ETSI TR 102 825-8 V1.1.1 (2008-07)

Technical Report

Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 8: CPCM Authorized Domain Management scenarios

Reference
DTR/JTC-DVB-222-8

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

Contents

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 Report (TR) 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

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 8 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].

1 Scope

The present document specifies the Scenarios that are envisaged for the Digital Video Broadcasting (DVB) Content Protection and Copy Management (CPCM) system. It is provided for informative purposes only and will be revised in due course as more scenarios are defined.

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.

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".

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 Informative Authorized Domain Management (ADM) scenarios

4.1 Scenario 1 - Solitary Device Initialization

Scenario 1 covers the case where a single, Blank Instance (ADM) is activated in isolation from all other CPCM Instances. The Instance is unable to Join an existing AD, so it will perform alone.

4.1.1 Entry Conditions

At the beginning of Scenario 1, there is a single device with a Blank ADM Instance.

4.1.2 Process

- The ADM in Device A is initialized by the Device Application.
- The ADM in Device A initiates a Discovery process to find an AD to Join.
- No response is received.
- ADM asks the Device Application for permission to create a new AD.
- The ADM implementation generates a random ADID and asks the Security Control to create the necessary secret(s).
- The ADM issues an *AD Update Indication* to notify other CPCM Instances of the creation of the AD.

4.1.3 Information Flows

Figure 1 describes the information flows required for Scenario 1.

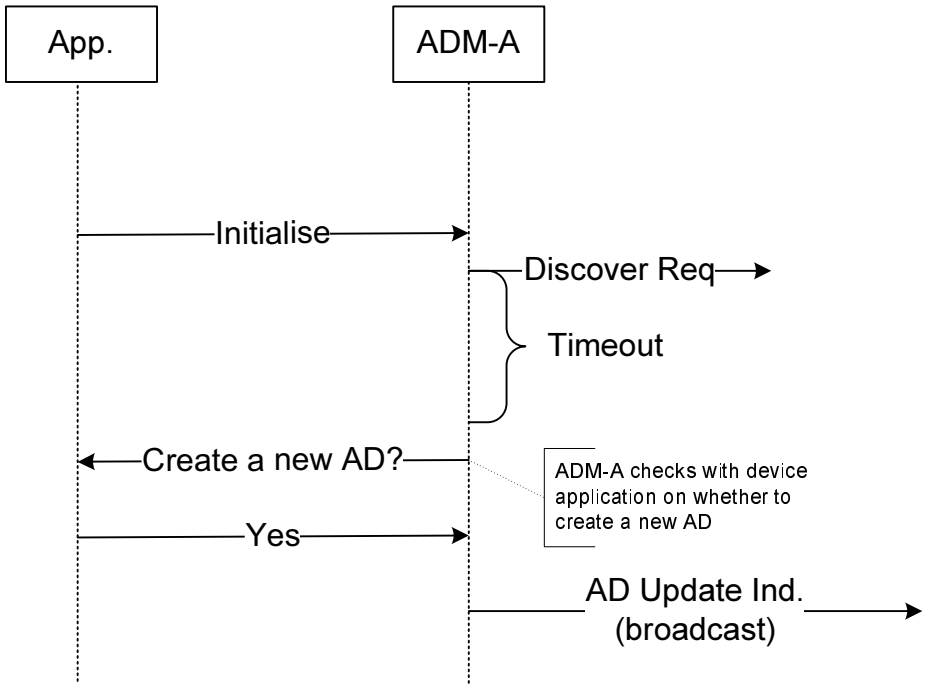


Figure 1: Scenario 1 Flows - Solitary Device Initialization

4.1.4 Exit Conditions

After Scenario 1 has been completed, the following conditions apply:

- The ADM implementation within Device A has an ADID assigned.
- The Security Control implementation within Device A has security information for the AD assigned and associated with the ADID.

4.2 Scenario 2 - Two Blank Devices

4.2.1 Use Case

Scenario 2 covers the case where two Blank Devices are activated simultaneously.

4.2.2 Entry Conditions

At the beginning of Scenario 2, we have:

- Blank Device A.
- Blank Device B.

4.2.3 Process

- The Device Application in Device A initializes ADM-A.
- ADM-A initiates a Discovery (broadcast). The Discovery message indicates that there is no AD membership.
- No response.

- The Device Application in Device B initializes ADM-B.
- ADM-B initiates a Discovery.
- ADM-A responds with a *Discovery Response* but indicates it has no current AD membership.
- The ADM with the lower Instance ID (ADM-A in this case) asks its Device Application whether to create a new AD.
- ADM-A creates the new AD as per scenario 1.
- ADM-A sends a broadcast *AD Update Indication* describing the new AD.
- ADM-B responds to the *AD Update Indication* by restarting its own Discovery process.
- The scenario continues as in Scenario 3 below.

4.2.4 Information Flows

Figure 2 describes the information flows required for Scenario 2.

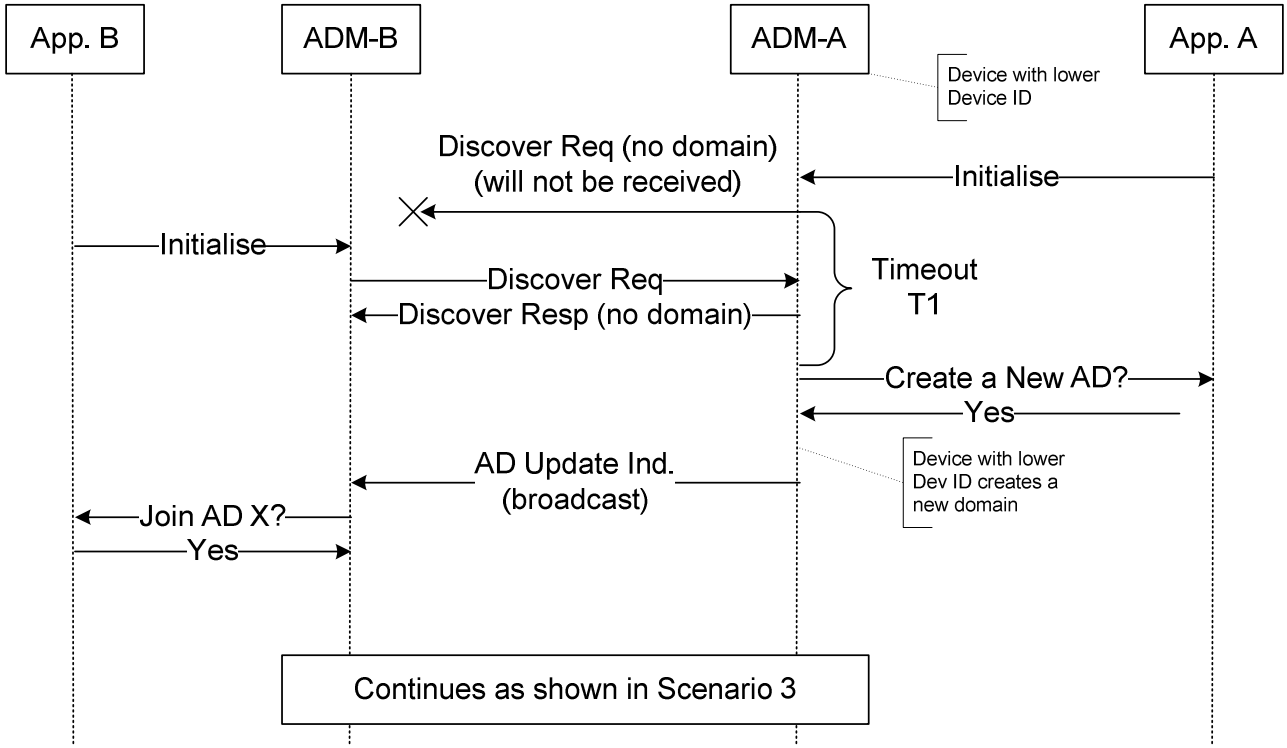


Figure 2: Scenario 2 Flows - Two Blank Devices

4.2.5 Exit Conditions

After Scenario 2 has been completed, both devices proceed automatically to Scenario 3.

4.3 Scenario 3 - Basic AD Join

This provides the basis for **all** AD Joining scenarios.

4.3.1 Use Case

Scenario 3 covers the case where one device has already created a single-member AD, and a second blank device is activated. In this case the two devices are Local to each other.

4.3.2 Entry Conditions

At the beginning of Scenario 3, we have:

- ADM-A is the sole member of AD X.
- ADM-B is Blank.

4.3.3 Process

- ADM-B is initialized.
- ADM-B initiates a Discovery (broadcast, indicating a self-managed AD Join is intended).
- ADM-A responds with the AD X information.
- ADM-B asks the Device Application to confirm that it should Join AD X.
- ADM-B commences an AD Join transaction with ADM-A.
- ADM-A verifies with its own Device Application whether to allow ADM-B to Join the AD. If the Device Application agrees, the following steps are taken.
- ADM-A runs the ADSE tests to verify that AD growth is acceptable, assumes this is true.
- ADM-A asks SEC-A to establish a SAC to SEC-B (see figure 4).
- (Mutual authentication takes place during SAC establishment).
- ADM-A asks SEC-A to send the AD Secret(s) to SEC-B.
- ADM-A responds with the ADID to ADM-B.
- ADM-B confirms receipt of this information.
- The Domain Internal Records on both devices are updated.

4.3.4 Information Flows

Figures 3 and 4 describe the information flows required for Scenario 3.

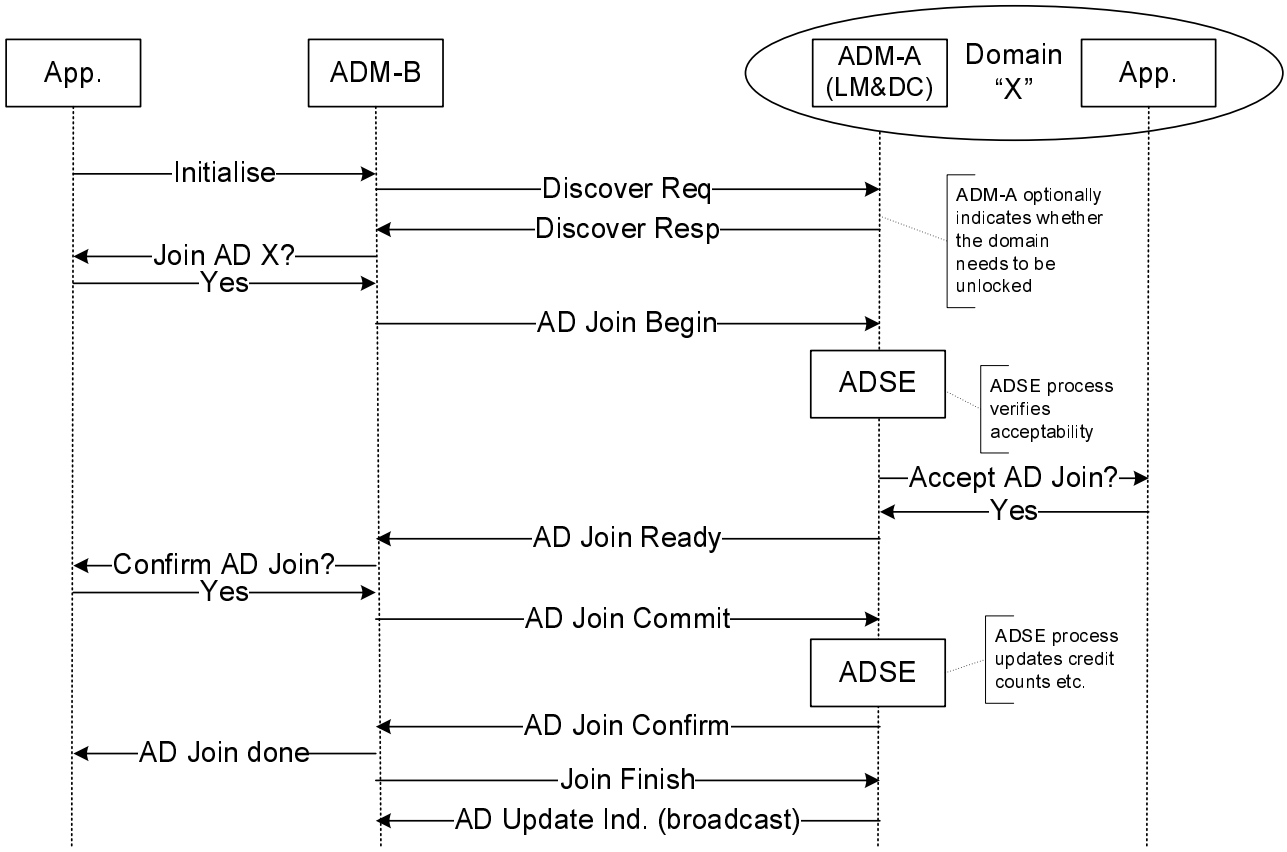


Figure 3: Scenario 3 Flows - Basic AD Join

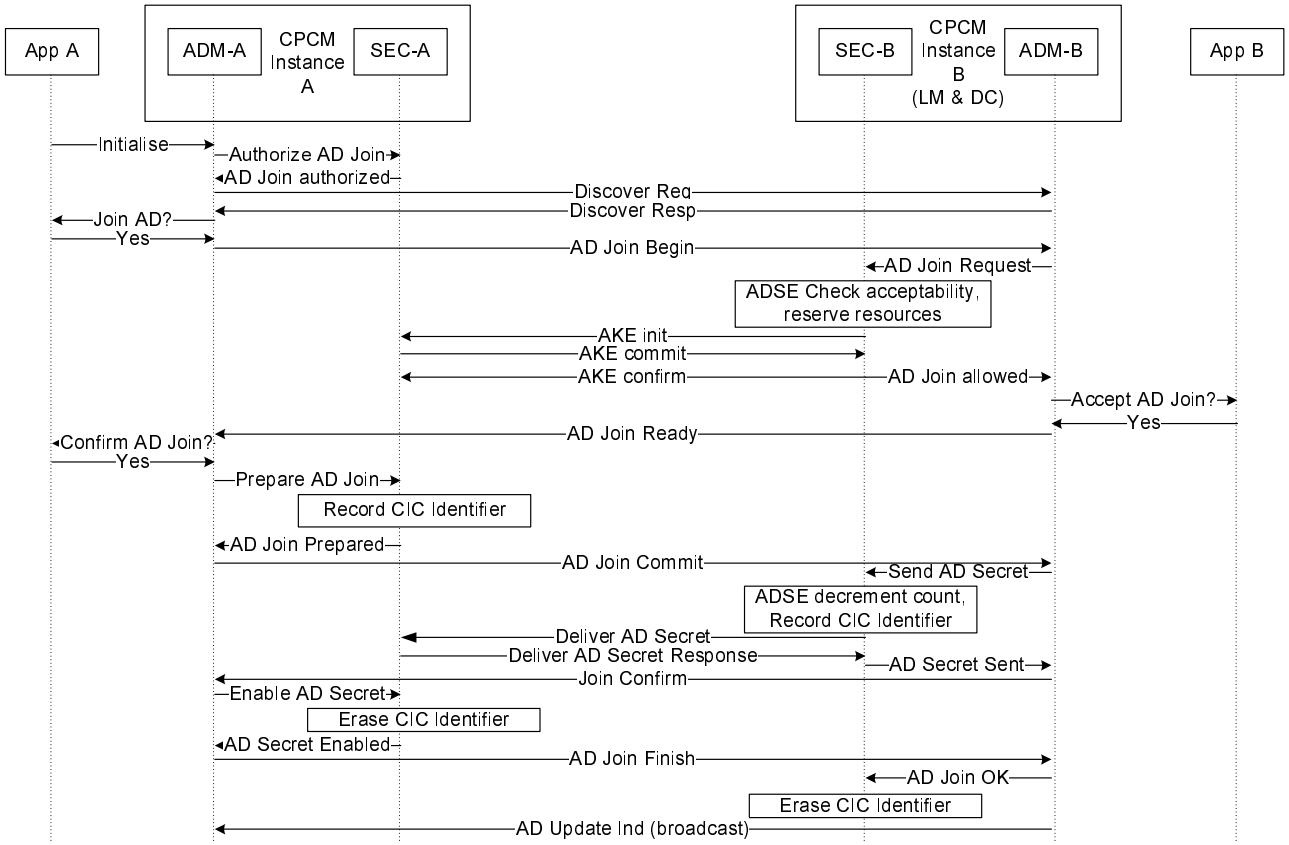


Figure 4: Scenario 3 Flows - ADM/SEC interaction during Basic AD Join

4.3.5 Exit Conditions

After Scenario 3 has been completed both devices have the same ADID and access to the secrets.

4.4 Scenario 4 - Remote AD Join

This variant provides for Joining an AD where the Domain Controller is in another location.

4.4.1 Use Case

Scenario 4 covers the case where one device has already created a single-member AD, and a second blank device is activated. In this case both devices are Remote from each other.

4.4.2 Entry Conditions

At the beginning of Scenario 4, we have:

- ADM-D is the sole Domain Controller of Domain X.
- The Blank ADM-B is in a different AD than ADM-A and is ADSE countable.
- ADM-B is the Local Master of the AD where ADM-A is located.

NOTE: If B is not ADSE countable, the AD Join occurs with the Local Master.

4.4.3 Process

- ADM-B is initialized.
- ADM-B initiates a Discovery (broadcast, indicating a self-managed AD Join is intended).
- ADM-A responds with the AD X information.
- ADM-B asks the Device Application to confirm that it should Join AD X.
- ADM-B commences a AD Join transaction with ADM-A.
- ADM-A forwards the request to ADM-D.
- ADM-D verifies with its own Device Application whether to allow ADM-B to Join the AD. If the Device Application agrees, the following steps are taken.
- ADM-D runs the ADSE tests to verify that AD growth is acceptable, if this is true;
- ADM-D informs ADM-B that the AD Join is possible.
- ADM-A asks SEC-A to establish a SAC to SEC-B (see figure 6).
- (Mutual authentication takes place during SAC establishment).
- ADM-D asks ADM-A to send the AD Secret(s) to SEC-B.
- ADM-A responds with the ADID to ADM-B.
- ADM-B confirms receipt of this information to ADM-A which then forwards it onto ADM-D.
- The Domain Internal Record on all devices is updated.

4.4.4 Information Flows

Figure 5 and 6 describe the information flows required for Scenario 4.

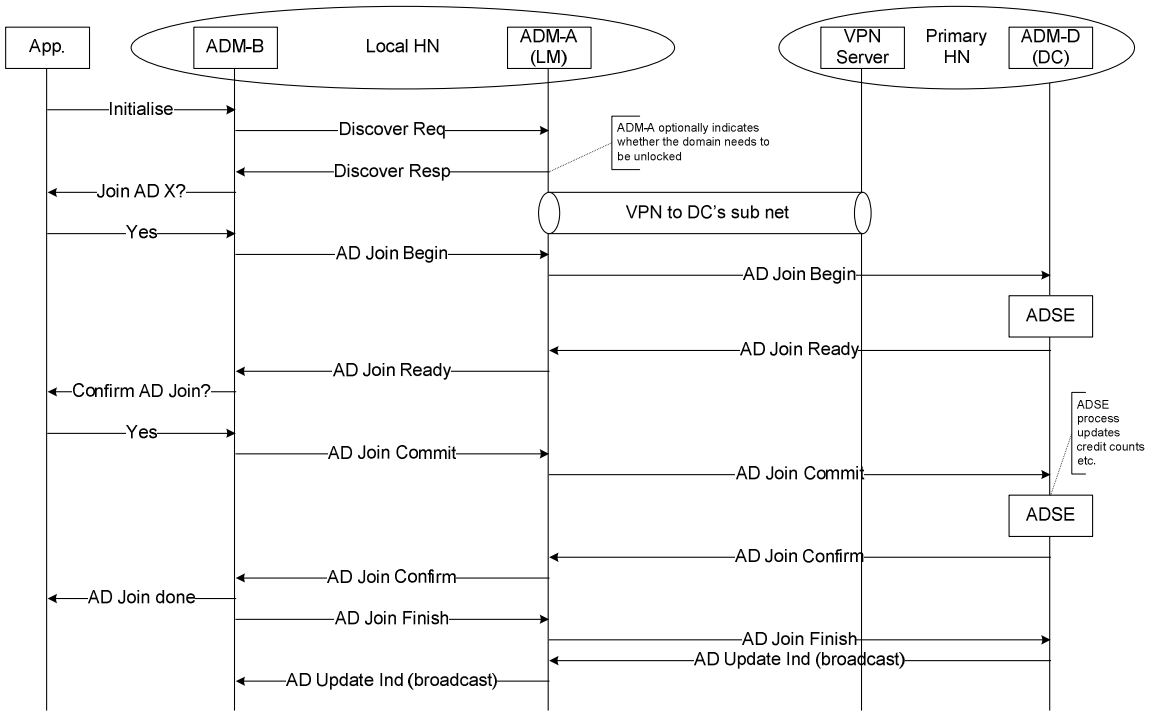


Figure 5: Scenario 4 Flows - Remote AD Join

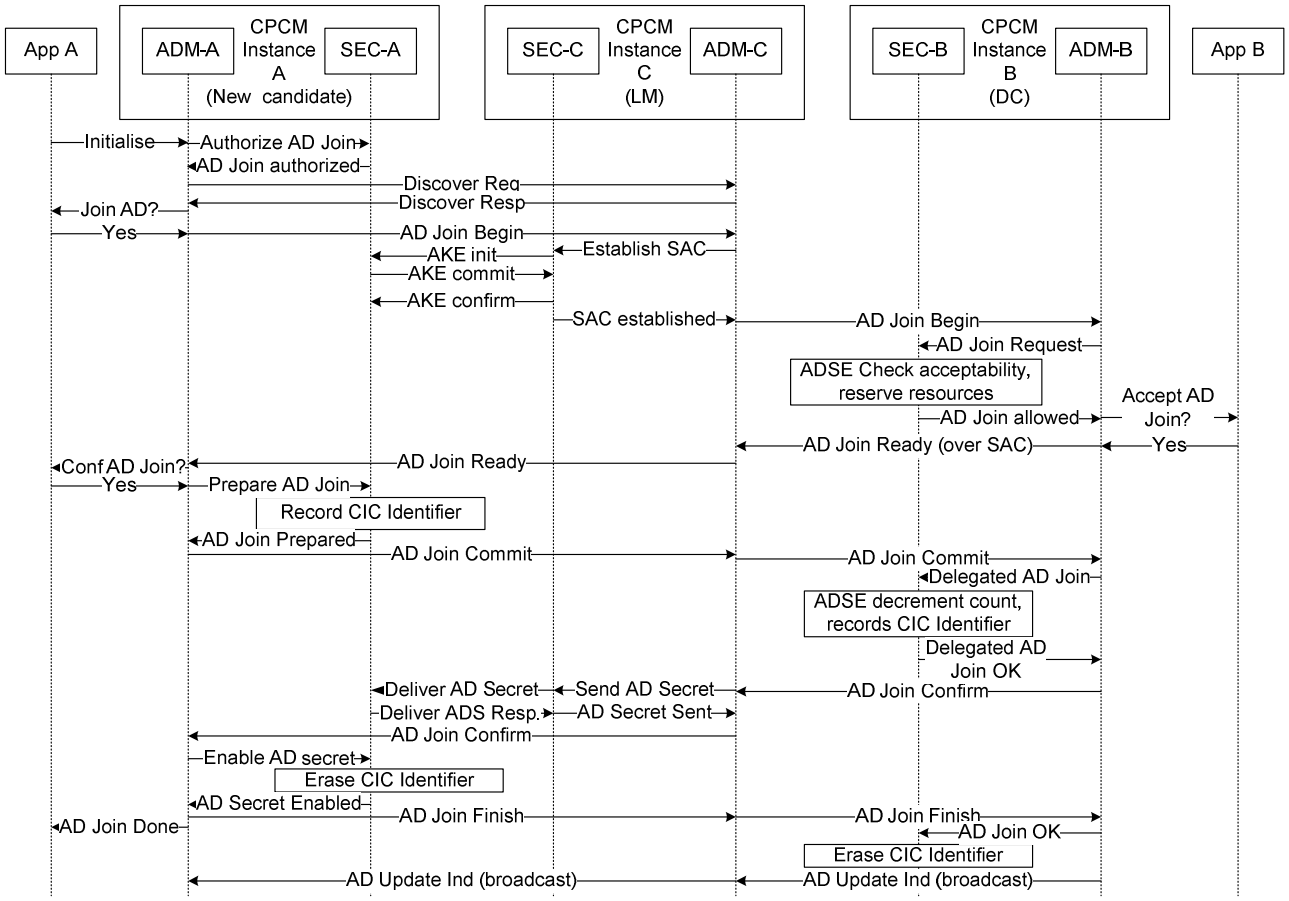


Figure 6: Scenario 4 Flows - ADM/SEC interaction during Remote AD Join

4.4.5 Exit Conditions

After Scenario 4 has been completed all three devices have the same ADID and access to the secrets.

4.5 Scenario 5 - AD Join by Invitation

4.5.1 Use Case

Scenario 5 covers the case where a device is *invited* to Join the AD by another device that is already an AD member. The inviting device may by the Domain Controller or Local Master, though this is not essential.

4.5.2 Entry Conditions

At the beginning of Scenario 5, we have:

- ADM-A is the Local Master of AD X.
- ADM-B is Blank.

Both devices are connected to the network.

4.5.3 Process

- The Device Application A instructs ADM-A to invite Device B into the AD.
- ADM-A send an Invitation Indication for AD X to ADM-B.
- ADM-B initiates a Discovery, as per Scenario 3 - Basic AD Join.
- The process continues exactly as per Scenario 3 - Basic AD Join.
- After the process is achieved, ADM-B informs ADM-A of the protocol results

NOTE: If there are multiple ADs responding to the Discover, "Scenario 7 - Device Joining with Multiple ADs available" will apply.

4.5.4 Information Flows

Figure 7 describes the information flows required for Scenario 5.

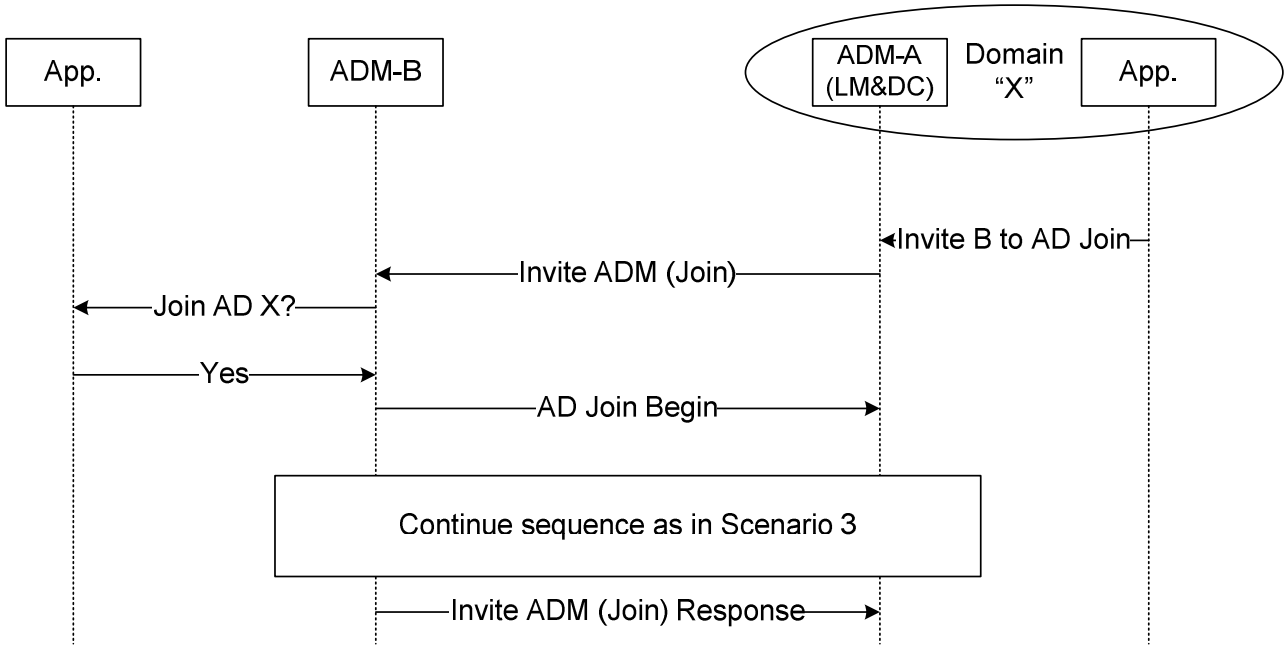


Figure 7: Scenario 5 Flows - AD Join by Invitation

4.5.5 Exit Conditions

After Scenario 5 has been completed both devices have same ADID and access to the secrets.

4.6 Scenario 6 - Subsequent Device Joining

4.6.1 Use Case

Scenario 6 covers the case where a third or later device is added to a multi-device AD that already has one or more active members.

NOTE: This scenario can also be triggered by initialization, local request from the Device Application, or by Invitation, as per Scenario 5 - AD Join by Invitation. The latter case is identical to this sequence, following the Invitation Indication described in that scenario.

4.6.2 Entry Conditions

At the beginning of Scenario 6, we have:

- Authorized AD "X" with two or more devices Joined to it.
- Two or more AD member devices (ADM-A and ADM-B) are active and connected.
- ADM-C is Blank.

4.6.3 Process

- The Blank ADM-C is connected, initialized, or receives an Invitation.
- ADM-C initiates a Discovery.
- The Local ADM Master responds.
- The Device Application confirms that it wants to Join the device to AD "X".
- The ADSE function confirms that AD growth is acceptable.
- ADM-C obtains the ADID from ADM-A, and Security Control exchanges AD Secret as per Scenario 3 - Basic AD Join.

4.6.4 Information Flows

Figure 8 describes the information flows required for Scenario 6.

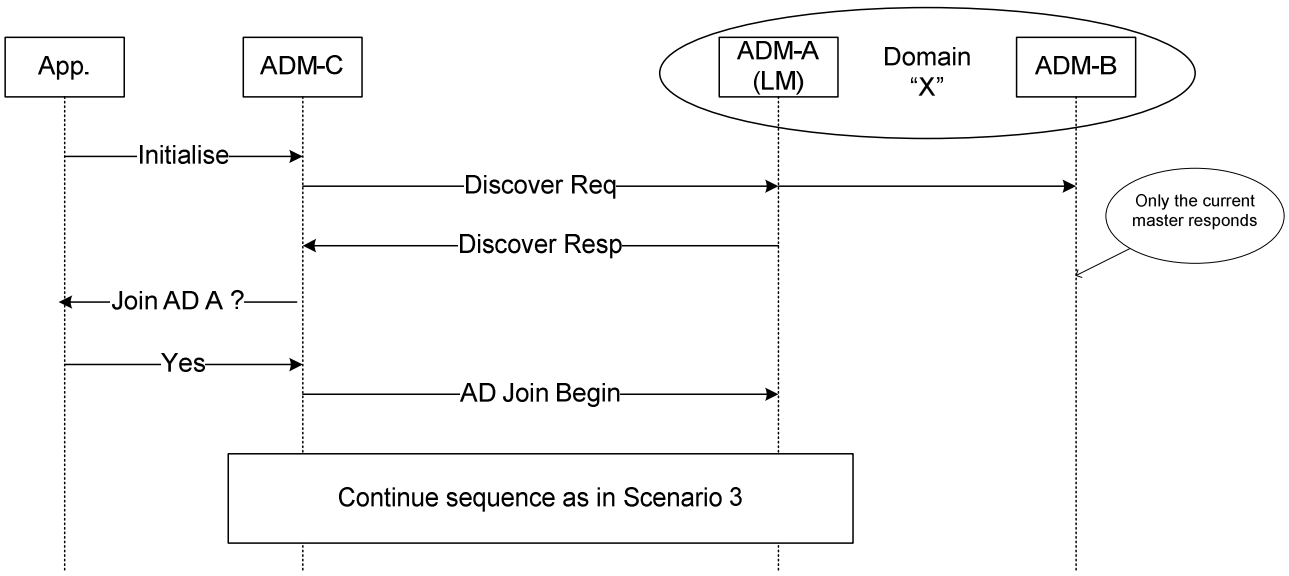


Figure 8: Scenario 6 Flows - Subsequent Device Joining

NOTE: A specific case for ADSE delegation is where the AD Joining device is in proximity to a Local Master, but remote from the Domain Controller. In such a case, the Domain Controller could delegate some of the ADSE tests to the Local Master as part of the AD Join process.

4.6.5 Exit Conditions

After Scenario 6 has been completed Device C shares the ADID and secrets with Devices A and B.

4.7 Scenario 7 - Device Joining with Multiple ADs available

NOTE: In this scenario we have only two variations from the set of three shown in Scenario 3. This is because an Invited AD Join inherently comes from a single AD, so the multiple AD environments have no effect.

4.7.1 Use Case

Scenario 7 covers the case where a third or later device is added to a multi-device AD that already has one or more active members, but where there are one or more additional ADs also present on the same network.

4.7.2 Entry Conditions

At the beginning of Scenario 7, we have:

- Two ADs "X" and "Y" exist with one or more devices Joined to each.
- At least one AD member from each is active and connected.
- ADM-C is Blank.

4.7.3 Process

- ADM-C is connected and/or initialized.
- ADM-C initiates a Discovery.
- All existing devices respond.
- ADM-C offers the Device Application a choice of available ADs (or none).
- If the Device Application is able to do so, it offers the user a choice between the available ADs.
- If a AD has been chosen, ADM-C device requests to Join the chosen AD (or none). See figures 9 and 10.
- If a specific AD has not been chosen, ADM-C asks to Join all available ADs but only one is expected to respond.
- The Device Application confirms that they want to Join the AD.
- Implementations may choose to skip this step; it is left it in here for logical consistency with other scenarios.
- The ADSE tests are passed.
- The Secrets are delivered as in Scenario 3.

4.7.4 Information Flows

Figures 9 and 10 describe the information flows required for Scenario 7.

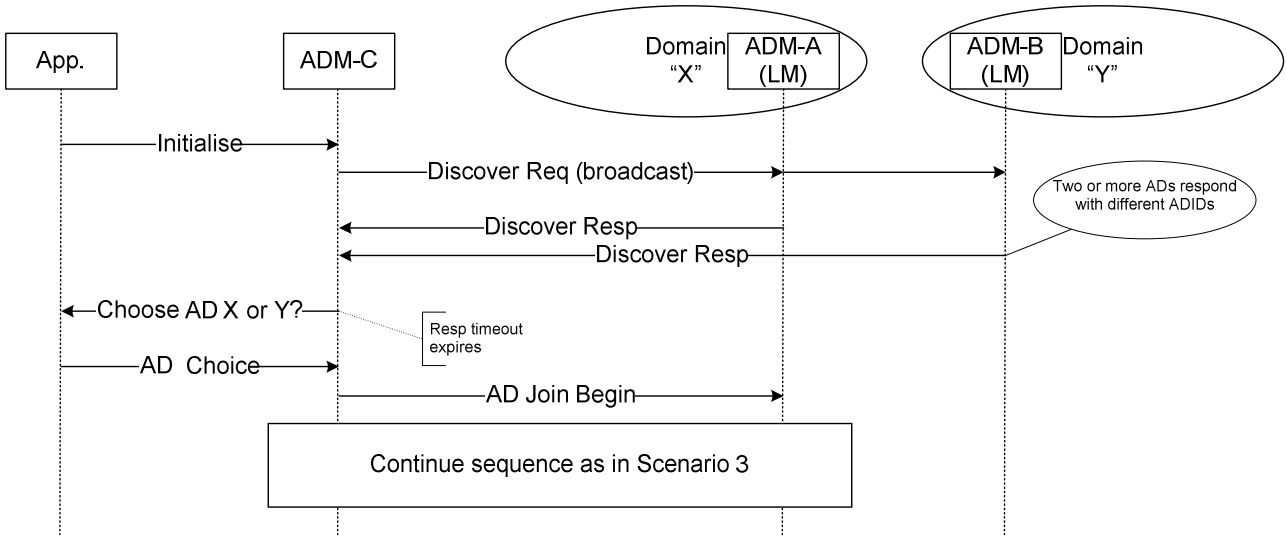
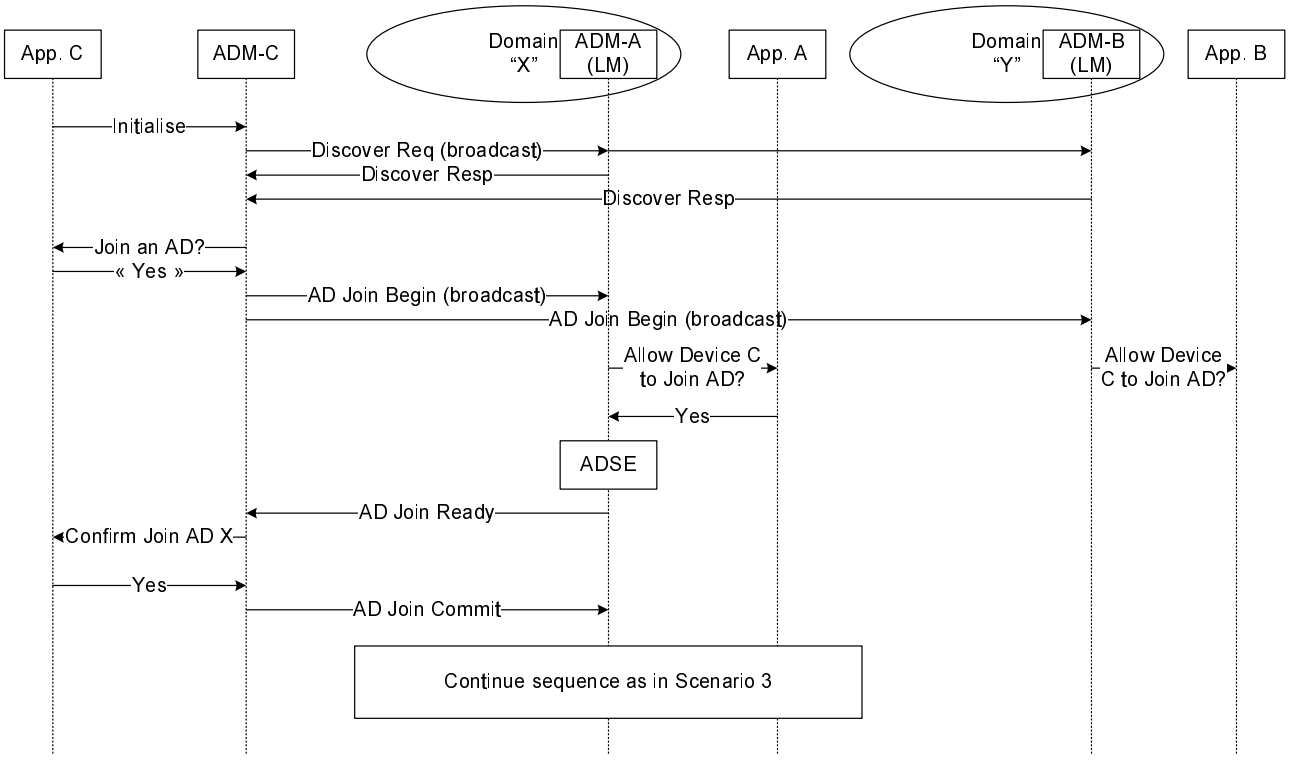


Figure 9: Scenario 7a Flows - Choice of ADs with AD Selection



NOTE: If more than one AD responds with "AD Join Ready", the transaction will be rolled back and another attempt made.

Figure 10: Scenario 7b Flows - Choice of ADs without AD Selection

4.7.5 Exit Conditions

After Scenario 7 has been completed the new device shares the ADID and secrets.

4.8 Scenario 8 - Device Reconnection

4.8.1 Use Case

Scenario 8 covers the case where a device which has previously been connected to a multi-device Authorized Domain is reconnected after an interval.

4.8.2 Entry Conditions

At the beginning of Scenario 8, we have:

- ADM-A is Joined to the AD, connected to the network and acting as the Local Master.
- ADM-B was previously Joined to the same AD, but has been disconnected from the network.

4.8.3 Process

- ADM-B is reconnected.
- ADM-B discovers the Local Master ADM-A.
- ADM-B sends an *AD Update Request* containing its current Domain Internal Record to the Local Master.
- ADM-A authenticates the request and checks whether the received record is more recent than its own or not.
- If not, then ADM-A responds with the updated AD information and ADM-B updates its Domain Internal Record.
- If yes, then ADM-A updates it's Domain Internal Record and broadcasts the new record to the whole AD.

4.8.4 Information Flows

Figure 11 describes the information flows required for Scenario 8.

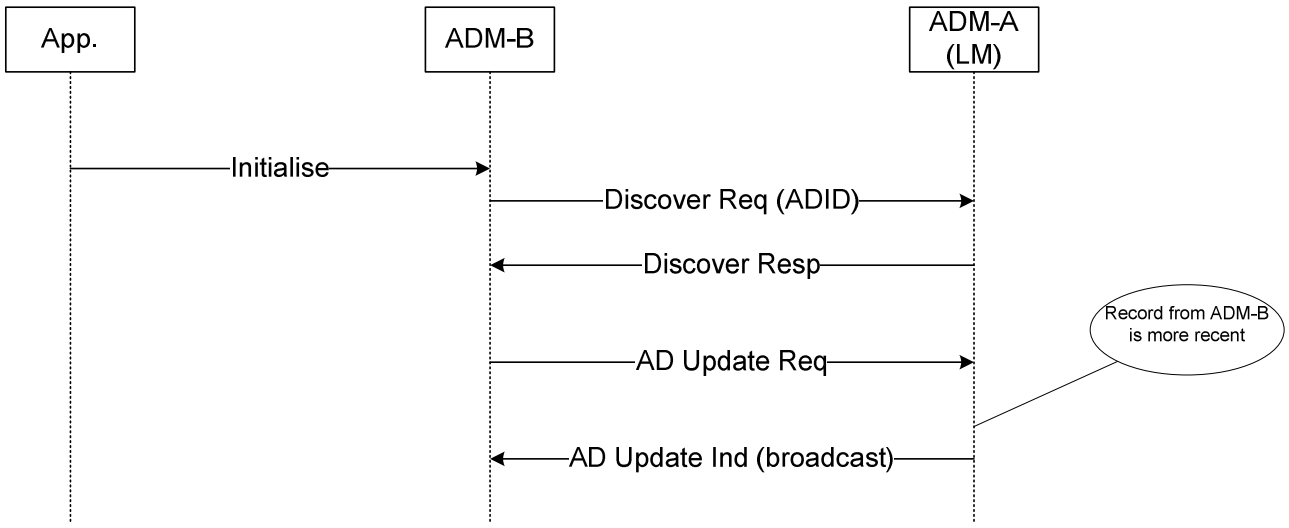


Figure 11: Scenario 8 Flows - Device Reconnection

4.8.5 Exit Conditions

After Scenario 8 has been completed all AD devices have current Domain Internal Records.

4.9 Scenario 9 - Remove a Device from the AD

4.9.1 Use Case

Scenario 9 covers the case where the user tells a device to remove itself from the AD. This makes the device into a single-member AD. This case is only used when there is **no** desire to maintain AD-bound Content for use with the removed device.

NOTE 1: Executing this scenario on an ADSE-countable device that is not connected to other AD members will cause loss of ADSE credit, and the size of the AD will not be correctly tracked.

NOTE 2: In the event that a user wishes to destroy an AD entirely, the final device (which is inherently both Domain Controller and Local Master, and which will see an AD size of 1) can simply erase the Domain Internal Record without any need for signalling. Any Content bond to the destroyed AD will be lost.

NOTE 3: If there are multiple DCs in the AD, it is necessary to ensure that the device being removed is not the only Domain Controller. If it is, then the Domain Controller function should preferably be Transferred first (see clause 4.12).

4.9.2 Entry Conditions

At the beginning of Scenario 9, we have:

- Two or more devices Joined to an AD.
- One or more devices that belong to the same AD.
- A Domain Controller is present.

4.9.3 Process

The process below is described in the case when the current Local Master is the Domain Controller and the AD Leaving device is ADSE countable:

- The user requests for a device to Leave the current AD.
- ADM-B broadcasts a Discovery request.
- The Domain Controller replies with a Discovery Response.
- ADM-B sends an *AD Leave Begin* message to the Domain Controller.
- The Domain Controller sends an *AD Leave Ready* to ADM-B.
- ADM disables the AD Secret and sends an *AD Leave Commit* to the Domain Controller.
- The Domain Controller updates its ADSE values and sends *AD Leave Confirm* to ADM-B.
- ADM-B erases all stored AD information including secrets and the ADID and any past AD memberships.
- ADM-B sends an *AD Leave Finish* to the Domain Controller.
- ADM-A broadcasts an *AD Update Indication*.
- Other devices adjust their AD size counts to the revised value.
- The ADM-B device reverts to Blank.
- OR, as an implementation option, ADM-B generates a new ADID and secrets and it creates a single-member AD.

- If the device does not count for ADSE, then the Local Master proceeds with the departure even if it is not a Domain Controller. If the device counts for ADSE and the Local Master is not a Domain Controller, then the Local Master forwards all messages to the Domain Controller.

4.9.4 Information Flows

Figures 12 to 15 describe the information flows required for Scenario 9.

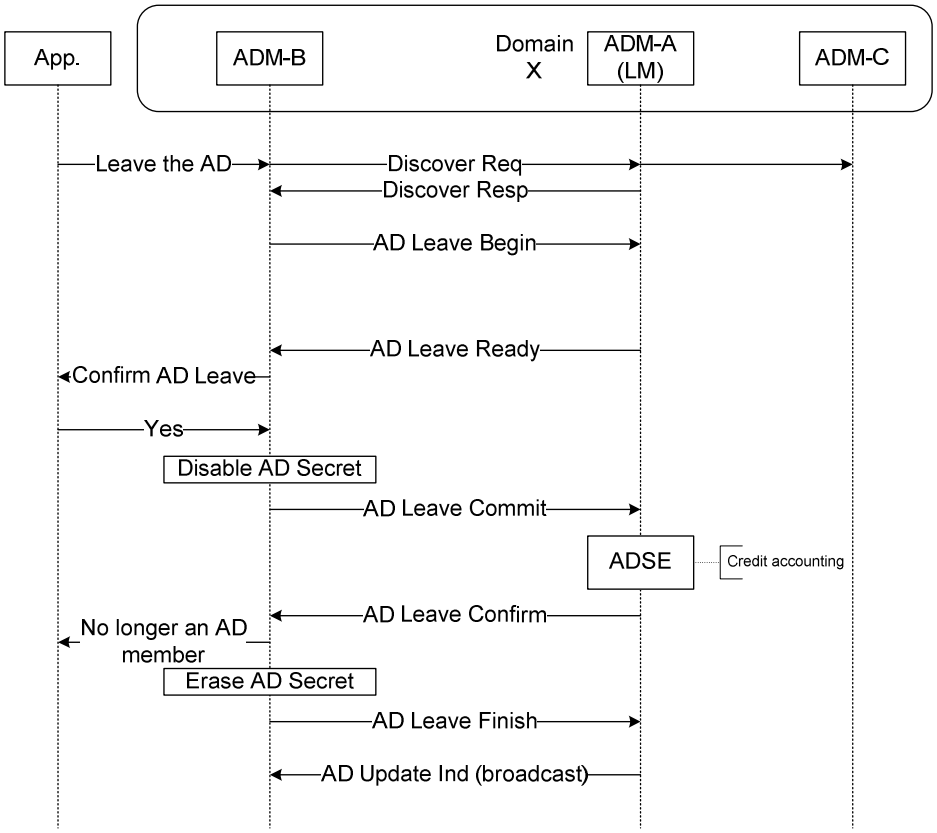


Figure 12: Scenario 9a Flows - AD Leave

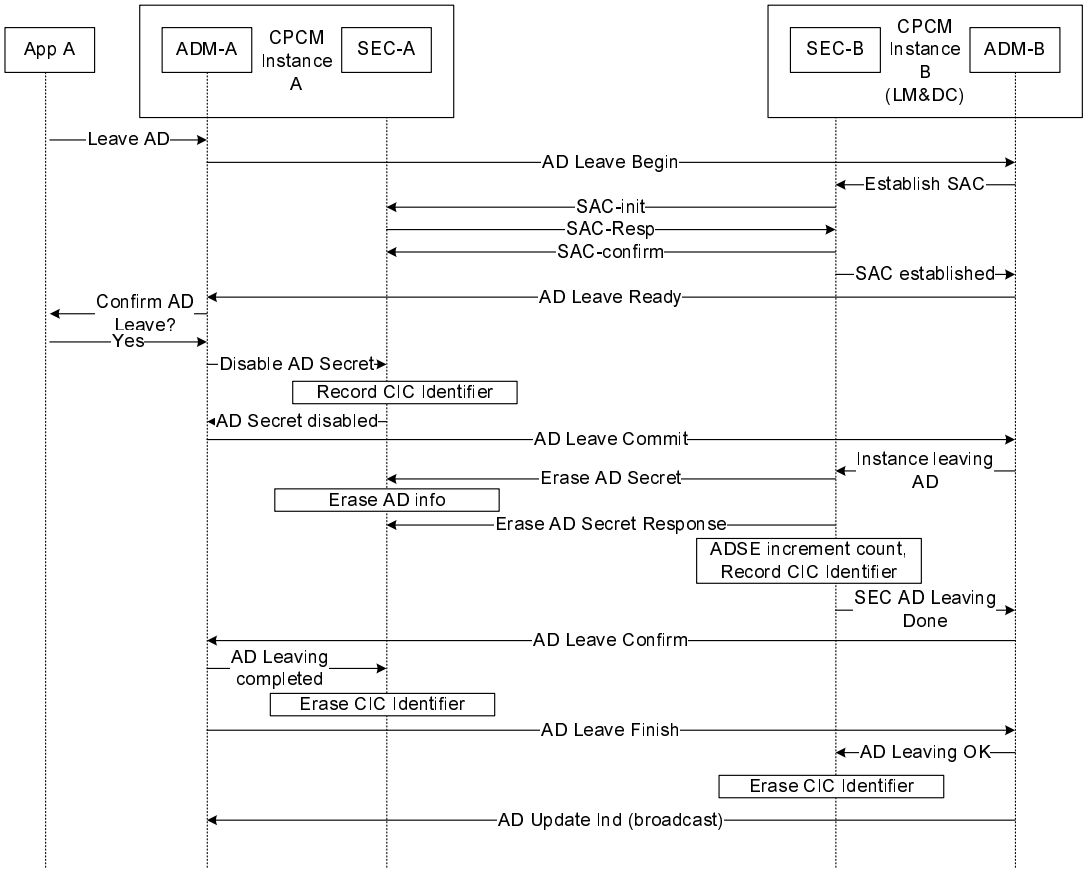


Figure 13: Scenario 9b Flows - ADM/SEC Interaction during Basic AD Leave

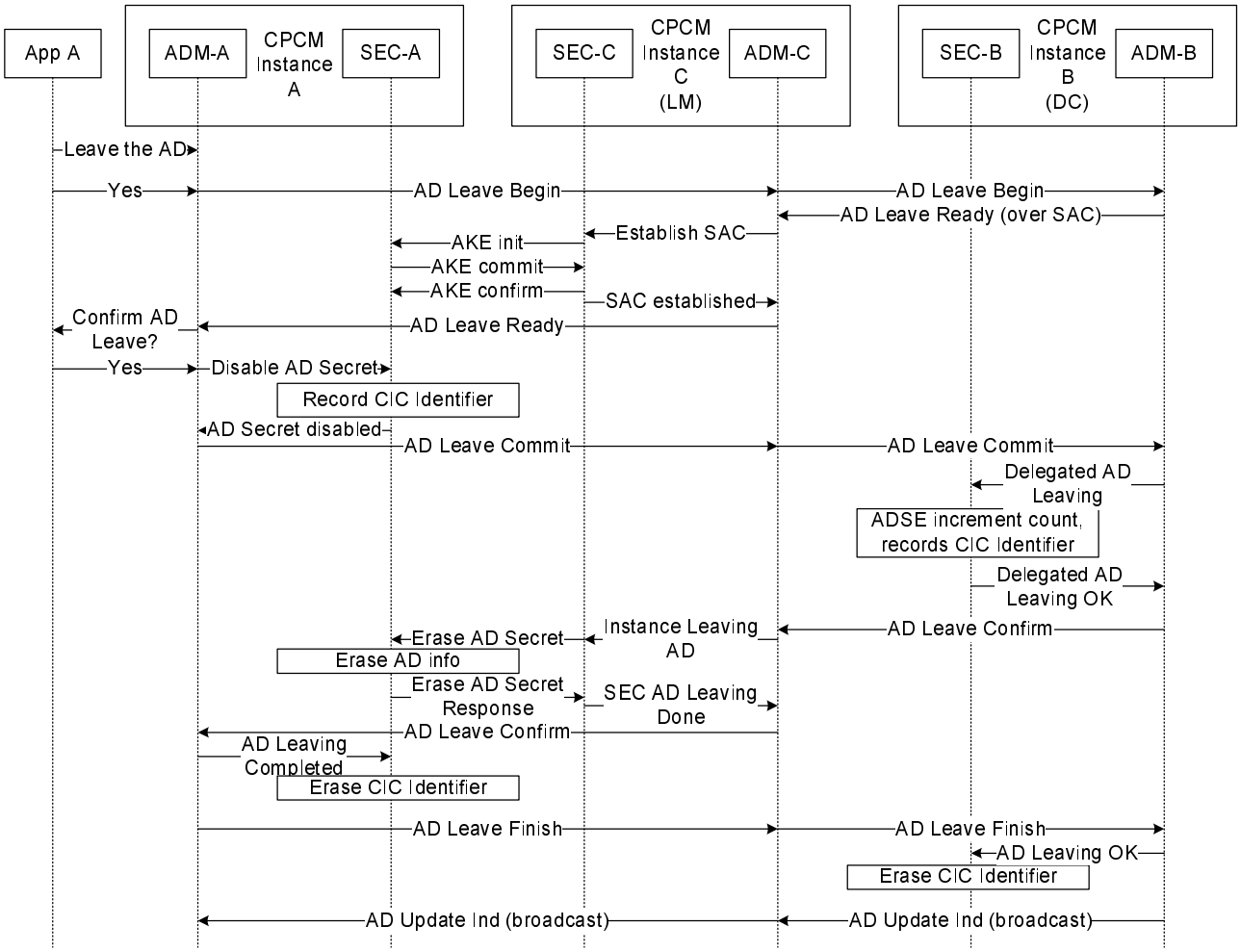


Figure 14: Scenario 9c Flows - ADM/SEC Interaction during Remote AD Leave

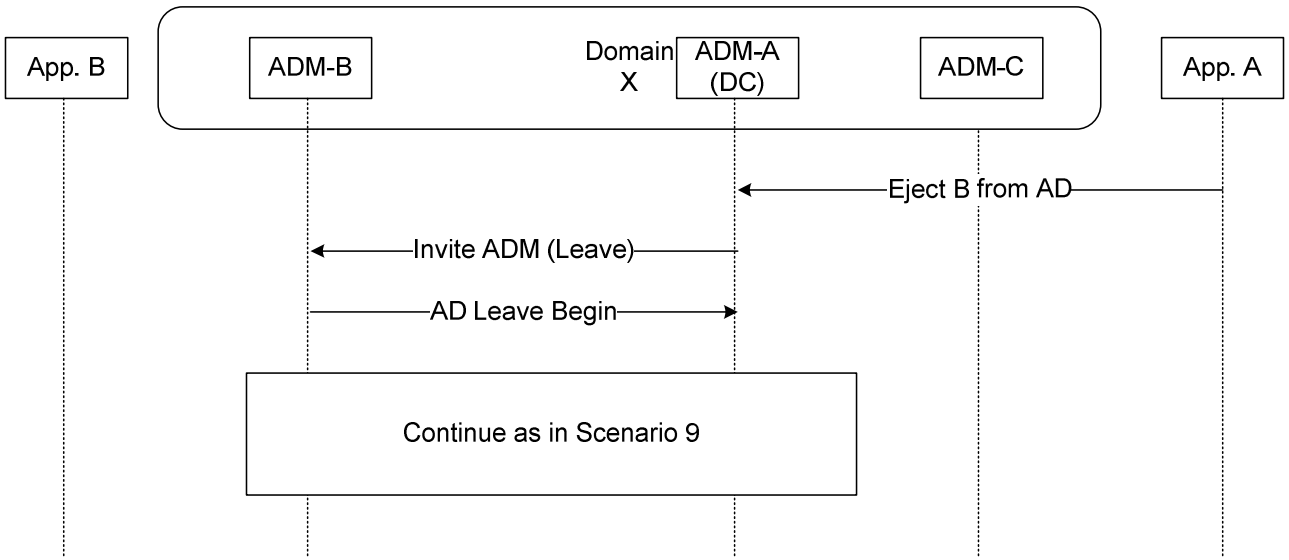


Figure 15: Scenario 9d Flows - "Ejection" from AD

4.9.5 Exit Conditions

After Scenario 9 has been completed:

- ADM-B is blank or forms a single-member AD.
- Other devices in the original AD remain members.

4.10 Scenario 10 - AD naming/renaming

4.10.1 Use Case

Scenario 10 covers the case where the user changes the "friendly" name of an AD. All devices need to be updated with this information, including those that are not connected at the time.

4.10.2 Entry Conditions

At the beginning of Scenario 10, we have:

- The ADMs in Devices A, B, and C belong to the same multi-device AD.
- ADMs A and B are currently connected and active.
- ADM-C is not connected (or is not active).

4.10.3 Process

- User tells ADM-A to change the name of the AD.
- ADM-A broadcasts an *AD Update Indicator*. with the new name for the ADID.
- ADM-B updates its own record of the AD name.
- ADM-C reconnects to the network.
- ADM-C broadcasts a *Discovery Request* to discover the Local Master.
- ADM-B responds with a *Discovery Response* message.
- ADM-C sends an *AD Update Request* to ADM-A.
- ADM-B sends an *AD Update Response* to ADM-C.
- ADM-C updates its own record with the new AD name.

4.10.4 Information Flows

Figure 16 describes the information flows required for Scenario 10.

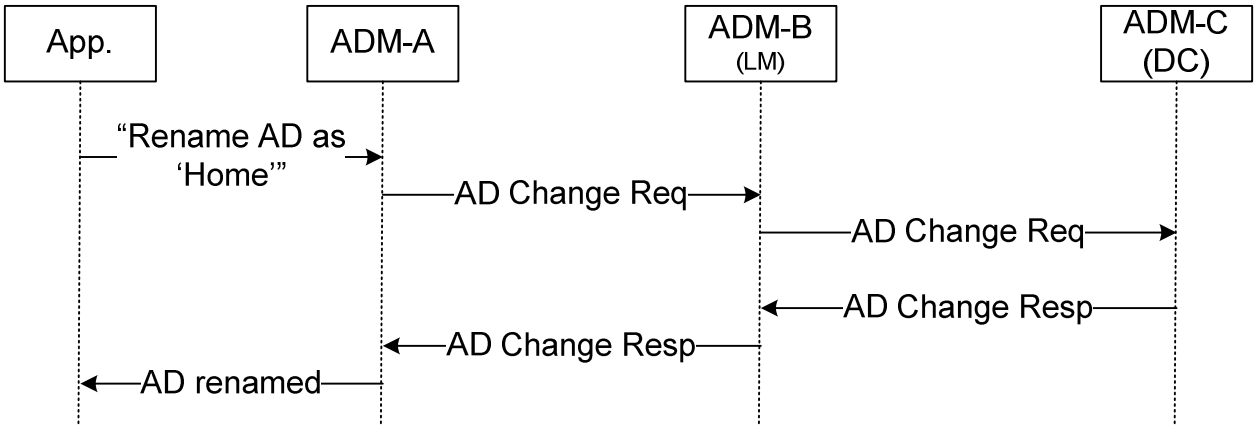


Figure 16: Scenario 10 Flows - AD Update / Rename

4.10.5 Exit Conditions

After Scenario 10 has been completed all three devices have the new name for the AD.

4.10.6 Notes

There are implementation issues with disambiguating similar AD Name strings. These are probably best left for individual implementations to resolve.

4.11 Scenario 11 - Changing the Local Master

4.11.1 Use Case

This scenario may arise for many reasons. The intent is that the most capable local device is always elected as the Local Master to retain local AD consistency and reduce the burden on less capable devices.

Situations that may cause this scenario include but are not limited to:

- Change of Domain Controller.
- At the request of a human user or Device Application.
- Addition of a new device to the network.
- Failure of the current Local Master to respond.
- Planned removal of the Local Master.

The election should result in the device with the highest current LM Capability becoming the new local master.

4.11.2 Entry Conditions

At the beginning of Scenario 11, we have:

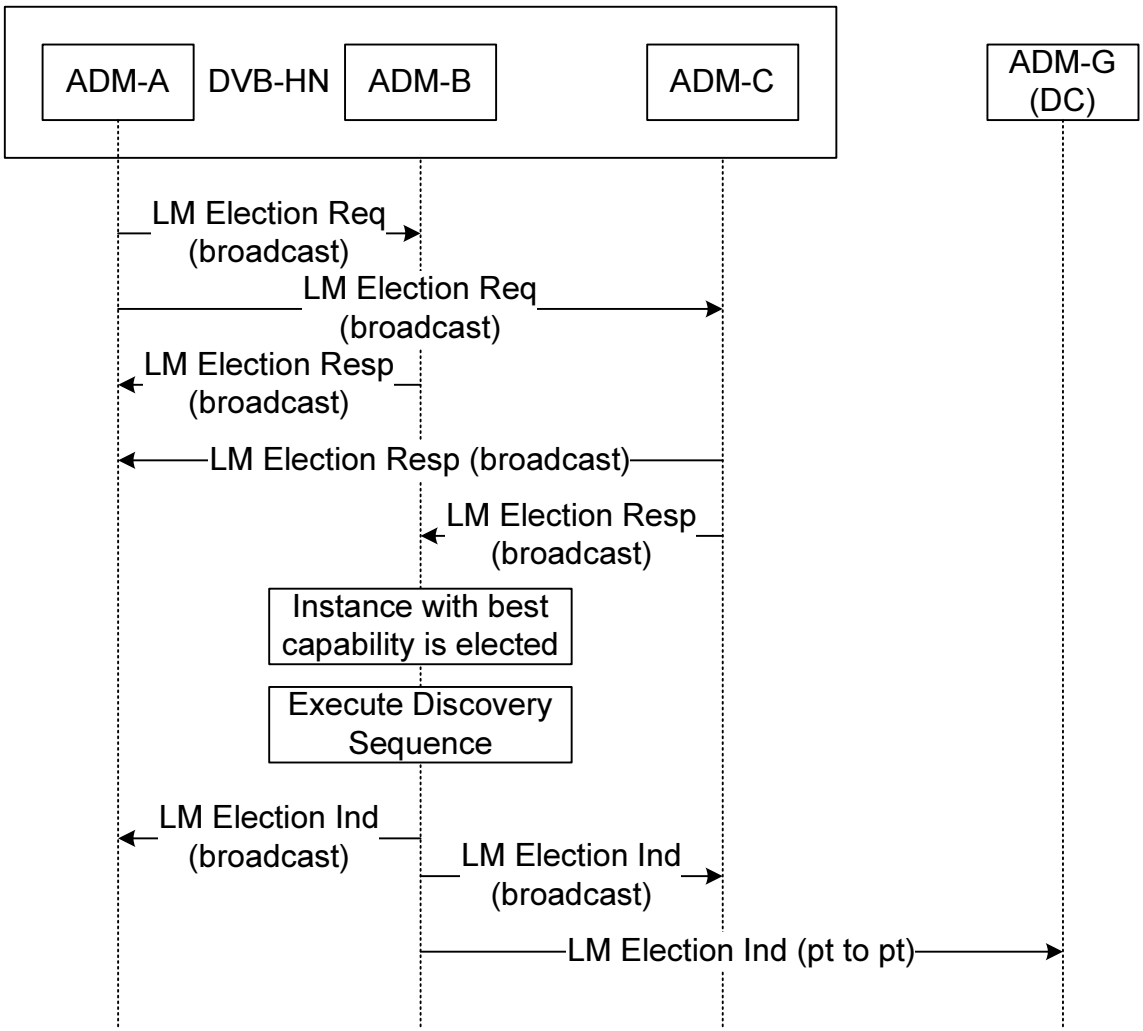
- An AD X with multiple member devices.

4.11.3 Process

- An AD member (ADM-A) initiates an election between connected devices.
- ADM-A broadcasts a *Local Master Election Request.*
- Each ADM in the same AD on the same HN broadcasts a *Local Master Election Response*, signalling its own ADM capability level.
- After a suitable timeout, the ADM with the highest capability level broadcasts a Local Master Election Indication, notifying all (local) ADMs that it has now become the Local Master.
- The new Local Master sends a Local Master Election Indication to the Domain Controller, if available.

4.11.4 Information Flows

Figure 17 describes the information flows required for Scenario 11.



NOTE: Figure 17 shows a remote Domain Controller. Where the Domain Controller is local, it will always act as Local Master.

Figure 17: Scenario 11 Flows - Changing the Local Master

4.11.5 Exit Conditions

After Scenario 11 has been completed, the present device that has the greater LM capability is new Local Master.

4.12 Scenario 12 - Changing the Domain Controller

4.12.1 Use Case

The user needs to take with him the Domain Controller device to be able to let a new device Join when travelling, consequently the portable mobile player will become a new Domain Controller.

4.12.2 Entry Conditions

At the beginning of Scenario 12, we have:

- Two or more devices Joined to the AD.
- The CPCM Instance A is the Domain Controller and thus Local Master.
- User triggers DC Transfer from CPCM Instance A to CPCM Instance B.

4.12.3 Process

- CPCM Instance B broadcasts a *Discovery Request* message.
- CPCM Instance A replies with a *Discovery Response* as usual.
- CPCM Instance B sends a *Domain Controller Transfer Begin*.
- CPCM Instance A replies with a *Domain Controller Transfer Ready*.
- CPCM Instance B replies with a *Domain Controller Transfer Commit*.
- CPCM Instance A request SEC-A to deliver all ADSE values and ceases to be a Domain Controller.
- CPCM Instance A sends a *Domain Controller Transfer Confirm* message.
- CPCM Instance B becomes a Domain Controller and sends a *Domain Controller Transfer Finish* message.
- CPCM Instance B broadcasts an *AD Update Indication* message to inform other AD Members of the Domain Controller change.
- CPCM Instance B triggers a new Local Master Election.

NOTE: If the Domain Controller is Remote, the CPCM Instance to which Domain Controller is to be Transferred will first trigger a Local Master Election where it sets is capability to the higher level. The protocol will thus occur directly between the two involved devices and never use delegation.

4.12.4 Information Flows

Figure 18 describes the information flows required for Scenario 12.

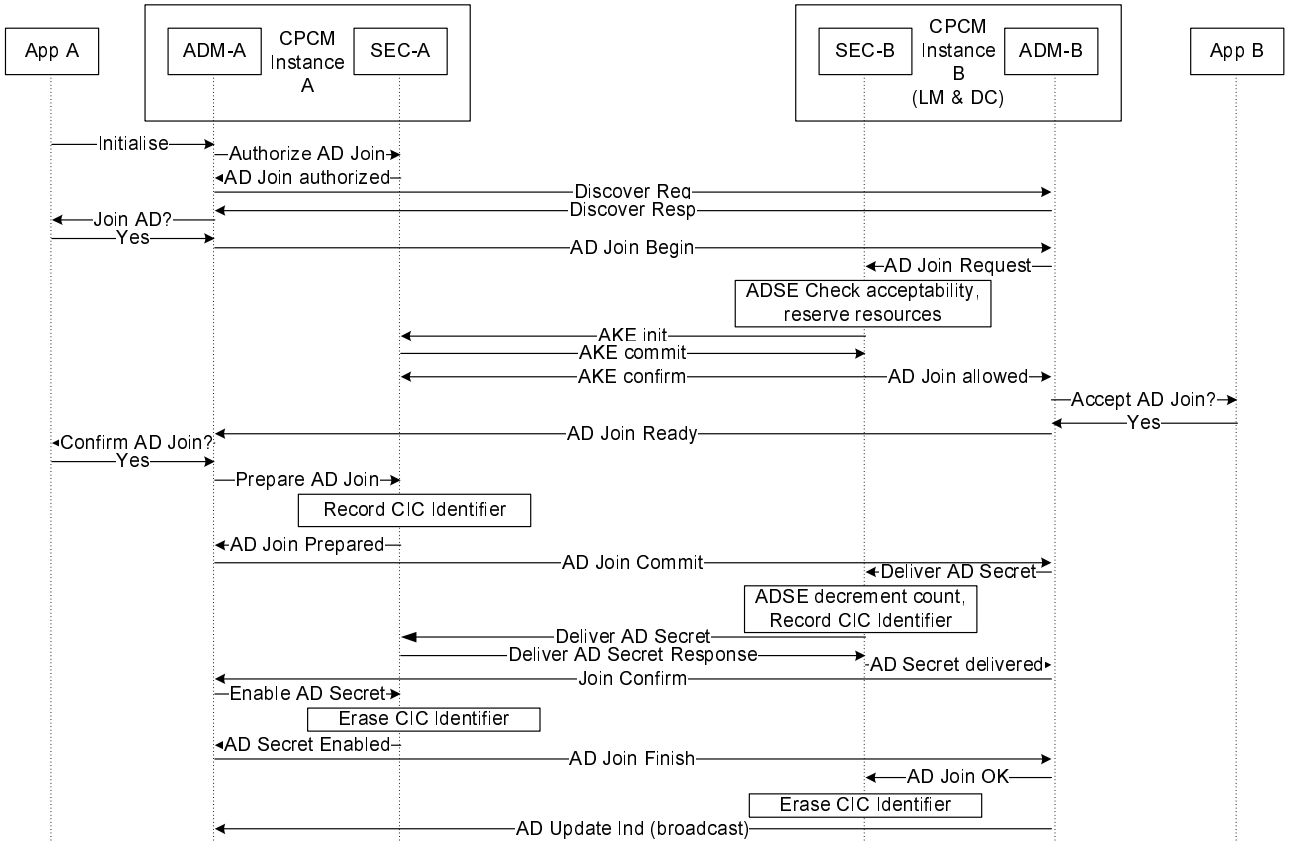


Figure 18: Scenario 12 Flows - Changing the Domain Controller

4.12.5 Exit Conditions

After Scenario 12 has been completed:

- CPCM Instance A is AD member.
- CPCM Instance B is a Domain Controller and the Local Master.

4.13 Scenario 13 - Splitting the Domain Controller function

4.13.1 Use Case

The user wants to have more than one Domain Controller, either for reasons of fault-tolerance, or because they want to operate in two or more locations without network connectivity between them.

4.13.2 Entry Conditions

At the beginning of Scenario 13, we have:

- Two or more devices Joined to the AD.
- The CPCM Instance A is the Domain Controller and thus Local Master.
- The user triggers a DC Split from CPCM Instance A to CPCM Instance B.

4.13.3 Process

- CPCM Instance B broadcasts a *Discovery Request* message.
- CPCM Instance A replies as Local Master with a *Discovery Response* as usual.
- CPCM Instance B sends a *Domain Controller Merge Begin*.
- CPCM Instance A replies with a *Domain Controller Merge Ready*.
- CPCM Instance B replies with a *Domain Controller Merge Commit*.
- CPCM Instance A requests SEC-A to deliver the ADSE values.
- CPCM Instance A sends a *Domain Controller Merge Confirm* message.
- CPCM Instance B becomes a Domain Controller and sends a *Domain Controller Merge Finish* message.
- CPCM Instance B broadcasts an *AD Update Indication* message to inform the other AD Members of the Domain Controller change.

NOTE: If the Domain Controller is Remote, the CPCM Instance which the DC Split occurs will first trigger a Local Master Election where it sets is capability to the higher level. The protocol will thus always occur directly between the two involved devices and never use delegation.

4.13.4 Information Flows

Figure 19 describes the information flows required for Scenario 13.

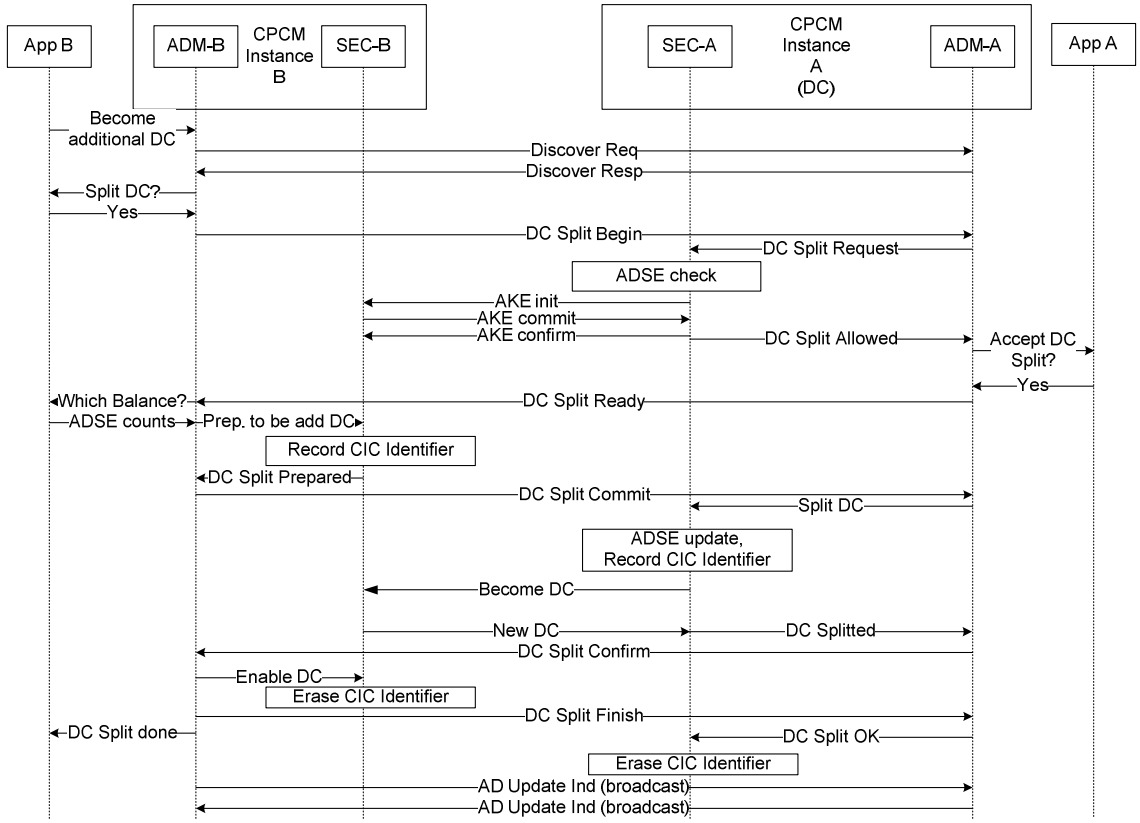


Figure 19: Scenario 13 Flows - Splitting the Domain Controller function

4.13.5 Exit Conditions

After Scenario 13 has been completed both ADM A and ADM B are Domain Controllers.

4.14 Scenario 14 - Merging Domain Controller functions

4.14.1 Use Case

A user running an AD with two Domain Controllers wished to downgrade one of them to become a non-DC Instance, perhaps because it is no longer required and will shortly be removed. The user wants to recover the ADSE quotas that have previously been allocated to this Instance.

4.14.2 Entry Conditions

At the beginning of Scenario 14, we have:

- Two or more devices Joined to the AD.
- Both CPCM Instance A and CPCM Instance B are Domain Controllers in the same AD.
- The user requests A to cease to be a Domain Controller and to transfer its function into B.

4.14.3 Process

- CPCM Instance A broadcasts a *Discovery Request* message.
- CPCM Instance B replies as Domain Controller with a *Discovery Response* as usual.
- CPCM Instance A sends a *Domain Controller Merge Begin*.
- CPCM Instance B replies with a *Domain Controller Merge Ready*.
- CPCM Instance A disables its Domain Controller capability.
- CPCM Instance A replies with a *Domain Controller Merge Commit*.
- CPCM Instance B request SEC-B to proceed with the DC Merge.
- CPCM Instance B sends a *Domain Controller Merge Confirm*.
- CPCM Instance A ceases to be a Domain Controller.
- CPCM Instance A sends a *Domain Controller Merge Finish*.
- CPCM Instance B broadcasts an *AD Update Indication* message to inform the other AD Members of the Domain Controller Merge.
- CPCM Instance A broadcasts an *AD Update Indication* message to inform the other AD Members of the Domain Controller Merge.

4.14.4 Information Flows

Figure 20 describes the information flows required for Scenario 14.

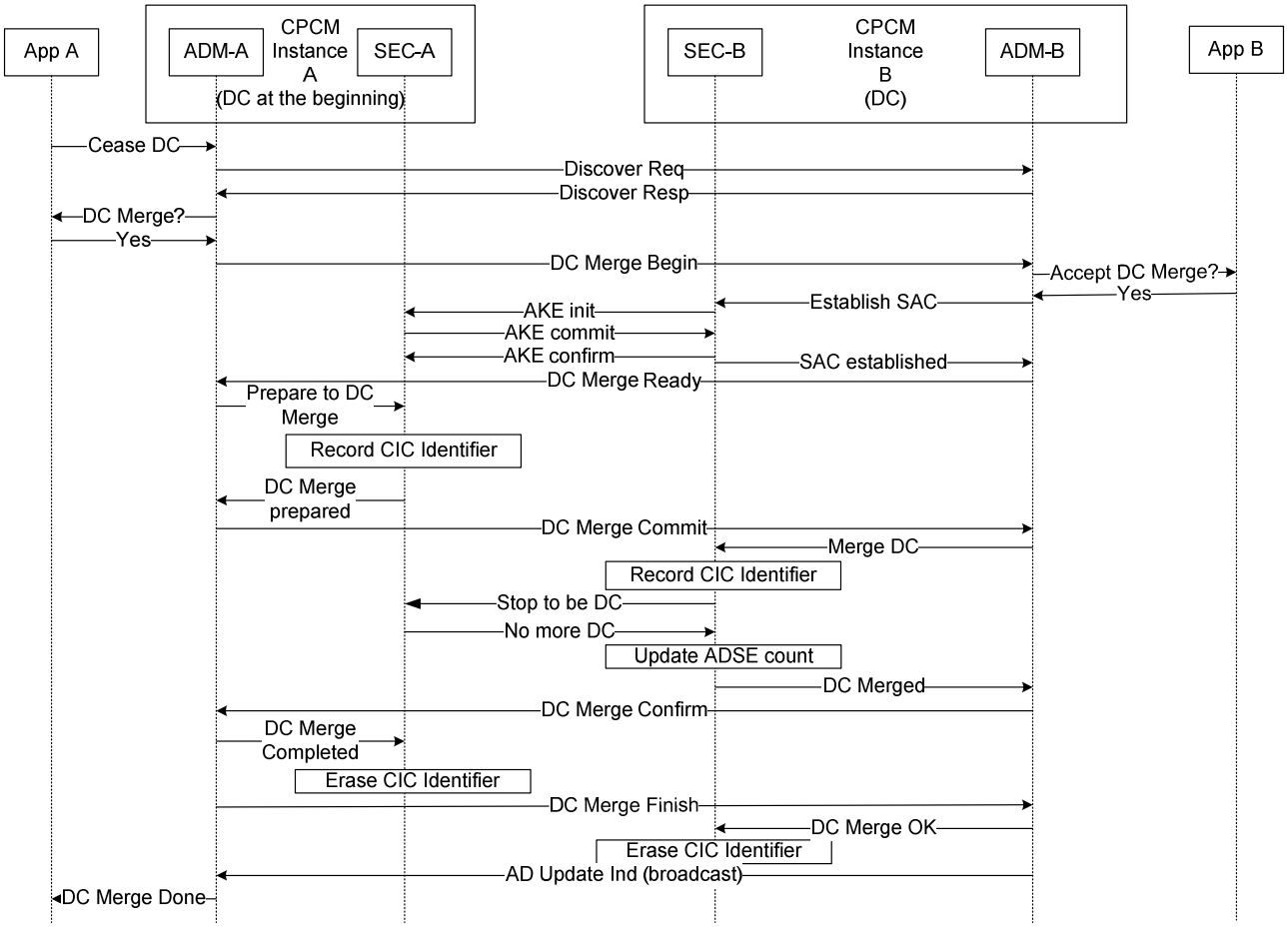


Figure 20: Scenario 14 Flows - Merging Domain Controller functions

4.14.5 Exit Conditions

After Scenario 14 has been completed the CPCM Instance A is AD member and Instance B is the Domain Controller.

4.15 Scenario 15 - Rebalancing Domain Controllers

4.15.1 Use Case

An AD with more than one Domain Controller requires an adjustment to the spread of ADSE allocations between the controllers.

4.15.2 Entry Conditions

At the beginning of Scenario 15, we have:

- Both CPCM Instance A and CPCM Instance B are Domain Controllers in the same AD.

4.15.3 Process

- CPCM Instance A broadcasts a *Discovery Request* message.
- CPCM Instance B replies as a Domain Controller with a *Discovery response* as usual.
- CPCM Instance A sends a *Domain Controller Rebalance Begin*.
- CPCM Instance B replies with a *Domain Controller Rebalance Ready*.
- CPCM Instance A replies with a *Domain Controller Rebalance Commit*.
- CPCM Instance B request SEC-B to proceed with the DC Rebalance.
- CPCM Instance B sends a *Domain Controller Merge Confirm*.
- CPCM Instance A enables the new ADSE counts and sends a *Domain Controller Merge Finish*.
- CPCM Instance B enables the new ADSE counts and broadcasts an *AD Update Indication* message to inform the other AD Members of the Domain Controller Merge.
- CPCM Instance A broadcasts an *AD Update Indication* message to inform the other AD Members of the Domain Controller Merge.

4.15.4 Information Flows

Figure 21 describes the information flows required for Scenario 15.

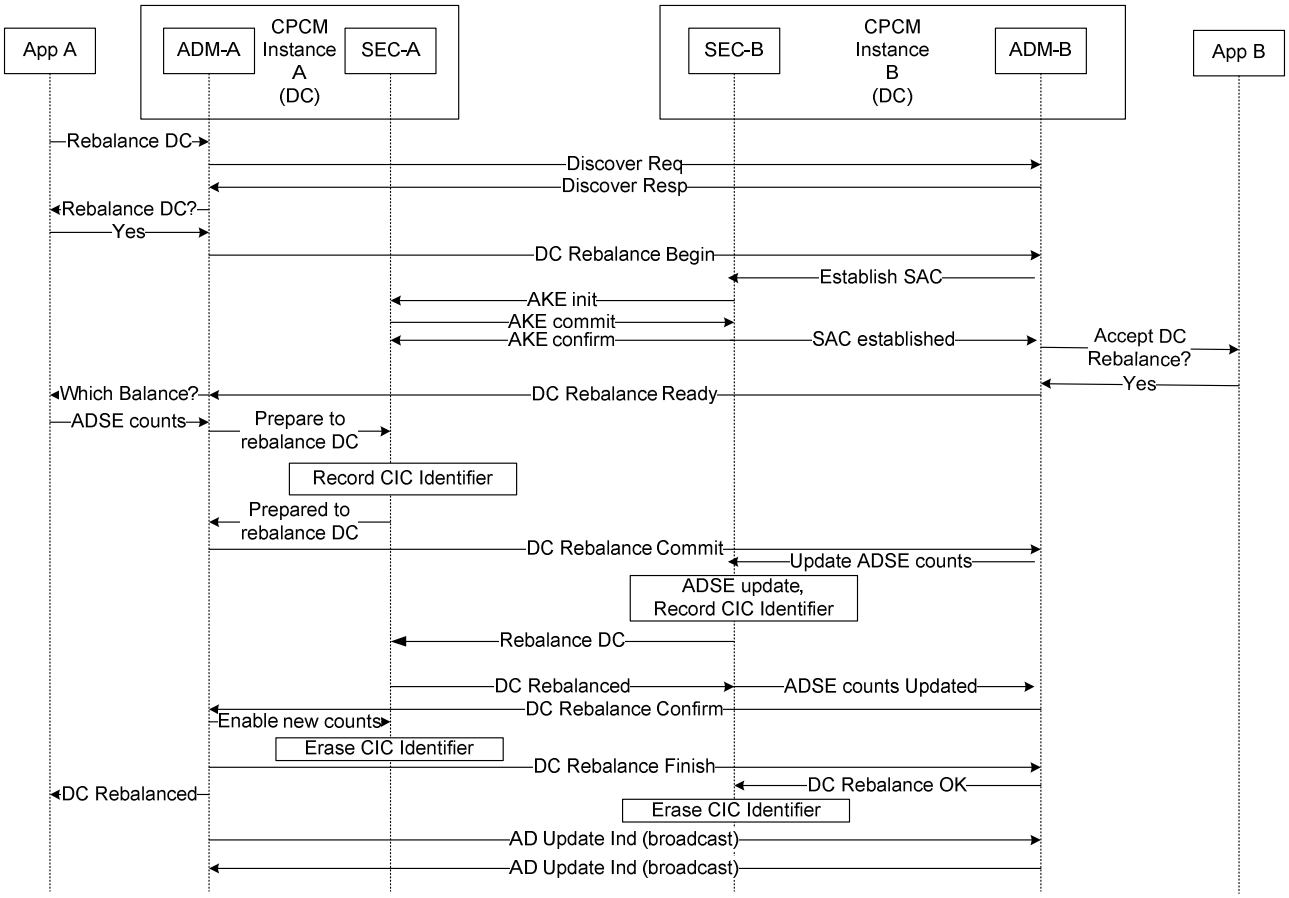


Figure 21: Scenario 15 Flows - Rebalancing Domain Controller ADSE quotas

4.15.5 Exit Conditions

After Scenario 15 has been completed both ADM A and ADM B are still Domain Controllers but with changed ADSE records.

List of figures

History

Document history		
V1.1.1	July 2008	Publication