levels 1, 2 or 3. Different subsets as defined by lists of addresses may be sent different appropriate configurations. The formation of these subsets may be implemented outside of AM.

– End-user info mechanism – is dependent upon permission levels 2 or 3. Since the only sub-addressing mechanism which may be permission level aware is device addresses, end user info sub-addressing can only be used in combination with the device addresses mechanism.

II.2.2 Internal permission mode

With this method, the request and receipt of end-user permission occurs within the AM system, such as in the situation illustrated in Figure II.2.

Conditions that may lead to this method being selected include:

1) The desire that deployment of a permission system be closely coupled to the deployment of the audience measurement system.

2) A preference to communicate with end users through a resident application which is an integral part of the audience measurement software.

3) An alternative real-time audience messaging system is not available.

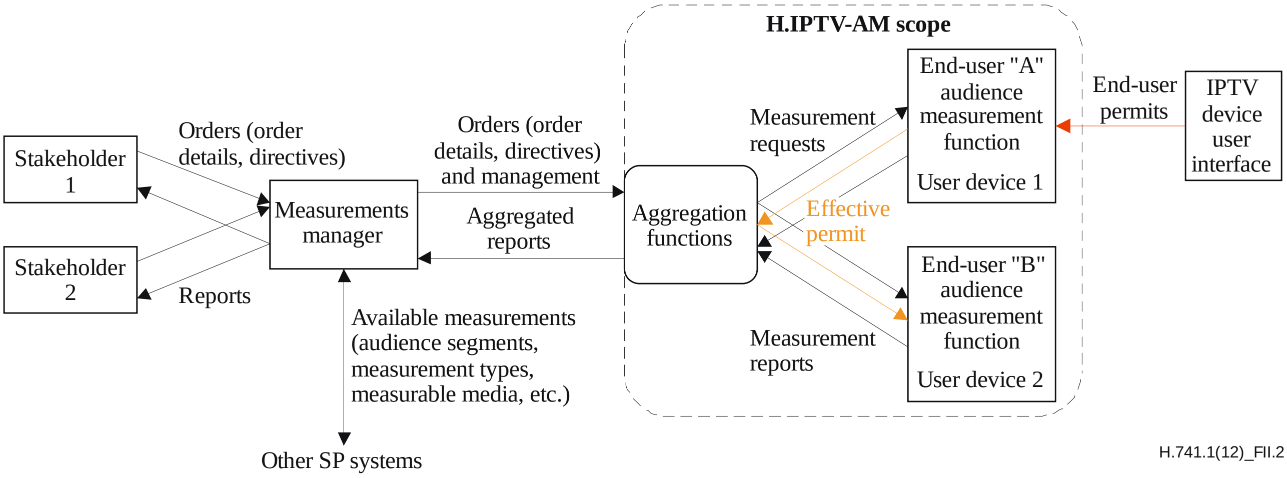

H.IPTV-AM scope
Stakeholder 1
Stakeholder 2
Orders (order details, directives)
Reports
Measurements manager
Orders (order details, directives) and management
Aggregated reports
Available measurements (audience segments, measurement types, measurable media, etc.)
Other SP systems
Aggregation functions
Measurement requests
Effective permit
Measurement reports
End-user "A" audience measurement function
User device 1
End-user "B" audience measurement function
User device 2
End-user permits
IPTV device user interface
H.741.1(12)_FII.2

Figure II.2 – Example of internal permission mode

In the above figure, an example flow of end-user permits and effective permits are shown by red and orange arrows. Multiple end-user permits may be input to a TD-AMF which combines them into an effective permit for filtering the configuration package instructions. The aggregation functions may use the effective permit itself, and may send the effective permit to other TD-AMFs of the end user (for federation of permissions) that the end user has specified.

Using internal permission mode, visibility into the audience segmented by permission levels may be obtained by the Measurements Manager from the AM system.

II.2.3 Hybrid permission mode

In this mode, illustrated in Figure II.3, the request and receipt of end-user permissions occurs within the SP system. The TD-AMF requests the permit from the SP system, and may use the permit for local filtering, or send it to the aggregation functions to filter configuration packages.

Conditions that may lead to this mode being selected include:

1) The deployment of a broad customer communications system, which lends itself to integration of end-user permission functions such as directly asking for an end-user's permission, and storing responses (permits).

2) A preference to communicate with end users through an SP customer-care channel, rather than through AM.

3) The wish for the AM system to be aware of end-user permissions.

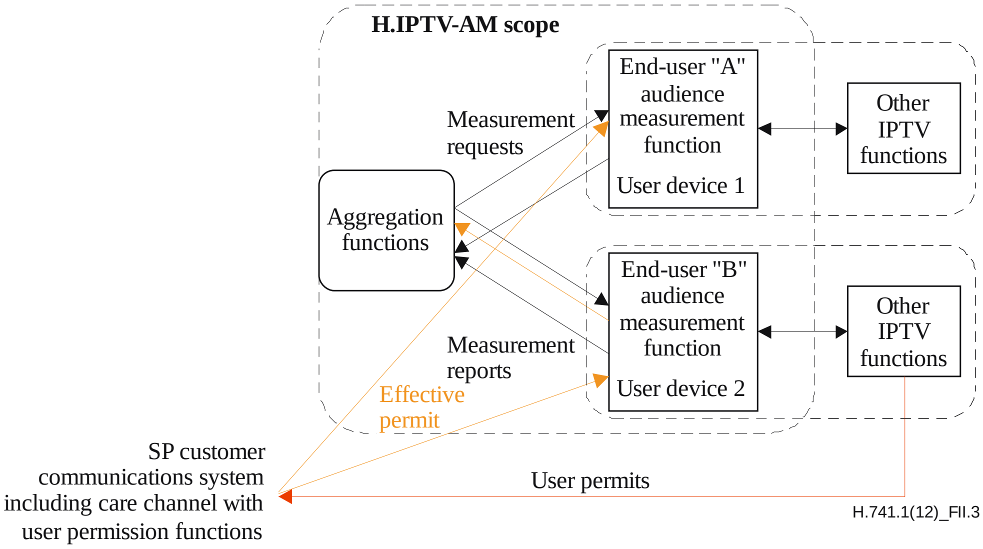


Figure II.3 – Example of hybrid permission mode

In the above figure, an example flow of end-user permits and effective permits is shown by red and orange arrows. Multiple end-user permits may be input to a SP which combines them into an effective permit for use in filtering the configuration package instructions.

Using hybrid permission mode, the end user could specify which devices the end-user permit(s) covers (for federation of permissions) and the SP could forward the effective permit to all specified devices (which would each forward the effective permit to the aggregation functions.

II.2.4 Example method of setting multiple permits in a household

The method of setting and managing permits is out of the scope of this Recommendation. However, Figure II.4 gives an example to show how end-user permits may be used with AM.

In this example, the subscriber–administrator allocates rights to household members. The mother:

- creates an identity for the father, who may set his permissions without further access by the mother;
- creates an identity for Son1, who may set or reduce his permissions only with his mother's approval;
- creates identities for Son2 and Son3, and sets their permissions.

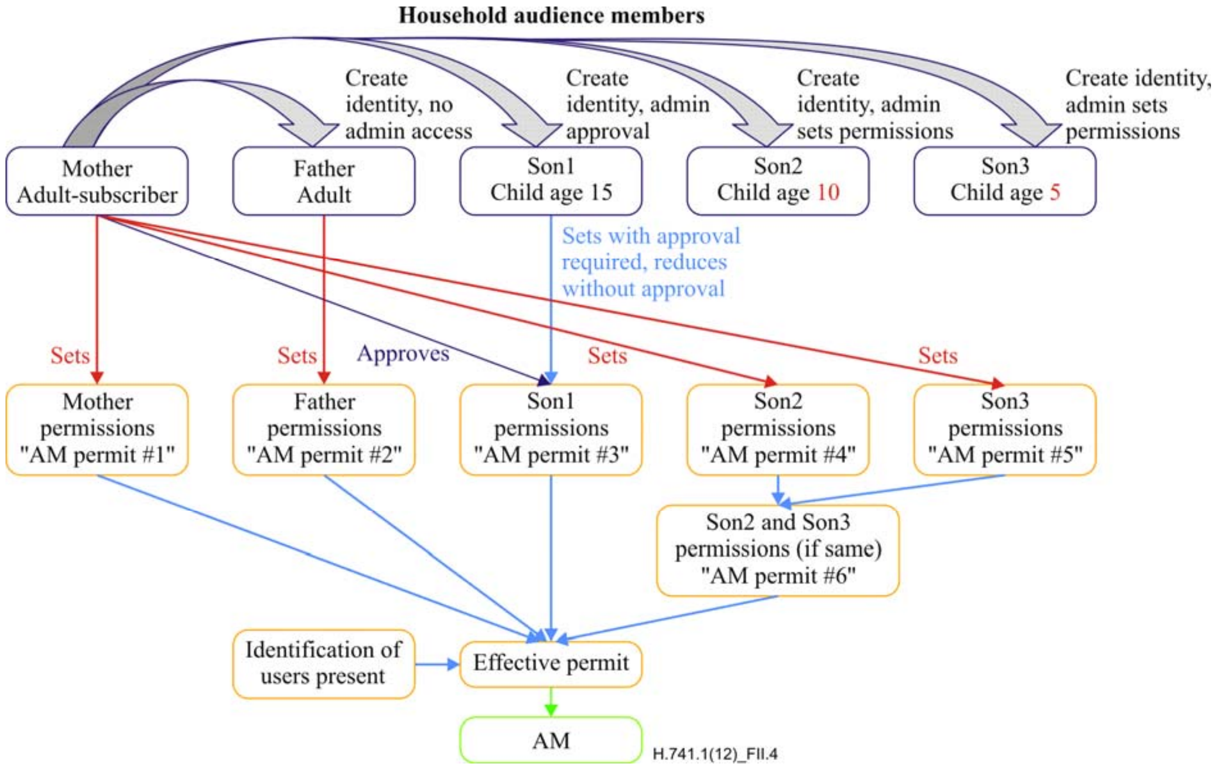

Household audience members
Create identity, no admin access
Create identity, admin approval
Create identity, admin sets permissions
Create identity, admin sets permissions
Mother Adult-subscriber
Father Adult
Son1 Child age 15
Son2 Child age 10
Son3 Child age 5
Sets with approval required, reduces without approval
Sets
Sets
Approves
Sets
Sets
Mother permissions "AM permit #1"
Father permissions "AM permit #2"
Son1 permissions "AM permit #3"
Son2 permissions "AM permit #4"
Son3 permissions "AM permit #5"
Son2 and Son3 permissions (if same) "AM permit #6"
Identification of users present
Effective permit
AM
H.741.1(12)_FII.4

Figure II.4 – Example method of setting multiple permits in a household

The permit input method may occur via an IPTV device end-user interface driven either:

– internally to AM per clause II.2.2 (internal permission mode), or

– externally of AM per clause II.2.1 (external permission mode), or II.2.3 (hybrid permission mode).

Rules to determine the effective permit include:

1) If household members are not distinguishable, then only a single household permit is needed.

2) If a single household member is identified as being present, then the associated permit would be used.

3) Where multiple end users are believed to be engaging with content, the effective permit is the most restrictive combination of permits of identified end users present.

Only one effective permit is used at any time.

II.3 Considerations on using content filtering in configuration packages

Content filtering may be supported via configuration and user permit mechanisms.

The configuration of content filtering as set by the AM provider (see clause 7.1.2.2), could be driven by either the AM provider or the end user (in external permission mode). In internal or hybrid modes, a permit may specify content filtering.

Conditions that may lead to configuration of content filtering being used by an AM provider include:

1) Content genres are available in TD-AMFs to support content filtering.

2) The SP believes that end users will be more likely to grant higher permission levels if certain sensitive genres are excluded from measurement.

3) Support of external permission mode which incorporates end user permissions regarding content restrictions.

4) Industry guidelines and/or regulations.

II.4 Considerations on using different measurement triggers

Audience measurement supports three types of measurement triggers, the following clauses discuss considerations to help decide when to use each type.

II.4.1 Considerations on using time-based sampling of elements

Audience measurement provides a rich set of event-driven measurements, which are the recommended measurement mechanism. However, there are situations under which end-user behaviours do not trigger desired events or reports of those events. Time-based sampling of elements helps capture those end-user behaviours and reports. If these situations occur frequently and/or the missed event reports have a high value, then it is recommended that time-based sampling be configured.

Time based sampling provides "checkpointing" capabilities for events that would have been measured and reported after event-driven measurement and reporting stopped. For example, if an end user watched a programme then powered down the device, and no channel change event is measured, then sampling informs AM of the programme watched.

The reporting of time-based sampling can be optimized when a new sample value is found to be effectively the same as a previous sample. Per the NothingNewReportMode element, the report of the new sample value can be ignored; an empty report can be sent, or a complete report may be sent. By selecting the option of reporting using an empty report, TD-AMFs will send small periodic messages which can be used to indicate a TD-AMF's health. TD-AMFs can be configured such that a single type of time-based sample value sends an empty report, thus avoiding duplicate health indicators from a single TD-AMF.

Conditions that may lead to time-driven sampling being selected include:

1) When measured programmes are usually the last programme that is watched prior to device power down.

2) When the additional resource overhead of time-driven sampling costs less than the value of missed event based audience measurements.

3) When the programmes are of longer duration and need less frequent sampling.

4) When the programmes are scheduled such that samples provide strong inferences (e.g., five minutes before the hour for hourly scheduled programmes).

Multiple measurement requests can be configured to cause the generation of duplicate measurement reports. For example, two measurement requests can both be configured to measure linear and common events, for both the same channel and time. It is recommended that the TD-AMF recognizes duplicate measurement reports awaiting transmission and discards all but one.

II.4.2 Consideration on using "sample" versus "service start" measurements

While event measurements are the recommended main method to measure behaviours, AM's two sampling mechanisms are useful for checkpointing, or for measuring slowly changing information. Consider that the following information from [ITU-T H.741.2], typically changes at different rates:

– UserID is anticipated to change frequently as the viewing end users change.

– UserIDMethod, and UserIDConfidence elements are anticipated to change slowly since they are associated with the capabilities of the system.

– Some hardware information such as TVInformation may change slower than others MobileDeviceInformation.

– Some end-user information never changes, such as Birthday and BirthLocation.

Service start measurements are better suited to collect slowly changing information, since this method does not use device resources to measure elements frequently then discard them if they have not changed or use network resources to send a report during consumption of every service. If it is desired to measure elements each time a service starts during a day, or once every number of days, then service-start measurements are recommended.

II.5 Considerations for using AM message acknowledgements

In a message passing system it is sometimes useful to monitor the health of the system and to enable problem debug using acknowledgments. Some of the supported transport protocols may support acknowledgements that the IP packets holding AM messages have been delivered. These transport acknowledgements do not indicate if the contents of the message were understood. Therefore AM includes an optional, flexible and low overhead acknowledgement request mechanism (response qualifier) for the multicast configuration message. Together with the addressability of AM to sets of devices such as STBs, acknowledgments may be selectively configured on a set of devices which act as device samples for the greater population.

Conditions that may lead to the use of acknowledgements being requested include:

1) Pre-deployment testing to help gain familiarity with system operations.

2) Initial limited deployments to help gain confidence in system operations.

3) On-going monitoring of system operations using a subset of TD-AMFs.

4) Trouble-shooting system operations.

When an acknowledge (without requesting an error report) has been requested and none is received, the following causes may be considered:

– Configuration message was configured incorrectly, not transmitted, or not received by the targeted TD-AMFs.

– The targeted TD-AMF(s) was/were offline, software was not installed/working/compatible, was unable to transmit ACK, or was not received by the aggregation functions.

Actions that are recommended for consideration include:

– Re-send same multicast configuration message assuming the problem was temporary.

– Re-send multicast configuration message with an error report request to obtain more information.

– Narrow the subset of TD-AMFs to pin-point and better understand the problem.

– Extend the subset of TD-AMFs assuming it was too small.

– Analyse configuration message for errors; if found, then fix and resend.

II.6 Considerations for configuration mode selection

There are three modes to send configuration packages to TD-AMFs:

– **Configuration Pull Mode**: TD-AMFs initiate the transfer request for a configuration package from the aggregation functions using the configuration package request message, which may result in a configuration package request response message.

– **Configuration Push Mode**: Aggregation functions initiate and send configuration packages using the configuration message.

– **Configuration Hybrid Mode**: A combination of the pull and push modes.

For configuration pull mode and for configuration pull and push (hybrid) mode, a configuration package check delay is defined, which triggers subsequent checks for availability of a new configuration package. An initial multicast configuration request response message (e.g., when AM is first turned on) may synchronize subsequent checking by many TD-AMFs. Therefore, it is recommended that the value of the configuration package check delay be configured to vary across TD-AMFs if the multicast configuration request response message is used.

The following are considerations of the situations for which each mode is best suited.

II.6.1 Configuration Pull Mode

In this mode, TD-AMFs individually send requests to the aggregation functions to check and conditionally receive a new configuration package.

Conditions that may lead to this method being selected include:

1) Sufficient upstream bandwidth is available for configuration request messages.
2) Information regarding TD-AMFs currently online is not otherwise available to AM (it is provided by the configuration request messages).
3) A substantial number of TD-AMFs are periodically turned off or disconnected from the network (configuration push messages could be missed).
4) A substantial number of TD-AMFs are mobile and the configuration packages are location dependent.

II.6.2 Configuration Push Mode

In this mode, aggregation functions send unicast or multicast configuration package message(s) to TD-AMFs. Aggregation functions may obtain information regarding TD-AMFs that are online from other IPTV services, including but not limited to:

- TD-AMF unicast reachability information.
- TD-AMF type and MAC addresses for multicast sub-addressing.
- TD-AMF capabilities.

Configuration push mode provides aggregation functions with autonomy, independent of the receipt of "pull requests" from TD-AMFs. The use cases where aggregation functions are recommended to immediately send a new push configuration include:

a) A revised effective permit has just been received in external permission mode.
b) An unplanned immediate change in a stakeholder AM order has been received.
c) Potential recovery actions to abnormal situations ("Message high level error", "Configuration message or configuration request response message error", "Configuration request message error", "Storage overrun", and "TD-AMF sends inappropriate but valid AM messages").

Conditions that may lead to unicast configuration push being selected include:

1) Minimization of AM configuration pull sequence messages is important.
2) A multicast protocol is not supported.
3) Information regarding TD-AMFs currently online is available.
4) Continuous tracking of configuration error and/or measurement reports is available to modify configuration messages e.g., contents and timing of configuration messages.
5) Minimization of TD-AMF multicast sub-addressing processing (especially for handling abnormal situations) by non-target TD-AMFs.

The advantage of using multicast push mode is that a single message can be sent to configure many TD-AMFs. By using target qualification elements, by MAC address, target device type, and/or percentage of devices, configuration of multiple sets can be achieved by sending few different configuration messages. In addition, multiple multicast transport delivery protocols can be used. Together these capabilities form the basic tools for multicast configuration push mode.

In practice the number of TD-AMFs responding to any configuration could be tracked and used as feedback to modify the frequency and time of configuration messages.

Conditions that may lead to this method being selected include:

1) Minimization of AM configuration pull sequence messages is important.
2) A multicast protocol is supported.
3) Information regarding TD-AMFs currently online is available.
4) Continuous tracking of measurement reports is available to modify configuration messages.

II.6.3 Configuration Hybrid Mode

In this mode, TD-AMFs may individually send requests to the aggregation functions to check and conditionally receive a new configuration package. Subsequently aggregation functions may send unicast or multicast configuration package message(s) to TD-AMFs.

Conditions that may lead to this method being selected include:

1) Sufficient upstream bandwidth is available for a reduced frequency of configuration request messages (limited pull).
2) A mixture of some or all of the conditions of clauses II.6.1 and II.6.2 occur.

II.7 Considerations regarding methods of obtaining end-user permits

Several methods may be available for AM and/or IPTV service providers to obtain end-user permits. Some methods include:

- An interactive IPTV customer care channel.
- IPTV audience measurement using internal permission mode.
- Web customer care portal.

To help select and implement a method, the following three processes are recommended for consideration:

1) Permission requests to an end user to measure, collect and use end-user information may be triggered by the following events:
   a) Initial deployment of services to an end user.
   b) Addition of an end-user measurement function to an existing device associated with services.
   c) Addition of a new device which supports end-user measurement function associated with services.
   d) Before applying any material change to data collection and use policy that is less restrictive to data collected prior to such material change.
   e) Elapse of prior duration-limited permission granted by an end user, which is recommended to be no more than one year.
   f) Request by end user to change permissions.
2) The AM service may optionally support an end-user's request to purge prior AM information.

3) To select the same service method to obtain end-user permits as the IPTV service, it is recommended that either an IPTV customer care channel or IPTV AM be selected.

4) It is recommended that the language and format of the request be selected to match the end user and device.

II.8 Considerations for using multicast sub-addressing mechanisms

When using multicast messages, AM provides four mechanisms which enable addressing subsets of TD-AMFs. A low network traffic method is thereby provided to uniquely configure large subsets of TD-AMFs.

Threshold ranges

The first mechanism is the use of threshold ranges. To efficiently create and control subsets of many TD-AMFs, each TD-AMF generates a random number between 0-10000 at boot-up, which it compares with configurable threshold ranges in the multicast message. Only if the TD-AMF random number matches the range does the TD-AMF accept the message. For example, only three multicast (push) messages are needed to configure three subsets of devices:

1) "normal responders (no error or acknowledgements)" = threshold range 0-4090

2) "positive acknowledge sentries" = threshold range 4100-4190

3) "error responders" = threshold range 4200-4290.

Here approximately 40% of the total TD-AMF population would not send error or acknowledgement messages. Approximately 1% of the total TD-AMF population would generate error messages following error detection. Approximately 1% of the total TD-AMF population would generate acknowledge messages to provide a health indication.

In order to limit the network resources used, the total percentage of responding AMFs can optionally be controlled as the total number of TD-AMFs increases. In the above example, the number of "normal responders" could be reduced as the total number of TD-AMFs increases in order to avoid increases in AM network traffic.

Conditions that may lead to multicast threshold ranges being used include:

1) Network-level multicast or application-level multicast (e.g., XMPP) is supported.

2) Network resources need to be controlled as the number of TD-AMFs increase.

3) Subsets of TD-AMFs need to have different configurations.

List of device addresses

The second address qualifier mechanism is to specify the list of device addresses (hash of MAC address) for the multicast message, in a binary header.

Conditions that may lead to the list of device addresses being used include:

1) Network-level multicast or application-level multicast is supported.

2) Subsets of TD-AMFs need to have different configurations.

3) Subsets of reports from TD-AMFs are desired.

The threshold ranges and device address list mechanisms may be used in combination for the "multicast configuration message" and/or "multicast measurement report request message".

This multicast subset addressing mechanism for the device address list may be used in the "multicast configuration request response message". It may be used as a single multicast message to respond to many TD-AMFs simultaneously requesting configuration using unicast, for example, in the case following recovery from a local geographic event such as a power or network outage.

Sets of TD-AMFs requiring different configuration could distinguish multicast responses by examination of the terminal device target list. TD-AMFs would need to examine all AM multicasts for a certain time to determine if their MAC address is in the list of each response.

Device type

The third address qualifier mechanism is to specify which type of device the multicast message is for: TV, PC, tablet, mobile or other. This third mechanism is supported in the "multicast configuration message". It may be used in combination with the other three mechanisms.

Conditions that may lead to multicast subset addressing by type of device being used include:

1) Network level multicast or application-level multicast is supported.

2) Subsets of TD-AMFs types need to have different configurations, purely by type, e.g., PC and Tablet.

3) A subset of TD-AMFs types needs to have a different configuration, combining type and percentage using threshold ranges, e.g., 50% of STBs.

4) A subset of TD-AMFs types needs to have different configurations, combining type and specific MAC address when the type of TD-AMF at a specific MAC address is not known.

End-user information

The fourth address qualifier mechanism is to specify target values of provider-defined end-user elements, which match those associated with a TD-AMF in order for the configuration to be further processed by that TD-AMF. This mechanism supports whether to ignore the matching rule in the case where the specified end-user data is not available. This fourth mechanism is supported in the "multicast configuration message" and "multicast configuration request response message". It may be used in combination with the other three mechanisms.

For example, as in Table II.1, a configuration package specifying an end-user info element type "occupation" and associated element value "doctor" will only be processed by the set of TD-AMFs having an end-user info element type of "occupation" and associated element value of "doctor". The TD-AMF will also process the configuration package if it specifies "ignore if unavailable" and the TD-AMF end-user info element type "occupation" is unavailable.

Table II.1 – Example of using end-user information for sub-addressing of TD-AMFs

Target end-user info element type	Target end-user info element value	Ignore if unavailable	TD-AMF end-user info element type	TD-AMF end-user info element value	TD-AMF action
"occupation"	"doctor"	False	"occupation"	"doctor"	Process config
"occupation"	"doctor"	True	"occupation"	"doctor"	Process config
"occupation"	"doctor"	False	"occupation"	Not "doctor"	Do not process config
"occupation"	"doctor"	True	"occupation"	Not "doctor"	Do not process config
"occupation"	"doctor"	False	"occupation" not available	–	Do not process config
"occupation"	"doctor"	True	"occupation" not available	–	Process config

Multiple end-user info elements may be specified within one configuration package. For example, a configuration package can require "occupation" is "doctor" and that "income" is "over 200 000 Euros", in which case they must both be matched for a TD-AMF to process that configuration package. This fourth mechanism may be used with the above three mechanisms, in which case, the qualifiers of all used mechanisms must match for the configuration to be processed by a TD-AMF.

Conditions that may lead to the use of end-user info sub-addressing include:

1) Network-level multicast or application-level multicast is supported.
2) End-user permission levels 2 or 3 have been granted for the target TD-AMFs. Where the permission level required depends upon whether the desired match is against generic or controlled end-user information.
3) End-user info elements suitable for targeting have been requested by AM stakeholders.
4) End users have provided the data for elements suitable for targeting.
5) Multiple different configurations for subsets of TD-AMFs are desired.

The use of the "Ignore if available" option is recommended to be considered when enrichment of a subset population including end users having a particular info element value (trait) is desired. It maximizes the number of TD-AMFs that accept a configuration package having a specific trait even if not made available, with the side effect of including some end users that do not have that trait.

II.9 Considerations for requesting error message responses to multicast messages

Error message responses to unicast messages are mandatory when an error is detected; however error message responses to multicast messages are configurable. In particular, a response qualifier which can request error message responses is supported in three messages:

- Multicast configuration request response message.
- Multicast configuration message.
- Multicast measurement report request message.

Conditions that may lead to use of error message responses being requested include:

1) Pre-deployment testing to help gain familiarity with system operations.
2) Initial limited deployments to help gain confidence in system operations.
3) On-going monitoring of system operations using subsets of TD-AMFs.
4) Trouble-shooting system operations.

Error messages (see [ITU-T H.741.2] Table 8) indicate the source AM message, indication of whether the errored message was partially accepted or rejected, error codes and related information. Error types indicated include:

- Multicast high level errors – not well formed XML message (syntax error), invalid XML message, unrecognized message (not compliant with the schema), or sourced major version is not equal to the receiver's version.
- Multicast configuration errors – element not supported, element information not available, element not permitted, and event not supported. Related information includes errored element and event name.
- Multicast report request errors – Requested measurement request ID which was not previously configured. Related information includes the errored element and measurement request ID.

Actions that are recommended to be considered include those in Table 2 and the following multicast-specific actions:

- Narrow the subset of TD-AMFs by the use of multicast sub-addressing, to pin-point and better understand the problem.

II.10 Considerations for delivery mode selection

There are four modes that may be used to deliver measurement reports to aggregation functions. These may be used alone or in combination specified by configuration of measurement requests.

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.

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 case 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 randomly picked time 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 considerations of the situations for which each mode is best suited.

II.10.1 Immediate Push Mode

Conditions that may lead to this mode being selected include:

1) The audience measurement data is of higher value when made available to other applications or stakeholders in near real-time.

2) Upstream network resources to aggregation functions are available during an AM measurement period.

3) Expected TD-AMF available storage in comparison to the volume of expected measurements is limited, and would likely result in loss of measurements if not reported immediately.

For example, measurements acquired during non-peak network usage periods might be reported immediately.

II.10.2 Delayed Push Mode

Conditions that may lead to this mode being selected include:

1) The audience measurement data remains valuable when made available to other applications or stakeholders within a delayed time period.

2) Upstream network resources to aggregation functions are expected to be available during a known period after measurement acquisition starts.

3) Expected TD-AMF available storage in comparison to the volume of expected measurements until reporting is sufficient, or loss of lower-priority measurements due to storage congestion is acceptable.

For example, measurements acquired during peak network usage periods might be reported during non-peak periods.

II.10.3 Pull Mode

Conditions that may lead to this mode being selected include:

1) The audience measurement data remains of value when made available to other applications or stakeholders within a delayed time period, but sooner is more valuable.

2) The availability of upstream network resources to aggregation functions may not be predictable. Upstream and some downstream network availability may be opportunely used to retrieve reports.

3) Expected TD-AMF available storage in comparison to the volume of expected measurements until reporting is sufficient, or loss of lower-priority measurements due to storage congestion is acceptable.

For example, measurements acquired during peak network usage periods might be collected as soon as sufficient network availability is detected.

II.10.4 Delayed Push and Pull Mode

Conditions that may lead to this mode being selected include:

1) The audience measurement data remains valuable when made available to other applications or stakeholders within a delayed time period; however sooner is more valuable.

2) The availability of upstream network resources to aggregation functions may not be predictable. Upstream and some downstream network availability may be opportunely used to retrieve reports. If an opportunity does not occur sufficiently in advance, then downstream network consumption can be avoided by waiting for the delayed push.

3) Sufficient available storage is anticipated for the TD-AMF as compared to the volume of measurements expected until reporting; or the loss of lower-priority measurements due to storage congestion is acceptable.

4) It is desirable that a single delivery mode be configured, but certain triggers will cause aggregation functions to collect audience measurement data sooner than scheduled. Examples of pull mode triggers include:

   a) day of week

   b) content programming event

   c) audience measurement data previously collected by aggregation functions.

For example, transmission of reports may be scheduled for 0200 hours, but on election evening the measurement reports are collected earlier.

II.10.5 Mixed delivery modes

To process a complete service history, all events and samples prior to and including service stop (or subsequent service start) must be received by the aggregation functions.

The fastest way to obtain a complete service history is to report all events and samples using immediate delivery mode. However, if it is desired to use mixed delivery in order to obtain a complete service history as soon as possible, then it is recommended that service start and service stop be delivered using immediate delivery mode, and that other events and samples be delivered using pull mode or delayed push and pull mode. When aggregation functions receive a service stop (or subsequent service start) event report from a TD-AMF, it is recommended that they pull all reports from that TD-AMF.

II.11 Considerations on using end-user information to filter measurement requests

End user provided information associated with a TD-AMF may be used to filter out specific measurement requests while others are to be processed. The advantage of using measurement request filtering is to be able to deploy fewer configuration packages that are suitable for many TD-AMFs. For example, if in a set of TD-AMFs, an end-user info element type is "occupation" and the associated element value is "doctor", then measurement requests which are associated to "occupation" and "doctor" will only be processed by that set of TD-AMFs. If the "occupation" is not "doctor", then the specified measurement requests are ignored. A single configuration package can therefore be extended to qualify different measurement requests by several "occupations" or other end-user info types such as "income", "number of children", etc. Multiple end-user info qualifiers e.g., "doctor" and "over 200 000 Euros" may be associated to measurement requests, in which case they must both be matched for a TD-AMF to process the associated measurement request(s). The configuration also specifies whether to ignore the matching rule in the case where the specified end user data is not available.

Conditions that may lead to the use of end-user information for filtering measurement requests include:

1) Multiple different configurations are desired.

2) Fewer configuration packages are desired.

3) End-user permission levels 2 or 3 have been granted for the target TD-AMFs. Where the permission level required depends upon whether the desired match is against generic or controlled information.

4) Elements suitable for targeting have been requested by AM stakeholders.

5) Elements suitable for targeting have been requested from end users.

6) End users have provided the data for elements suitable for targeting.

The use of the "Ignore if available" option is recommended to be considered when enrichment of a subset population including end users having a particular info element value (trait) is desired. It maximizes the number of TD-AMFs that accept a configuration package having a specific trait, even if not made available, with the side effect of including some end users that do not have that trait.

Appendix III

Examples of TD-AMF configurations, reports and permits

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

III.1 Example of use of configuration package data structure for service-common measurements

Assuming the following example requirements:

1) General
   - a) External permission mode with permission level 3
   - b) Send all reports to the same address
   - c) Re-transmit up to five additional times following transport non-acknowledgement from aggregation functions.
2) Fast-changing information
   - a) Information to be frequently sampled and reported includes:
     - i) Active service type
     - ii) Content ID info
     - iii) Sample times
     - iv) End-user ID info (with method and confidence parameters)
     - v) End-user presence confidence (with method parameter)
     - vi) Current location (if moved over 30 metres since last sample value)
   - b) Events to be measured and reported include
     - i) Video resize (with parameters)
   - c) Measurement times
     - i) Measurement period 1 = Event plus time sampling every five minutes between 1400 hours-2300 hours
     - ii) Measurement period 2 = Time sampling every ten minutes between 2300 hours-1400 hours
     - iii) Ignore the sample if its sample value is the same as the previous sample's value
   - d) Reporting
     - i) Report events immediately
     - ii) Report sample values every ten minutes
     - iii) Measurements are stored if the TD-AMF is unable to send reports
3) Slowly-changing information
   - a) Slowly changing information to be sampled and reported includes:
     - i) End user's device information
     - ii) End user's biographic information (e.g., gender, birth date, birth location and residential address)
   - b) Measurement times
     - i) Anytime
   - c) Reporting
     - i) Report anytime daily, or on demand

ii) Store measurements if the TD-AMF is unable to send reports

iii) Store with lower priority relative to other measurements

The solution example in Figure III.1 shows values assigned to the configuration package data structure to meet the above requirements. Relevant defaults are shown in *gray*; these are not required to be explicitly included in the configuration.

```
AMFConfigPackage (1)
   PackageID (0-1)[ PackageVersion (0-1)] = 12345, 2
   EffectivityDateAndTime (0-1) = 2013-10-10T12:00:00.00
   MeasurementRequestSet (1-*)
      DefaultDeliveryAddress (0-*) = http://defaultdeliveryaddress.com
      DefaultRetransmitNumber (0-1) = 5
      DefaultDayOfTheWeek (0-*) = 0 (Everyday)
      DefaultNothingNewReportMode (0-1) = 0 (send nothing if same value)
      DefaultMeasurementReportNumberByPush (0-1) = 1
      DefaultMaxTimeBetweenDelivery (0-1) = 0 (infinite)
      DefaultStartTime (0-1) = 00:00:00.00
      DefaultEndTime (0-1) = 23:59:59.99
      DefaultStartDeliveryWindowTime (0-1) = 00:00:00.00
      DefaultEndDeliveryWindowTime (0-1) = 23:59:59.99
      MeasurementRequest (1-*)
         MeasurementRequestID (1) = 1
         MeasurementSchedule (1-*)
            MeasurementPeriod (0-*)
               StartTime (0-1) = 14:00:00.00
               EndTime (0-1) = 23:00:00.00
            EventTrigger (0-*)
               Event (0-*) = VideoResize
               Priority (0-1) = 5
            TimeTrigger (0-1)
               SampleSet (0-*)[SampleSetIdentifier(1)] = "UserList"
               SampleSet (0-*)[SampleSetIdentifier(1)] = "UserPresent"
               SampleSet (0-*)[SampleSetIdentifier(1)] = "TDLocation"
                  SampleSetQualifier (0-*) = "30"
               Periodicity (1)= 300
               Priority (0-1) = 5
         MeasurementSchedule (1-*)
            MeasurementPeriod (0-*)
               StartTime (0-*) = 23:00:00.00
               EndTime (0-*) = 14:00:00.00
            TimeTrigger (0-1)
               SampleSet (0-*)[SampleSetIdentifier(1)] = "UserList"
      SampleSet (0-*)[SampleSetIdentifier(1)] = "UserPresent"
      SampleSet (0-*)[SampleSetIdentifier(1)] = "TDLocation"
        SampleSetQualifier (0-*) = "30"
      Periodicity (1) = 600
      Priority (0-1) = 5
  MeasurementDeliverySchedule (0-1)
    ImmediatePush (0-1)
MeasurementRequest (1-*)
  MeasurementRequestID (1) = 2
  MeasurementSchedule (1-*)
    ServiceStartTrigger (0-1)
      Interval (0-1) = 1
      SampleSet (0-*)[SampleSetIdentifier(1)] = "DeviceInfo"
      SampleSet (0-*)[SampleSetIdentifier(1)] = "UserBioInfo"
      Priority (0-1) = 1
  MeasurementDeliverySchedule (0-1)
    DelayedPushAndPull (0-1)
```

Figure III.1 – Service-common example configuration package

NOTE 1 – Active service type: The service-common measurements are only reported when a specific service is active. Correlation between service-common measurements and the active service may be achieved by using service start/end events of the active service. No additional configuration for this is needed. However if there is no service-specific report e.g., linear TV, then the active service type may not be known.

NOTE 2 – Sample times: MeasurementReportTriggerTime is used to report the time that an element is sampled. No additional configuration for this is needed.

NOTE 3 – For slowly-changing data, if the random delivery time is generated which is after the ServiceStartTrigger, then the delivery of that data occurs at the next day's random time.

NOTE 4 – Content ID info could be derived from content source and time for linearTV.

III.2 Example of measurement reports associated with configuration example of Figure III.1

Given the configuration example of Figure III.1, examples of end-user behaviours are assumed which, together with the configuration, result in a series of measurement reports being delivered.

During this two day example, a random delivery time is chosen at 0500 hours. Presence detection is assumed to be supported by key push measurements. The measurement periods and delivery windows of measurement requests 1 (MR1) and 2 (MR2) are shown for reference in Figure III.2. Measurement request 1 uses immediate delivery. Measurement request 2 uses delayed and pull delivery, and has a random delivery time.

The service-start and service-end events shown in Figure III.2 represent service-specific events described in [ITU-T H.741.3]. Since a TD-AMF may aggregate multiple measurement reports into a measurement package, it is likely that the service-start event would be aggregated into AM report packages (1), (4), (6) and (9). Four service periods labelled A-D occur between associated-service-start and service-end events.

It is assumed that the remote control has a button per family member which may be pressed when that member watches TV. This is used to indicate UserList change.

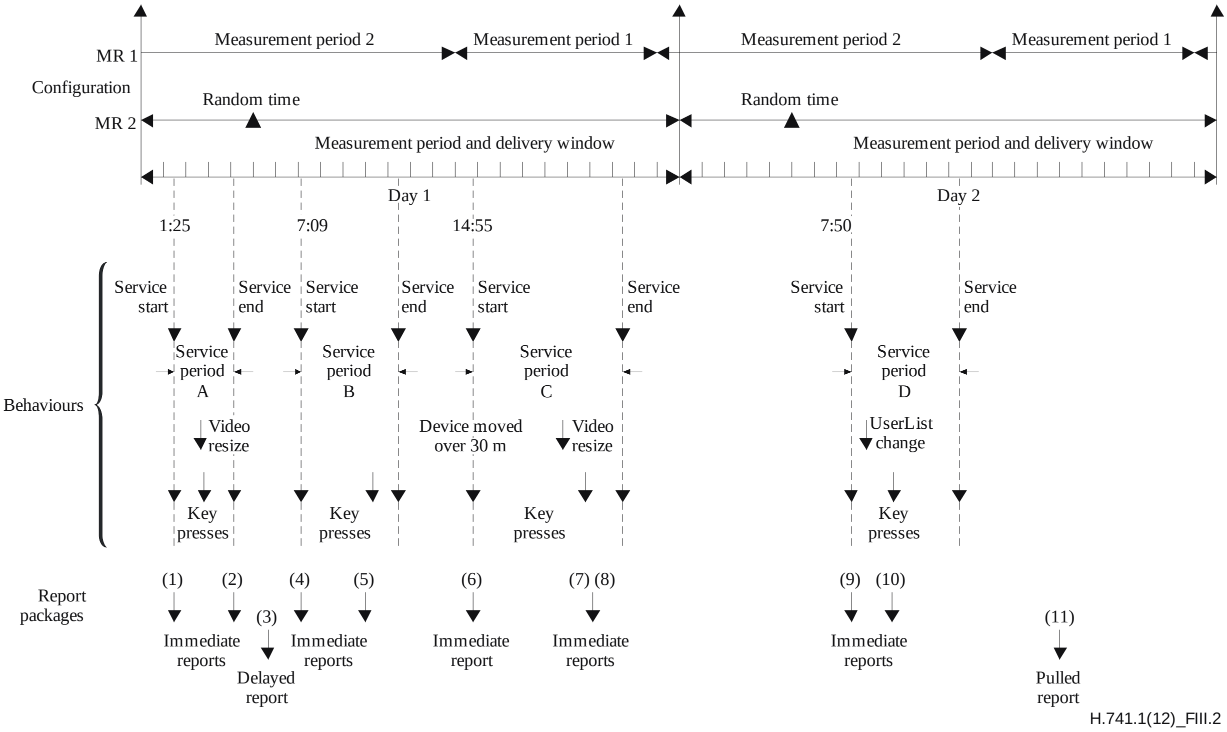


Figure III.2 – Example of end-user behaviours and measurement reports

Eleven report packages indicated in Figure III.2 are delivered as follows:

1) Per measurement request 2, on day one at about 0125 hours, the first measurement of sample values (DeviceInfo, UserBioInfo) is taken due to the occurrence of the first service start of the day. The associated delayed report (3) is delivered at the randomly picked time of 0500 hours.

2) During service period A, a video resize event is not measured. Per measurement request 1, UserList and TDLocation periodic samples are measured every ten minutes and pushed immediately if subsequent sample values change. We assume that all sampled values are new in service period A. UserPresent is also sampled every ten minutes and reported immediately for the service start and unmeasured video resize event since it was associated with a remote key press. The first immediate report (1) is delivered at about 0135 hours, with a second UserPresent report (2) following sampling of video resize key press. The UserPresent sample value for service end is not measured since the next sample time is not during a service period.

3) During service period B, no events are measured. The sample values of UserList and TDLocation are the same as measured during service period A and therefore are not to be reported. UserPresent is sampled every ten minutes and reported immediately for the service start (4) and an unrecognized remote key push (5). The UserPresent sample value for service end is not measured since the next sample time is not during a service period.

4) Between service periods B and C, the TD-AMF device is moved over 30 m, but it is not reported yet since there is no current service period. When service period C starts, the sample value UserList is the same as measured during service period A and therefore is not to be reported. The initial sample values of TDLocation and UserPresent have changed so they are immediately reported (6). A video resize event occurs which is immediately reported (7), followed at the next sample time with a UserPresent immediate report (8) from the video resize key push. The UserPresent sample value for service end is not measured since the next sample time is not during a service period.

5) For day 2, since there are no stored measurements to be reported at the randomly picked time in the delivery window, the associated scheduled delayed report is not sent.

6) At about 0750 hours, the first measurement of sample values (DeviceInfo and UserBioInfo) is taken due to the occurrence of the first service start of the day (service period D). The measurement report is stored.

7) When service period D starts, the sample values of UserList and TDLocation are the same as measured during service period C and therefore are not to be reported. The sample values of UserPresent have changed so an immediate report is sent (9). A UserList change occurs. The UserList and UserPresent which are sampled every ten minutes cause a report to be sent immediately (10) after the sample time where the change is detected. The UserPresent sample value for service end is not measured since the next sample time is not during a service period.

8) A measurement report request received after service period D pulls a report (11) of the stored service start measurements of service period D.

The contents of the 11 example AM report packages are as follows.

AM report package (1) immediately upon service start of service period A, due to the first sample TDLocation, UserList and UserPresent value changes.

```
AMReportPackage (1)
| SubscriberID (0-1) = "WorldspGold012345678"
| TerminalDeviceID (1) = 363566737
| MeasurementReport (1-*)
| | MeasurementRequestID (1) = 1
| | MeasurementReportTriggerTime (1) = 2012-05-30T01:35:00-06:00
| | TDLocation (0-1) = 49.27 -123.11
| | UserList (0-1)
| | | UserIDInfo (1-*)
| | | | UserID (0-1) = "34568234"
| | | | UserIDMethod (0-1)= "login"
| | | | UserIDConfidence(0-1)= 100.0
| | UserPresent (0-*)
| | | PresenceMethod (0-1) = "remotekeypush"
| | | PresenceTime (0-1) = 01:25:00
| | | PresenceConfidence (0-1) = 100.0
| MeasurementReport (1-*) for service specific ServiceStart (not shown)
```

Figure III.3 – Service-common example report package 1

AM report package (2) following ten-minute sampling of the video resize keypress.

```
AMReportPackage (1)
| SubscriberID (0-1) = "WorldspGold012345678"
| TerminalDeviceID (1) = 363566737
| MeasurementReport (1-*)
| | MeasurementRequestID (1) = 1
| | MeasurementReportTriggerTime (1) = 2012-05-30T03:05:00-06:00
| | TDLocation (0-1) = 49.27 -123.11
| | UserPresent (0-*) =
| | | PresenceMethod (0-1) = "remotekeypush"
| | | PresenceTime (0-1) = 02:58:00
| | | PresenceConfidence (0-1) = 100.0
```

Figure III.4 – Service-common example report package 2

AM report package (3) is a delayed report of DeviceInfo and UserBioInfo.

```
AMReportPackage (1)
| SubscriberID (0-1) = "WorldspGold012345678"
| TerminalDeviceID (1) = 363566737
| MeasurementReport (1-*)
| | MeasurementRequestID (1)= 2
| | MeasurementReportTriggerTime (1) = 2012-05-30T01:25:00-06:00
| | DeviceInformation (0-1)
| | | TVandSTBInformation (0-1)
| | | | TVInformation (0-1)
| | | | | TVManuf (0-1)= sam
| | | | | TVModel (0-1)= 3456
| | | | | TVSerialNum (0-1)= 12345678
| | | | STBInformation (0-1)
| | | | | STBManuf (0-1) = ABC457
| | | | | STBModel (0-1) = "3f345"
| | | | | STBSerialNum (0-1) = "142234324"
| | UserBiographicInformation (0-1)
| | | ControlledUserInfoTypeDate (0-*) = "Birthday";
ControlledUserInfoValueDate (1) = 1962-09-24
| | | ControlledUserInfoTypeString (0-*) = "Gender";
ControlledUserInfoValueString (1) = "M"
| | | ControlledUserInfoTypeAddress (0-*) = "BirthLocation";
ControlledUserInfoValueAddress (1) = FR, 75
| | | ControlledUserInfoTypeAddress (0-*) = "UserResidentialAddress";
ControlledUserInfoValueAddress (1) = FR, 75
```

Figure III.5 – Service-common example report package 3

AM report package (4) Following the start of service period B. The first sample value of UserPresent changed due to service start remote key press.

```
AMReportPackage (1)
| SubscriberID (0-1) = "WorldspGold012345678"
| TerminalDeviceID (1) = 363566737
| MeasurementReport (1-*)
| | MeasurementRequestID (1) = 1
| | MeasurementReportTriggerTime (1) = 2012-05-30T07:19:00-06:00
| | UserPresent (0-*)
| | | PresenceMethod (0-1) = "remotekeypush"
| | | PresenceTime (0-1) = 07:09:00
| | | PresenceConfidence (0-1) = 100.0
| MeasurementReport (1-*) for service specific ServiceStart (not shown)
```

Figure III.6 – Service-common example report package 4

AM report package (5) following service start of service period B due to sampling of UserPresent due to an unknown remote key press.

```
AMReportPackage (1)
| SubscriberID (0-1) = "WorldspGold012345678"
| TerminalDeviceID (1) = 363566737
| MeasurementReport (1-*)
| | MeasurementRequestID (1) = 1
| | MeasurementReportTriggerTime (1) = 2012-05-30T10:09:00-06:00
| | UserPresent (0-*)
| | | PresenceMethod (0-1) = "remotekeypush"
| | | PresenceTime (0-1) = 09:59:10
| | | PresenceConfidence (0-1) = 100.0
```

Figure III.7 – Service-common example report package 5

AM report package (6) following the start of service period C. The first sample values of TDLocation and UserPresent have changed.

```
AMReportPackage (1)
| SubscriberID (0-1) = "WorldspGold012345678"
| TerminalDeviceID (1) = 363566737
| MeasurementReport (1-*)
| | MeasurementRequestID (1) = 1
| | MeasurementReportTriggerTime (1)= 2012-05-30T15:05:00-06:00
| | TDLocation (0-1) = 49.27 -123.13
| | UserPresent (0-*)
| | | PresenceMethod (0-1) = "remotekeypush"
| | | PresenceTime (0-1)= 14:55:00
| | | PresenceConfidence (0-1) = 100.0
| MeasurementReport (1-*) for service specific ServiceStart (not shown)
```

Figure III.8 – Service-common example report package 6

AM report package (7) following a video resize event within service period C, an immediate report is sent.

```
AMReportPackage (1)
| SubscriberID (0-1) = "WorldspGold012345678"
| TerminalDeviceID (1) = 363566737
| MeasurementReport (1-*)
| | MeasurementRequestID (1) = 1
| | MeasurementReportTriggerTime (1)= 2012-05-30T19:00:00-06:00
| VideoResize (0-1)
| | ServiceInstanceID (1) = 1
| | ImageWidth (1) = 640
| | ImageHeight (1) = 480
```

Figure III.9 – Service-common example report package 7

AM report package (8) following keypress of video resize within service period C, a UserPresent report is sent due to five-minute sampling.

```
AMReportPackage (1)
| SubscriberID (0-1) = "WorldspGold012345678"
| TerminalDeviceID (1) = 363566737
| MeasurementReport (1-*)
| | MeasurementRequestID (1) = 1
| | MeasurementReportTriggerTime (1)= 2012-05-30T19:05:00-06:00
| | UserPresent (0-*)
| | | PresenceMethod (0-1) = "remotekeypush"
| | | PresenceTime (0-1)= 19:00:01
| | | PresenceConfidence (0-1) = 100.0
```

Figure III.10 – Service-common example report package 8

AM report package (9) Following the start of service period D. The first sample value of UserPresent changed due to service start remote key press.

```
AMReportPackage (1)
| SubscriberID (0-1) = "WorldspGold012345678"
| TerminalDeviceID (1) = 363566737
| MeasurementReport (1-*)
| | MeasurementRequestID (1) = 1
| | MeasurementReportTriggerTime (1)= 2012-05-31T08:00:00-06:00
| | UserPresent (0-*)
| | | PresenceMethod (0-1) = "remotekeypush"
| | | PresenceTime (0-1)= 07:50:00
| | | PresenceConfidence (0-1) = 100.0
| MeasurementReport (1-*) for service specific ServiceStart (not shown)
```

Figure III.11 – Service-common example report package 9

AM report package (10) A UserList change occurs. The UserList and UserPresent which are sampled every ten minutes cause a report to be sent immediately (10) after the sample time where the change is detected.

```
AMReportPackage (1)
| SubscriberID (0-1) = "WorldspGold012345678"
| TerminalDeviceID (1) = 363566737
| MeasurementReport (1-*)
| | MeasurementRequestID (1) = 1
| | MeasurementReportTriggerTime (1)= 2012-05-31T09:10:00-06:00
| | UserList (0-1)
| | | UserIDInfo (1-*)
| | | | UserID (0-1) = "34568233"
| | | | UserIDMethod (0-1)= "login"
| | | | UserIDConfidence(0-1)= 100.0
| | | UserIDInfo (1-*)
| | | | UserID (0-1) = "34568234"
| | | | UserIDMethod (0-1)= "remote personalisation"
| | | | UserIDConfidence(0-1)= 90.0
| | UserPresent (0-*)
| | | PresenceMethod (0-1)= "remotekeypush"
| | | PresenceTime (0-1) = 09:06:00
| | | PresenceConfidence (0-1) = 100.0
```

Figure III.12 – Service-common example report package 10

AM report package (11) following a measurement report request message, service start time stored sample values of DeviceInfo and UserBioInfo are reported.

```
AMReportPackage (1)
| SubscriberID (0-1) = "WorldspGold012345678"
| TerminalDeviceID (1) = 363566737
| MeasurementReport (1-*)
| | MeasurementRequestID (1) = 2
```

```
 | | MeasurementReportTriggerTime (1)= 2012-05-31T16:30:00-06:00
 | | DeviceInformation (0-1)
 | | | TVandSTBInformation (0-1)
 | | | | TVInformation (0-1)
 | | | | | TVManuf (0-1)= sam
 | | | | | TVModel (0-1)= 3456
 | | | | | TVSerialNum (0-1)= 12345678
 | | | | STBInformation (0-1)
 | | | | | STBManuf (0-1) = ABC457
 | | | | | STBModel (0-1) = "3f345"
 | | | | | STBSerialNum (0-1) = "142234324"
 | | UserBiographicInformation (0-1)
 | | | ControlledUserInfoTypeDate (0-*) = "Birthday";
ControlledUserInfoValueDate (1) = 1962-09-24
 | | | ControlledUserInfoTypeString (0-*) = "Gender";
ControlledUserInfoValueString (1) = "M"
 | | | ControlledUserInfoTypeAddress (0-*) = "BirthLocation";
ControlledUserInfoValueAddress (1) = FR, 75
 | | | ControlledUserInfoTypeAddress (0-*) = "UserResidentialAddress";
ControlledUserInfoValueAddress (1) = FR, 75
```

Figure III.13 – Service-common example report package 11

NOTE – The information reported in AM report package (11) refers to the user who started service period D, rather than the one who ended it, identified in AM report package (10).

III.3 Examples using end-user information for filtering configuration packages

When multicast delivery of configuration packages is used, end-user information filtering may be used at the configuration message level, or at the measurement request level, or at both levels.

This first multicast configuration message (defined in Table 7 of [ITU-T H.741.4]) example uses the example user info values given in clause II.11. Relevant defaults are shown in *gray*; these are not required to be explicitly included in the multicast configuration message. The delivery dependent XML is shown without the configuration packages detail.

```
MulticastConfigurationMsg
 | MessageType (1) = 4 (multicast configuration message)
 | ExpirationTime (1)
 | Digest (1)
 | Signature (1)
 | ProtocolVersionMajorID (1) = 1
 | ProtocolVersionMinorID (1) = 0
 | MessageID (1) = 562256
 | LowerThreshold (1) = 0 (Thresholds not used)
 | UpperThreshold (1) = 0 (Thresholds not used)
 | ResponseQualifier (1) = 0 (no acknowledge or error response requested)
 | UserInfoTarget (0-*)
 | | UserInfoTypeString (1) = "occupation"
 | | IgnoreIfUnavailable (0-1) = 0 (do not ignore if "occupation" is unavailable)
 | | UserInfoValueString (1) = "doctor"
 | UserInfoTarget (0-*)
 | | UserInfoTypeString (1) = "income"
 | | IgnoreIfUnavailable (0-1) = 1 (ignore if "income" is unavailable)
 | | UserInfoValueString (1) = "over 200,000 Euros"
 | ImmediateAndFutureConfiguration (1)
```

Figure III.14 – End-user information for configuration packages – Example 1

The AMFConfigPackages contained in ImmediateAndFutureConfiguration (ConfigPackageRequestResponse in [ITU-T H.741.2]) will only be processed by TD-AMFs having a permission level of at least 2, and if an end user has provided generic end user info "occupation" = "doctor" and either "income" = "over 200 000 Euros" or has not provided "income". The use of the ignore if unavailable feature with "income" maximizes the number of TD-AMFs that accept the configuration packages having "income" = "over 200 000 Euros" even if "income" is not made available, with the side effect of including some end users not having "income"= "over 200 000 Euros".

The following configuration package example includes end-user information filtering to qualify individual measurement requests. The details of individual Measurement Requests are not shown.

```
AMFConfigPackage (1)
   PackageID (1) = 9345
   MeasurementRequestSet (1-*)
      MeasurementRequest (1-*) (Measurement Request 1 – details omitted)
         MeasurementRequestID (1-*) = 1
         MeasurementSchedule (1-*)
      MeasurementRequest (1-*) (Measurement Request 2 – details omitted)
         MeasurementRequestID (1-*) = 2
         MeasurementSchedule (1-*)
      MeasurementRequest (1-*) (Measurement Request 3 – details omitted)
         MeasurementRequestID (1-*) = 3
         MeasurementSchedule (1-*)
   MeasurementRequestSetFilter (0-*)
      UserInfoTarget (1-*)
         UserInfoTypeString (1) = "language spoken"
         IgnoreIfUnavailable (0-1) = 0 (do not ignore if "language spoken" is unavailable)
         UserInfoValueString (1) = "French"
      MeasurementRequestID (1-*) = 2
   MeasurementRequestSetFilter (0-*)
      UserInfoTarget (1-*)
         UserInfoTypeString (1) = "language spoken"
         IgnoreIfUnavailable (0-1) = 0 (do not ignore if "language spoken" is
unavailable)
         UserInfoValueString (1) = "German"
      MeasurementRequestID (1-*) = 3
```

Figure III.15 – End-user information filtering of measurement requests – Example 2

In this second example, Measurement Request 1 is configured in the receiving TD-AMF unconditionally. Measurement Request 2 is conditionally configured only if "language spoken" = "French". Measurement Request 3 is conditionally configured only if "language spoken" = "German".

The above two examples could be combined. In which case the filtering at the multicast configuration message level occurs first, then if the TD-AMF processes the configuration package the measurement request filtering will follow.

III.4 Example of UserPermit

The data structure for UserPermit is defined in [ITU-T H.741.2]. In this example, permission level 3 is granted for linear TV channels 150 and 153, on STB and TV, for all content genres except religious or health. Additionally, permission level 2 is granted for all other linear TV channels, on STB, TV and mobile, and for all content genres except religious. Measurements are forbidden when specific permissions are not granted in a permit; in this example, since mobile device measurement is not specified for linear TV channels 150 and 153, this combination must not be measured.

```
UserPermit
   ExpirationDate (0-1) = 2012-09-24
   DefaultPermissionLevel(0-1) = 2
   DefaultAllContentClassExceptList(0-1)
      ContentClassDomain (1-*) = "TV-Anytime"
      ContentClassID (1-*) = "Religious"
   AnonUserID (0-1) = 24566778
   UserID (0-1) = "34568234"
   UserPermissionSet (0-*)
      PermissionLevel (0-1) = 3
      UserPermission (1-*)
         ChannelQualifier (0-1)
           ChannelList (0-1)
              ServiceIdentifier (1-*) =  "channel50"
              ServiceIdentifier (1-*) =  "channel53"
         TerminalDeviceSet (0-1)
            TerminalDeviceType (1-*) = 0
            TerminalDeviceType (1-*) = 1
         AllContentClassExceptList (0-1)
            ContentClassDomain (1-*) = "TV-Anytime"
               ContentClassID (1-*) = "Health"
               ContentClassID (1-*) = "Religious"
```

```
UserPermissionSet (0-*)
   UserPermission (1-*)
      ChannelQualifier (0-1)
        AllChannelsExceptList (0-1)
           ServiceIdentifier (1-*) =  "channel50"
           ServiceIdentifier (1-*) =  "channel53"
      TerminalDeviceSet (0-1)
         TerminalDeviceType (1-*) = 0
         TerminalDeviceType (1-*) = 1
         TerminalDeviceType (1-*) = 2
```

Figure III.16 – Example user permit

The XML schema instances for examples of TD-AMF configurations, reports and permits are in Appendix IX.

Appendix IV

Considerations of end-user permission levels

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

Table IV.1 relates the measurements, the implications for the AM system, the potential for an end-user's data profile to threaten privacy, and services for the four permission levels of AM.

Table IV.1 – AM permission levels, their impact on the AM system, privacy infringement potential and supportable services

	Permission Level 0 (default)	**Permission Level 1**	**Permission Level 2**	**Permission Level 3**
End-user permission	Not required	Required	Required	Required
Permitted measured data	None	End-user behaviours and device info, distinguishable end user, no end-user information	End-user behaviours and device info, distinguishable end user, and anonymous end-user information	End-user behaviours and device info, distinguishable end user, anonymous end-user information, and identifiable subscriber or end-user information
Example data	No data is measured	Channel 5 was watched by anonymous end user #12683304 on mobile device model "X"	Channel 5 was watched by anonymous end user #12683304, interested in gardening, on mobile device model "X"	Channel 5 was watched on mobile device model "X" being used by subscriber or end user "John Smith" who is interested in gardening
Other impact on AM system	Prevent or filter out measurements request	Correlation among end-users' devices possible	Correlation among end-users' devices possible	Correlation among end-users' devices possible Controlled subscriber/end user information requires special security handling
Privacy infringement potential	None	Measured data alone may not influence privacy profile. Measured data plus additional data may influence privacy profile	Measured data alone may not influence privacy profile. Measured data plus additional data may influence privacy profile	Measured data alone may influence privacy profile

Table IV.1 – AM permission levels, their impact on the AM system, privacy infringement potential and supportable services

	Permission Level 0 (default)	Permission Level 1	Permission Level 2	Permission Level 3
Additional SP services supportable	Plain subscription	Targeted advertisement and content recommendation Content rating and engagement reporting	Better targeted advertisement and content recommendation Content rating and engagement reporting	IPTV end-user engagement driven personalized communications Even better targeted advertisement and content recommendation Content rating and engagement reporting

Appendix V

Considerations regarding the unlinkability property

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

Clause 9.1.5 briefly explains that the AM system relies upon the AGF to remove unintentional linkability information before providing information to higher functions. However, a network-based approach to provide unlinkability for AM may be possible. This appendix provides considerations for such an approach.

It is possible to correlate an anonymous end user (either in permission level 2 or permission level 1) with other information previously or subsequently obtained about that user. To avoid such a correlation, unlinkability property for AM report submission is recommended – that is, the AGF may communicate directly with TD-AMFs but TD-AMFs send their AM reports indirectly. Indirection of AM reports is the basis to implement unlinkability which requires the use of additional network bandwidth.

Following two scenarios highlight the need for the unlinkability property in AM architecture to achieve anonymity for TD-AMF from an AGF:

1) Source IP address: When an end user submits AM reports with permission level 3 (in which all possible end user attributes – controlled or un-controlled information may become part of AM reports) and later changes permission level to either 2 or 1. Even though AM reports with permission level 1 do not have any personally identifiable information of the end user and sent with AnonID, the AGF can correlate AM reports with permission level 2 or 1 to AM reports with permission level 3 based on the source IP address of AM report messages.

2) MessageID: In pull delivery mode, an AGF sends a measurement report request with a unique identifier called MessageID. In response to the measurement report request, a TD-AMF generates its AM report consisting of the MessageID provided by the AGF. Assuming that the "source address" unlinkability is supported in AM system, use of persistent of identifiers like MessageID undermine the unlinkability property since AGF knows to which TD-AMF a particular MessageID is sent. Even if TD-AMF manages to hide its source address, the MessageID element in the AM report reveals the identity of the TD-AMF.

   There can be other persistent identifiers similar to MessageID which may have potential to de-anonymize end users with permission level 1 or 2. Further study of AM message communications and study of overall AM architecture is needed.

The unlinkability property can be achieved using privacy enhancing technologies from two broad classes of alternatives:

A. TTP (Trusted third party): Employing a trusted third party that acts as a proxy for TD-AMFs to submit AM reports, see Figure V.1.

B. P2P (peer-to-peer): Collaboration among peer TD-AMFs to forward each other's AM reports to an AGF, see Figure V.2.

One method from each alternative class is provided below:

- TOR (The Onion Router [b-TOR]) – In this type of TTP-based method, an intermediary is introduced between an AM report sender (TD-AMF) and the receiver (AGF). The internal designs of this kind of method may vary from each other but the input and output interfaces are similar: they accept a communication from sender and deliver it to intended receiver in such a fashion that the receiver cannot provably find out who the sender is. It is recommended that TD-AMFs choose the TTP instead of AGF suggesting one. To achieve unlinkability from AGF, TD-AMFs (end users) put their trust in a trusted-third-party.

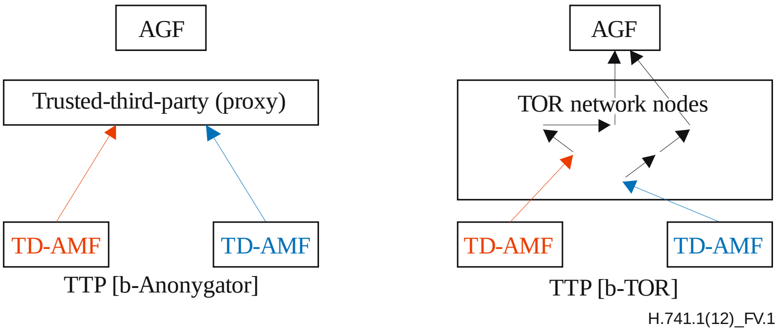


Figure V.1 – Trusted third-party methods

– Crowds [b-Crowds] – In this type of P2P-based method, a set of TD-AMFs becomes part of a group called the anonymous set. The anonymous set may be formed by an AGF or can be formed among TD-AMFs themselves. Each member of the anonymous set forwards its own AM report and other incoming AM reports to a randomly chosen neighbour. The AGF may be allowed to be part of the anonymous set. When the AGF is not part of the anonymous set, the TD-AMFs in the anonymous set submit all the reports directly to the AGF after performing shuffling of their reports for a fixed time period. In Figure V.2 at time t_1 the TD-AMFs belonging to an anonymous set exchange their AM reports. Subsequently at time t_2 these reports are sent to the AGF. To achieve unlinkability from AGF, TD-AMFs pay a cost in terms of extra inter-TD-AMF computation and temporary local storage.

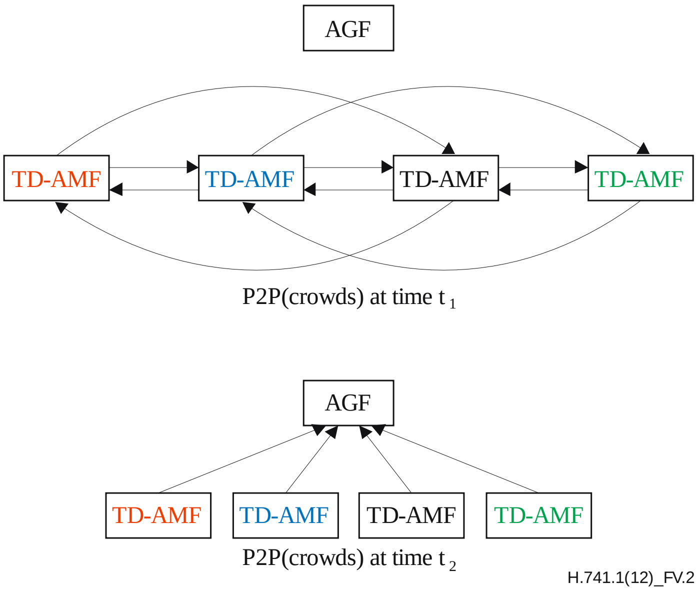


Figure V.2 – P2P methods

The P2P-based alternative is preferred over the TTP-based alternative. In the P2P-based alternative, the trust of the TD-AMF is spread across peer TD-AMFs whereas in the TTP-based alternative, absolute trust is placed in the trusted-third-party and collusion of such a trusted-third-party with AGF or other stakeholders interested in end-user PII puts the end users' anonymity at stake. Therefore the P2P-based approach limits the scope of an attacker in comparison to the TTP-based approach.

While choosing among the alternative methods to achieve unlinkability, it is important to consider the required modifications to the AM architecture. P2P-based alternative can achieve unlinkability without introducing any new entity to the AM architecture, whereas TTP-based alternative introduces a trusted-third-party to the AM architecture. It is possible to keep the trusted-third-party outside of AM architecture and re-route the AM reports via the trusted-third-party but that will make AM architecture incapable of providing complete anonymity to end users on its own.

Other considerations for unlinkability

Even after providing unlinkability property in AM architecture with the help of a P2P/TTP-based alternative, it is possible for an AGF to link end users to their reports. Following are the scenarios that may lead to linkability of end users, if left unaddressed.

– Correlation with the help of other applications – The end user access terminal may be running other interactive non-AM applications. If other applications running on end-user's terminal are reporting information that is part of AM reports being submitted anonymously, the unlinkability property of AM will be undermined.

– Correlation with the content consumption logs – The IPTV content provider has logs of each subscriber's content access. Such logs correlated with the anonymous reports may reveal identity of the report's generator.

The impact of unlinkability implementations on AM abnormal situation handling and non-repudiation needs further study, since TD-AMFs which generate incorrect reports need to be addressed.

The implementation and design of the unlinkability property for AM are recommended to be in line with the current guidelines on privacy per [b-NIST PUB 800-122] and [b-FTC 120326] and is for further study.

Appendix VI

Considerations for AM vendors

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

Aggregation methods

Analysis of measurements may lead to aggregation by many methods including aggregation:

- over a subscriber's end-user device
- over a user's end-user device
- over audience measurement functions in end-user functions, network functions and content delivery functions
- over time
- over device types
- over a geography
- over linear channels in the linear service
- over the x-PVR service
- over the VoD service
- over content
- over end-user's behaviours
- over combinations of the above.

There may be value to multiple stakeholders derivable from each aggregation method. For example, aggregation over a geographic area may be valuable to geographic businesses for location-based advertising; aggregation over time may be valuable to industry metrics that are defined by all viewing that occurs, including live broadcast plus three days; and aggregation across content from the same studio for content providers to guide future content.

Appendix VII

Audience measurement capabilities and profiles

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

Table VII.1 lists the capabilities of TD-AMFs.

Table VII.1 – TD-AMF capability list

Area of capability	Capability	References
Transport protocols	Specific protocols are out of scope of AM	[ITU-T H.741.4]
Transport delivery mode	Unicast	[ITU-T H.741.4]
	Multicast	[ITU-T H.741.4]
Cryptographic protocols	TLS	Clause 9.1
	TLS-SRP	Clause 9.1
Permission mode	External	Clause 9.2.1
	Internal	Clause 9.2.2
	Hybrid	Clause 9.2.3
Configuration mode	Push	[ITU-T H.741.0]
	Pull	[ITU-T H.741.0]
	Hybrid	[ITU-T H.741.0]
Measurement Triggers	Event	Clause 7.1.2.4
	Time sampling	Clause 7.1.2.4
	Service start sampling	Clause 7.1.2.4
Report delivery mode	Immediate Push	Clause 7.1.2.6
	Delayed Push	Clause 7.1.2.6
	Pull	Clause 7.1.2.6
	Delayed Push and Pull	Clause 7.1.2.6
Operational Management	Multicast Acknowledgements	Clause 7.1.1.2
	Multicast threshold ranges sub-addressing	Clause 7.1.1.2
	Multicast device type sub-addressing	Clause 7.1.1.2
	Multicast end-user info sub-addressing	Clause 7.1.1.2
	Multicast MAC addresses sub-addressing	Clause 7.1.1.2
	Multicast error reporting	Clause 7.1.1.2
	Measurement report end user info filtering	Clause 7.1.2
	Content Filtering	Clause 7.1.2.2

These capabilities are included in the capability data structure (see Table 2 of [ITU-T H.741.2]).

A set of AM capability profiles as a short-hand way to identify subsets of capability options for TD-AMFs would be useful. Capability profiles would make it easier for vendors, integrators and service providers to understand product capabilities. TD-AMFs could be identified as having AM capability profile 1, or 2, or 3, etc. which would relate to a specific subset of capability options from Table VIII.1 and service-specific capability options listed in an appendix of [ITU-T H.741.3]. The definition of such capability profiles is for further study.

Appendix VIII

XML schema on the data structures for audience measurement service discovery

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

This is the XML schema that can be exchanged for audience measurement service discovery.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns:am1="urn:itut:iptv:am:part1:2012"
xmlns:am2="urn:itut:iptv:am:part2:2012" xmlns="http://www.w3.org/2001/XMLSchema"
targetNamespace="urn:itut:iptv:am:part1:2012" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <annotation>
    <documentation xml:lang="en"><![CDATA[
      This schema (H.770-v1.xsd) contains the elements to be
      included in [b-ITU-T H.770] for the discovery of AM services,
      which are described in Appendix I of H.741.1.doc.
      The namespace of the schema is "urn:itut:iptv:am:part1:2012", and
      its preferred namespace prefix is "am1".]]>
    </documentation>
  </annotation>
  <import namespace="urn:itut:iptv:am:part2:2012" schemaLocation="H.741.2-
v1.xsd"/>
  <import namespace="http://www.w3.org/XML/1998/namespace"
schemaLocation="http://www.w3.org/2001/03/xml.xsd"/>
  <!-- ================================================================ -->
  <!-- ================================================================ -->
  <!-- Data Elements for H.741 Part.1 -->
  <!-- ================================================================ -->
  <!-- ================================================================ -->
  <!-- ============================================== -->
  <!-- Elements for the discovery of AM services (Table I.1) -->
  <!-- ============================================== -->
  <element name="AMServiceDiscovery" type="am1:AMServiceDiscoveryType"/>
  <complexType name="AMServiceDiscoveryType">
    <sequence>
      <element name="PermissionOperationModes" type="am1:PermissionLevelType"
maxOccurs="unbounded"/>
      <element name="Addresses" type="am1:AddressesType"/>
      <element name="ConfigurationModes" type="am1:ConfigurationModesType"/>
      <element name="MeasurementReportTransportProtocol" type="am1:ProtocolType"
maxOccurs="unbounded"/>
      <element name="CryptographicProtocol"
type="am1:CryptographicProtocolWithPreferredType" maxOccurs="unbounded"/>
      <element name="Compression" type="am1:CompressionWithPreferredType"
minOccurs="0" maxOccurs="unbounded"/>
    </sequence>
    <attribute name="preferred" type="boolean" use="optional" default="false"/>
  </complexType>
  <!-- ============================================== -->
  <simpleType name="PermissionLevelType">
    <restriction base="NMTOKEN">
      <enumeration value="External"/>
      <enumeration value="Internal"/>
      <enumeration value="Hybrid"/>
    </restriction>
  </simpleType>
  <!-- ============================================== -->
  <complexType name="AddressesType">
    <sequence>
```

```
      <element name="Unicast" type="am1:UnicastType" minOccurs="0"/>
      <element name="Multicast" type="am1:MulticastType" minOccurs="0"/>
    </sequence>
  </complexType>
  <complexType name="UnicastType">
    <sequence>
      <element name="ConfigRequestAddress" type="am2:URL" minOccurs="0"/>
      <element name="ErrorAddress" type="am2:URL" minOccurs="0"/>
    </sequence>
  </complexType>
  <complexType name="MulticastType">
    <sequence>
      <element name="MulticastHybridAddress" type="am1:MulticastAddressType"
minOccurs="0"/>
      <element name="MulticastPushAddress" type="am1:MulticastAddressType"
minOccurs="0"/>
      <element name="ErrorAddress" type="am2:URL" minOccurs="0"/>
      <element name="AckAddress" type="am2:URL" minOccurs="0"/>
    </sequence>
  </complexType>
  <complexType name="MulticastAddressType">
    <simpleContent>
      <extension base="am2:IpAddressType">
        <attribute name="port" type="unsignedShort" use="required"/>
        <attribute name="sourceAddress" type="am2:IpAddressType"
use="required"/>
      </extension>
    </simpleContent>
  </complexType>
  <!-- ============================================== -->
  <complexType name="ConfigurationModesType">
    <sequence>
      <element name="Push" type="am1:ConfigurationModeType" minOccurs="0"/>
      <element name="Pull" type="am1:ConfigurationModeType" minOccurs="0"/>
      <element name="Hybrid" type="am1:ConfigurationModeType" minOccurs="0"/>
    </sequence>
  </complexType>
  <complexType name="ConfigurationModeType">
    <sequence>
      <element name="TransportProtocol" type="am1:ProtocolType"
maxOccurs="unbounded"/>
      <!-- The element name "TransportProtocols" is changed into
"TransportProtocol" for consistency with the       -->
    </sequence>
    <attribute name="preferred" type="boolean" use="optional" default="false"/>
  </complexType>
  <complexType name="ProtocolType">
    <simpleContent>
      <extension base="NMTOKEN">
        <attribute name="preferred" type="boolean" use="optional"
default="false"/>
      </extension>
    </simpleContent>
  </complexType>
  <!-- ============================================== -->
  <complexType name="CryptographicProtocolWithPreferredType">
    <simpleContent>
      <extension base="am2:CryptographicProtocolType">
        <attribute name="preferred" type="boolean" use="optional"
default="false"/>
      </extension>
    </simpleContent>
  </complexType>
  <!-- ============================================== -->
  <complexType name="CompressionWithPreferredType">
    <simpleContent>
      <extension base="am2:CompressionType">
        <attribute name="preferred" type="boolean" use="optional"
default="false"/>
      </extension>
    </simpleContent>
  </complexType>
</schema>
```

Appendix IX

XML schema instances for TD-AMF configurations, reports and permits

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

These are the XML schema instances for examples of TD-AMF configurations, reports and permits defined in Appendix III. These instances are based on Appendix VIII.

IX.1 Instance based on clause III.1

Figure III.1 (Service-common example configuration package) shows values assigned to the configuration package data structure.

Figure IX.1 is an instance based on Figure III.1.

```
<AMFConfigurationPackage packageId="12345" packageVersion="2"
effectivityDateAndTime="2013-10-10T12:00:00.00">
  <MeasurementRequestSet>
    <DefaultMeasurementPeriod>
      <DayOfTheWeek>Everyday</DayOfTheWeek>
    </DefaultMeasurementPeriod>
    <DefaultNothingNewReportMode>
      CreateCompleteAMSample
    </DefaultNothingNewReportMode>
    <DefaultDeliveryAddress>
    http://defaultdeliveryaddress.com</DefaultDeliveryAddress>
    <DefaultRetransmitNumber>5</DefaultRetransmitNumber>
    <DefaultMeasurementReportNumberByPush>
    AMReportPushedAsSoonAsProduced</DefaultMeasurementReportNumberByPush>
    <DefaultMaxTimeBetweenDelivery>0</DefaultMaxTimeBetweenDelivery>
    <DefaultDeliveryWindow startTime="00:00:00.00" endTime="23:59:59.99"/>
    <MeasurementRequest measurementRequestId="1">
      <MeasurementSchedule>
        <MeasurementPeriod>
          <DayOfTheWeek startTime="14:00:00.00"
endTime="23:00:00.00">Everyday</DayOfTheWeek>
        </MeasurementPeriod>
        <EventTrigger>
          <Priority>5</Priority>
          <Event eventName="VideoResize"/>
        </EventTrigger>
        <TimeTrigger>
          <Priority>5</Priority>
          <Periodicity>300</Periodicity>
          <SampleSet sampleSetName="UserList"/>
          <SampleSet sampleSetName="UserPresent"/>
          <SampleSet sampleSetName="TDLocation">
            <SampleSetQualifier>30</SampleSetQualifier>
          </SampleSet>
        </TimeTrigger>
      </MeasurementSchedule>
      <MeasurementSchedule>
        <MeasurementPeriod>
          <DayOfTheWeek startTime="23:00:00.00"
endTime="14:00:00.00">Everyday</DayOfTheWeek>
        </MeasurementPeriod>
        <TimeTrigger>
          <Priority>5</Priority>
          <Periodicity>600</Periodicity>
          <SampleSet sampleSetName="UserList"/>
          <SampleSet sampleSetName="UserPresent"/>
          <SampleSet sampleSetName="TDLocation">
            <SampleSetQualifier>30</SampleSetQualifier>
          </SampleSet>
        </TimeTrigger>
      </MeasurementSchedule>
      <MeasurementDeliverySchedule>
        <ImmediatePush/>
      </MeasurementDeliverySchedule>
    </MeasurementRequest>
    <MeasurementRequest measurementRequestId="2">
      <MeasurementSchedule>
        <ServiceStartTrigger>
          <Priority>1</Priority>
          <Interval>1</Interval>
          <SampleSet sampleSetName="DeviceInfo"/>
          <SampleSet sampleSetName="UserBioInfo"/>
        </ServiceStartTrigger>
      </MeasurementSchedule>
      <MeasurementDeliverySchedule>
        <DelayedPushAndPull/>
      </MeasurementDeliverySchedule>
    </MeasurementRequest>
  </MeasurementRequestSet>
</AMFConfigurationPackage>
```

Figure IX.1 – Instance for service-common example configuration package

IX.2 Instances based on clause III.2

Figure III.2 is an example of end-user behaviours and measurement reports. Eleven figures, Figures III.3 to III.13, are service-common example report packages.

IX.2.1 Instance based on Figure III.3

Figure IX.2 is an instance based on Figure III.3 (Service-common example report package 1).

```
<am4:AMReportPackage subscriberIdref="WorldspGold012345678"
terminalDeviceIdref="36356673">

  <MeasurementReport measurementRequestIdref="1"
measurementReportTriggerTime="2012-05-30T01:35:00-06:00">

    <TDLocation latitude="49.27" longitude="-123.11"/>

    <UserList>

      <UserIdInfo userId="34568234">

        <UserIdMethod>login</UserIdMethod>

        <UserIdConfidence>100.0</UserIdConfidence>

      </UserIdInfo>

    </UserList>

    <UserPresent>

      <PresenceMethod>RemoteKeyPush</PresenceMethod>

      <PresenceTime>01:25:00</PresenceTime>

      <PresenceConfidence>100.0</PresenceConfidence>

    </UserPresent>

  </MeasurementReport>

</am4:AMReportPackage>
```

Figure IX.2 – Instance for service-common example report package 1

IX.2.2 Instance based on Figure III.4

Figure IX.3 is an instance based on Figure III.4 (Service-common example report package 2).

```
<am4:AMReportPackage subscriberIdref="WorldspGold012345678"
terminalDeviceIdref="36356673">
  <MeasurementReport measurementRequestIdref="1"
measurementReportTriggerTime="2012-05-30T03:05:00-06:00">
    <TDLocation latitude="49.27" longitude="-123.11"/>
    <UserPresent>
      <PresenceMethod>RemoteKeyPush</PresenceMethod>
      <PresenceTime>02:58:00</PresenceTime>
      <PresenceConfidence>100.0</PresenceConfidence>
    </UserPresent>
  </MeasurementReport>
</am4:AMReportPackage>
```

Figure IX.3 – Instance for service-common example report package 2

IX.2.3 Instance based on Figure III.5

Figure IX.4 is an instance based on Figure III.5 (Service-common example report package 3).

```
<am4:AMReportPackage subscriberIdref="WorldspGold012345678"
terminalDeviceIdref="36356673">
  <MeasurementReport measurementRequestIdref="2"
measurementReportTriggerTime="2012-05-30T01:25:00-06:00">
    <DeviceInformation>
      <STBInformation>
        <Manufacturer>ABC457</Manufacturer>
        <Model>3f345</Model>
        <SerialNum>142234324</SerialNum>
      </STBInformation>
      <TVInformation>
        <Manufacturer>sam</Manufacturer>
        <Model>3456</Model>
        <SerialNum>12345678</SerialNum>
      </TVInformation>
    </DeviceInformation>
    <UserBiographicInformation>
      <UserIdBioInfo>
        <ControlledUserInfoString type="Gender">M</ControlledUserInfoString>
        <ControlledUserInfoDate type="BirthDay">1962-09-
24</ControlledUserInfoDate>
        <ControlledUserInfoAddress type="BirthLocation">FR,
75</ControlledUserInfoAddress>
        <ControlledUserInfoAddress type="UserResidentialAddress">FR,
75</ControlledUserInfoAddress>
      </UserIdBioInfo>
    </UserBiographicInformation>
  </MeasurementReport>
</am4:AMReportPackage>
```

Figure IX.4 – Instance for service-common example report package 3

IX.2.4 Instance based on Figure III.6

Figure IX.5 is an instance based on Figure III.6 (Service-common example report package 4).

```
<am4:AMReportPackage subscriberIdref="WorldspGold012345678"
terminalDeviceIdref="36356673">
  <MeasurementReport measurementRequestIdref="1"
measurementReportTriggerTime="2012-05-30T07:19:00-06:00">
    <UserPresent>
      <PresenceMethod>RemoteKeyPush</PresenceMethod>
      <PresenceTime>07:09:00</PresenceTime>
      <PresenceConfidence>100.0</PresenceConfidence>
    </UserPresent>
  </MeasurementReport>
</am4:AMReportPackage>
```

Figure IX.5 – Instance for service-common example report package 4

IX.2.5 Instance based on Figure III.7

Figure IX.6 is an instance based on Figure III.7 (Service-common example report package 5).

```
<am4:AMReportPackage subscriberIdref="WorldspGold012345678"
terminalDeviceIdref="36356673">
  <MeasurementReport measurementRequestIdref="1"
measurementReportTriggerTime="2012-05-30T10:09:00-06:00">
    <UserPresent>
      <PresenceMethod>RemoteKeyPush</PresenceMethod>
      <PresenceTime>09:59:00</PresenceTime>
      <PresenceConfidence>100.0</PresenceConfidence>
    </UserPresent>
  </MeasurementReport>
</am4:AMReportPackage>
```

Figure IX.6 – Instance for service-common example report package 5

IX.2.6 Instance based on Figure III.8

Figure IX.7 is an instance based on Figure III.8 (Service-common example report package 6).

```
<am4:AMReportPackage subscriberIdref="WorldspGold012345678"
terminalDeviceIdref="36356673">
  <MeasurementReport measurementRequestIdref="1"
measurementReportTriggerTime="2012-05-30T15:05:00-06:00">
    <TDLocation latitude="49.27" longitude="-123.13"/>
    <UserPresent>
      <PresenceMethod>RemoteKeyPush</PresenceMethod>
      <PresenceTime>14:55:00</PresenceTime>
      <PresenceConfidence>100.0</PresenceConfidence>
    </UserPresent>
  </MeasurementReport>
</am4:AMReportPackage>
```

Figure IX.7 – Instance for service-common example report package 6

IX.2.7 Instance based on Figure III.9

Figure IX.8 is an instance based on Figure III.9 (Service-common example report package 7).

```
<am4:AMReportPackage subscriberIdref="WorldspGold012345678"
terminalDeviceIdref="36356673">
  <MeasurementReport measurementRequestIdref="1"
measurementReportTriggerTime="2012-05-30T19:00:00-06:00">
    <VideoResize serviceInstanceIdref="1">
      <ResizedImage width="640" height="480"/>
    </VideoResize>
  </MeasurementReport>
</am4:AMReportPackage>
```

Figure IX.8 – Instance for service-common example report package 7

IX.2.8 Instance based on Figure III.10

Figure IX.9 is an instance based on Figure III.10 (Service-common example report package 8).

```
<am4:AMReportPackage subscriberIdref="WorldspGold012345678"
terminalDeviceIdref="36356673">
  <MeasurementReport measurementRequestIdref="1"
measurementReportTriggerTime="2012-05-30T09:05:00-06:00">
    <UserPresent>
      <PresenceMethod>RemoteKeyPush</PresenceMethod>
      <PresenceTime>19:09:01</PresenceTime>
      <PresenceConfidence>100.0</PresenceConfidence>
    </UserPresent>
  </MeasurementReport>
</am4:AMReportPackage>
```

Figure IX.9 – Instance for service-common example report package 8

IX.2.9 Instance based on Figure III.11

Figure IX.10 is an instance based on Figure III.11 (Service-common example report package 9).

```
<am4:AMReportPackage subscriberIdref="WorldspGold012345678"
terminalDeviceIdref="36356673">
  <MeasurementReport measurementRequestIdref="1"
measurementReportTriggerTime="2012-05-31T08:00:00-06:00">
    <UserPresent>
      <PresenceMethod>RemoteKeyPush</PresenceMethod>
      <PresenceTime>07:50:00</PresenceTime>
      <PresenceConfidence>100.0</PresenceConfidence>
    </UserPresent>
  </MeasurementReport>
</am4:AMReportPackage>
```

Figure IX.10 – Instance for service-common example report package 9

IX.2.10 Instance based on Figure III.12

Figure IX.11 is an instance based on Figure III.12 (Service-common example report package 10).

```xml
<am4:AMReportPackage subscriberIdref="WorldspGold012345678"
terminalDeviceIdref="36356673">
  <MeasurementReport measurementRequestIdref="1"
measurementReportTriggerTime="2012-05-31T09:10:00-06:00">
    <UserList>
      <UserIdInfo userId="34568233">
        <UserIdMethod>login</UserIdMethod>
        <UserIdConfidence>100.0</UserIdConfidence>
      </UserIdInfo>
      <UserIdInfo userId="34568234">
        <UserIdMethod>remotepersonalization</UserIdMethod>
        <UserIdConfidence>90.0</UserIdConfidence>
      </UserIdInfo>
    </UserList>
    <UserPresent>
      <PresenceMethod>RemoteKeyPush</PresenceMethod>
      <PresenceTime>09:06:00</PresenceTime>
      <PresenceConfidence>100.0</PresenceConfidence>
    </UserPresent>
  </MeasurementReport>
</am4:AMReportPackage>
```

Figure IX.11 – Instance for service-common example report package 10

IX.2.11 Instance based on Figure III.13

Figure IX.12 is an instance based on Figure III.13 (Service-common example report package 11).

```xml
<am4:AMReportPackage subscriberIdref="WorldspGold012345678"
terminalDeviceIdref="36356673">
  <MeasurementReport measurementRequestIdref="2"
measurementReportTriggerTime="2012-05-31T16:30:00-06:00">
    <DeviceInformation>
      <TVInformation>
        <Manufacturer>sam</Manufacturer>
        <Model>3456</Model>
        <SerialNum>12345678</SerialNum>
      </TVInformation>
      <STBInformation>
        <Manufacturer>ABC457</Manufacturer>
        <Model>3f345</Model>
        <SerialNum>142234324</SerialNum>
      </STBInformation>
      </DeviceInformation>
    <UserBiographicInformation>
      <UserIdBioInfo>
        <ControlledUserInfoString type="Gender">M</ControlledUserInfoString>
        <ControlledUserInfoDate type="BirthDay">1962-09-
24</ControlledUserInfoDate>
        <ControlledUserInfoAddress type="BirthLocation">FR,
75</ControlledUserInfoAddress>
        <ControlledUserInfoAddress type="UserResidentialAddress">FR,
75</ControlledUserInfoAddress>
      </UserIdBioInfo>
    </UserBiographicInformation>
  </MeasurementReport>
</am4:AMReportPackage>
```

Figure IX.12 – Instance for service-common example report package 11

IX.3 Instances based on Appendix III.3

Figure III.14 is an example of end-user information for configuration packages. Figure III.15 is an example of end-user information filtering of measurement requests.

IX.3.1 Instance based on Figure III.14

Figure IX.13 is an instance based on Figure III.14 (End-user information for configuration packages).

```
<?xml version="1.0" encoding="UTF-8"?>
<am4:MulticastConfigMsg protocolVersionMajorId="3F"
protocolVersionMinorId="57" messageId="562256" expirationTime="2012-05-
05T23:59:59" xmlns:am4="urn:itut:iptv:am:part4:2012"
xmlns:am3="urn:itut:iptv:am:part3:2012"  xmlns="urn:itut:iptv:am:part2:2012"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:itut:iptv:am:part4:2012 H.741.4-v1.xsd">
  <am4:MessageType>MulticastConfigurationMsg</am4:MessageType>
  <am4:Digest></am4:Digest>
  <am4:Signature>12</am4:Signature>
  <am4:ResponseQualifier>NoAcknowledge_Or_ErrorResponseRequested
</am4:ResponseQualifier>
  <am4:ThresholdRange lower="00" upper="00"/>
  <am4:UserInfoTargetString type="occupation"
ignoreIfUnavailable="false">doctor</am4:UserInfoTargetString>
  <am4:UserInfoTargetString type="income" ignoreIfUnavailable="true">over
200,000 Euros</am4:UserInfoTargetString>
  <am4:ImmediateAndFutureConfiguration/>
</am4:MulticastConfigMsg>
```

Figure IX.13 – Instance for end-user information for configuration packages

IX.3.2 Instance based on Figure III.15

Figure IX.14 is an instance based on Figure III.15 (End-user information filtering of measurement requests).

```
<AMFConfigurationPackage packageId="9345">
  <MeasurementRequestSet>
    <MeasurementRequest measurementRequestId="1">
      <MeasurementSchedule/>
    </MeasurementRequest>
    <MeasurementRequest measurementRequestId="2">
      <MeasurementSchedule/>
    </MeasurementRequest>
    <MeasurementRequest measurementRequestId="3">
      <MeasurementSchedule/>
    </MeasurementRequest>
  </MeasurementRequestSet>
  <MeasurementRequestSetFilter measurementRequestIdref="2">
    <UserInfoTargetString type="language spoken">French</UserInfoTargetString>
  </MeasurementRequestSetFilter>
  <MeasurementRequestSetFilter measurementRequestIdref="3">
    <UserInfoTargetString type="language spoken">German</UserInfoTargetString>
  </MeasurementRequestSetFilter>
</AMFConfigurationPackage>
```

Figure IX.14 – Instance for end-user information filtering of measurement requests

IX.4 Instance based on Appendix III.4

Figure III.16 is an example of user permit.

Figure IX.15 is an instance based on Figure III.16 (Example user permit).

```
<UserPermitInfo>
  <UserPermit anonUserIdref="24566778" userIdref="34568234"
expirationDate="2012-09-24">
    <DefaultPermissionLevel>NoInformation</DefaultPermissionLevel>
    <DefaultAllContentClassExceptList>
      <ContentClass domain="TV-Anytime">Religious</ContentClass>
    </DefaultAllContentClassExceptList>
    <UserPermissionSet>
      <PermissionLevel>OnlyDistinguishabilityInfo</PermissionLevel>
      <UserPermission xsi:type="am3:LTVUserPermissionType">
        <TerminalDeviceSet>
          <TerminalDeviceType>STB</TerminalDeviceType>
          <TerminalDeviceType>TV</TerminalDeviceType>
        </TerminalDeviceSet>
        <AllContentClassExceptList>
          <ContentClass domain="TV-Anytime">Health</ContentClass>
          <ContentClass domain="TV-Anytime">Religious</ContentClass>
        </AllContentClassExceptList>
        <am3:ChannelQualifier>
          <am3:ChannelList serviceIdref="channel50 channel53"/>
        </am3:ChannelQualifier>
      </UserPermission>
    </UserPermissionSet>
    <UserPermissionSet>
      <UserPermission xsi:type="am3:LTVUserPermissionType">
        <TerminalDeviceSet>
          <TerminalDeviceType>STB</TerminalDeviceType>
          <TerminalDeviceType>TV</TerminalDeviceType>
          <TerminalDeviceType>Mobile</TerminalDeviceType>
        </TerminalDeviceSet>
        <am3:ChannelQualifier>
          <am3:ChannelList serviceIdref="channel50 channel53"/>
        </am3:ChannelQualifier>
      </UserPermission>
    </UserPermissionSet>
  </UserPermit>
</UserPermitInfo>
```

Figure IX.15 – Instance for example user permit

Bibliography

[b-ITU-T H.720] Recommendation ITU-T H.720 (2008), *Overview of IPTV terminal devices and end systems.*

[b-ITU-T H.721] Recommendation ITU-T H.721(2009), *IPTV terminal devices: Basic model Amendment 1: New Appendix II on terminal device implementation example.*

[b-ITU-T H.740 Amd.1] Recommendation ITU-T H.740 Amd.1 (2011), *Application event handling for IPTV services: New video handling sensor event scenario in Appendix II.*

[b-ITU-T H.770] Recommendation ITU-T H.770 (2009), *Mechanisms for service discovery and selection for IPTV services.*

[b-ITU-T J.183] Recommendation ITU-T J.183 (2001), *Time-division multiplexing of multiple MPEG-2 transport streams over cable television systems*.

[b-ITU-T J.200] Recommendation ITU-T J.200 (2010), *Worldwide common core – Application environment for digital interactive television services.*

[b-ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions.*

[b-ITU-T M.1400] Recommendation ITU-T M.1400 (2006), *Designations for interconnections among operators' networks*.

[b-ITU-T M.3050.1] Recommendation ITU-T M.3050.1 (2004), *Enhanced Telecom Operations Map (eTOM) – The business process framework.*

[b-ITU-T T.174] Recommendation ITU-T T.174 (1996), *Application programming interface (API) for MHEG-1*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *security architecture for open system interconnection for CCIT applications*.

[b-ITU-T X.891] Recommendation ITU-T X.891 (2005) | ISO/IEC 24824-1 (2007), *Information technology – Generic applications of ASN.1: Fast infoset*.

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology – Terms and definitions*.

[b-ITU-T Y.1901] Recommendation ITU-T Y.1901 (2009), *Requirements for the support of IPTV services*.

[b-ITU-T Y.1910] Recommendation ITU-T Y.1910 (2008), *IPTV functional architecture*.

[b-Anonygator] *Anonymity-Preserving Data Aggregation using Anonygator*, Microsoft Research, Nov. 2009.
<http://research.microsoft.com/en-us/projects/anonygator/main.pdf>

[b-ATIS 0800026] ATIS 0800026 (2010), *Global Types XML Schema Description*.

[b-Crowds] ACM TISSEC (April 1998), *Michael K. Reiter and Aviel D. Rubin, Crowds: Anonymity for Web Transactions*.

[b-ETSI TS 102 472] ETSI TS 102 472 V1.3.1 (2009), *Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Content Delivery Protocols*.

[b-FIPS PUB 197] FIPS PUB 197 (2001), *Advanced Encryption Algorithm (AES).*

[b-FIPS PUB 198-1] FIPS PUB 198-1 (2008), *The Keyed-Hash Message Authentication Code (HMAC).*

[b-NIST PUB 800-122] NIST Special PUB 800-122 (2010), *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).*

[b-FTC 120326] FTC 120326 (2012), *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*.

[b-IETF RFC 3986] IETF RFC 3986 (2005), *Uniform Resource Identifier (URI): Generic Syntax*.

[b-IETF RFC 5054] IETF RFC 5054 (2007), *Using the Secure Remote Password (SRP) Protocol for TLS Authentication*.

[b-ISO/IEC 23001-1] ISO/IEC 23001-1:(2006, *Information technology – MPEG systems technologies – Part 1: Binary MPEG format for XML.*

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements.*

[b-ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management.*

[b-TOR] *The Onion Routing project.*
See <https://www.torproject.org/>

[b-W3C EXI] W3C Recommendations (2011), *Efficient XML Interchange (EXI) Format 1.0*.

[b-W3C XMLSchemaP2] W3C Recommendations (2004), *XML Schema Part 2: Datatypes (Second Edition).*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013