ETSI TS 102 825-7 V1.1.1 (2008-07)

Technical Specification

Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 7: CPCM Authorized Domain Management

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/...-102-825-7-v1.1.1-...

European Broadcasting Union — Union Européenne de Radio-Télévision

EBU·UER

DVB Digital Video Broadcasting

ETSI

Reference
DTS/JTC-DVB-222-7

Keywords
broadcast, DVB

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/dc3fa47-2884-4e99-eed-7c4986305c6/etsi-ts-102825-7-v1.1.1-2008-07

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2008.
© European Broadcasting Union 2008.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™, **TIPHON**™, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/dc73fa47-2e24-4e9e-956d-7c70886305c6/etsi-ts-102-825-7-v1.1.1-2008-07

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/dc73fa47-29e4-49e5-5ed-7c7d9853056/etsi-ts-102-825-7-v1.1.1-2008-07

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by Joint Technical Committee (JTC) Broadcast of the European Broadcasting Union (EBU), Comité Européen de Normalisation ELECtrotechnique (CENELEC) and the European Telecommunications Standards Institute (ETSI).

NOTE: The EBU/ETSI JTC Broadcast was established in 1990 to co-ordinate the drafting of standards in the specific field of broadcasting and related fields. Since 1995 the JTC Broadcast became a tripartite body by including in the Memorandum of Understanding also CENELEC, which is responsible for the standardization of radio and television receivers. The EBU is a professional association of broadcasting organizations whose work includes the co-ordination of its members' activities in the technical, legal, programme-making and programme-exchange domains. The EBU has active members in about 60 countries in the European broadcasting area; its headquarters is in Geneva.

European Broadcasting Union
CH-1218 GRAND SACONNEX (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/
2008-07

Founded in September 1993, the DVB Project is a market-led consortium of public and private sector organizations in the television industry. Its aim is to establish the framework for the introduction of MPEG-2 based digital television services. Now comprising over 200 organizations from more than 25 countries around the world, DVB fosters market-led systems, which meet the real needs, and economic circumstances, of the consumer electronics and the broadcast industry.

The present document is part 7 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.3].

Introduction

CPCM is a system for Content Protection and Copy Management of commercial digital content delivered to consumer products. CPCM manages content usage from acquisition into the CPCM system until final consumption, or export from the CPCM system, in accordance with the particular usage rules of that content. Possible sources for commercial digital content include broadcast (e.g. cable, satellite, and terrestrial), Internet-based services, packaged media, and mobile services, among others. CPCM is intended for use in protecting all types of content - audio, video and associated applications and data. CPCM specifications facilitate interoperability of such content after acquisition into CPCM by networked consumer devices for both home networking and remote access.

This first phase of the specification addresses CPCM for digital Content encoded and transported by linear transport systems in accordance with TS 101 154 [i.1]. A later second phase will address CPCM for Content encoded and transported by systems that are based upon Internet Protocols in accordance with TS 102 005 [i.2].

Note for New Readers:

Readers who are unfamiliar with the present document may find it helpful to first read the information scenarios described in TR 102 825-11 [i.5].

1 Scope

The present document specifies the Authorized Domain Management for the Digital Video Broadcasting (DVB) Content Protection and Copy Management (CPCM) system.

The present document defines messages and state machines that together define the conformant behaviour of an implementation.

The present document also defines a mandatory method for performing ADSE. Additionally, the present document describes a set of tools that may be used by a Compliance and Robustness C&R regime to extend the ADSE.

The present document also describes APIs to other CPCM components; however these are informative only and are not required to be implemented for conformance.

The hardware, software, middleware and other technologies employed are the sole choice of the implementer, governed by the requirements of the relevant (C&R) regime.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standards: https://standards.iteh.ai/catalog/standards/sist/dc731d47-2b64-4e9c-95e7-7c7d9863056c/etsi-ts-102-825-7-v1.1.1-2008-07

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI TS 101 154: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream".

[i.2] ETSI TS 102 005: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in DVB services delivered directly over IP protocols".

[i.3] ETSI TS 102 825-1: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 1: CPCM Abbreviations, Definitions and Terms".

[i.4] ETSI TS 102 825-2: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 2: CPCM Reference Model".

[i.5] ETSI TR 102 825-11: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 11: CPCM Content management scenarios".

[i.6] ETSI TS 102 825-4: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 4: CPCM System Specification".

[i.7] ETSI TS 102 825-5: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 5: CPCM Security Toolbox".

[i.8] ETSI TR 102 825-12: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 12: CPCM Implementation Guidelines".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/
etsi-ts-102-825-7-v1.1.1-2008-07

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 825-1 [i.3] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 102 825-1 [i.3] apply.

4 Authorized Domain Management (ADM)

ADM is the mechanism that allows CPCM Devices belonging to a household to establish and Join a DVB CPCM Authorized Domain (AD). It also provides an interoperable means of managing that AD.

Basic expectations on ADM are given in TS 102 825-2 [i.4].

4.1 ADM in the CPCM System

Figure 1 shows how ADM fits into the CPCM Reference Model.

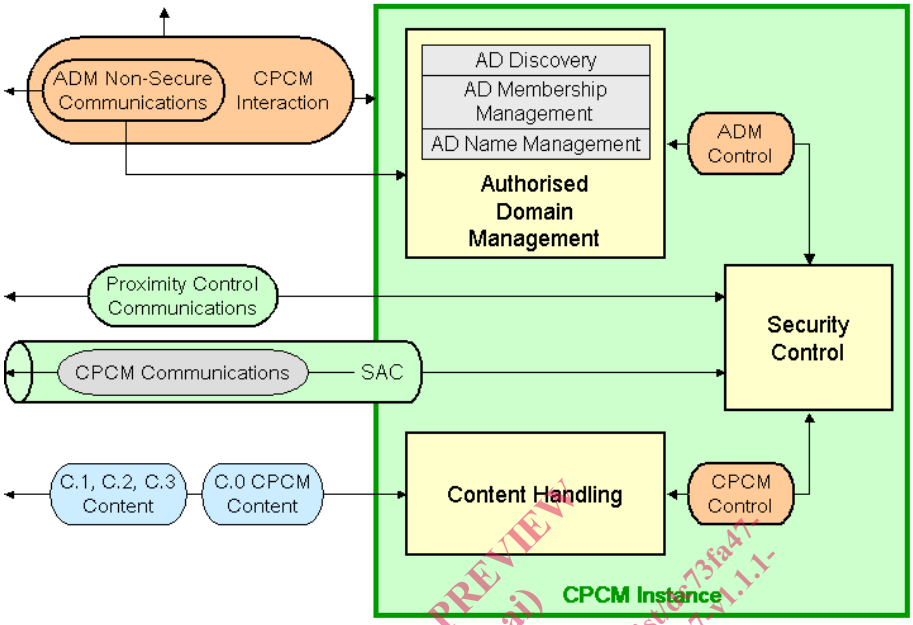

Figure 1: ADM in the CPCM Reference Model

Figure 2 provides another view of ADM within a CPCM implementation. It identifies that there are three key internal sub-systems with which the ADM Sub-system must communicate.

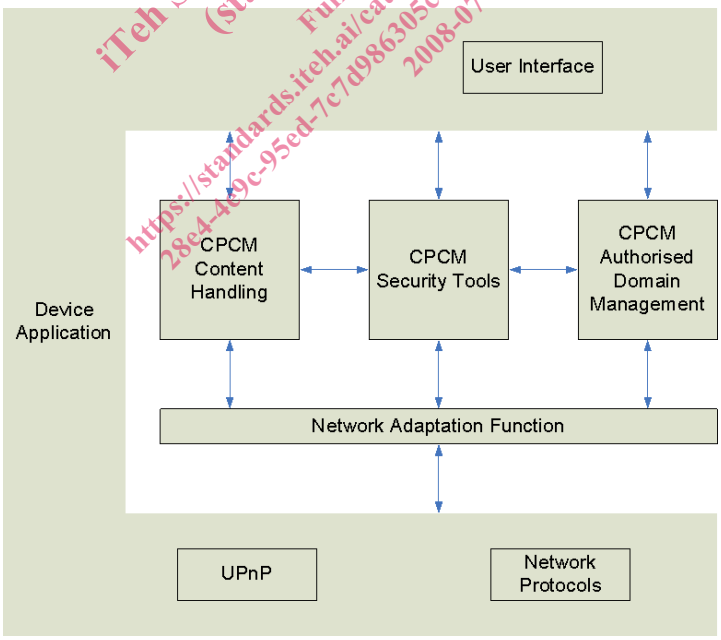

Figure 2: ADM Interfaces to other CPCM Sub-systems

It would be possible to build a CPCM implementation that strictly follows the architecture in figure 2, but this is not required. For reasons of clarity the present document is written in terms of the interfaces in figure 3.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/...

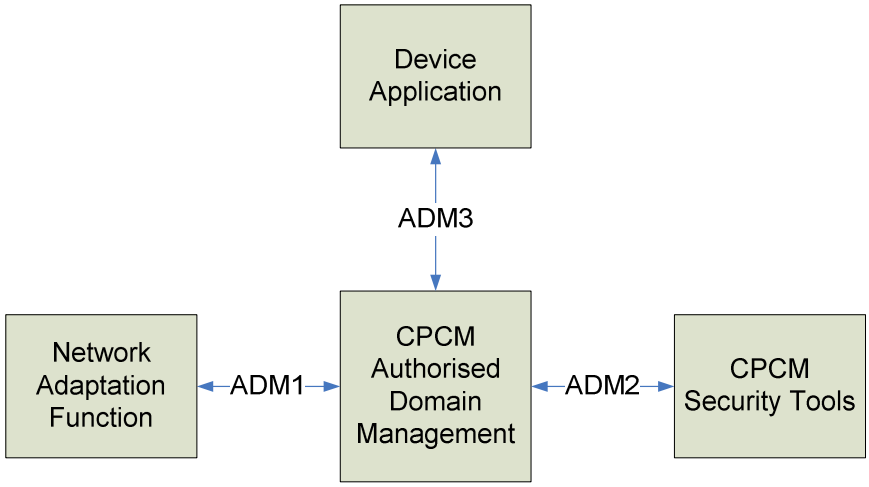

Figure 3: ADM Interfaces

ADM1 is the interface which is used to communicate with peer ADM Instances in other devices, via a Network Adaptation function that is specific to each network technology.

EXAMPLE: On DVB-HN (Home Network) conformant systems, ADM messages will be transferred using the UPnP protocols. However, for other situations such as serial Smartcard or CI interfaces, ADM messages will be transferred without UPnP support.

The present document includes a formal description of the ADM1 interface.

ADM2 is the interface to the Security Tools Sub-system of CPCM. The present document defines the normative behaviour of the Security Control and provides an informative API for use across this interface.

ADM3 is the informative interface between a Device Application and the ADM.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/dc75a47-18e-4e9c-85ed-7c...9863056/etsi-ts-102-825-7-v1.1.1-2008-07

4.2 Local ADM Master and Domain Controller

4.2.1 ADM Local Master Concept and Requirements

A single CPCM Instance acts as a temporary Local ADM Master for the AD members in the Local network. The ADM Local Master has no specific additional data (i.e. the same AD data is replicated to all Instances in the AD). The Local Master can be replaced at any time to avoid a single-point-of-failure.

Figure 12 and clause 5.1.7 describe how to determine which Instance fulfils this role at any given moment.

The basic behaviour is as follows:

- The first Instance to create the Authorized Domain immediately becomes the Local Master.
- When an Instance attempts to discover available ADs or properties of connected Instances, each connected CPCM Instance responds.
- When an Instance requests to Join an AD, the request is directed to the Local Master.
- Instances belonging to the same AD elect or otherwise determine which device is the most suitable Instance to act as their Local ADM Master.
- Each Instance has a "Local Master capability".
- An election may be called by any member Instance at any time.
- The Instance with highest capability is elected as Local Master.

The Local Master concept is used to reduce the complexity of ADM protocol interactions. It does not solve issues relating to Authorized Domain Size and Extent (ADSE) threats. These are addressed by the Domain Controller concept described below.

4.2.2 The Global Domain Controller Concept

ADM defines a Domain Controller for Secure Authorized Domain Size and Extent implementation. The Domain Controller is responsible for all AD operations (including AD Joining and Leaving) that may affect ADSE records and decision making processes. The user is able to Transfer Domain Controller functionality from one CPCM Instance to another, or to Split the Domain Controller function between two or more CPCM Instances. Each Domain Controller has additional data that reflects the current state of the AD. This data is replicated to all other CPCM Instances within the same AD to limit the risk of a single point of failure.

The basic behaviour is as follows:

- The first capable Instance to create the AD becomes Domain Controller.
- If there is a single Domain Controller, then that Domain Controller will always be chosen as the Local ADM Master. If several Domain Controllers are present, the Local ADM Master shall be one of them.
- Local ADM Masters are able to discover a Remote Domain Controller and will give relevant information to Instances needing to contact the Local Domain Controller (e.g. for AD Joining or Leaving).
- The Domain Controller function can be Transferred from one Instance to another.
- The Domain Controller can be Split over several Instances and later re-Merged. ADSE records are Split and re-Merged as well. ADSE records may be Rebalanced between two Domain Controllers.

NOTE: This is not the same concept as Splitting the AD itself into two new ADs. The AD Splitting function, while planned for the future, is not included in the present document.

Figure 21 and clause 5.1.12 describe the process for changing the assigned Domain Controller.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/dc72fa47-28e4-4e9c-95ed-7...ts102-825-7-v1.1.1-2008-07

4.3 Authorized Domain capabilities

CPCM Instances shall publish their Authorized Domain Management capability through the following fields in the certificate.

Table 1: ADM Fields

Field	Meaning
`AD_aware`	An AD aware CPCM Instance is one that is able to securely create or record the AD Secret. It has direct access to Content that is bound to its AD. It is able to handle AD restricted CPCM Content. If the `AD_aware` certificate field is not asserted then the CPCM Instance is not able to get or create the AD Secret in any way, and cannot Join any AD.
`ADM_capable`	An ADM capable CPCM Instance that is AD aware and can also run ADM protocols. The `AD_aware` certificate field shall be also asserted in this case.
`ADM_LM_capable`	An ADM LM capable CPCM Instance is ADM capable and can also act is a Local Master. A Local Master is able to run as a proxy for other CPCM Instances in their communications with Domain Controllers. The `ADM_capable` certificate field shall also be asserted in this case.
`ADM_DC_capable`	An ADM Domain Controller capable CPCM Instance is ADM capable and can also act as a Domain Controller. A Domain Controller shall be able to securely run ADSE enforcement and to securely manage ADSE values. The `ADM_LM_capable` certificate field shall also be asserted in this case. A DC capable Instance is always an ADSE countable Instance and always `ADM_LM_capable`.
`ADSE_countable`	An ADSE countable CPCM Instance (which is also a Countable Instance of CPCM Functionality (CICF)) is able to Consume or Export Content and shall thus be counted in ADSE tests (see next clause). The `AD_aware` certificate field shall be also asserted in this case.

Please see TS 102 825-5 [i.7] for more details of the CPCM Certificate fields.

Some CPCM Instances may be AD aware without being ADM capable. This might, for instance, be the case for smart cards implementing a proprietary CA or DRM that is plugged into a Set-Top-Box with proprietary software and CPCM Instance. The set-top-box CPCM Instance may let the smart card CPCM Instance Join using proprietary protocols in accordance with rules set forth in a particular C&R regime.

4.4 Authorized Domain Size and Extent

Authorized Domain Size and Extent (ADSE) ensures that CPCM Instances do not violate the AD size, scope and extent requirements when they attempt to become members of the same AD.

4.4.1 ADSE Counts and Values

The ADSE method makes use of the following counters and ceilings.

Table 2: ADSE values maintained by the DC

Variable	Bits	Type	Meaning
`total_count`	16	uimsbf	The current number of CICF in the AD.
`total_ceiling`	16	uimsbf	The maximum number of CICF allowed in the Authorized Domain
`remote_count`	16	uimsbf	The current number of CICF in the AD that Joined Remotely to the Domain Controller that authorized the AD Join.
`remote_ceiling`	16	uimsbf	The maximum number of CICF that may Remotely Join the AD.
`local_count`	16	uimsbf	The current number of CICF in the AD that have Joined Locally to the Domain Controller that authorized the AD Join.
`local_ceiling`	16	uimsbf	The maximum number of CICF that may Locally Join the AD without running the Quorum test.
`DC_split_count`	16	uimsbf	The current count of Domain Controller Splits.
`DC_split_ceiling`	16	uimsbf	The maximum number of DC Splits that may occur.
`DC_remote_count`	16	uimsbf	The current count of Remote Transfer or Remote Splits of the Domain Controller.
`DC_remote_ceiling`	16	uimsbf	The maximum number of Remote Transfer or Remote Splits of the Domain Controller.
NOTE: `total_ceiling` is greater than the sum of `local_ceiling` and `remote_ceiling`.			

iTeh STANDARD PREVIEW (standards.iteh.ai) Full standard: https://standards.iteh.ai/catalog/standards/sist/d673fa97-28e4-4e9c-95e8-7c7d86305c6d/etsi-ts-102-825-7-v1.1.1-2008-07

Table 3: ADSE values maintained by each Instance

Variable	Bits	Type	Meaning
`history_count`	16	uimsbf	The total number of individual Authorized Domains that the CPCM Instance has Joined.
`history_ceiling`	16	uimsbf	The maximum number of Authorized Domains that the CPCM Instance can Join, as set by the C&R regime.
NOTE: The `history_ceiling` variable can be used to accommodate the anticipated differences between owned and rented CPCM Devices.			

These counter and ceiling values are named throughout the document ADSE counts or ADSE values.

If a ceiling field value is set to 0xFFFF then the ceiling is considered to be infinite and no ceiling limits shall be applied.

4.4.2 ADSE Method Description

The ADSE Method is defined by the following rules:

1) There is one logical Domain Controller per AD, initially instantiated in a single physical Domain Controller contained within a single CPCM Instance within a single CPCM Device. The logical Domain Controller function may then be Transferred from one physical device to another or may be shared between two or more devices. This Logical Domain Controller is an instantiation of the Single Household Metric (see clause 7.1).

2) One Domain Controller functionality may be Transferred Locally or a limited number of times Remotely.

3) One Domain Controller functionality is required for a CICF to be able to Join an AD. This includes Remote AD Joins.

4) Non-CICF Instances may be Joined to the AD by any CPCM Instance that is a member of that AD, but only Locally.

5) The `total_ceiling` shall be greater than the sum of `remote_ceiling` and the `local_ceiling`. This method is based on the Quorum Test (see clause 7.4).

6) Each time a new CICF attempts to Join an AD, the following process must be followed:

   a. If the `total_count` is equal to `total_ceiling`, then the CICF is denied permission to Join the AD, unless AD Membership Assignment by Authorized Authenticated Agent (ADMAAA) (please see clause 7.8) can be performed successfully.

   b. If the CICF is Remote and the `remote_count` is equal to the `remote_ceiling`,

      i. then the CICF is denied permission to Join the AD, unless ADMAAA can be performed successfully.

      ii. else, the CICF is granted permission to Join the AD and the counters for `remote_count` and `total_count` are incremented by one.

   d. If the CICF is Local and `local_count` is lower than the `local_ceiling`, then the CICF is granted permission to Join the AD. The `local_count` and `total_count` are both incremented by one.

   e. If the CICF is Local and `local_count` is equal to or greater than `local_ceiling`, a quorum test is performed with other CICFs:

      i. A Challenge is broadcast together with the ADID.

      ii. Each CICF of the same AD responses through a message carrying the same Challenge and its own identifier. This message is protected using the AD Secret.

      iii. The Domain Controller runs a Proximity Test with each CICF that responded properly.

      iv. If the number of other Local CICFs that are connected at that time is equal to or greater than the "quorum percentage" of the `total_count` then:

         1. The CICF is granted permission to Join the AD: both `local_count` and `total_count` are both incremented by one.

         2. Else the CICF is denied permission to Join the AD, unless ADMAAA can be performed successfully.

NOTE 1: The "quorum percentage" is a value to be defined by the C&R regime.

7) When a CICF that Joined Remotely becomes Local to the Domain Controller functionality that allowed it to Join, the Domain Controller functionality may decrement by one the `remote_count` and increment by one the `local_count` if one of the following conditions is met:

   a. The `local_count` is less than the `local_ceiling`; or

   b. The `local_count` is equal to or greater than the `local_ceiling` and the number of Local CICFs is equal to or greater than the "quorum percentage" of the `total_count` value;

   c. ADMAAA authorizes it.

8) Each time a CICF attempts to Leave an AD:

   a. If the AD Leaving is Local, then `local_count` and `total_count` are decremented by one (if `local_count` was zero, `remote_count` is decremented instead of `local_count`).

   b. If the AD Leaving is Remote, then `remote_count` and `total_count` counters are decremented by one (if `remote_count` was zero, `local_count` is decremented instead of `remote_count`).

iTeh STANDARD PREVIEW (standards.iteh.ai) Full standard:

9) Domain Controller functionality can be Split into multiple parts. The number of Splits will be limited by the C&R regime. Domain Controller functionalities can also be re-Merged. A DC Merge re-credits the Split counters for any unused counts.

10) A Domain Controller must be instantiated within a CICF.

11) The Domain Controller functionality may be Split Locally, i.e. the CICF gaining Domain Controller functionality must be Local to the CICF giving the Domain Controller functionality.

12) The total number of Remote Domain Controller Transfers and Splits shall not exceed a ceiling fixed by the C&R regime.

13) Counters and ceilings may be Rebalanced between different Split Domain Controller functionalities of the same AD.

14) After a Domain Controller Split, Merge or Rebalance, the sums for `total_count`, `total_ceiling`, `remote_count`, `remote_ceiling`, `local_count`, `local_ceiling`, `DC_remote_count`, `DC_remote_ceiling`, `DC_split_count` and `DC_split_ceiling` over the involved Domain Controller functionalities shall be the same as before the activity. Upon DC Rebalancing and Splitting, the way each counter and ceiling is affected is left to the implementer as long as the following consistency rules are obeyed:

    a. For each Domain Controller, the sum of `local_count` and `remote_count` shall be equal to `total_count`.

    b. For each Domain Controller, `total_count`, `remote_count`, `DC_split_count` and `DC_remote_count` shall be lower than the corresponding ceiling.

15) The ceilings can be changed at any time by an ADMAAA or by any test approved by the C&R regime.

16) An Instance shall not Join an AD if it has exceeded the AD Join/Leave Frequency/Repetition Rate as describe in the Domain Membership History (DMH) tool (see clause 7.6).

A CICF is characterized by the fact that its `ADSE_countable` certificate field is asserted.

A count of '1' shall be assigned to each CPCM Device that is able to Output (Consume or Export) Content; such an Instance shall be deemed a "Countable Instance of CPCM Functionality", or CICF.

NOTE 2: The C&R regime may place constraints upon the number of potential Outputs that may be included in a single CICF. The Instance Certificate includes a field that contains a '0' or '1'. The C&R regime may require that a future CPCM Device be counted as more than '1' if it has too many Instance Certificates that should have a '1' count. In that case, the CPCM Device will embed several CPCM Instances with a '1' count.

Constraints on single AD memberships for CPCM Instances embedded in a single device are beyond the scope of the present document and may be defined by the C&R regime.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/dc73fa47-28e4-4a9c-95ad-7c7d9b65c5c6/etsi-ts-102-825-7-v1.1.1-2008-07