ETSI TR 102 825-11 V1.1.1 (2011-03)

Technical Report

Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 11: CPCM Content Management Scenarios

Reference
DTR/JTC-DVB-222-11

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

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 2011.
© European Broadcasting Union 2011.
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.
LTE™ is a Trade Mark of ETSI currently being registered
for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

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

The Digital Video Broadcasting Project (DVB) is an industry-led consortium of broadcasters, manufacturers, network operators, software developers, regulatory bodies, content owners and others committed to designing global standards for the delivery of digital television and data services. DVB fosters market driven solutions that meet the needs and economic circumstances of broadcast industry stakeholders and consumers. DVB standards cover all aspects of digital television from transmission through interfacing, conditional access and interactivity for digital video, audio and data. The consortium came together in 1993 to provide global standardisation, interoperability and future proof specifications.

The present document is part 11 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 & 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; 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 such as 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.

The present document describes some example approaches of implementation of Content Management Scenarios using DVB-CPCM which support the identified business models. The examples described in the present document are not exhaustive.

The present document is informative, and not binding on manufacturers for conformance to the specification.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

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

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 necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[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 EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".

[i.5] ETSI TS 102 833: "Digital Video Broadcasting (DVB); File Format Specification for the Storage and Playback of DVB Services".

[i.6] ETSI TS 102 825-10: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM) Part 10: CPCM Acquisition, Consumption and Export Mappings".

[i.7] ETSI TS 102 825-3: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM) Part 3: CPCM Usage State Information".

[i.8] ETSI TS 102 825-7: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM) Part 7: CPCM Authorized Domain Management".

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.

NOTE: In some cases, for ease of reading, definitions are repeated in the present document. In case of conflict, the terms in TS 102 825-1 [i.3] will take precedence.

For ease of reading by non-specialists, the present document employs some simplified language. Readers seeking detailed technical understanding are directed to the normative specifications and definitions of terms.

3.1.1 Instance and Device

In the CPCM specifications, much use is made of the term CPCM instance. This is good for the technical specification, as it leaves the option open for manufacturers to support multiple instances in a single device while remaining conformant. However, in the present document we often use the term Device. This is simply for reasons of ease of understanding for the majority of readers. Unless otherwise stated, within the present document the term device refers to a physical item of equipment that implements a single CPCM instance. This neither precludes the inclusion of multiple instances in a physical unit, nor the distribution of the functionality of a single CPCM instance across multiple physical units.

3.1.2 CPCM Device

The present document is focussed on describing CPCM devices. As such, the term device used in isolation should be read as CPCM Device unless otherwise indicated.

3.1.3 CPCM Content

Likewise, where mention is made of content, this should be assumed to be CPCM content unless otherwise indicated.

3.1.4 Server

We use the term server for the device acting as source of the current content.

3.1.5 Player

We use the term player for the device acting as sink for the current content.

3.2 Abbreviations

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

NOTE: In some cases, for ease of reading, abbreviations are repeated in the present document. In case of conflict, the abbreviation in TS 102 825-1 [i.3] will take precedence.

AAA Authorised Authenticated Agent

NOTE: Service provider function.

AD Authorised Domain
C1 Copy Once
CCI Copy Control Information
CCNA Copy Control Not Asserted
CLC Content Licence Creator
CN Copy Never

CNM	Copy No More
DNCS	Do Not CPCM Scramble
DVB-FF	DVB File Format specification

NOTE: See TS 102 833 [i.5].

MAD	Movement and copying allowed within Authorised Domain
MCPCM	Movement and copying allowed to any CPCM device
MCPI	Move and Copy Propagation Information
MGAD	Movement and copying allowed within *Geographically constrained* Authorised Domain
MLAD	Movement and copying allowed within *Localised* Authorised Domain
MLocal	Movement and copying allowed to devices in close proximity, even when not AD members
SVC	Simultaneous View Count
USI	Usage State Information
VAD	Viewing allowed within Authorised Domain
VCPCM	Viewing allowed by any CPCM device
VGAD	Viewing allowed within a geographically constrained Authorised Domain
VLAD	Viewing allowed within a localised Authorised Domain
VLocal	Viewing allowed by devices in close proximity, even when not AD members
VPI	Viewing Propagation Information

4 Common Content Management Scenarios

The following scenarios cover situations that can be supported by CPCM without significant additional complexity or extensions.

These scenarios cover a broad range of business and usage models, but are not exhaustive.

In some cases the scenarios can be combined. In others they may be mutually exclusive. Unfortunately it is not possible to provide a definitive list of all possible combinations.

Most scenarios are presented in the same general manner:

1) Business Intent.

2) Suggested USI settings.

3) Operation of CPCM under these settings.

Some basic scenarios are written in close detail. Others assume a degree of understanding of earlier, simpler cases.

As an informative document, the intent has been readability rather than technical precision and completeness.

In many scenarios, some of the suggested USI settings are more important than others. In such cases, the more important values are shown underlined in the USI tables.

4.1 Scenario 1 - Unrestricted Free-to-Air

4.1.1 Business Intent

This scenario covers content that is broadcast with minimal restrictions, for example content that is open for all consumers within the broadcast footprint, and which can also be redistributed to other users both within and beyond the broadcast footprint.

NOTE: This scenario applies where content is brought under CPCM control so as to be governed by the rules of a C&R Regime. Where there is no need to follow such rules, the content will not be brought under CPCM control. Situations where content is not brought under CPCM control are out of scope for the present document. This allows for co-existence of CPCM Devices and non-CPCM Devices in a network environment such that both types of device may handle non-CPCM content.

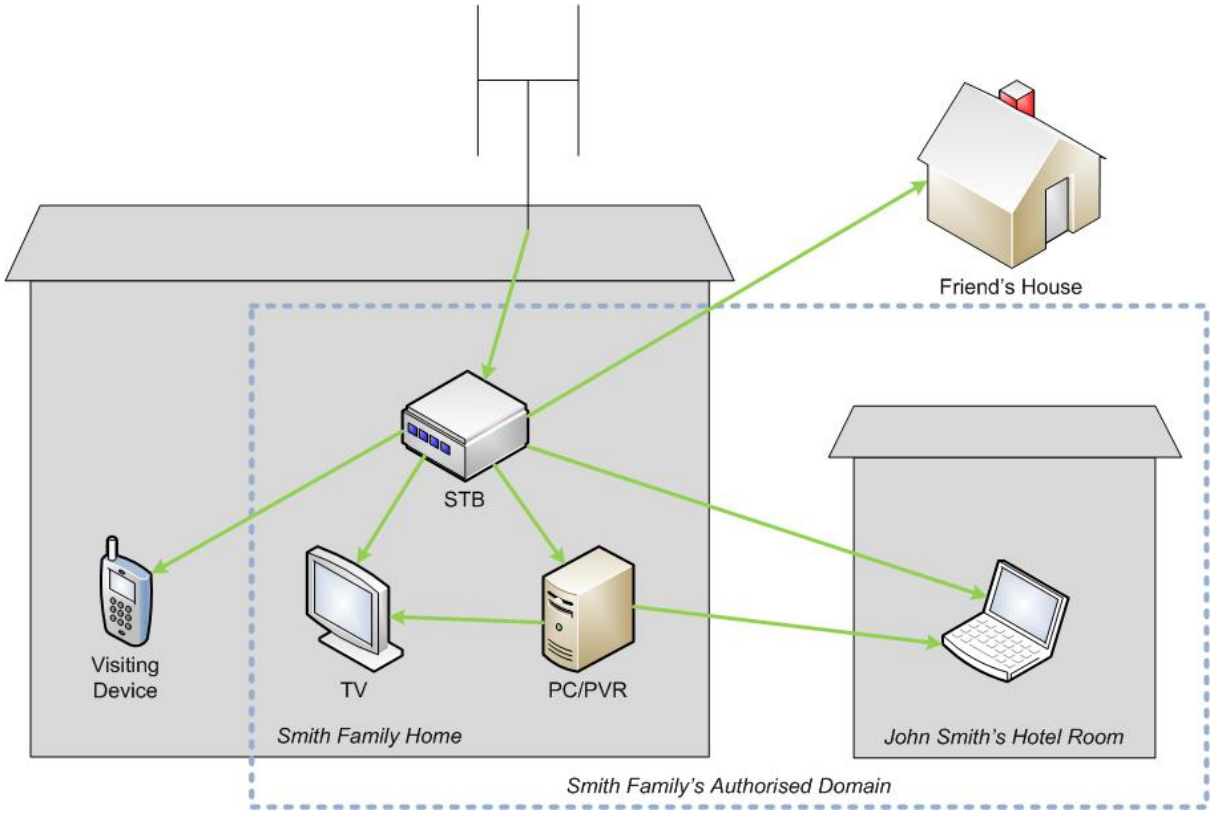

Figure 1: Unrestricted Free-to-Air Content Flow

4.1.2 Usage State Information

This scenario corresponds to the 00 setting of the control_remote_access_over_internet field of the DVB-SI FTA content management descriptor. For the normative description of this signal, see reference [i.4].

The following USI settings will enforce this usage of content.

Table 1: Unrestricted Free-to-Air USI

Type of Control	**Propagation Control**				**Copy Control**
	Movement		**View**		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	**MCPCM**	(Ignored)	**VCPCM**	(Ignored)	**CCNA**
NOTE: The values of the MLocal and VLocal fields are ignored when MCPCM and VCPCM are asserted, because proximity is not a factor.					

4.1.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

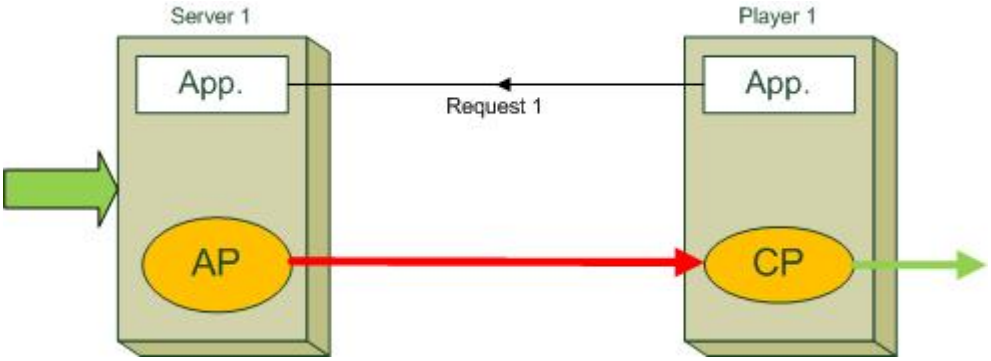

Figure 2: Unrestricted Free-to-Air Operation

CPCM operation will proceed as follows:

a) Request 1 comes from another CPCM device be it local or remote.

b) Server 1's application asks its CPCM Acquisition Point (AP) function to provide content to Player 1.

c) The AP function establishes trust with Player 1 CPCM Consumption Point (CP) function. Implicitly, Player 1 is authenticated as a CPCM compliant device with matching C&R Regime for this content item.

d) The two devices establish a secure authenticated channel (SAC) session.

e) Server 1's AP permits the CPCM content to flow to Player 1, along with a CPCM content licence protected with the session key.

4.2 Scenario 2 - Free-to-Air Domain-Bound with Immediate Remote Access

4.2.1 Business Intent

This scenario covers content that is broadcast with some restrictions on redistribution:

- Redistribution to other local devices is always permitted.
- Redistribution to remote devices belonging to members of the same household is permitted, no matter what their current location.
- Redistribution to non-local devices that do not belong to household members is prevented.

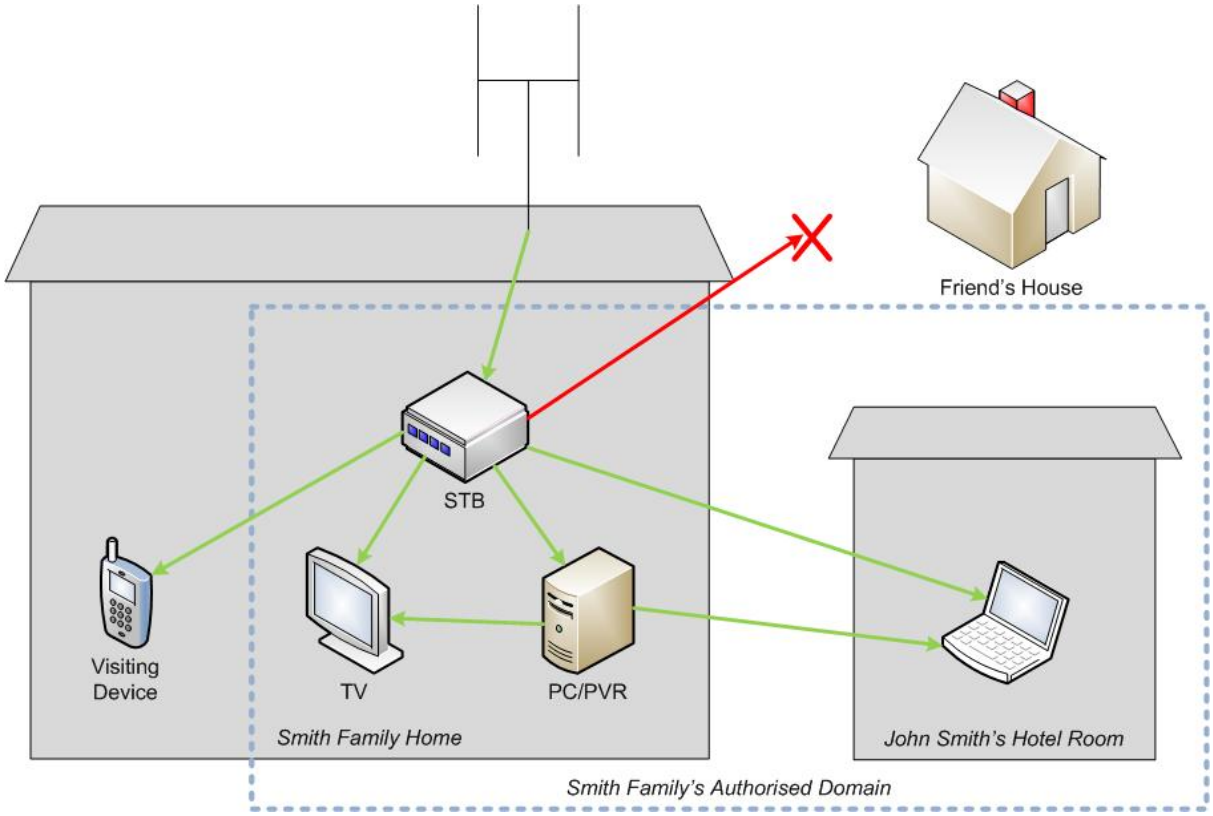

Figure 3: Free-to-Air Domain-Bound with Immediate Remote Access Content Flow

4.2.2 Usage State Information

This scenario corresponds to the 01 setting of the control_remote_access_over_internet field of the DVB-SI FTA content management descriptor.

The following USI settings will enforce this usage of content.

Table 2: Free-to-Air Domain-Bound with Immediate Remote Access USI

Type of Control	**Propagation Control**				**Copy Control**
	Movement		**View**		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	**MAD**	**Asserted**	**VAD**	**Asserted**	**CCNA**

4.2.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

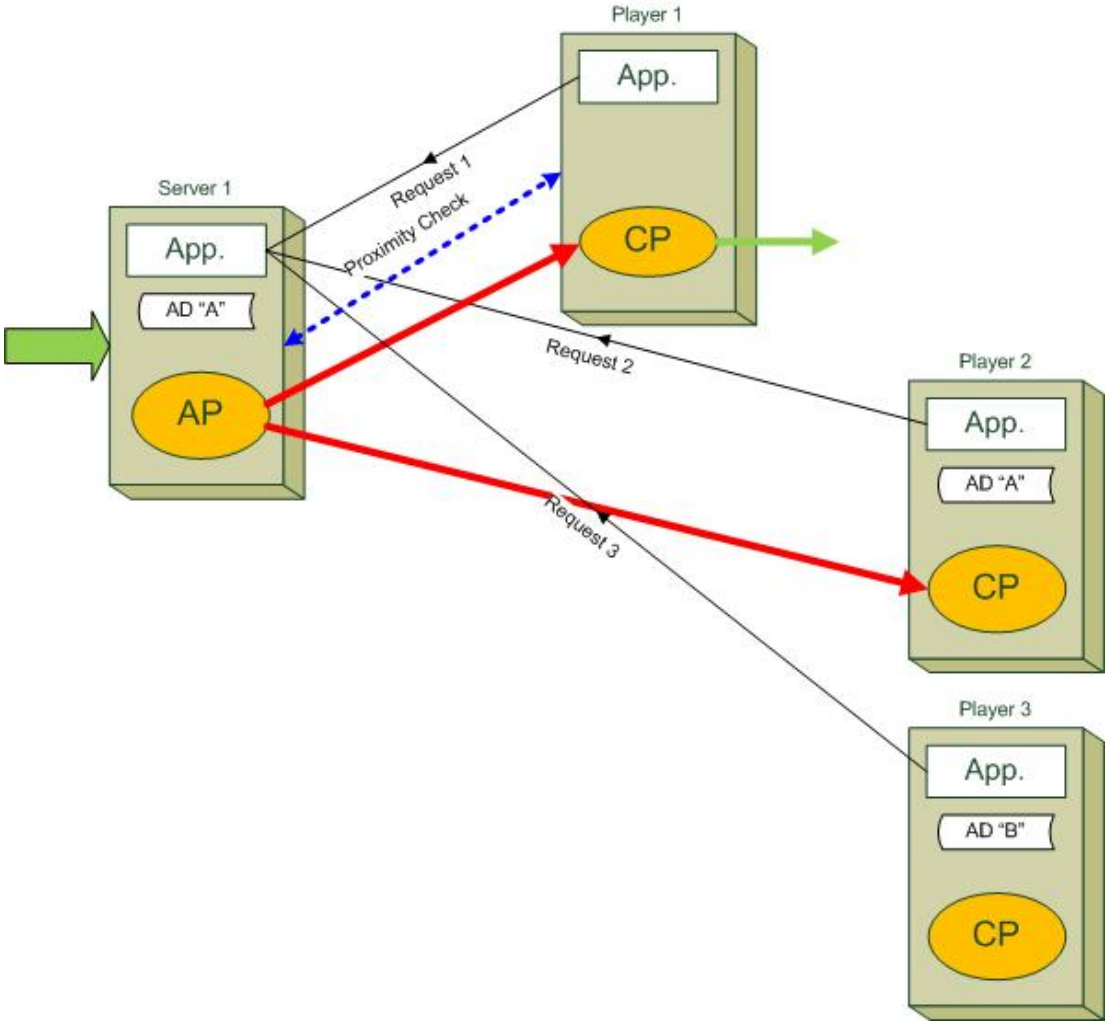

Figure 4: Free-to-Air Domain-Bound with Immediate Remote Access Operation

These USI settings require a server to determine that the requesting player is either:

- Local, which means in close proximity; or
- Is a member of the same Authorised Domain (AD).

CPCM operation will therefore proceed as follows:

1) Request 1 comes from a local device.

   a) Server 1's application asks its CPCM Acquisition Point (AP) function to provide content to Player 1.

   b) The AP function establishes trust with Player 1's CPCM Consumption Point (CP) function. Implicitly, Player 1 is authenticated as a CPCM compliant device with matching C&R Regime for this content item.

   c) The two devices establish a secure authenticated channel (SAC) session, Session 1.

   d) Server 1 employs proximity tests to determine that Player 1 is in close proximity.

   e) If the proximity tests are satisfied, Server 1's AP permits the CPCM content to flow to Player 1, along with a CPCM content licence protected with the Session 1 key.

2) Request 2 comes from a remote device that is member of the same AD but not local.

   a) Server 1's application asks its CPCM Acquisition Point (AP) function to provide content to Player 2.

   b) The AP function establishes trust with Player 2's CPCM Consumption Point (CP) function. Implicitly, Player 2 is authenticated as a CPCM compliant device with matching C&R Regime for this Content Item.

   c) The two devices establish a secure authenticated channel (SAC) session, Session 2.

   d) Server 1 employs proximity tests to determine that Player 2 is not in close proximity.

   e) Server 1 determines that Player 2 is a member of the same AD, AD-A.

   f) Content item Server 1's AP permits the CPCM content to flow to Player 1, along with a CPCM content licence protected with either the Session 2 key or the AD key.

3) Request 3 comes from a remote device that is not a member of the same AD.

   a) Server 1's application asks its CPCM Acquisition Point (AP) function to provide content to Player 3.

   b) The AP function establishes trust with Player 3's CPCM Consumption Point (CP) function. Implicitly, Player 3 is authenticated as a CPCM compliant device with matching C&R Regime for this content item.

   c) The two devices establish a secure authenticated channel (SAC) session Session 3.

   d) Server 1 employs proximity tests to determine that Player 3 is not in close proximity.

   e) Server 1 determines that Player 3 is not a member of the same AD, AD-A.

   f) Server 1 therefore refuses to deliver this content item, and Player 3 displays a suitable error message to the user.

4.3 Scenario 3 - Free-to-Air with Delayed Remote Access

4.3.1 Business Intent

This scenario covers content that is broadcast with some restrictions on redistribution:

- Redistribution to other local devices is always permitted.
- Delayed redistribution to remote devices belonging to members of the same household is permitted, no matter what their current location. Remote access to such content is permitted after a short delay, typically 24 hours.
- Redistribution to non-local devices that do not belong to household members is not authorised.

EXAMPLE: A situation in which the broadcaster applies more restrictive rights during the live showing of an event, such as a sporting event, and then, after the event, more relaxed rights allowing a consumer who recorded the event on their home PVR to watch it remotely at a later time.

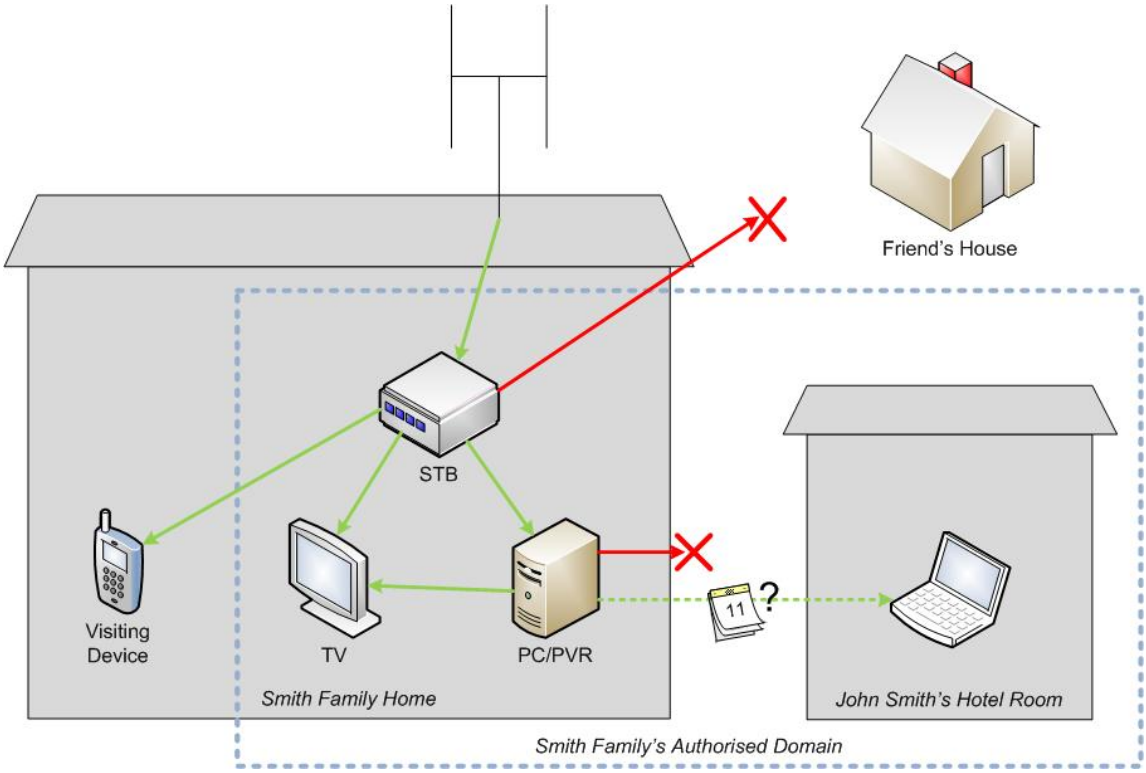

Figure 5: Free-to-Air with Delayed Remote Access Content Flow

4.3.2 Usage State Information

This scenario corresponds to the 10 setting of the control_remote_access_over_internet field of the DVB-SI FTA content management descriptor.

The following USI settings will enforce this usage of content.

Table 3: Free-to-Air with Delayed Remote Access USI

Type of Control	**Propagation Control**				**Copy Control**	**Remote Access**
	Movement		**View**			
USI Field	MCPI	MLocal	VPI	VLocal	CCI	Remote Access Date
Value	**MLAD**	**Asserted**	**VLAD**	**Asserted**	**CCNA**	**Now + 24 hours**

4.3.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

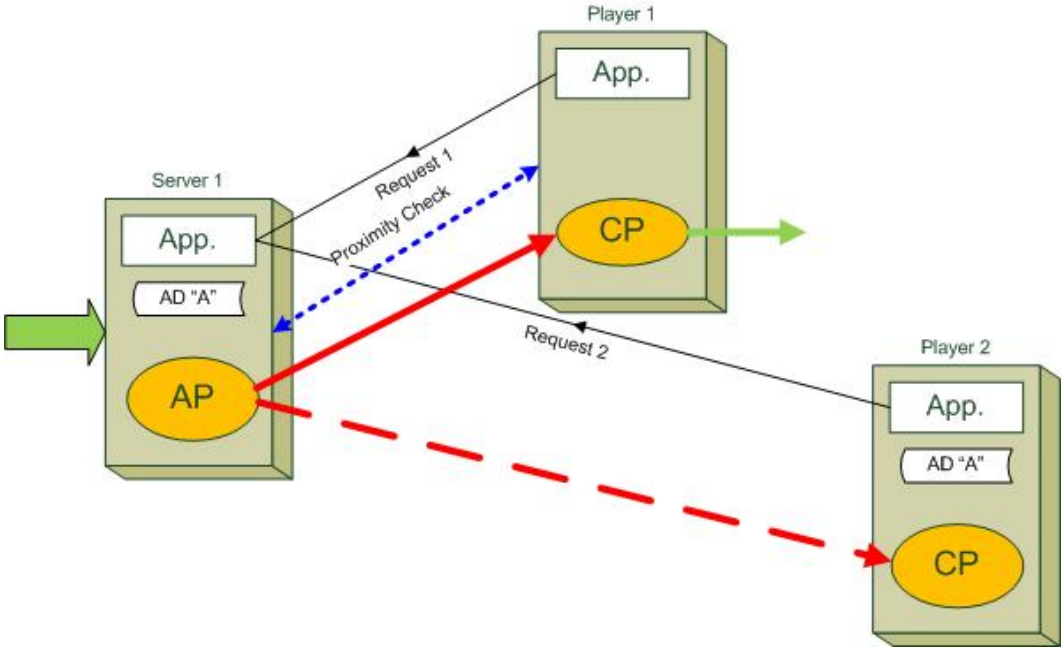

Figure 6: Free-to-Air with Delayed Remote Access Operation

The normal operation of this scenario is as for scenario 2, except as follows:

1) The server device checks the proximity of the destination device. If this is local, the content is allowed to flow.

2) If the destination is not local, the remote access rule is checked and the allowed time is compared with a secure time source available to the implementation. If the time is not yet expired, the content flow is rejected.

3) If the destination is not local, and the remote access time limit has passed, the AD membership of the two devices is compared:

   a) If they match, the content is permitted to flow.

   b) If they do not match, the content flow is rejected.

4.4 Scenario 4 - Free-to-Air without Remote Access

4.4.1 Business Intent

This scenario covers content that is broadcast without permission for remote access:

- Local access to such content is always permitted.
- Remote access from devices that do not belong to household members is prevented.
- Remote access to such content by household members is also prevented, unless otherwise permitted by the relevant C&R Regime.

EXAMPLE: A broadcast of content which is licensed into specific geographic markets and should not be permitted to leak into other territories.

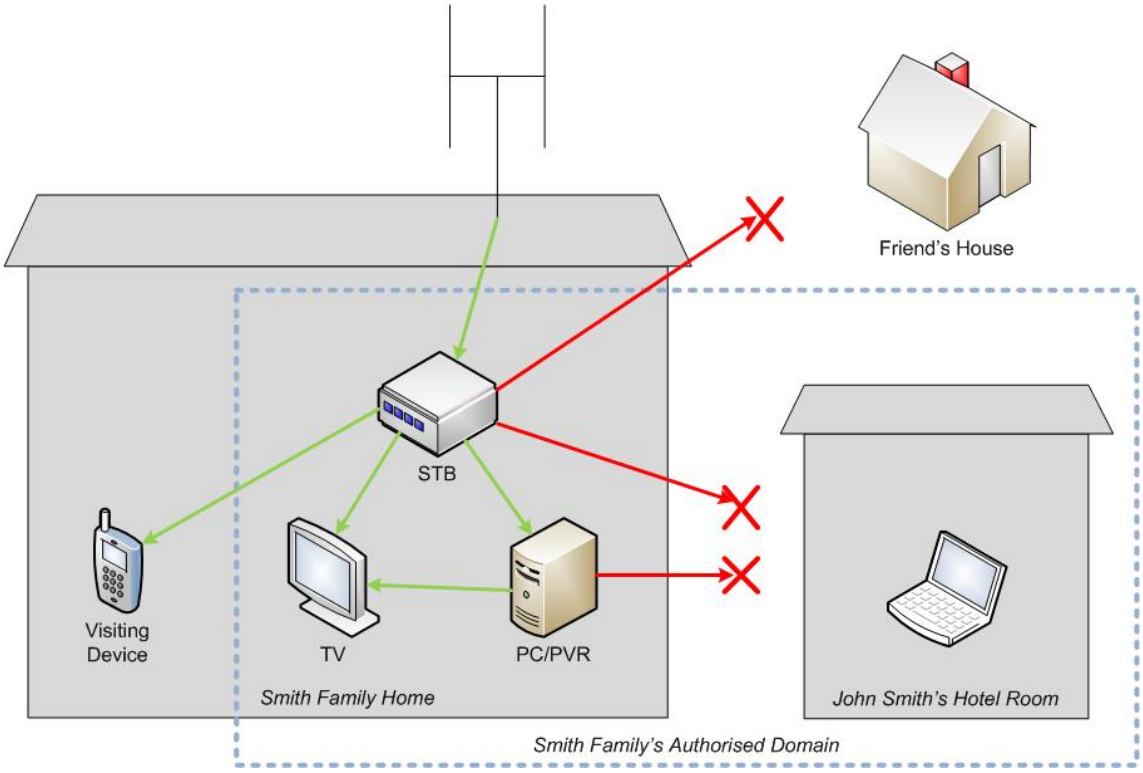

Figure 7: Free-to-Air without Remote Access Content Flow

4.4.2 Usage State Information

This scenario corresponds to the 11 setting of the control_remote_access_over_internet field of the DVB-SI FTA content management descriptor.

The following USI settings will enforce this usage of content.

Table 4: Free-to-Air without Remote Access USI

Type of Control	**Propagation Control**				**Copy Control**	**Remote Access Rule**
	Movement		**View**			
USI Field	MCPI	MLocal	VPI	VLocal	CCI	Remote Access Date
Value	**MLAD**	**Asserted**	**VLAD**	**Asserted**	**CCNA**	**FFFF235959**
NOTE: FFFF235959 is the maximum possible value as defined in TS 102 825-10 [i.6]. This value may be modified by a specific C&R Regime.						

4.4.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

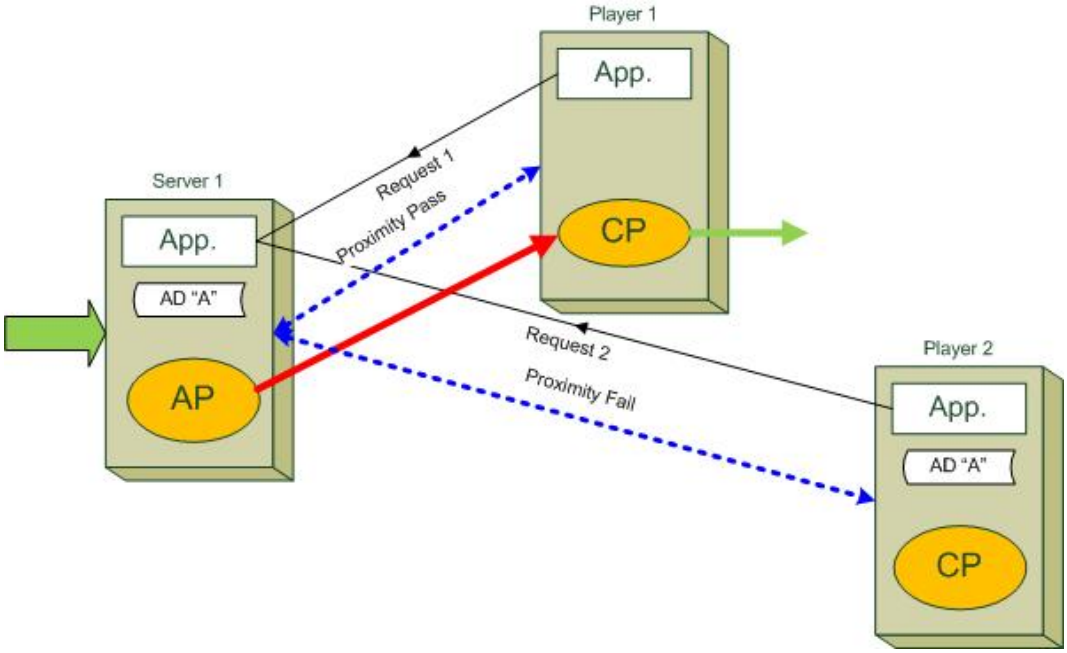

Figure 8: Free-to-Air without Remote Access Operation

The normal operation of this scenario is as follows:

1) The server device checks the proximity of the destination device. If this is local, the content is allowed to flow.

2) If the destination is not local, the remote access rule is checked and the allowed time is compared with a secure time source available to the implementation) If the time is not yet expired, the content flow is not allowed.

3) In the unlikely event that enough time has elapsed for the remote access restriction to be lifted the AD membership of the two devices is compared.

   a) If they match, the content is permitted to flow.

   b) If they do not match, the content flow is rejected.

4.5 Scenario 5 - PayTV (Local)

4.5.1 Business Intent

This scenario covers content that is broadcast under conditional access (CA) control, where the subscription service is limited to local devices that belong to the same household. Consumers are also allowed to make a single copy of this content on their PVR or storage media, but not to make additional copies.

NOTE 1: Services of this kind are required to identify a date and time for the local restriction to be lifted in accordance with the remote access rule. After this point in time, non-local devices that belong to the same household will be permitted to access the content. A CPCM Compliance and Robustness Regime may impose constraints on the use of the remote access rule.

EXAMPLE: Premium subscription channels on Pay-TV satellite or cable systems with no remote access permitted.

NOTE 2: Individual services might choose to adapt this scenario by enabling local viewing for non-AD bound devices, such as a rented projector, without allowing local copying, or other usages.

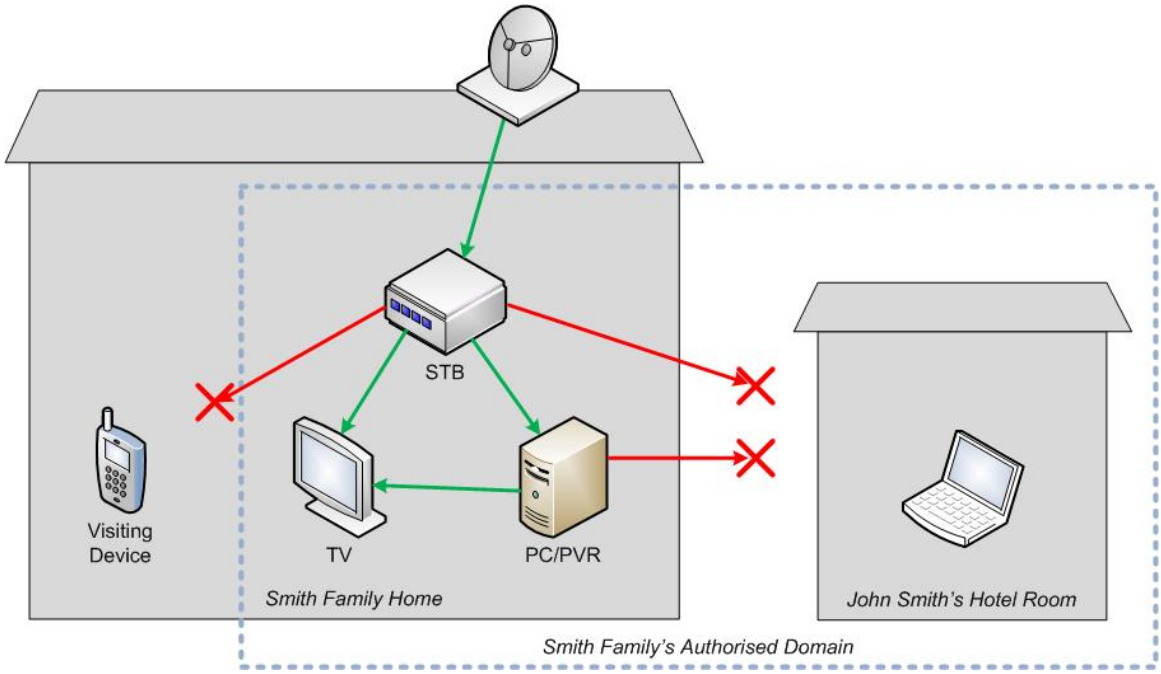

Figure 9: PayTV (Local) Content Flow

4.5.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 5: PayTV (Local) USI

Type of Control	**Propagation Control**					**Copy Control**
	Movement		**View**		**Remote Access**	
USI Field	MCPI	MLocal	VPI	VLocal	Remote Access Rule	CCI
Value	**MLAD**	**Not Asserted**	**VLAD**	**Not Asserted**	**Date/Time**	Copy Once

4.5.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

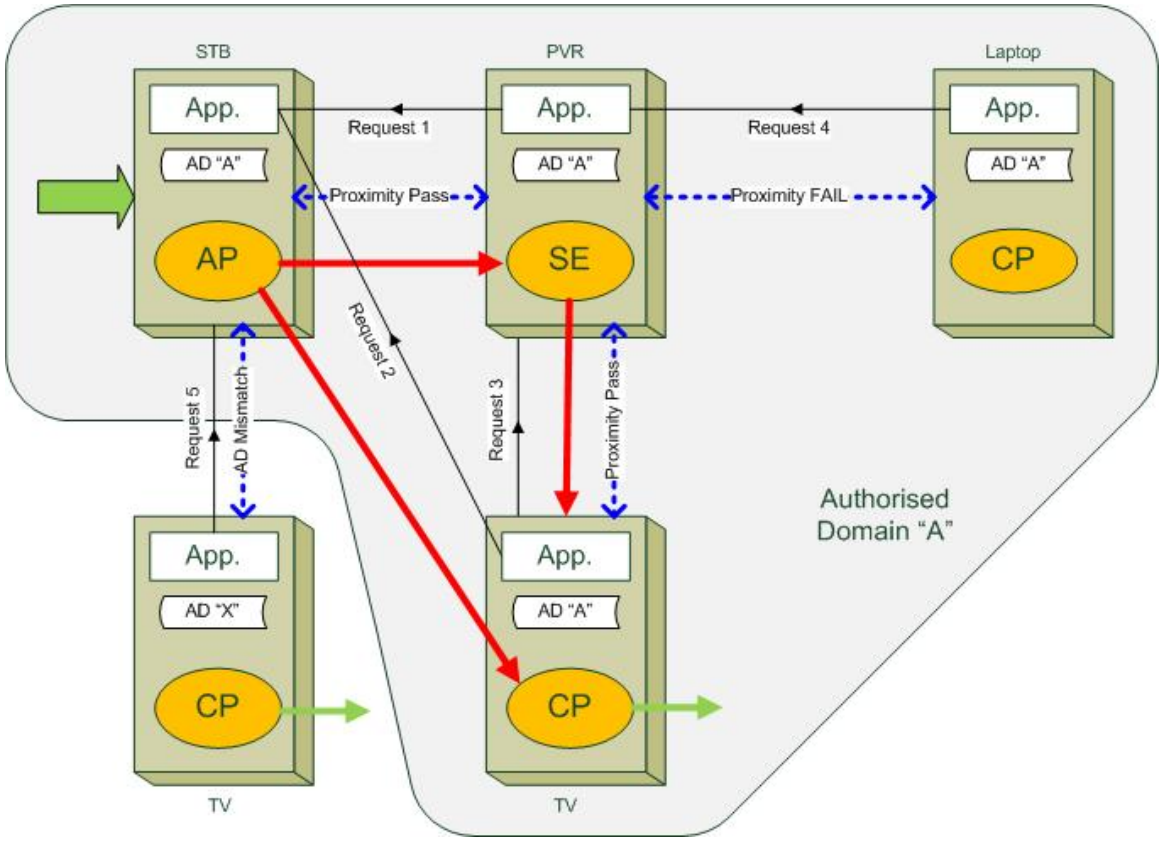

Figure 10: PayTV (Local) Operation

1) In Request 1, the requesting device, in this case a PVR, requests the content from the acquisition device, in this case the set to box (STB) receiver.

2) The STB checks the proximity of the PVR and determines it is local. It also checks the AD membership of the PVR and confirms a match. A content licence is generated and securely sent to the PVR, and the content begins to flow.

3) The stored content licence is modified by the PVR, changing the USI CCI field to Copy No More.

4) On receiving Request 2, assuming a different content item, the same process is applied. In this case, the proximity test may be run directly by the STB as above, or it may be unnecessary provided that the STB has some other means to verify proximity. Also, proximity can be determined by the proximity of the two to a common local device. This process is called proximity through association (PTA).

5) Further copies of the content cannot be made, though the single existing copy can legitimately be securely moved to another device at a later time. It will remain marked as Copy No More.

6) On receiving Request 3, the same process is followed between the TV and the PVR as described above.

7) On receiving Request 4, the proximity test will fail as the laptop is remote. If the remote access rule time has not expired, content flow will be blocked even though the device belongs to the correct domain. If the remote access rule time has expired, content will be permitted to flow.

8) On receiving Request 5, the request will be rejected as the AD identities do not match. In practice, such a request is unlikely to occur since the content directory would normally identify to which AD a content item is bound, so a content search will often not reveal to the user that such content is available. This behaviour is out of scope for DVB-CPCM, and may vary by implementation.

4.6 Scenario 6 - PayTV (Geographic)

4.6.1 Business Intent

This scenario covers content that is broadcast under conditional access (CA), where the subscription service is available to devices that belong to members of the same household, within a given geographical area. Consumers are also allowed to make a single copy of this content to a PVR hard drive or removable storage media but not to make additional copies.

NOTE: Services of this kind are required to identify a date and time for the local restriction to be lifted under the remote access rule. After this point in time, non-local devices that belong to the same Authorised Domain will be permitted to access the content. A CPCM Compliance and Robustness Regime may impose constraints on the use of the remote access rule.

EXAMPLE: Premium subscription channels on pay-tv satellite or cable systems that are available for use in the home, and are also usable by remote devices provided they can be proven to be within the same geographic area such as a broadcast service area. Such a service could allow streaming from a home PVR to a mobile phone or portable device whose location is identifiable by cell location, GPS, hotspot identity, or other trusted mechanism.

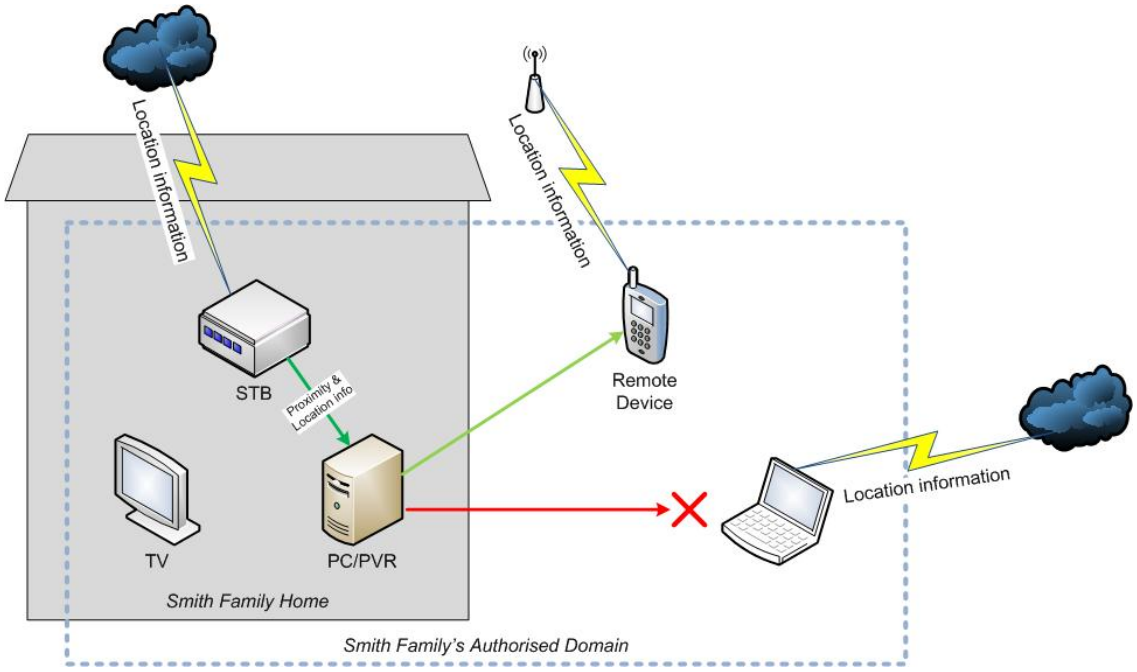

Figure 11: PayTV (Geographic) Content Flow

4.6.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 6: PayTV (Geographic) USI

Type of Control	**Propagation Control**					**Copy Control**
	Movement		**View**		**Remote Access**	
USI Field	MCPI	MLocal	VPI	VLocal	Remote Access Rule	CCI
Value	**MGAD**	**Not Asserted**	**VGAD**	**Not Asserted**	**Date/Time**	Copy Once
NOTE: The CPCM content licence auxiliary data will include information defining the geographic area to which the MGAD and VGAD settings apply.						

4.6.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

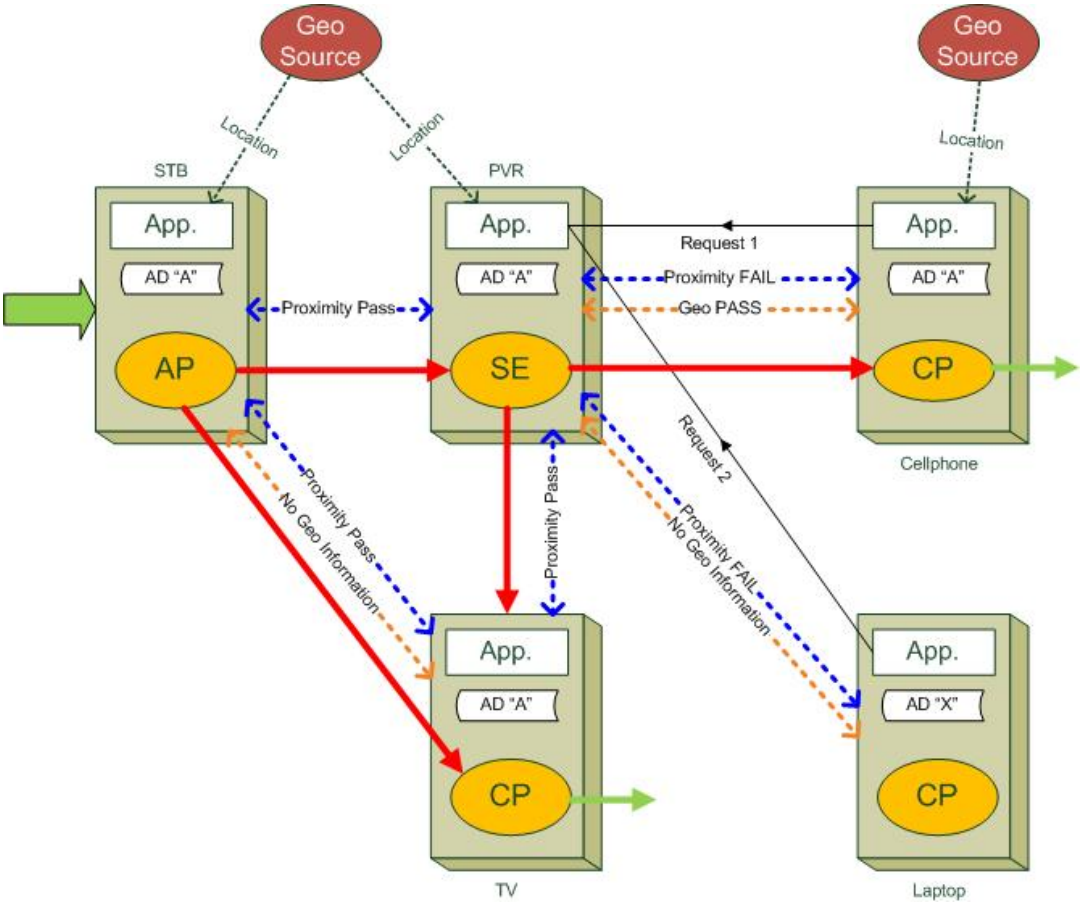

Figure 12: PayTV (Geographic) Operation

When content is marked for use in a specific geographic region, the following rules apply.

Firstly, any AD member device that is local to the content source, as verified by proximity tests, can always access the content, even when geographic information does not match the content licence. This ensures that content can always be physically moved remaining usable, and also provides good usability for devices with no geographic location awareness.

Therefore, the use of the geographic location tools are only required when content is being accessed remotely from the source.

Because this is also Copy Once content, the stored content licence will have been modified by the PVR, changing the USI CCI field to Copy No More as above.

1) When Request 1 is received, the server PVR, by default, checks first for proximity, then proceeds to check for a match of geographic location.

NOTE 1: Implementations may choose to use fast-answering proximity tests first, and then go to the geographic check before running longer-running proximity checks if necessary. This approach may give a quicker result to the user.

2) If the content source is not local, the destination device is required to use a secure source of location information, as defined by the relevant C&R Regime, and securely communicate its location to the server PVR.

NOTE 2: In some cases an Acquisition Point may need access to a secure location source so that it is able to correctly populate the geographic fields of the USI when creating a content licence. This mechanism will be defined by the relevant C&R Regime.

3) When Request 2 is received, the proximity test fails and there is no secure location information available. In this case, the content flow is denied.

4.7 Scenario 7 - PayTV (with full Remote Access)

4.7.1 Business Intent

This scenario is similar to scenario 5 which covers content that is broadcast under conditional access (CA), where the subscription service is limited to devices that belong to household members. However, in this case the service provider also permits remote access to the service by household member devices no matter what their location.

EXAMPLE: Premium subscription channels on pay-tv satellite or cable systems which charge an additional fee for global remote access permission.

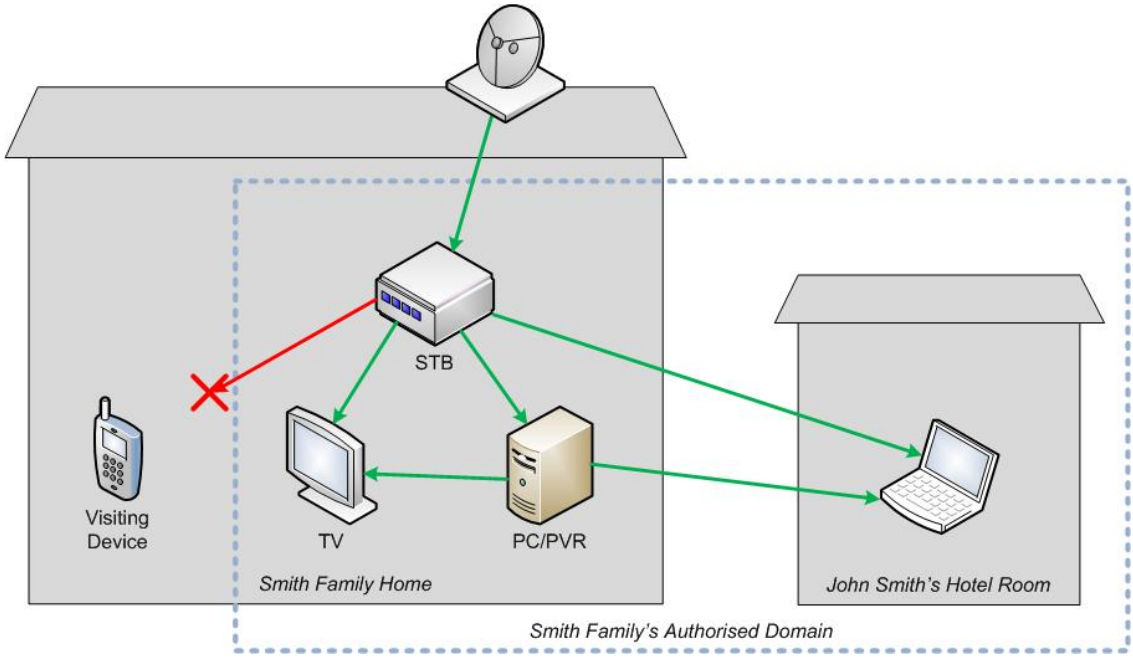

Figure 13: PayTV (with full Remote Access) Content Flow

4.7.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 7: PayTV (with full Remote Access) USI

Type of Control	Propagation Control				Copy Control
	Movement		View		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	**MAD**	**Not Asserted**	**VAD**	**Not Asserted**	Copy Once

4.7.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

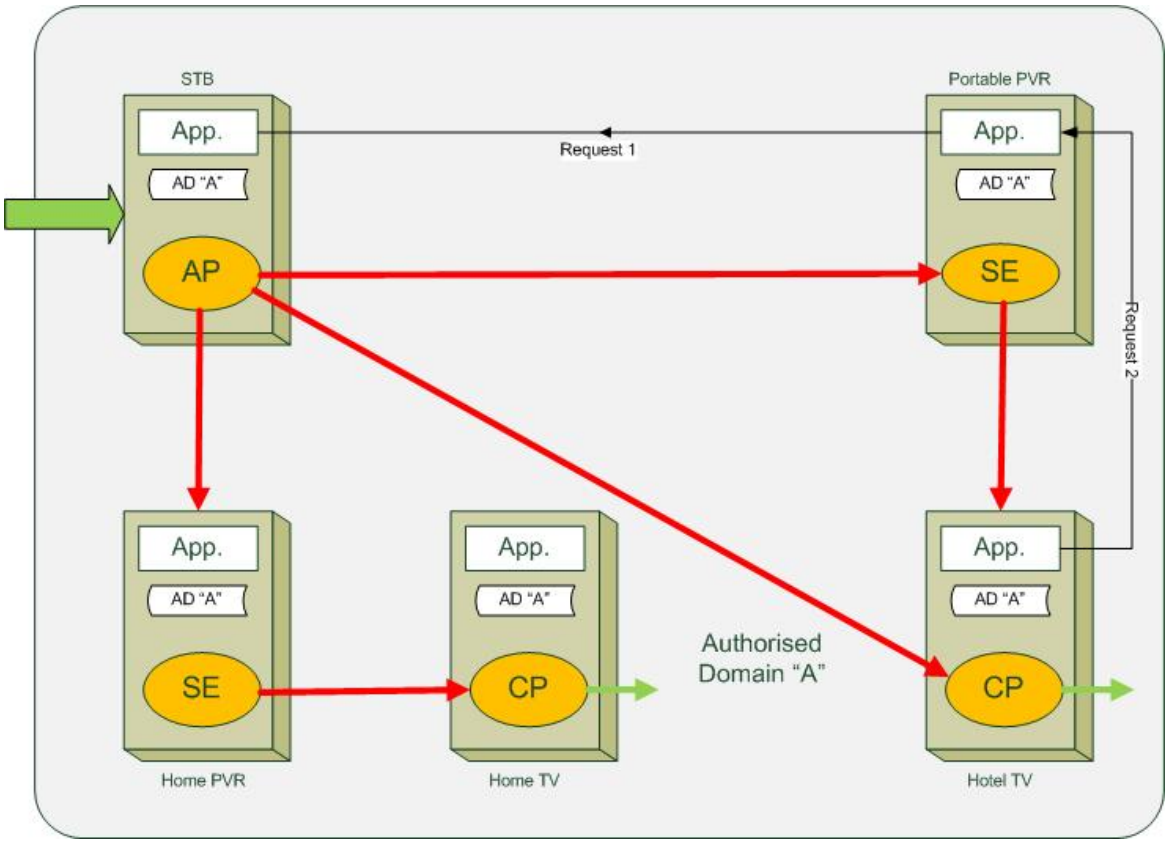

Figure 14: PayTV (with full Remote Access) Operation

The following process takes place:

1) When Request 1 is received, the server STB verifies the AD membership of the requester, as described earlier.

2) Once this is established, the content licence is created and sent securely to the remote PVR. This licence has the USI CCI field set to Copy Once as described earlier.

3) The content is sent to the remote PVR, which stores it for later retrieval.

4) The stored content licence is modified by the PVR, changing the USI CCI field to Copy No More.

5) When Request 2 is received, the content can be sent to the TV for consumption.

6) Because the USI does not indicate MLAD, MGAD, VLAD, VGAD, MLocal or VLocal, there is no need to run proximity tests during this scenario.

NOTE: This scenario shows a hotel TV that is temporarily joined to the consumer's own domain. Another alternative would be for the laptop to include a Consumption Point (thus terminating CPCM) that displays the content on the TV over an approved protected link such as HDCP.

4.8 Scenario 8 - Pay-Per-View

4.8.1 Business Intent

This scenario covers content which is offered for live viewing on a pay-per-view basis. Remote access is also permitted. Consumers are permitted to use PVR trick-mode functionality to pause, rewind and fast-forward the broadcast, but they are not permitted to make permanent copies.

EXAMPLE: Content such as live premium sporting events, special concerts, recent movie releases, and other high value content.

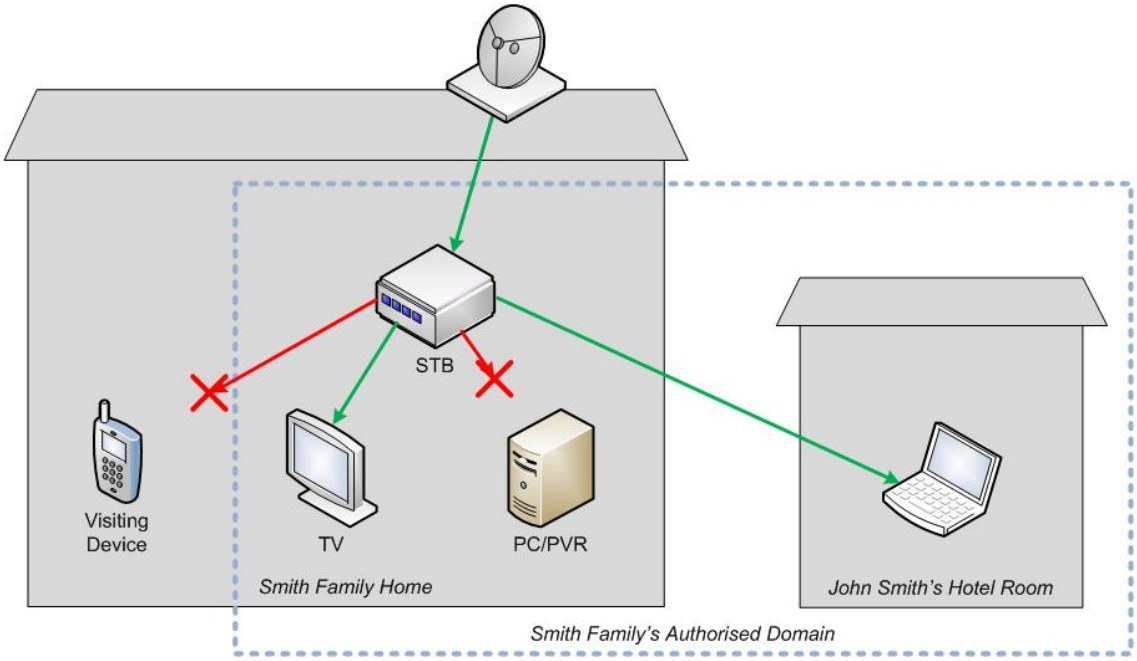

Figure 15: Pay-Per-View Content Flow

4.8.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 8: Pay-Per-View USI

Type of Control	**Propagation Control**				**Copy Control**	**Pause Control**
	Movement		**View**			
USI Field	MCPI	MLocal	VPI	VLocal	CCI	Zero Retention
Value	MAD	Not Asserted	**VAD**	**Not Asserted**	**Copy Never**	**Not Asserted**
NOTE: Although shown as MAD, the MCPI value is not significant in this scenario, as the CCI setting of Copy Never prevents any movement or copying.						

4.8.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

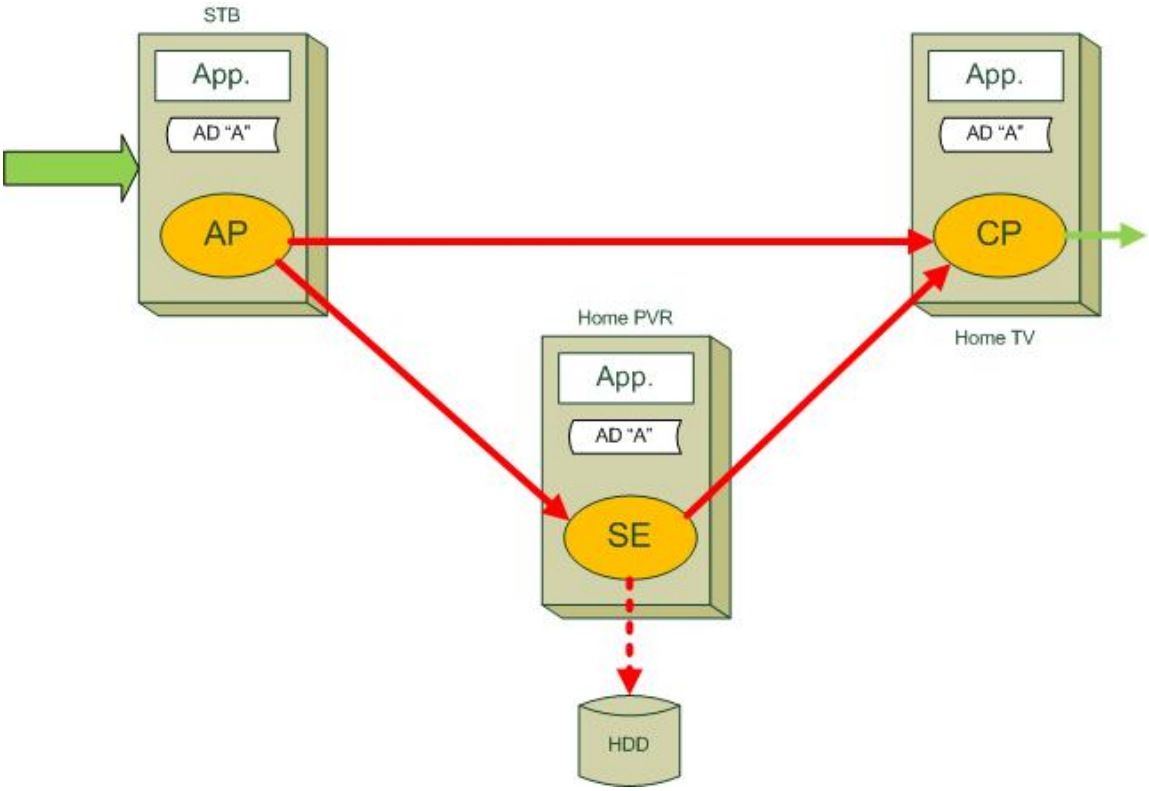

Figure 16: Pay-Per-View Operation

1) Content is permitted to flow directly from Acquisition Point (STB server) to Consumption Point (Home TV player).

2) Content is also permitted to flow via a Storage Entity or a Processing Entity however neither of these entities is permitted to make a copy or recording of the content as it flows through. They are however permitted to buffer the content sufficient to enable trick-mode operations as permitted by the C&R Regime. The use of hard-disk-drive storage is therefore permitted though under controlled conditions.

NOTE: Although the content is marked Zero Retention not asserted at the STB, it will be marked as Zero Retention asserted at the Storage Entity, in accordance with the rules in TS 102 825-3 [i.7].

4.9 Scenario 9 - Video-On-Demand (VoD)

4.9.1 Business Intent

This scenario covers content offered as a video-on-demand service, where trick-mode functions are provided within the network/service itself. The consumer is allowed to view the content, even remotely, but all pause and trick mode functions are requested from the service using the tools they provide.

NOTE: In this case, acquisition of content may be from a local storage under the control of a CA or other protection system.

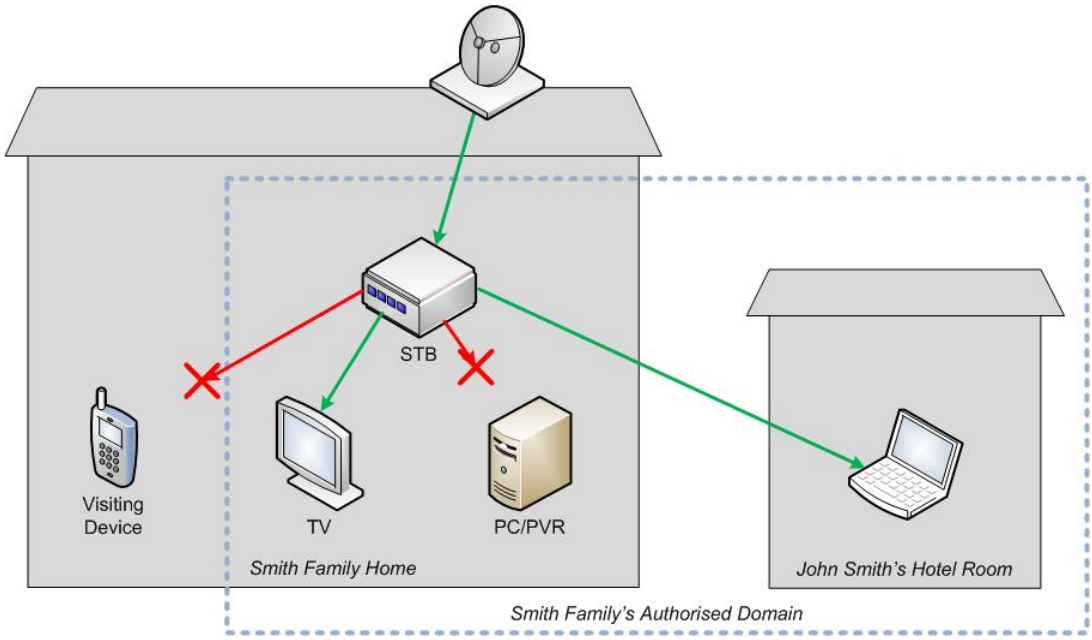

Figure 17: Video-On-Demand Content Flow

4.9.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 9: Video-On-Demand USI

Type of Control	Propagation Control				Copy Control	Pause Control
	Movement		View			
USI Field	MCPI	MLocal	VPI	VLocal	CCI	Zero Retention
Value	MAD	Not Asserted	**VAD**	**Not Asserted**	**Copy Never**	**Asserted**
NOTE: Although shown as MAD, the MCPI value is not significant in this scenario, as the CCI setting of Copy Never prevents any movement or copying.						

4.9.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

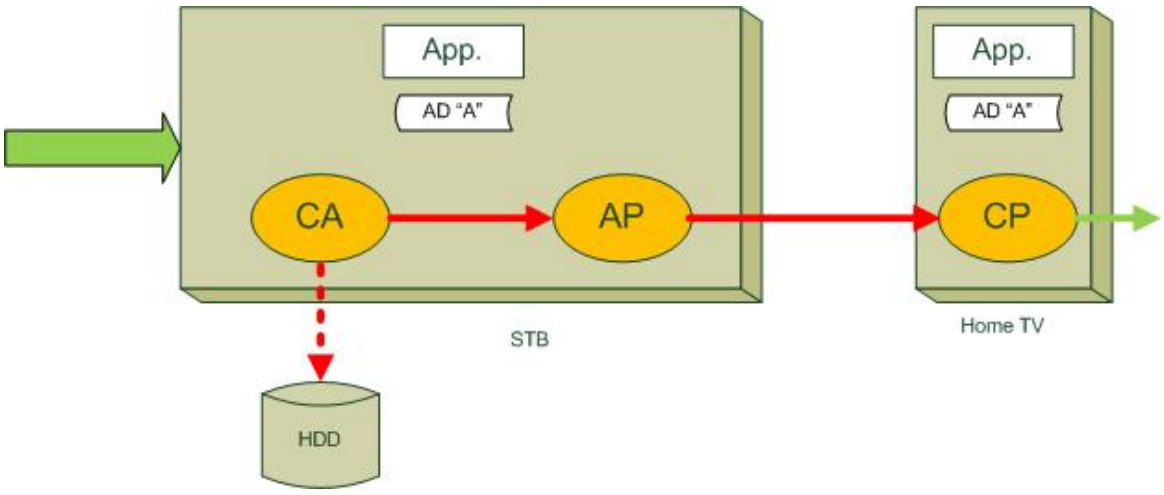

Figure 18: Video-On-Demand Operation

Video-on demand content may arrive directly from the service, such as a unicast from an online content library, or it may have already been pushed to local storage by the service provider. In the latter case, the CA or DRM system may use the same physical hard drive as is used for other purposes such as CPCM Storage Entity functions or user initiated recording of unrestricted content, though the content will remain under CA protection.

In either case, the CA system will obtain the content from its secure source and pass this to the CPCM Acquisition Point. Thereafter the content will be under CPCM control.

Because of the zero retention flag being asserted in the CPCM USI, the Acquisition Point is prohibited from passing the content to a dedicated CPCM Storage Entity. It may however pass the content to a CPCM Device that implements both a Storage Entity and a Consumption or Export Point. It then becomes the responsibility of the receiving entity to obey the zero retention rule.

This approach prohibits the use of trick-modes within CPCM Devices. It therefore requires all trick-mode requests to be passed back to the originating CA controlled source, whether local or remote for authorisation.

NOTE: This signalling is out of scope for CPCM, however it should be noted that such functions are defined in various home network protocols.

4.10 Scenario 10 - Push VoD

4.10.1 Business Intent

This scenario covers content which is pushed to devices at quiet times, and made available for purchase and immediate use at a later time. Once purchased, the video-on-demand service works as for scenario 9.

Whilst the user receives a copy of the content, they do not receive a persistent licence, so they are required to obtain a licence for each use of the content which requires decryption.

The traditional approach to this is for the CA system to retain full control of the content until payment is made and then allow acquisition into CPCM. This approach is covered in scenario 9.

However, allowing CPCM to control this process enables the content to move to storage devices without the CA functionality. Purchase of the content only requires obtaining an updated content licence from the AP, under CA management and there is no need to re-acquire or re-scramble the content.

NOTE: This scenario can be described as pushed not purchased, under joint CA and CPCM control, or tethered content.

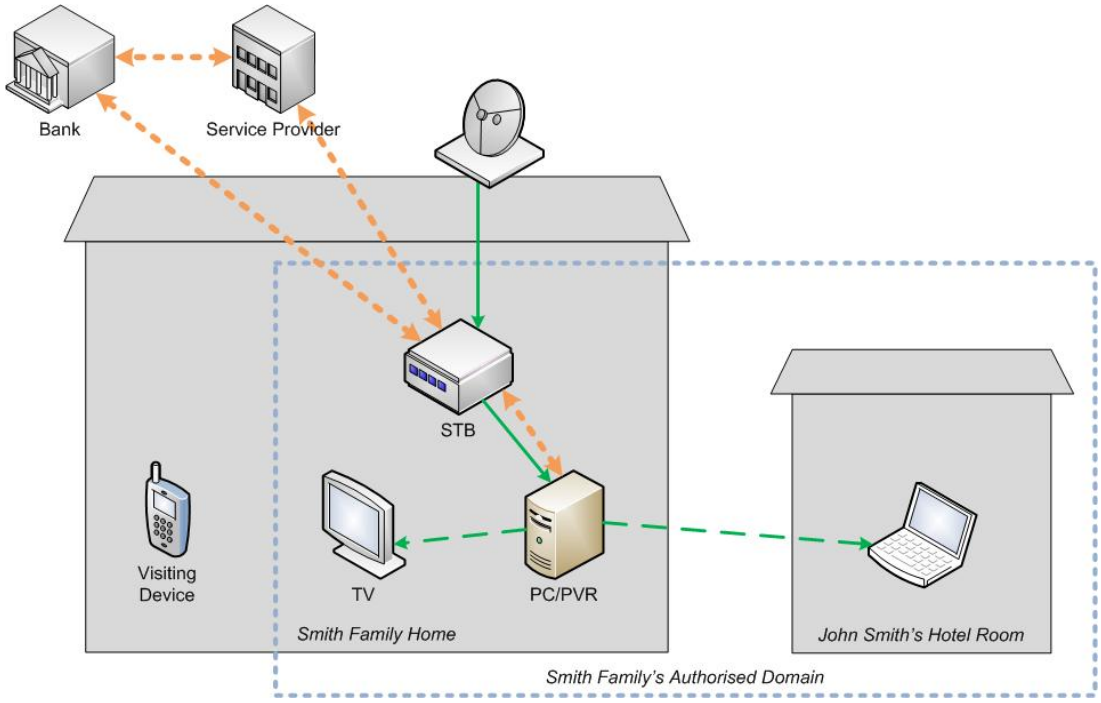

Figure 19: Push VoD Content Flow

4.10.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 10: Push VoD USI - Before Purchase

Type of Control	**Viewing**	**Propagation Control**				**Copy Control**
		Movement		**View**		
USI Field	Viewable	MCPI	MLocal	VPI	VLocal	CCI
Value	**Not Asserted**	**MAD**	**Not Asserted**	VAD	Not Asserted	**Copy Once**
NOTE 1: The USI field CCI will be set as Copy Once from the Acquisition Point, and will change to Copy No More once the content is on the Storage Entity, as is usual within CPCM. NOTE 2: In addition to the USI settings, it is also necessary for the content licence to carry sufficient information to allow the player application to make a Video-On-Demand purchase. This is accomplished by including information, such as a suitable URL, in the auxiliary data of the content licence.						

These settings would then be updated in a new licence when the purchase is completed, as follows.

Table 11: Push VoD USI - After Purchase

Type of Control	**Viewing**	**Propagation Control**				**Copy Control**
		Movement		**View**		
USI Field	Viewable	MCPI	MLocal	VPI	VLocal	CCI
Value	**Asserted**	MAD	Not Asserted	**VAD**	**Not Asserted**	**Copy Never**
NOTE 1: In addition to changing the USI field Viewable flag to Asserted, other USI fields may also be changed depending on the rights that have been purchased by the consumer. NOTE 2: The use of Copy Never in the CCI field prevents the Storage Entity from retaining a copy of the content licence. Thus any CPCM device trying to play the content is required to obtain a fresh licence from the Acquisition Point.						

4.10.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

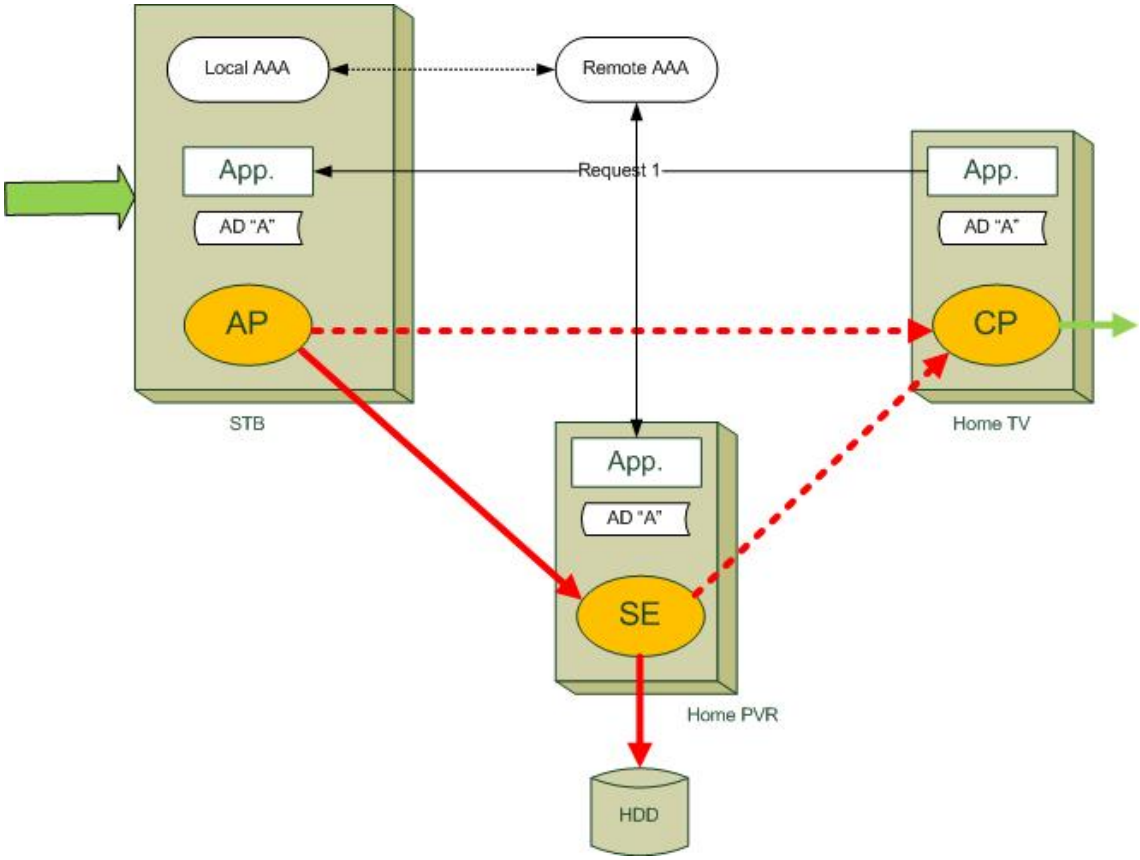

Figure 20: Push VoD Operation

Content is acquired into CPCM prior to purchase, and stored by the storage entity using the USI settings shown above to prevent viewing.

When the consumer requests to play, or purchase the right to play, the content, it is necessary for a CPCM instance to communicate with an authorised authenticated agent (AAA) to request the licence change to Viewable. The AAA may be embedded within the same device as the content source, within another device in the home, or be remote. The AAA may require a dialogue with the user prior to enabling the content, which may be to approve the transaction or take credit card information. This may be provided by; a local user interface (UI) on the player device or the TV; a remote UI from another device in the home; or a remote UI such as a web page on the internet. The AAA is then required to communicate securely with the content server to replace the non-Viewable licence with a Viewable one, along with whatever restrictions may apply.

NOTE: The communications protocols between AAA and the CPCM entities are out of scope for CPCM, and will be defined by some combination of manufacturer, service provider, and C&R Regime.

4.11 Scenario 11 - Multiple C&R Regimes

4.11.1 Business Intent

This scenario covers content, offered under one or more CPCM Compliance and Robustness Regimes, that is made available to devices that implement a mix of CPCM Compliance and Robustness Regimes.

EXAMPLE: An environment where there is a mix of premium pay-tv content and free-to-air content flowing through the same devices. The AD for the content remains the same however devices are prohibited from passing premium content to devices that do not meet the required C&R for handling premium content.

Some content may be marked as acceptable for multiple C&R regimes. Typically this will be content that has less-strict C&R requirements.

Any CPCM device is permitted to allow content to flow to another CPCM device if the receiving device's CPCM instance certificate indicates that it meets the C&R Requirements of any of the regimes indicated in the content licence.

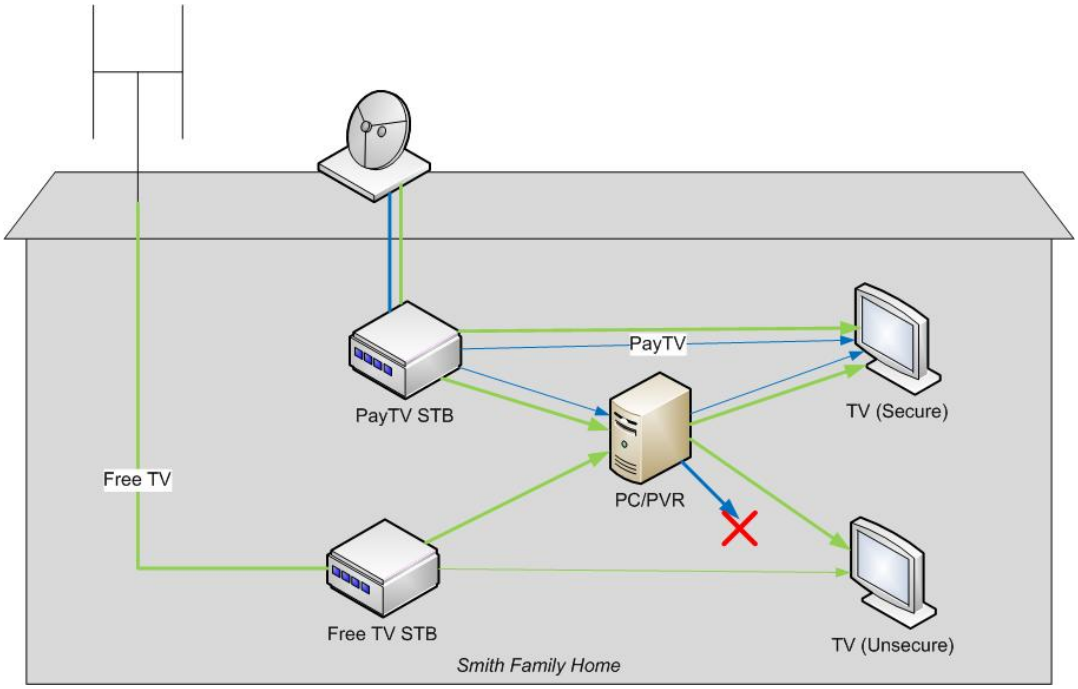

Figure 21: Multiple C&R Regimes Content Flow

4.11.2 Usage State Information

This scenario applies for any combination of USI settings. However, for simplicity of illustration the most open settings of USI are used as follows.

Table 12: Multiple C&R Regimes USI

Type of Control	Propagation Control				Copy Control
	Movement		View		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	(Any)	(Any)	(Any)	(Any)	(Any)
NOTE: The authorised C&R Regimes are not indicated in the USI, but elsewhere in the content licence.					

4.11.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

1) For each content item that is received or available, a CPCM content licence is created that identifies all of the C&R Regimes that are applicable for this specific content item.

2) Content items coming from free-to-air broadcasters may be marked with several C&R Regimes, as most regimes will probably meet the minimal requirements for such content.

3) Content items coming from pay-tv sources are expected to be limited to C&R Regimes that are specifically designed to meet their higher security requirements as demanded by the operators and CA vendors.

4) If the server is able to establish trust with the player, the content is permitted to flow according to the other USI signals. The Player will determine that it meets the requirements of at least one of the approved C&R Regimes identified in the Content Licence.

5) If trust is not established, the content flow is blocked, and an error is reported.

4.12 Scenario 12 - Bit-bucket storage (AD-based access)

4.12.1 Business Intent

This scenario describes the use of dumb bit bucket storage devices for CPCM content. The intent here is to support inexpensive storage devices, such as network attached storage; read/write optical disks; USB keys.

NOTE: The key point is that the storage device or media is totally unaware of CPCM, and is not required to implement any additional functionality.

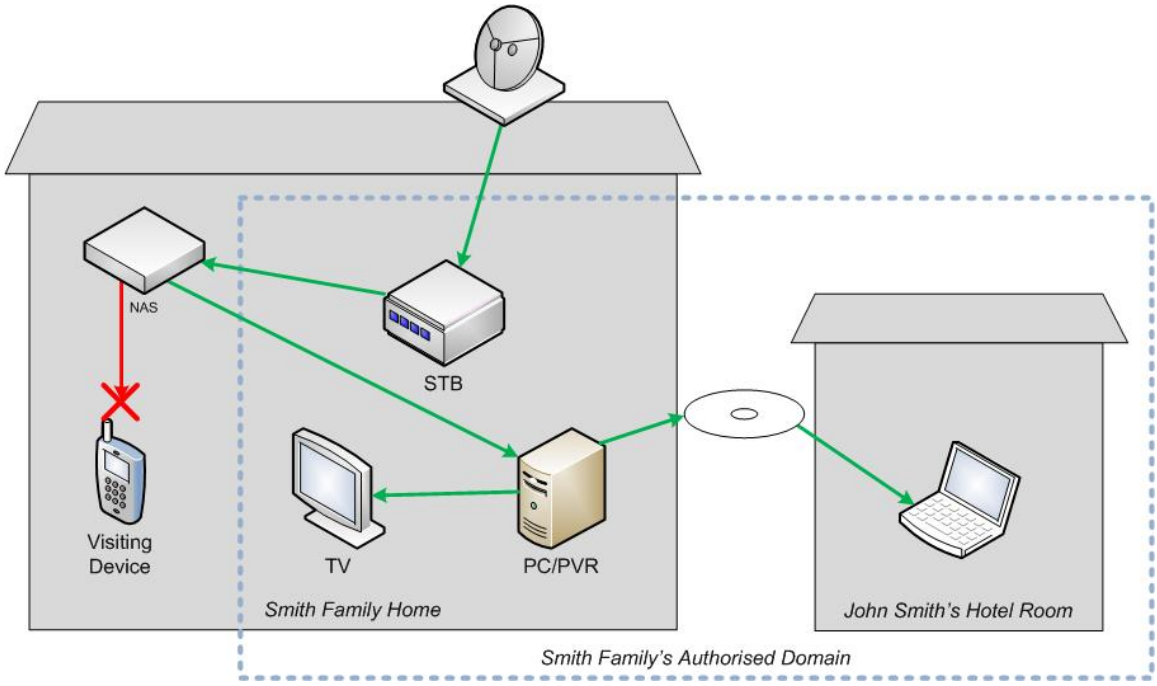

Figure 22: Bit-bucket storage (AD-based access) Content Flow

4.12.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 13: Bit-bucket storage (AD-based access) USI

Type of Control	Propagation Control				Copy Control
	Movement		View		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	**MAD**	**Not Asserted**	**VAD**	**Not Asserted**	**CCNA**
NOTE 1: Any setting of the CCI field other than CCNA will prevent the use of bit-bucket storage, as there is no means for the system to prevent bit-by-bit copying of the content NOTE 2: This scenario covers the case where content is free to move to any device in the AD. The following scenario covers the case where content usage requires remaining local to the Acquisition Point.					

4.12.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

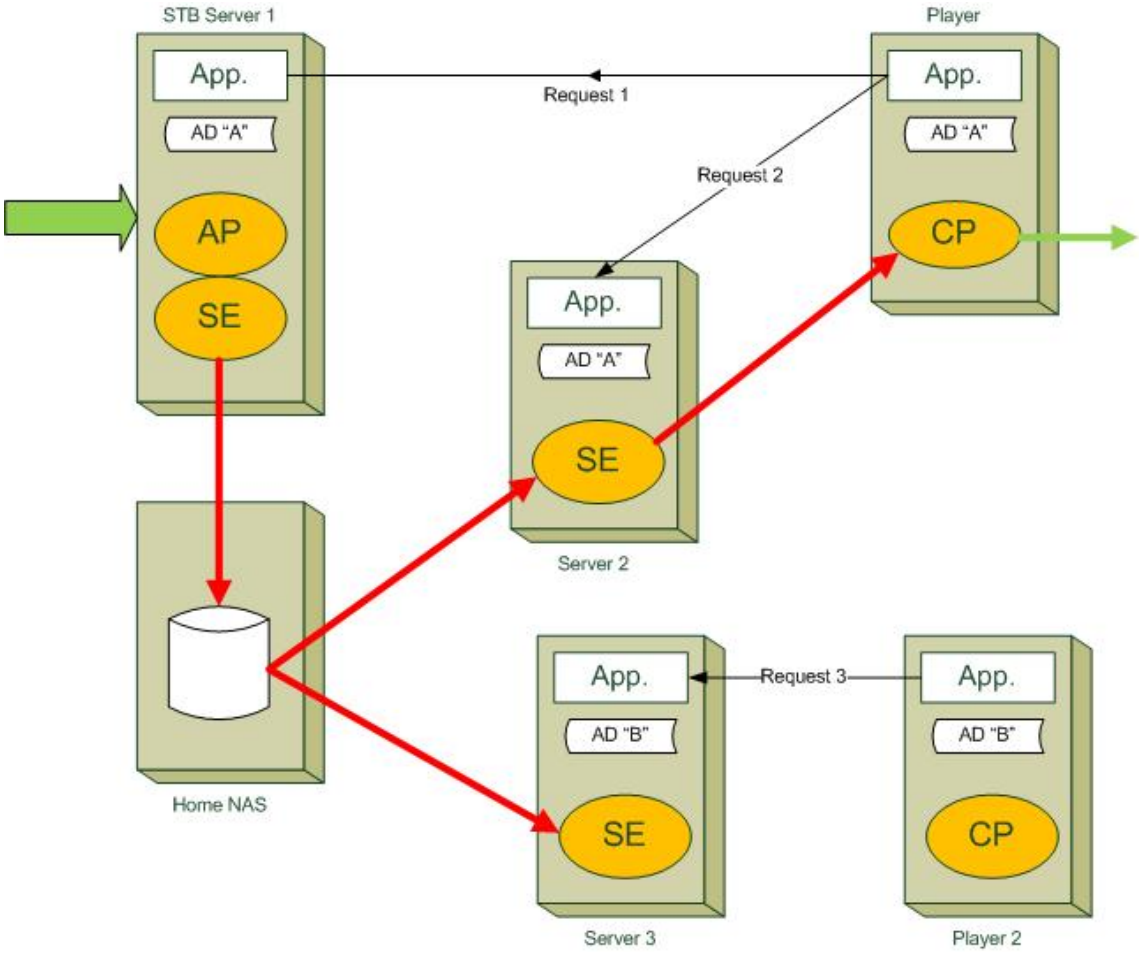

Figure 23: Bit-bucket storage (AD-based access) Operation

1) Request 1 asks Server 1 to move some CPCM content to a storage location that is not CPCM aware (i.e. a pure bit bucket).

   a) Server 1's application asks its CPCM Storage Entity (SE) function to prepare the content for storage on a non-CPCM aware device.

   b) The SE function protects the content licence using the AD secret and packs the content into a DVB-FF file.

   c) The SE function sends the content to the bit bucket.

   d) The bit bucket device stores the content unchanged.

2) Request 2 asks Server 2, which is a member of the same AD as Server 1, to play the content.

   a) The content is obtained from the bit bucket location unchanged.

   b) Server 2's application recovers the content licence from the DVB-FF file.

   c) As it is a member of the same AD, Server 2's CPCM instance decrypts and verifies the content licence.

   d) Server 2's CPCM instance accesses the content scrambling key and can thus decrypt the content.

3) Request 3 is made to a device that is a member of a different AD.

   a) The content is obtained from the bit bucket location unchanged.

   NOTE: It is not possible for the bit bucket to prevent this, as it is unaware of the authorised usage of the content item.

   b) Server 3's application recovers the content licence from the DVB-FF file.

   c) As it is member of a different AD and as the content licence does not authorise movement to a device in any other AD, whether it be local or remote, Server 3's CPCM instance identifies that it cannot access the content and reports an error to the Server 3 application, which then informs the user.

4.13 Scenario 13 - Bit-bucket storage (Local AD based access)

4.13.1 Business Intent

This scenario is similar to scenario 12 with the addition that authorisation is limited to movement of content to devices that are domain members and also local to the Acquisition Point.

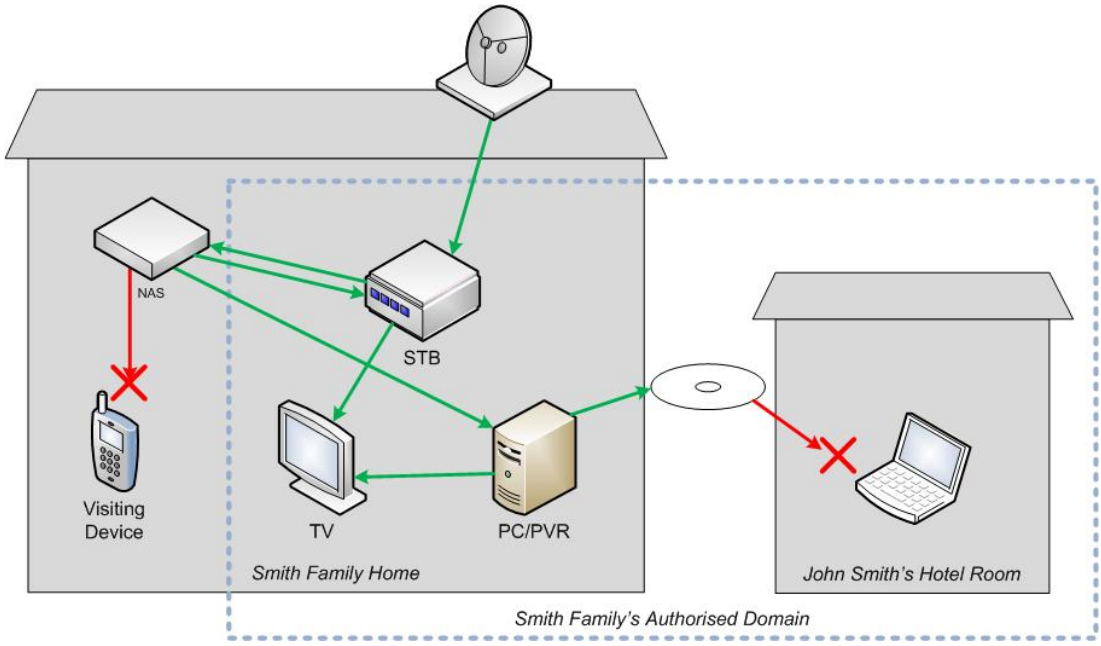

Figure 24: Bit-bucket storage (Local AD based access) Content Flow

4.13.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 14: Bit-bucket storage (Local AD based access) USI

Type of Control	Propagation Control				Copy Control	Remote Access
	Movement		View			
USI Field	MCPI	MLocal	VPI	VLocal	CCI	Remote Access Date
Value	**MLAD**	**Not Asserted**	**VLAD**	**Not Asserted**	**CCNA**	**July 1st 2015, 12:15 pm CET**
NOTE: Any setting of the CCI field other than CCNA will prevent the use of bit bucket storage, as there is no means for the system to prevent bit-by-bit copying of the content.						

4.13.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

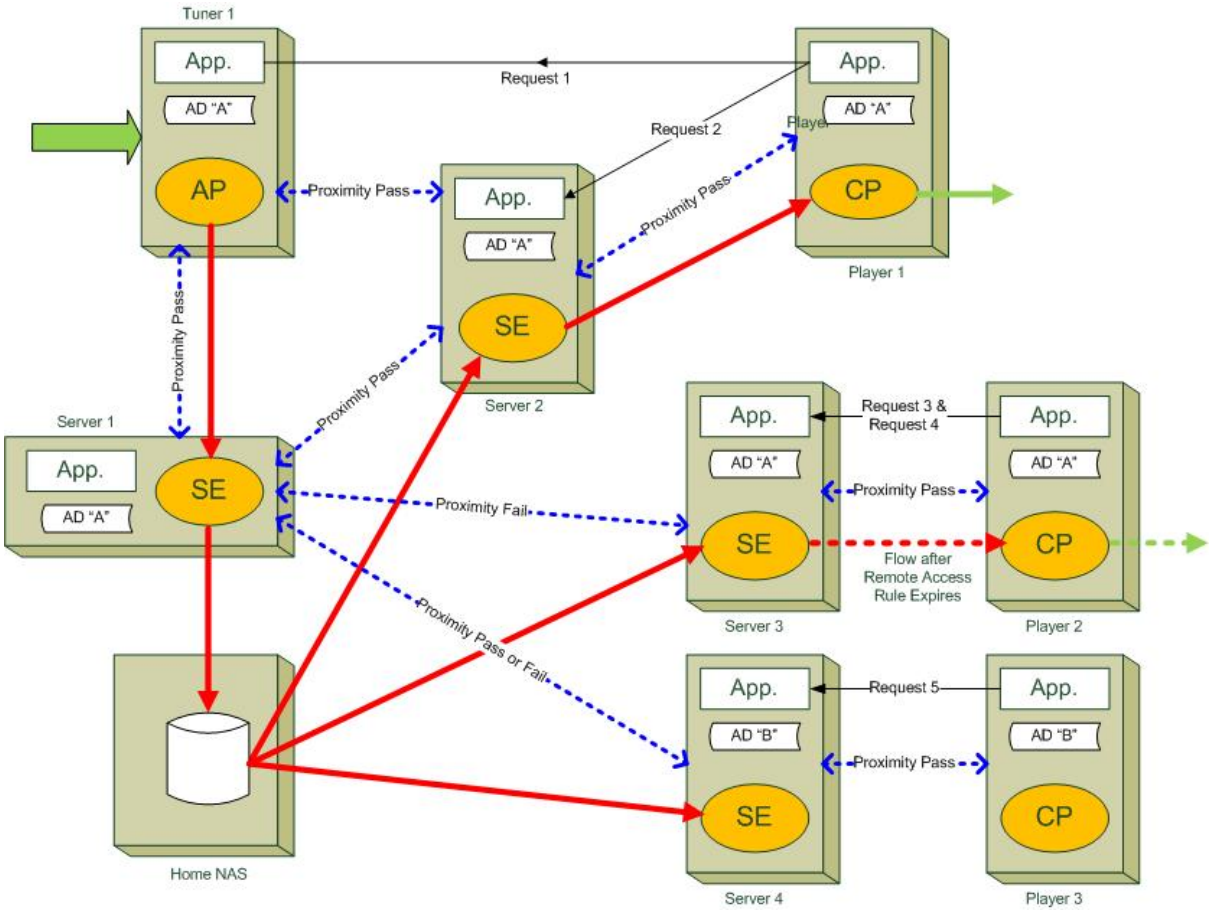

Figure 25: Bit-bucket storage (Local AD based access) Operation

1) Request 1 asks Tuner 1 to stream content to Server 1, which is to record the content to a local bit bucket device for storage.

   a) Because the content is locally constrained, Tuner 1's application uses proximity tests to verify that Server 1 is local to the source AP.

   b) Tuner 1 streams the content to Server 1 for recording.

   c) Server 1's application asks its CPCM Storage Entity (SE) function to prepare the content for storage on a non-CPCM aware device.

   d) The SE function protects the content licence using the AD secret and packs the content into a DVB-FF file.

   e) The SE function writes the content, including the embedded Content Licence, to the bit bucket.

2) Request 2 comes from a device that is a member of the same AD and in the proximity of Server 1.

   a) The bit bucket device sends the stored content unchanged.

   b) Server 2's application recovers the content L\licence from the DVB-FF-FF file.

   c) As it is a member of the same AD, Server 2's application decrypts and verifies the content licence.

   d) As the proximity restriction still applies, Server 2's application extracts Server 1's identity from the Last_CL_issuer field in the content licence.

e) Server 2's application performs a proximity test with Server 1. The test is successful.

f) Server 2's application can now handle the content.

NOTE: If Server 2 is not available, the player will be unable to access the content.

3) Request 3 comes on June 30th 2015, which in this case is before the remote access rule expires, from a device that is a member of the same AD but in a different location than Server 1.

a) The bit bucket device sends the stored content unchanged.

b) Server 3 application recovers the content licence from the DVB-FF file.

c) As it is member of the same AD, Server 3's application successfully decrypts and verifies content licence.

d) As the proximity restriction still applies, Server 3's application extracts Tuner 1's identity from Last_CL_issuer field in the content licence.

e) Server 3's application performs a proximity test with Tuner 1. The test fails.

f) Server 3's user interface displays an error message informing the user that the content is not accessible.

4) Request 4 comes on July 2nd 2015, which is after the remote access rule has expired, from a device that is member from the same AD but in a different location than Server 1.

a) The bit bucket device sends the stored content unchanged.

b) Server 3's application recovers the content licence from the DVB-FF file.

c) As it is member of the same AD, Server 3's application decrypts and verifies the content licence.

d) As the proximity restriction is expired, Server 3's application does not need to perform any proximity test and is able to handle the content.

5) Request 5 asks that the content be played by a device that is not a member of the same AD.

a) The bit bucket device sends the stored content unchanged.

b) Server 4's application recovers the content licence from the DVB-FF file.

c) Because Server 4 does not have the necessary AD secret, it is unable to extract the content keys from the content licence.

d) Server 4's application notifies the user that the content is not accessible.

4.14 Scenario 14 - Bit-bucket (with MLocal/VLocal asserted)

4.14.1 Business Intent

This scenario covers content which is bound to the local environment but not to the AD.

NOTE: Because there is no common secret that can be stored in the bit-bucket with the content, it is necessary for any device wishing to use the content to obtain a Content Licence from another source.

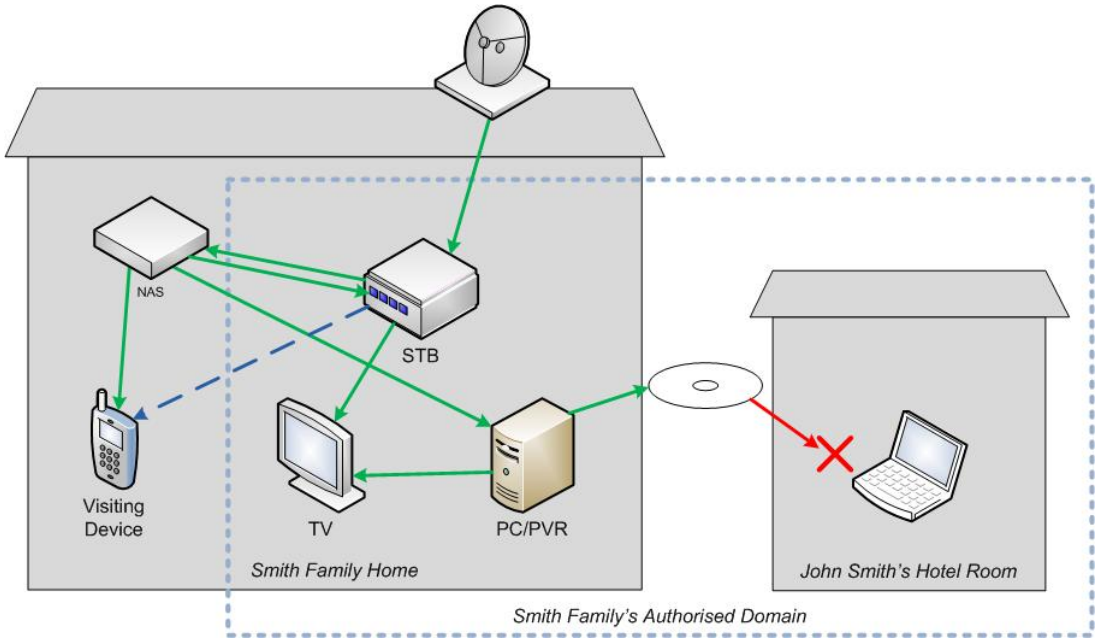

Figure 26: Bit-bucket (with MLocal/VLocal asserted) Content Flow

NOTE: The dashed arrow from STB to the visiting device indicates the delivery of a suitable content licence.

4.14.2 Usage State Information

The following USI settings support this scenario.

Table 15: Bit-bucket (with MLocal/VLocal asserted) USI

Type of Control	**Propagation Control**				**Copy Control**
	Movement		**View**		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	**MLAD**	**Asserted**	**VLAD**	**Asserted**	**CCNA**
NOTE: This scenario deals only with the MLocal and VLocal settings and the use of content by device that are not members of the same domain. See scenarios 12 and 13 for domain-based usage.					

4.14.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

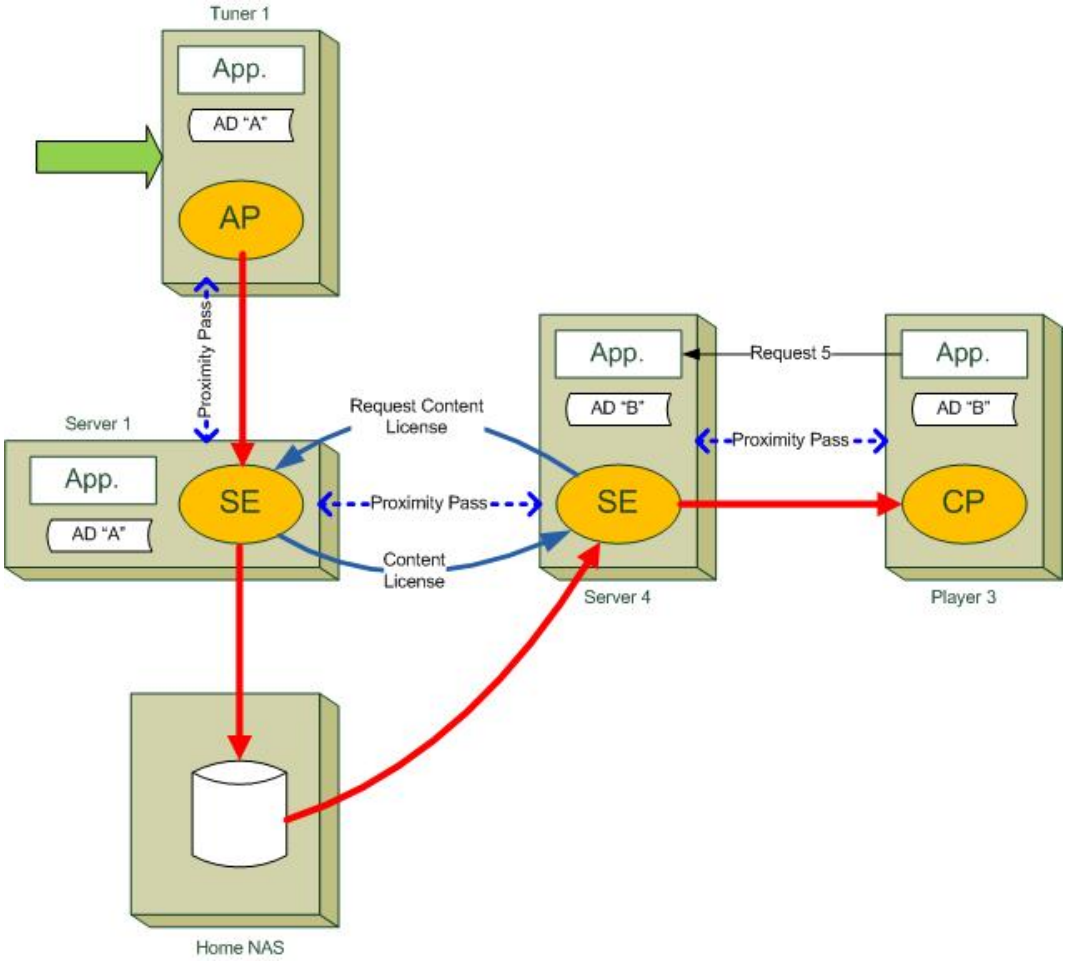

Figure 27: Bit-bucket (with MLocal/VLocal asserted) Operation

1) Content is recorded to the bit bucket as described in scenarios 12 and 13.

2) Request 5 asks that the content be played by a device that is not a member of the same AD.

   a) The bit bucket device sends the stored content unchanged.

   b) Server 4's application recovers the content licence from the DVB-FF file.

   c) Because Server 4 does not have the necessary AD secret, it is unable to extract the content keys from the content licence. However, Server 4 sees that MLocal and VLocal have been asserted.

   d) Server 4 identifies Server 1 from the Last_CL_issuer field in the content licence, which is available in the clear, that is unencrypted.

   e) Server 4 sends a request to Server 1 asking for a content licence for this content item.

   f) Server 1 employs proximity tests to verify that Server 4 is in the same local environment.

   g) Server 1 creates a suitable content licence including the descrambling key for the content, and sends it securely to Server 4 over the SAC.

   h) Server 4 receives the content licence, extracts the keys using the SAC session key, and binds the content licence to its own AD. It is now able to handle the content.

4.15 Scenario 15 - Bit-bucket (with DNCS asserted)

4.15.1 Business Intent

This scenario covers content offered for use under CPCM but with the Do Not CPCM Scramble (DNCS) bit set in the USI.

NOTE 1: The most likely source of such content is a free-to-air unencrypted broadcast which is signalled as Do Not Scramble.

NOTE 2: It is recognised that the technical protection of such content is inherently weak, as any device or software application is able to handle the unencrypted content without needing access to the licence or any descrambling keys. However, this scenario is described because usage of the content under territorial legislation and regulations may be applicable to content so marked.

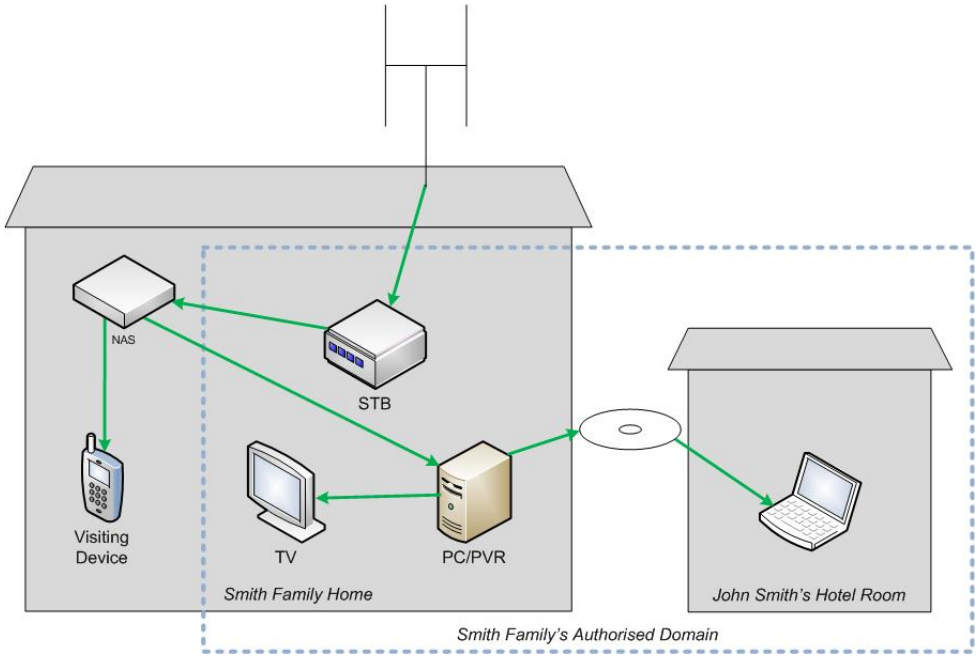

Figure 28: Bit-bucket (with DNCS asserted) Content Flow

4.15.2 Usage State Information

The following USI settings support this scenario.

Table 16: Bit-bucket (with DNCS asserted) USI

Type of Control	Propagation Control				Copy Control	Ancilliary Data
	Movement		View			
USI Field	MCPI	MLocal	VPI	VLocal	CCI	DNCS
Value	MCPCM	Asserted	VCPCM	Asserted	CCNA	**Asserted**

4.15.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as defined in all other scenarios. Devices, which are approved under the relevant CPCM C&R Regime or regulation, should treat the content in exactly the same way as described elsewhere.

NOTE 1: It will be technically possible for devices that implement the DVB-FF specification, but are not built according to applicable CPCM C&R rules, to access the content and ignore the restrictions that may be expressed in the USI.

NOTE 2: Content owners should be aware that this is an inherent result of the assertion of DNCS, and cannot be solved by technical means.

4.16 Scenario 16 - Limited Displays with Follow-Me

4.16.1 Business Intent

This scenario covers content where a limit is imposed on the number of simultaneous displays. This is typically used by Pay-TV networks for premium live events such as sports or live concerts. The consumer is permitted to use any displays they wish, up to the limit imposed. Additional displays beyond this limit can only be used after an existing display has stopped showing the content.

In this scenario, the recording of the live broadcast is not permitted, although trick play modes, such as pause, rewind, may be supported in the player devices.

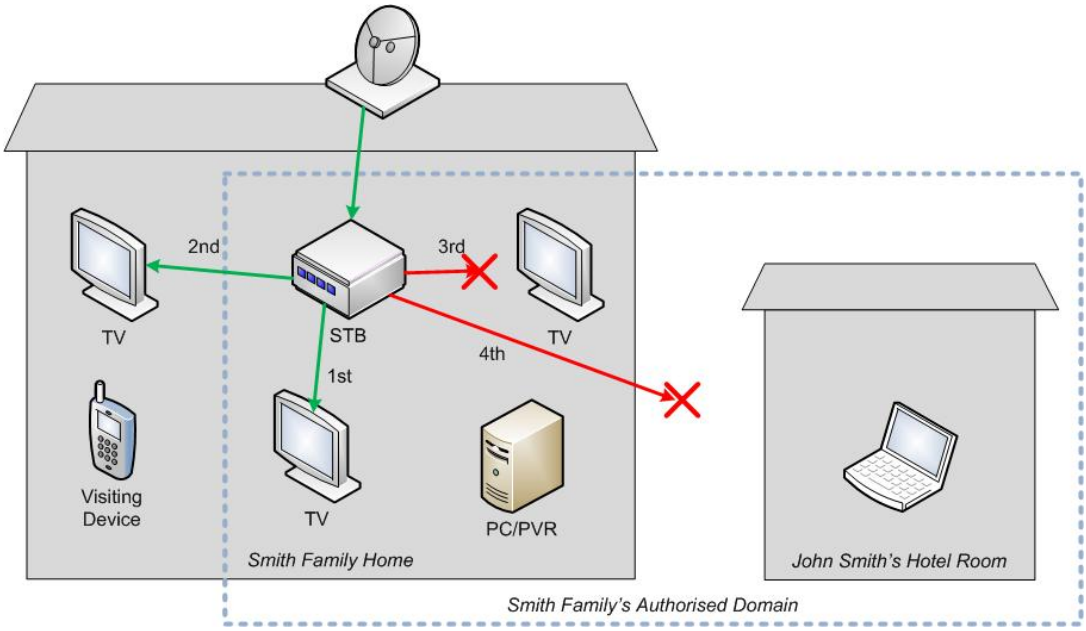

Figure 29: Limited Displays with Follow-Me Content Flow

4.16.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 17: Limited Displays with Follow-Me USI

Type of Control	Propagation Control					Copy Control	Pause Control
	Movement		View				
USI Field	MCPI	MLocal	VPI	VLocal	SVC	CCI	Zero Retention
Value	(Any)	(Any)	VAD	Asserted	2	**Copy Never**	Asserted

NOTE 1: The setting of CCI to Copy Never means that the MCPI and MLocal fields are not considered.
NOTE 2: This example uses Zero Retention to prevent trick-play or buffering of the content in player devices. However it is possible to permit such trick-play modes because the delayed play-out from a PVR will still count as an active display in the count.
NOTE 3: The setting of SVC covers all displays, whether AD members or not, local or remote. The service provider has the option to exclude non-AD and, or remote devices using the VPI and VLocal fields as described elsewhere in the present document.

4.16.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

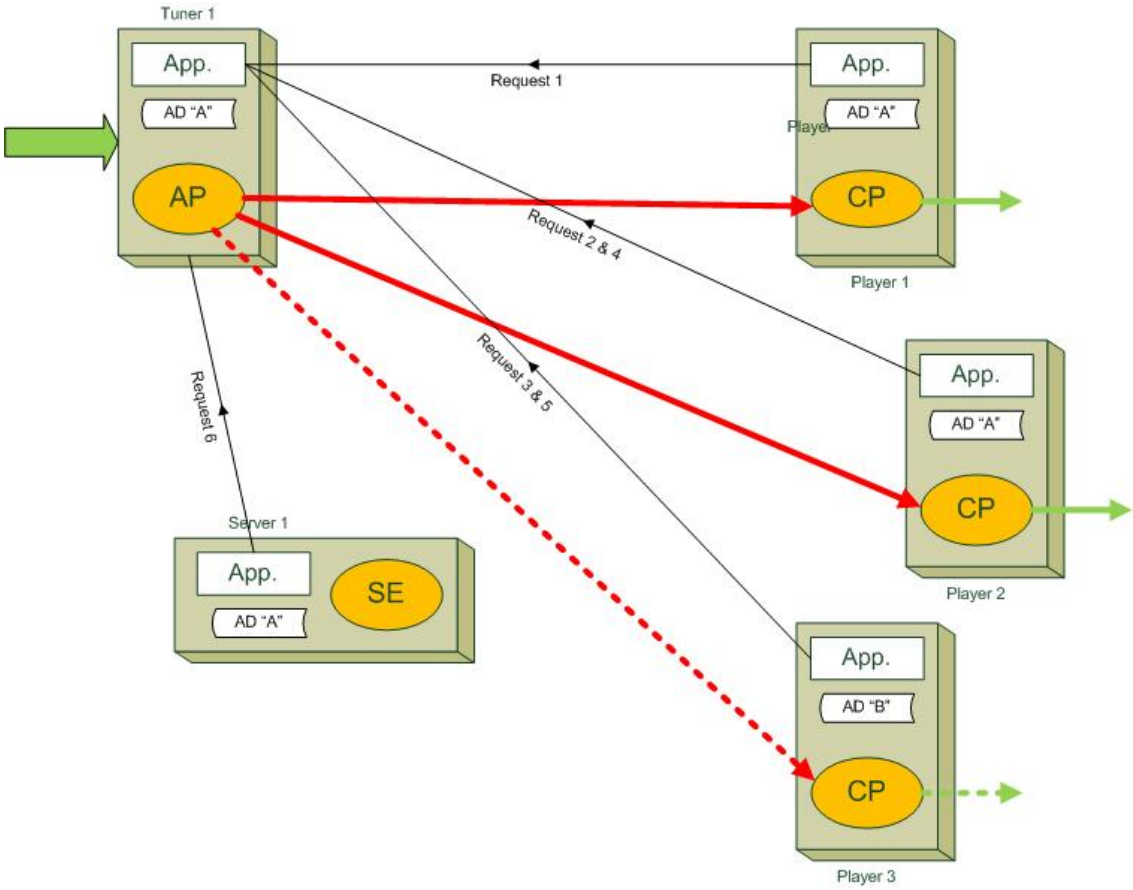

Figure 30: Limited Displays with Follow-Me Operation

For content that is delivered with a View Count limit set, the Server will issue a separate content licence for each player, with each content licence delivered over the SAC and encrypted for a specific device.

1) Player 1 requests the content stream; Request 1.

   NOTE: View Count is only meaningful for live streamed content.

2) Tuner 1 encrypts the content, and places the content key in a content licence specifically protected for use by Player 1 only.

3) Tuner 1 starts to stream the content to Player 1. It may do this using Unicast, or it may create a multicast to which Player 1 can join.

4) Player 2 also requests the content stream using Request 2. As mentioned above, Player 2 may already be receiving the encrypted content if it is being multicast on a home network. However, Player 2 will not have a content licence for decrypting this content, so it will need to request it from Tuner 1.

5) When Tuner 1 receives a request for a new display, and more displays are permitted, the count of active displays is incremented.

6) If no more displays are permitted, Tuner 1 will verify whether all currently allocated displays are still actively using the content. If they are, the new request is rejected.

7) If one or more of the allocated displays is no longer active, Tuner 1 will change the content descrambling key, and issue a new content licence to each active display, including the newly active display.

   NOTE: It is possible for implementations to periodically change the content descrambling keys, rather than wait for a change in active displays.

8) Should a device such as Server 1 request the content for recording, this will be rejected as the USI do not permit the making of a copy, nor buffering for trick play as Zero Retention is asserted.

4.17 Scenario 17 - Content Rental (limited period)

4.17.1 Business Intent

This scenario covers content offered as a rental service, where the content may be accessed for a limited period of time. In this scenario, the user is permitted to use the content as many times as they like for a fixed period from when it was acquired.

NOTE: Variants of this scenario will allow viewing for a limited time from first watching.

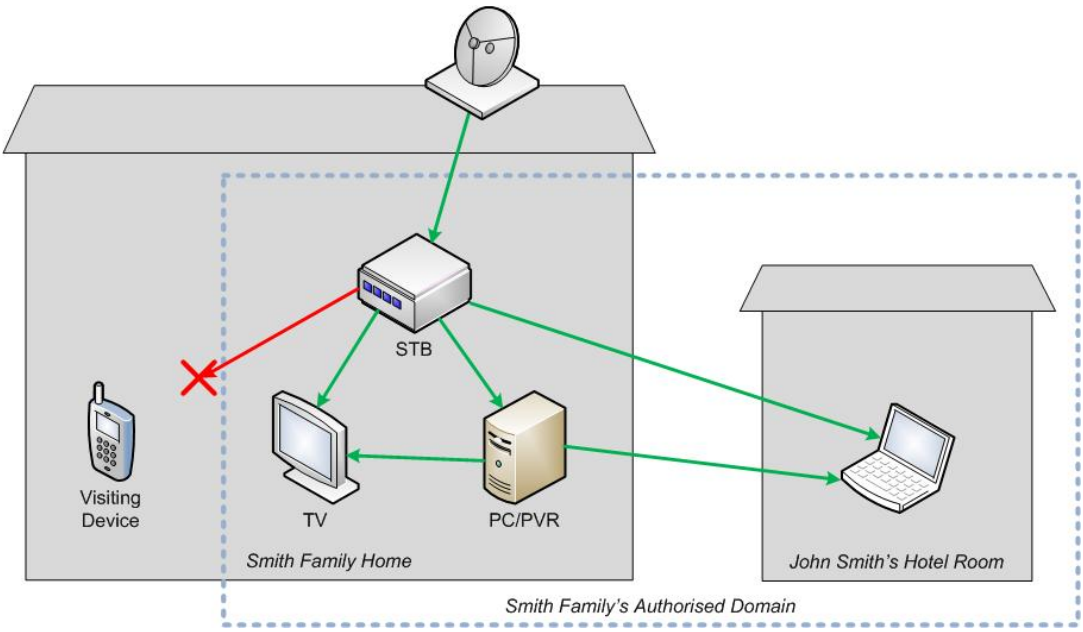

Figure 31: Content Rental (limited period) Content Flow

4.17.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 18: Content Rental (limited period) USI

Type of Control	Propagation Control					Copy Control
	Movement		View			
USI Field	MCPI	MLocal	VPI	VLocal	View Window End	CCI
Value	MAD	Not Asserted	VAD	Not Asserted	**Date/Time**	CCNA
NOTE 1: The CCI setting of CCNA allows the user to make copies, such as to transfer a rented movie on their portable device to watch during a journey. This is not a security threat, as all copies will expire at the same time. NOTE 2: In this scenario there is no need to set a View Window Start in the USI. Other scenarios will use this capability.						

4.17.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

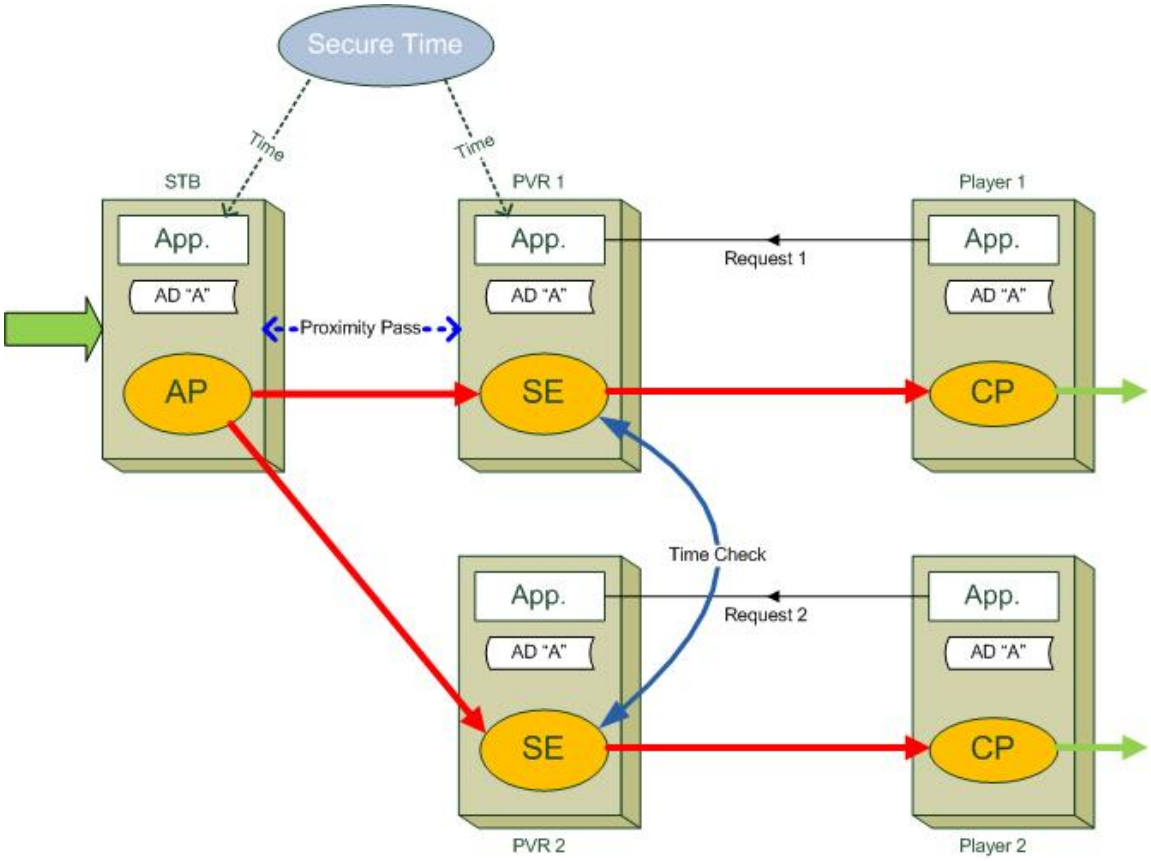

Figure 32: Content Rental (limited period) Operation

1) When a Server is asked to send, or a Player is asked to play, the CPCM instance needs to verify that the content licence is still valid.

2) The CPCM instance needs to obtain a source of secure time against which it can compare the View Window End field of the content licence.

3) If the View Window End is already passed, the content cannot be played by a conformant CPCM instance.

4) In the above scenario, Request 1 can be evaluated directly, as PVR 1 has access to a source of secure time. If the content licence has not expired, the content can be played.

5) Request 2 cannot be directly evaluated. PVR 2 needs to obtain the current time from another device which knows a source of secure time.

NOTE 1: The technical mechanism(s) used to obtain and signal secure time is an implementation choice, subject to Compliance and Robustness rules.

NOTE 2: It is an implementation choice how this content expiry could be explained to the user. Some implementations may choose to give a simple error message, others may offer to delete the expired content, or could do so on a regular basis, while others may allow the user to purchase additional rental time, assuming the service allows this and has provided the necessary AAA function to enable the transaction.

4.18 Scenario 18 - Movement of Copy-No-More Content

4.18.1 Business Intent

This scenario covers content where the consumer is permitted to make a single copy, and then wishes to move this copy between devices, perhaps changing format on the way.

At no point is the user permitted to have more than a single copy, however the user is able to move it securely between AD devices as necessary.

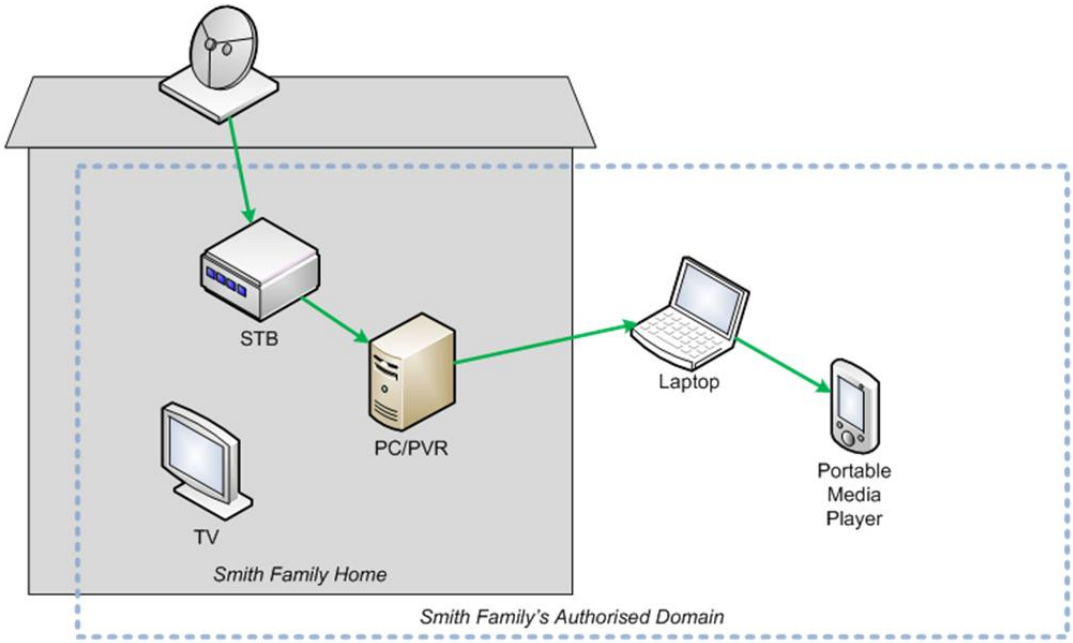

Figure 33: Movement of Copy-No-More Content - Content Flow

4.18.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 19: Movement of Copy-No-More Content USI

Type of Control	**Propagation Control**				**Copy Control**
	Movement		**View**		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	MAD	Not Asserted	VAD	Not Asserted	**Copy No More**

4.18.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

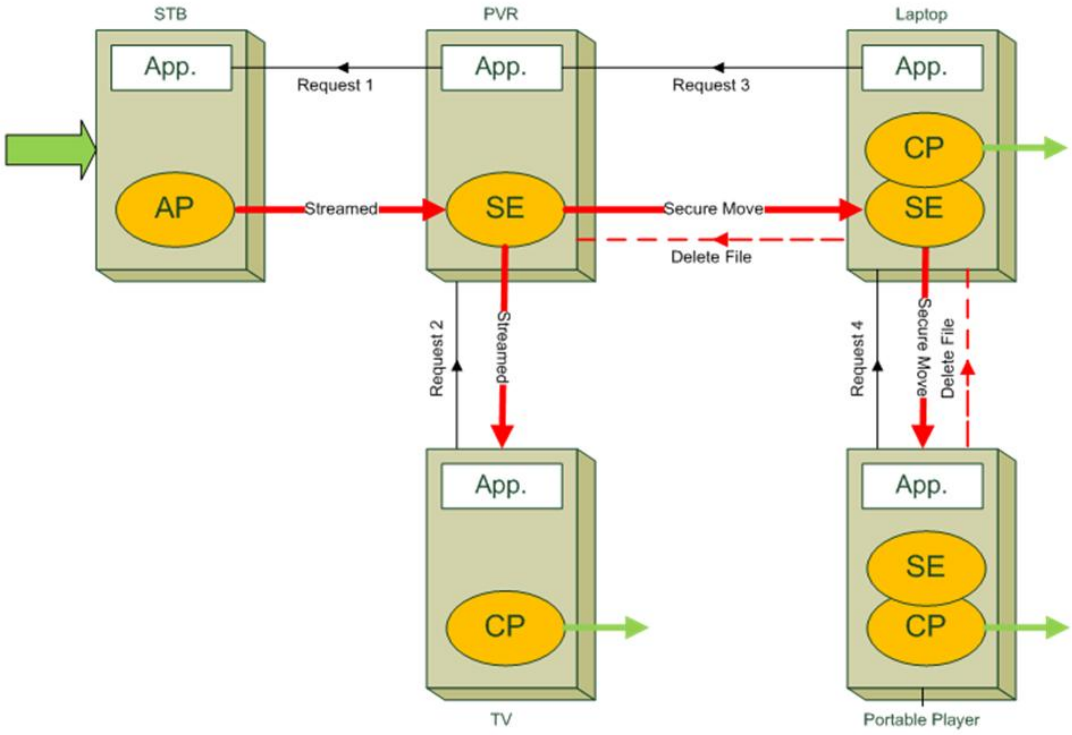

Figure 34: Movement of Copy-No-More Content Operation

When content is initially acquired by CPCM, it will have USI indicating either Copy Once, if it has not yet been recorded, or Copy No More when it has been recorded.

For purposes of this sequence of events, the STB and PVR devices are treated as separate entities. In practice they may often be combined in a single device.

1) Request 1 asks for content which is supplied as a stream marked as Copy Once. from the Acquisition Point.

2) The PVR device records the stream to a file, and updates the associated USI to indicate Copy No More.

3) Request 2 asks to view the file as a stream. Because this is a request to view and not to copy, the content is supplied with USI indicating Copy No More. The TV is able to display this content for the consumer.

4) Request 3 asks for a copy of the file to be moved to the laptop. Because the USI indicates Copy No More, a copy is prohibited. Therefore, a secure move of the file is required. This ensures that the original file and/or the key to access it is deleted from the PVR before the file is made available on the laptop. Hence only a single instance of the file remains playable at any time.

5) Request 4 asks for a copy of the file to be moved to the portable player. The same logic applies as in step 4. However, in this case the content needs also to be repurposed to the portable format. See scenario 23 for a scenario specific to this operation.

4.19 Scenario 19 - Local Blackout

4.19.1 Business Intent

This scenario covers content delivered with a constraint that it cannot be viewed within a certain area.

EXAMPLE: American football coverage is often not broadcast in the same city as the game is being played unless the stadium is filled, as a means to encourage attendance by fans.

In this typical case, the content cannot be acquired within the blackout area, so CPCM is concerned with preventing the content being acquired from outside the blackout zone.

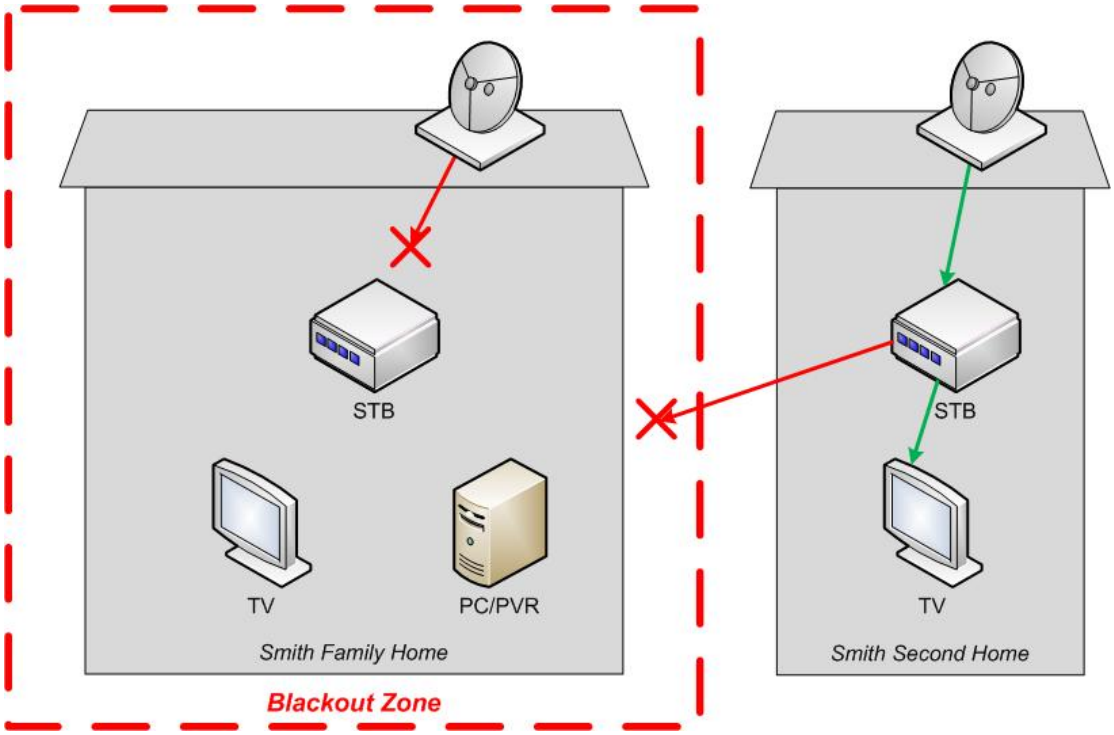

Figure 35: Local Blackout Content Flow

4.19.2 Usage State Information

The service provider wants to prevent content from being remotely accessed from inside the blacked-out area.

Table 20: Local Blackout USI

Type of Control	**Propagation Control**				**Copy Control**	**Geographic Area**
	Movement		**View**			
USI Field	MCPI	MLocal	VPI	VLocal	CCI	Auxilliary Data
Value	**MGAD**	Asserted	**VGAD**	Asserted	CCNA	**Blacked-out area**

NOTE: This setting of USI ensures that content cannot moved or streamed to within the blacked out area. If the sending device is unable to verify that the receiving device is located in a permitted location, it reverts to enforcement of use in the local environment.

The remote access rule (see TS 102 825-3 [i.7]) can be used to allow content recorded outside the blackout area to be viewed within the blackout area at a later time, such as after the match.

4.19.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

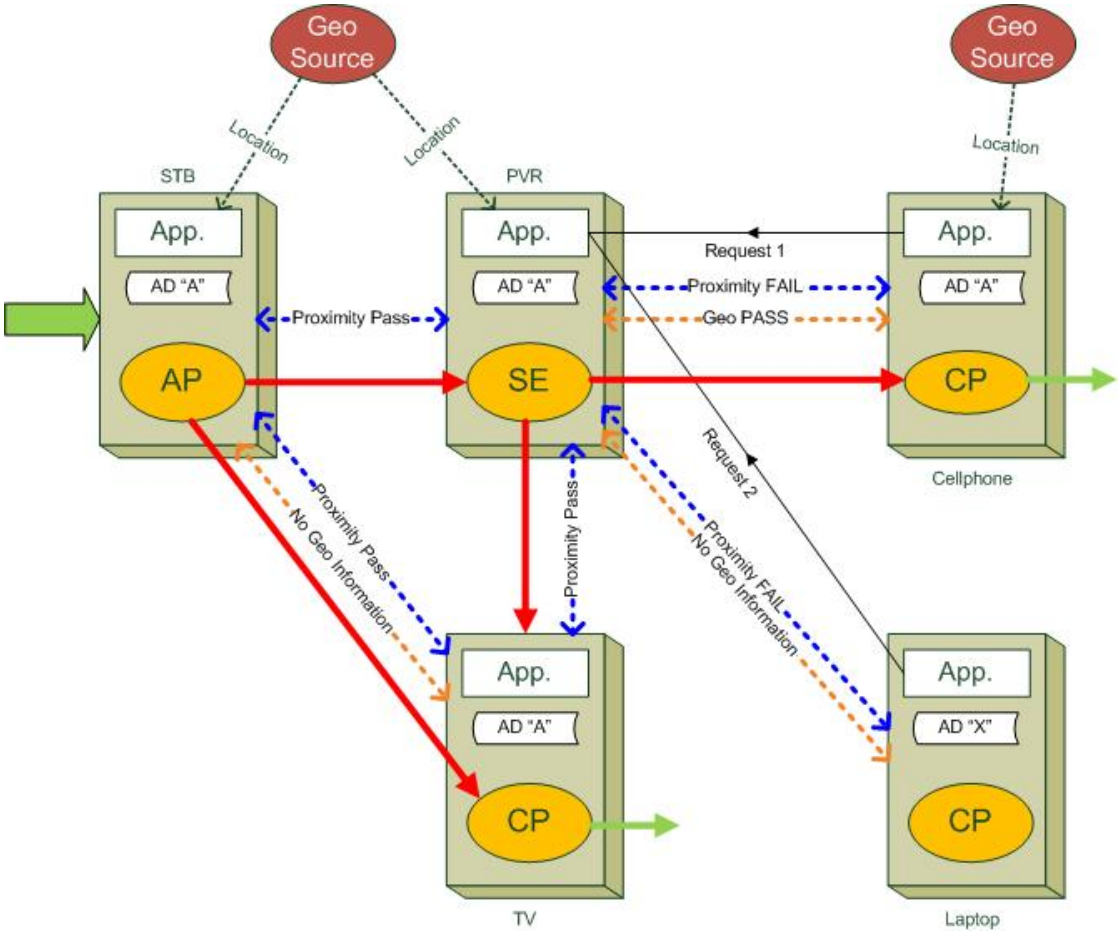

Figure 36: Local Blackout Operation

In this scenario it will not be possible to acquire content within the local blackout area and it is also necessary to ensure that devices outside the blackout area do not pass content into the blackout area.

1) The MLocal setting means that the acquisition point is able to stream or copy the content to any device within the local environment as determined by proximity tests.

2) Request 1 comes from a non-local device. The requesting device is able to identify its own location, and the player is able to verify that this is outside the blackout area, so the content can be viewed or copied to this device.

3) Since Request 2 comes from a non-local device that is unaware of its own location, it will not display the content.

4.20 Scenario 20 - Copy N Times

4.20.1 Business Intent

This scenario covers content offered such that a user is permitted to keep a specific number of copies and no more.

EXAMPLE: Some countries permit a fixed number of copies to be made of certain broadcasts, such as Japan.

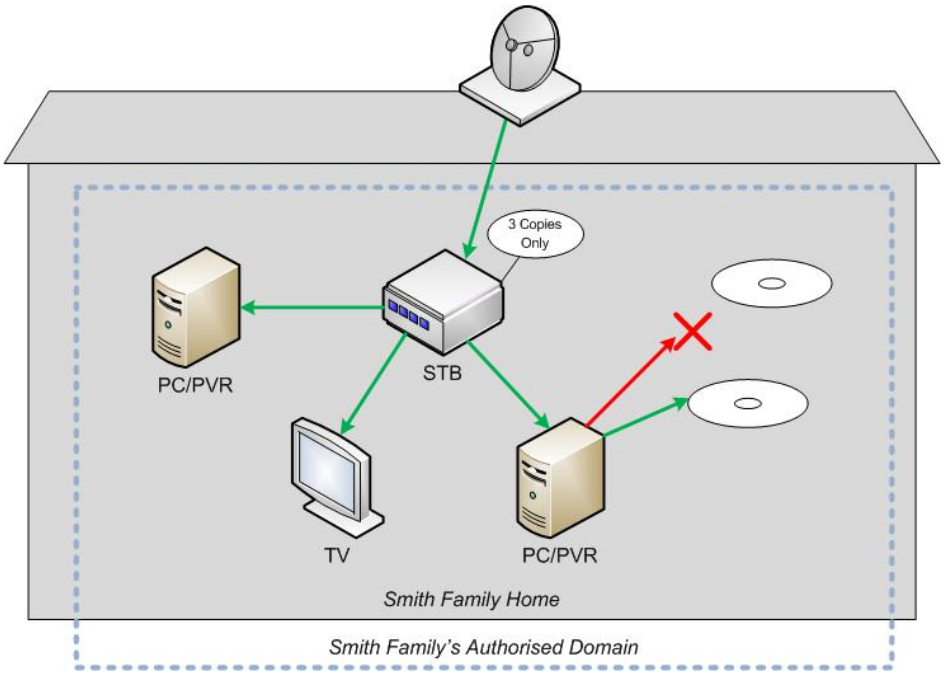

Figure 37: Copy N Times Content Flow

4.20.2 Usage State Information

The following USI settings support this scenario.

Table 21: Copy N Times USI

Type of Control	Propagation Control				Copy Control
	Movement		View		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	MAD	Not Asserted	VAD	Not Asserted	Copy Once

4.20.3 CPCM System Operation

This scenario operates by creating Copy Once instances with a limited number of licences of the same content item.

1) The original Acquisition Point implements the limit on the number of permitted copies within the household, based on whatever the external signalling (or regulation) indicates.

2) Each device asking to View the content from the AP is permitted to do so. This does not constitute a Copy, and does not affect the limit.

3) When content is sent to a Storage Entity for recording, the Acquisition Point creates a set of copy once content licences equal to the number of permitted copies. Each content licence will have a unique CLID, and on arrival at the SE each of these will become Copy No More.

4) Another device wanting a copy of the content will obtain a copy of the content item, plus it will securely move a single content licence, which is only usable by the receiving device, via the SAC marked as Copy Once or Copy No More.

5) A device wanting an additional copy to pass on to another device, or for writing to removable media, will need to request an additional Copy No More content licence.

NOTE 1: Depending on implementation choices, it may be possible to reuse the existing encrypted content file with the new licence. Otherwise a new copy is required.

NOTE 2: The Acquisition Point only creates a single content licence for each permitted copy, by which means the system enforces the global limit on the number of copies in circulation within the household.

4.21 Scenario 21 - Sneakernet

4.21.1 Business Intent

This scenario covers content offered with proximity or geographic limitations on distribution, where the content is physically transported to a remote location.

CPCM assumes a basic conditional permission for such movement, in that it is always allowed to move a device holding CPCM protected content without affecting the ability of the user to play the content. Where USI indicates that copies can be made, it is also permitted to physically move the device that holds the copy without affecting the ability to play it.

This allows the consumer to move content that is marked as MLAD or MGAD to a location outside the local environment or geographic area, and make use of it there, provided that this is done by physical carriage of the device, or removable media for MGAD content, containing the content.

As such, this scenario only applies to recorded content of a complete content item, or a segment thereof. The concept does not apply for streamed content until it has been recorded.

This exemption does not release the content from being bound to a domain. It simply removes the need to employ proximity and geographic enforcement tools.

NOTE: Removable bit-bucket media such as recorded DVDs, USB keys, or other devices that do not include CPCM functionality can be used in this way, though in a more limited sense. It is permitted to store MLAD content on bit buckets, but the content will not be accessible once it has been moved to a remote location (unless the storage entity is also moved).

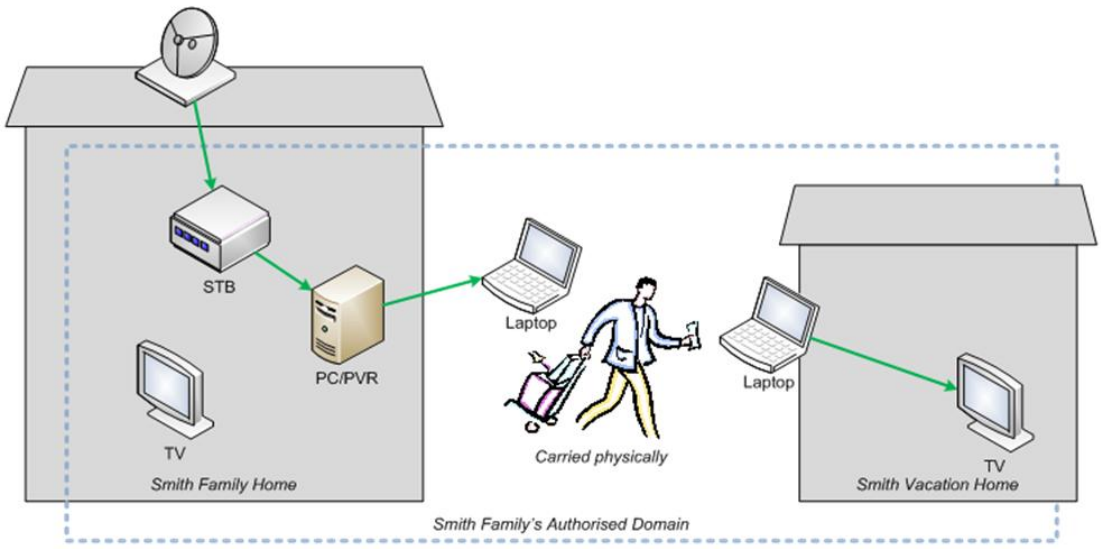

Figure 38: Sneakernet Content Flow

4.21.2 Usage State Information

The following USI settings support this scenario.

Table 22: Sneakernet USI

Type of Control	Propagation Control				Copy Control
	Movement		View		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	**MLAD**	Not Asserted	**VLAD**	Asserted	CCNA
NOTE: This scenario also applies to MCPI/VPI values of **MGAD** and **VGAD**.					

4.21.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

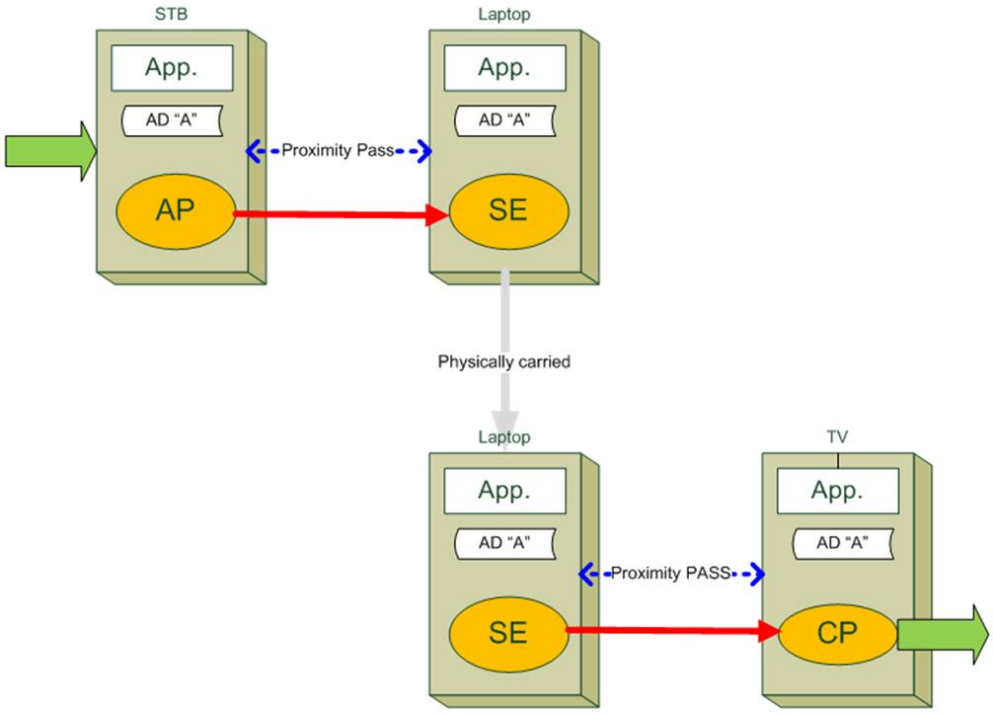

Figure 39: Sneakernet Operation

1) Content is transferred from an Acquisition Point to a device that includes a Storage Entity.

2) The device holding the content item is physically moved to a new location.

3) The Storage Entity holding the content item is now able to stream or copy the content item according to the USI, using proximity tests based on the new location.

NOTE: If the Content Item is marked MGAD, local movement of the content item is permitted even when outside the permitted geographic area or areas.

4.22 Scenario 22 - Reformat for Mobile Device (Copy)

4.22.1 Business Intent

This scenario covers content offered in one format, being repurposed within the home to another format. In this specific case, the consumer is allowed to make additional copies of the content. So making an additional copy in a new format is implicitly permitted.

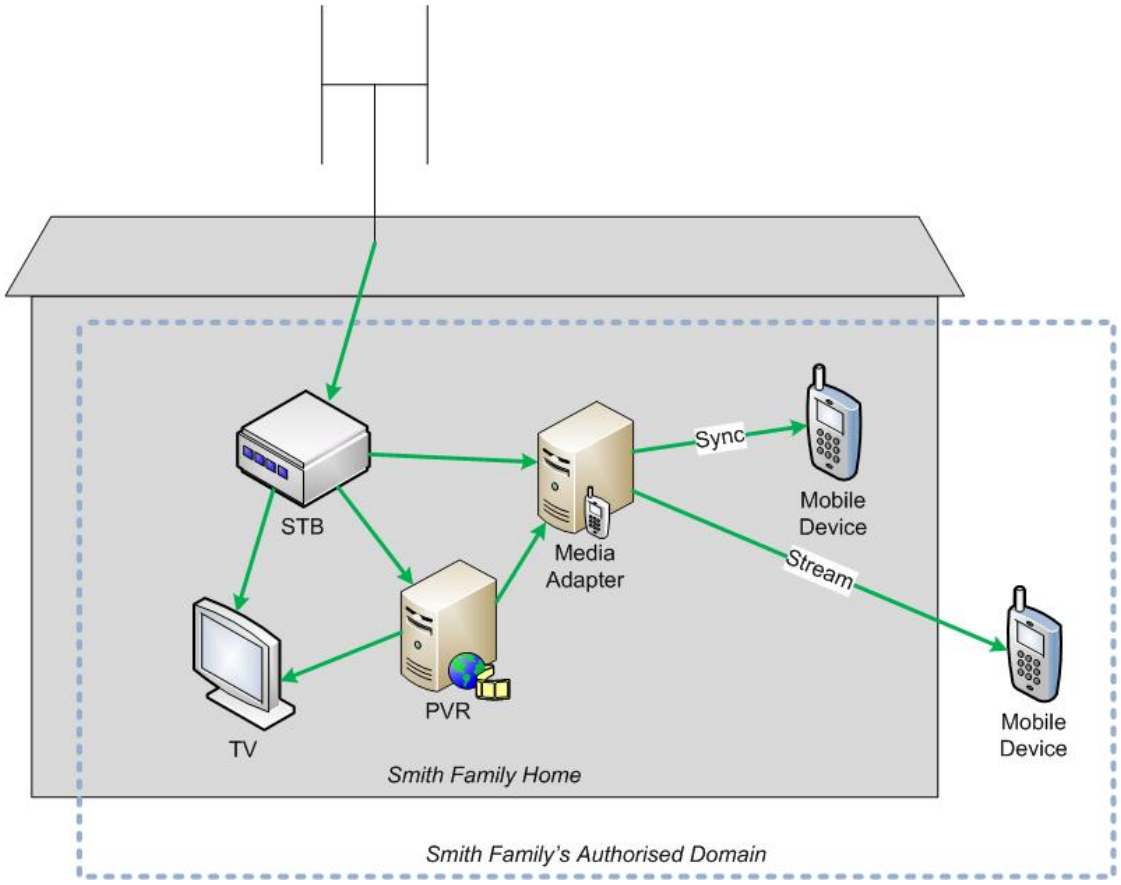

Figure 40: Reformat for Mobile Device (Copy) Content Flow

4.22.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 23: Reformat for Mobile Device (Copy) USI

Type of Control	Propagation Control				Copy Control
	Movement		View		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	MAD	Asserted	VAD	Asserted	**CCNA**

4.22.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

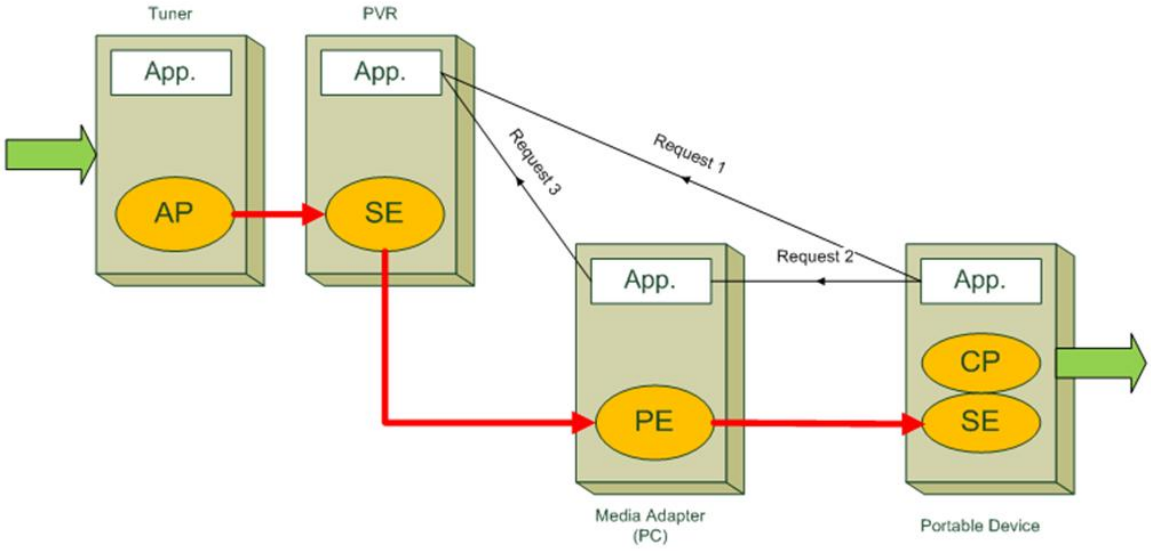

Figure 41: Reformat for Mobile Device (Copy) Operation

Conversion of content to a new format requires content to be securely descrambled and then re-scrambled by CPCM. This type of modification of protected content is provided by a Processing Entity, which may be independent or integrated as part of another CPCM Device.

For this scenario we use a free-standing media adapter.

1) Content is recorded in native full resolution by the PVR.

2) The portable device requests the content. There are several ways this could be supported. The precise method is out of scope for CPCM.

   a) The device asks the content source directly using an ISAN or some other form of content identifier; Request 1.

   b) The device browses a content discovery service provided by the home network and finds content that it is unable to play, so it then searches for a suitable adapter.

   c) The media adapter advertises the content in the formats that it can support, thus providing a virtual server able to deliver content from the real source.

3) The device requests the content from the media adapter; Request 2.

4) The media adapter requests the content from the PVR; Request 3.

5) The PVR sends the content to the media adapter, which decrypts the content, reformats it as required, and encrypts it again.

6) The media adapter generates a new content licence and passes this to the mobile device along with the protected content in its new form.

4.23 Scenario 23 - Reformat for Mobile Device (Move)

4.23.1 Business Intent

This scenario covers content offered in one format, being repurposed within the home to another format. In this specific case, the consumer is not allowed to make additional copies, so the original copy is deleted or disabled when the copy on the mobile device becomes available.

NOTE 1: The repurposed copy of the content is degraded from the original, so moving it back to the original device does not recover the full viewing experience. Therefore it is advantageous to provide some means whereby the content can be recovered for use at full resolution.

NOTE 2: This scenario demonstrates that it is possible to employ CPCM to manage the movement of Copy Once or Copy No More content to mobile devices. However, the complexity and drawbacks described below should be seriously considered by those planning to signal Copy Once on services intended for a mixed population of conventional and mobile devices. It may be simpler to signal CCNA and mitigate the risks of proliferation in other ways, such as; by using AD restriction, which is recommended; expiring licences; or signalling content as Not Viewable and using an AAA function to enable viewing as required.

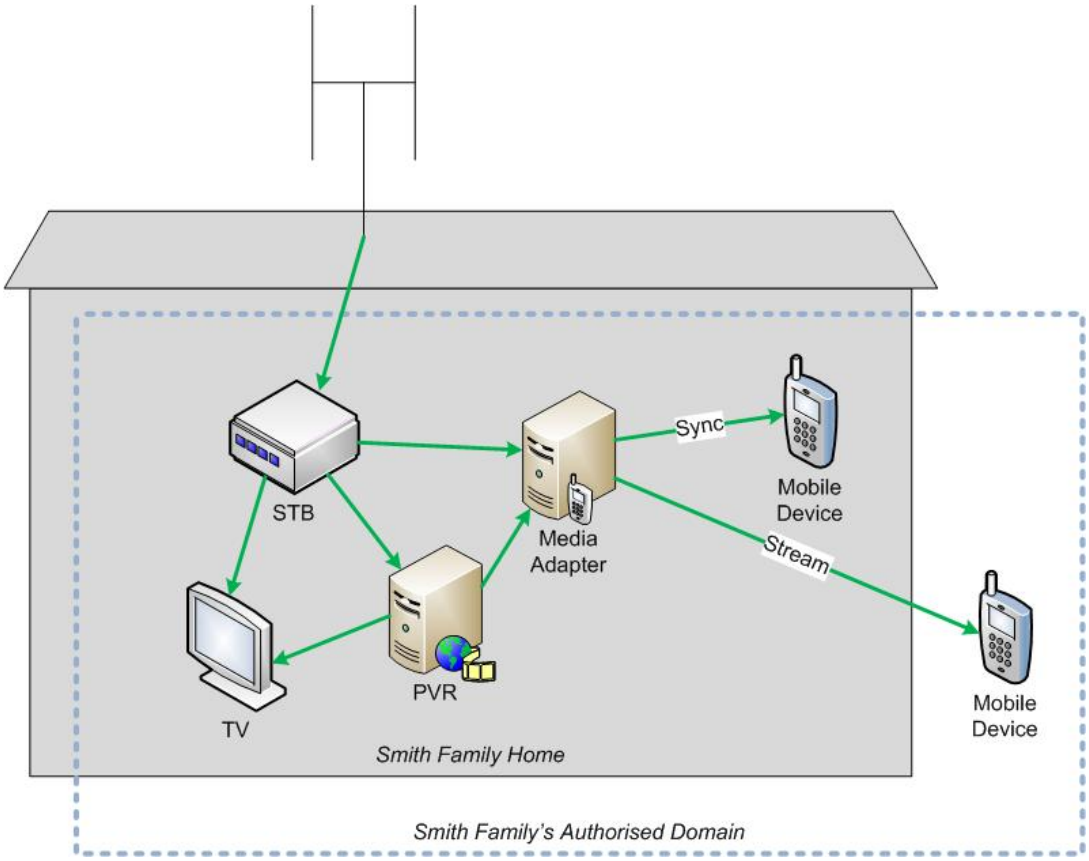

Figure 42: Reformat for Mobile Device (Move) Content Flow

4.23.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 24: Reformat for Mobile Device (Move) USI

Type of Control	Propagation Control				Copy Control
	Movement		View		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	MAD	Asserted	VAD	Asserted	**Copy Once**

4.23.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

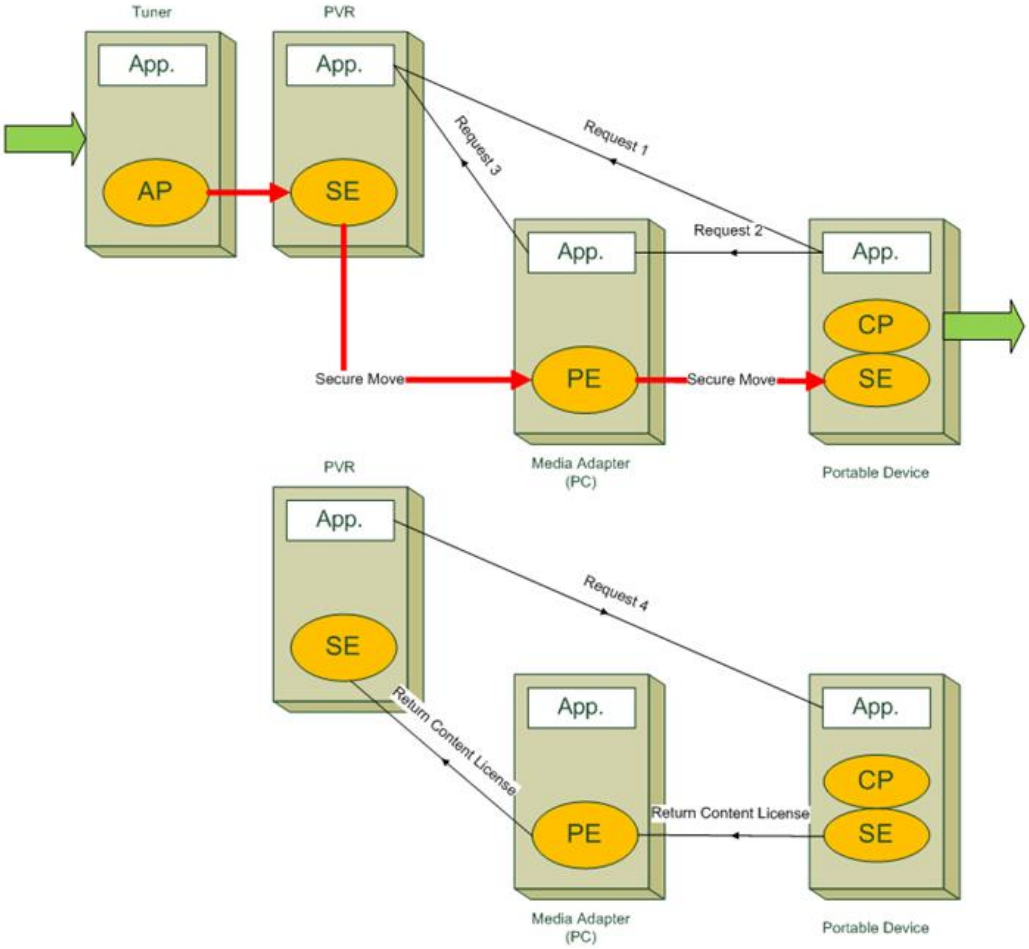

Figure 43: Reformat for Mobile Device (Move) Operation

The scenario proceeds in a similar way as in scenario 22. However, there are some additional steps required to prevent retention of the content, and to retain the quality of the viewing experience.

The USI setting requires a secure move of the content from the PVR to the media adapter, meaning that the content licence cannot be retained on the source PVR. However, in this case it is highly recommended that the original media file be retained on the PVR, although it is no longer playable.

As described above, the Processing Entity is responsible for generating a new content licence for use by the mobile device. There are at least two possible approaches to this as follows.

4.23.3.1 Content Licence based

In this approach, the original content licence is not returned to the SE until the mobile device returns its own content licence to the Processing Entity.

1) The request to move the content proceeds as in scenario 22.

2) The content is copied, not moved, to the Processing Entity.

3) The PVR securely moves the associated content licence to the Processing Entity.

4) The media adapter securely stores the incoming content licence, or just the descrambling keys, for future use.

5) The media adapter generates a new content licence based on the incoming one, with new keys for the modified content.

6) The media adapter protects the modified content using CPCM, and passes it with the new content licence to the mobile device.

7) The user enjoys the content on the mobile device.

8) The user initiates a request to move the content back to the PVR; Request 4.

9) The mobile device securely moves the content licence back from the mobile device to the media adapter and removes the content licence from its own storage.

10) The media adapter locates the original content licence that was used to make the content licence for the mobile device

11) The media adapter securely moves the original content licence back to the PVR, and either destroys or securely retains the content licence from the mobile device for future use. If the content item is deleted from the mobile device, the content licence on the mobile device can be deleted as the keys are no longer useful.

NOTE: There are some disadvantages to this method. Firstly, there is a need for persistent storage and indexing of content licences or, at a minimum, descrambling keys, in the Processing Entity which in this case is the media adapter. Secondly, the path back has to go through the same media adapter which may not be available or may have failed in the meantime. Thirdly, should the mobile device be lost the content associated with it will not be recoverable.

4.23.3.2 Time-based

In this approach, a time-window is chosen and the two content licences are created so that only one is valid at any given time. There is no need to return the content licence, or to reuse the media adapter. By this method the content is available on both devices but not during the same time window. On the expiration of the content licence for the mobile device the content licence for the PVR becomes active, giving the appearance to the user that the content has returned to the PVR.

1) The request to move the content proceeds as in scenario 22.

2) The content item is copied, not moved, to the Processing Entity.

3) The content licence is securely moved to the Processing Entity so no copy is retained on the PVR.

4) The system determines from the user how long the content should be valid on the mobile device. The answer provides the return time.

5) The media adapter modifies the original content licence by activating the View window and setting a start time equal to the return time. This modified content licence is returned to the PVR.

6) The media adapter generates a new content licence based on the incoming one, with new keys for the modified content. This new licence has the View window set such that the licence expires at the return time.

7) The original licence received from the PVR is deleted.

8) The media adapter protects the modified content using CPCM, and passes it with the new licence to the mobile device.

9) The user enjoys the content on the mobile device.

10) When the return time is reached, the content on the mobile device ceases to play, and the content on the PVR becomes usable again.

NOTE 1: The advantage of this approach is the apparent return of the content without any need to connect devices. This approach also works should devices be lost or stolen.

NOTE 2: This method may be precluded if the time window fields are already in use. It is possible, but quite complex, to daisy chain multiple moves.

NOTE 3: The approach may be a little hard for some consumers to understand, which could result in confusion and support calls, though this can be alleviated by good product and UI design.

4.24 Scenario 24 - Content-based Domain Join

4.24.1 Business Intent

This scenario covers the situation where a newly purchased device, which has not yet been joined to a domain, is used to view content that is limited to use by members of the same household.

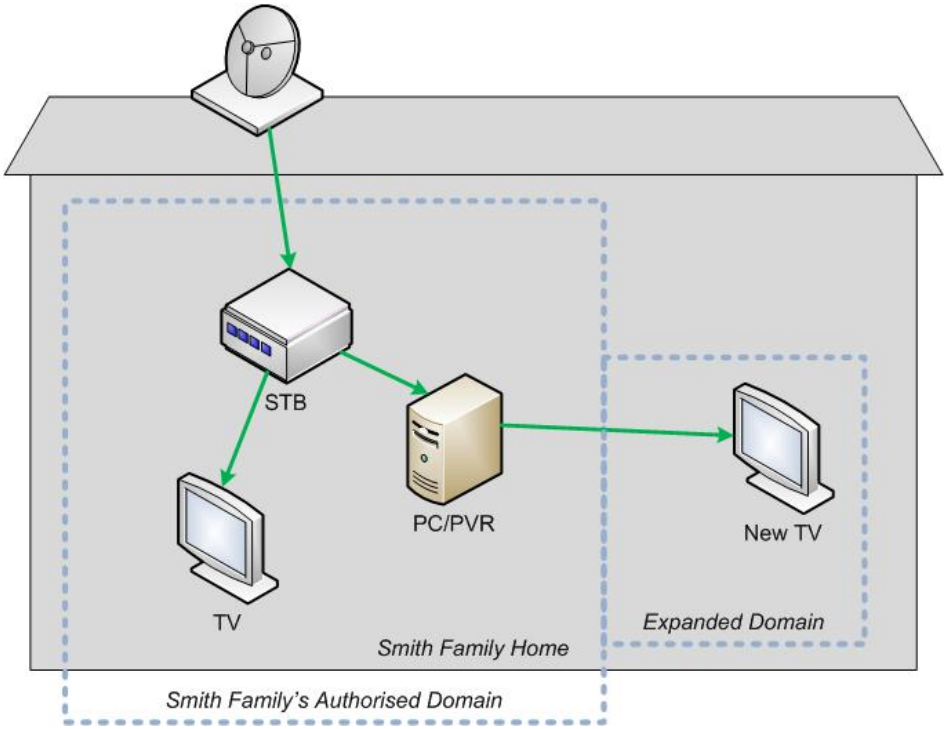

Figure 44: Content-based Domain Join Content Flow

4.24.2 Usage State Information

The following USI settings support this scenario.

Table 25: Content-based Domain Join USI

Type of Control	**Propagation Control**				**Copy Control**
	Movement		**View**		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	**MAD**	Not Asserted	**VAD**	**Not Asserted**	CCNA
NOTE: This scenario would also apply to content marked as MLAD, MGAD, VLAD or VGAD. This scenario would not apply to content marked with MCPCM, VCPCM, or where VLocal is asserted, as these cases do not require domain membership for content viewing.					

4.24.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

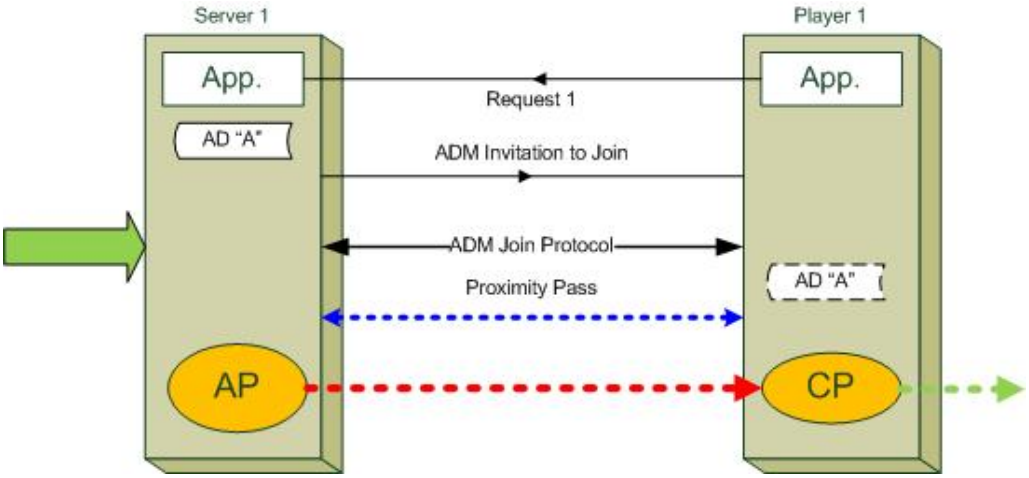

Figure 45: Content-based Domain Join Operation

1) Player 1, which is new and not an AD member, asks to view a content item that is AD bound.

2) EITHER:

   a) Player 1 reads the AD id of the content in the directory, and starts an ADM Join protocol to join the required domain; or

   b) Server 1 recognises that Player 1 is not currently a member of any domain, and issues an ADM Invitation for Player 1 to join the domain, as shown in figure 45.

3) Player 1 completes the ADM procedure to join the domain, and thereby obtains the domain secrets for the domain.

4) Player 1 is now recognised as an AD member and able to receive and play AD bound content.

NOTE: This behaviour is intended only for new devices which do not currently belong to an AD. It is recommended that devices with existing domain membership (in another domain) avoid such automatic behaviour, as it may adversely affect the user experience.

4.25 Scenario 25 - Early Content Delivery for Timed Release

4.25.1 Business Intent

This scenario covers the case where CPCM allows content to be acquired by background downloading or overnight broadcast so that it will then be ready for immediate consumption at a predefined date and time.

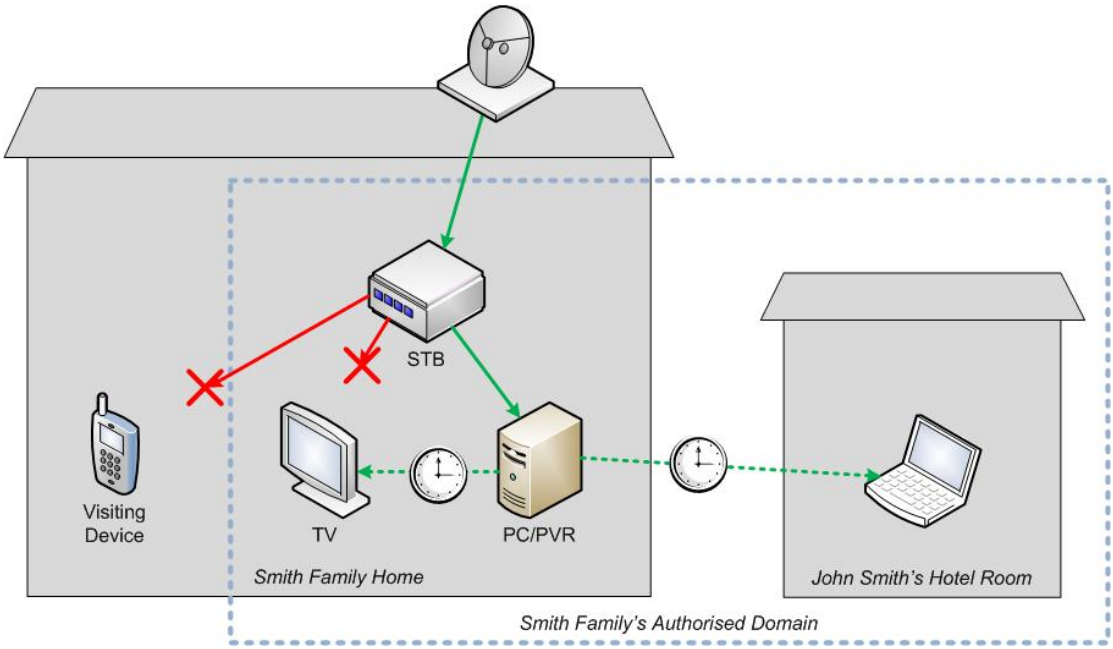

Figure 46: Early Content Delivery for Timed Release Content Flow

4.25.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 26: Early Content Delivery for Timed Release USI

Type of Control	Propagation Control				Copy Control	View Window
	Movement		View			
USI Field	MCPI	MLocal	VPI	VLocal	CCI	Start
Value	MAD	Not Asserted	VAD	Not Asserted	Varies by Service	**Day-Date of Release**

4.25.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

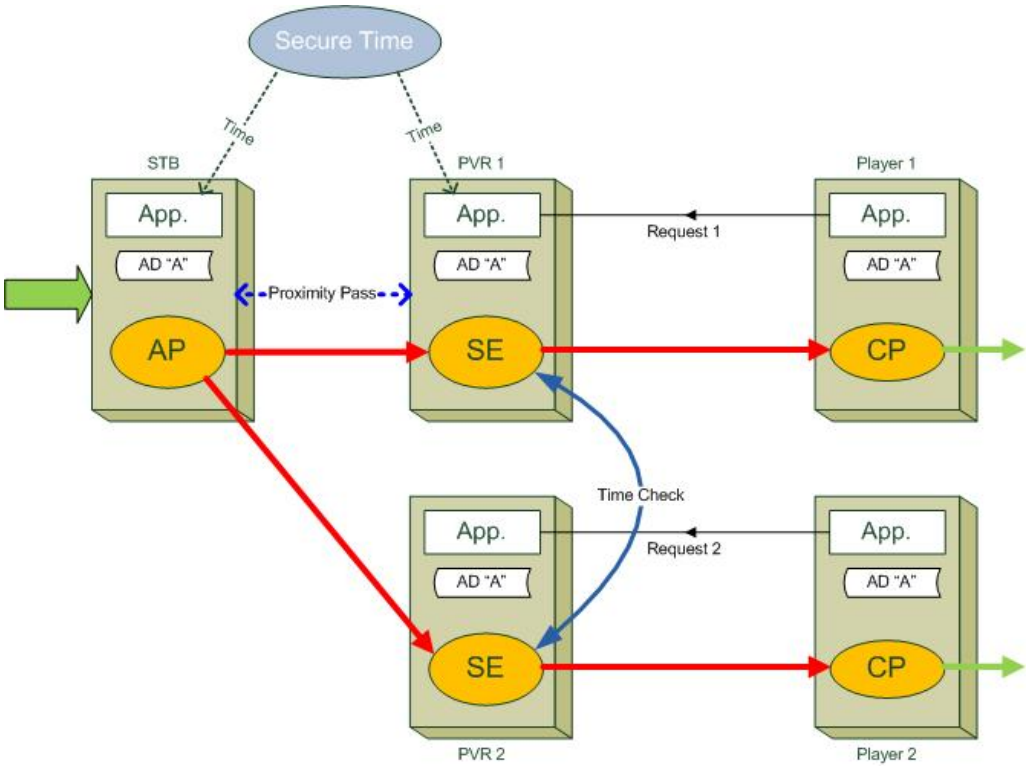

Figure 47: Early Content Delivery for Timed Release Operation

1) Content is received by the STB. A content licence is created using the Release Date/Time information received in the original broadcast.

2) The content is recorded on one or more PVR. In this example PVR1 and PVR2 are shown.

3) The PVR may either:

   a) Delay the advertising of the availability of the content to players until the release time has passed; or

   b) Advertise the content, but indicate in the catalogue that the content will not be available for playing until the release time

4) The point in time of release passes before which all requests to View content are rejected.

5) Player 1 issues Request 1.

6) PVR1 checks that the current time from a secure time source is after the release time for the content.

7) PVR1 sends the content to Player 1 for viewing.

8) Player 2 issues Request 2.

9) PVR2 has no direct access to a secure time source. Therefore it requests a time check from another device, in this case PVR1.

10) There are two options by which PVR2 verifies that the release time is passed.

Either:

a) PVR2 may update a data record to indicate that this content has now been unlocked. This will allow it to continue to distribute the content without further reference to a source of secure time; or

b) PVR2 may replace the Content Licence with a new one that does not include the View Window. Such a Licence will be usable by devices without access to a source of secure time. The original USI in the auxiliary data is not modified.

11) PVR2 sends the content to Player 2 for viewing.

4.26 Scenario 26 - Viewing in Single Local Environment

4.26.1 Business Intent

This scenario covers content offered for use only in a single local environment at a time. The consumer is allowed to move the content to another location, but only one such location can have a playable copy. This can be considered as replicating the experience of a physical media container such as a DVD, which can be moved but can only be used in one place at a time.

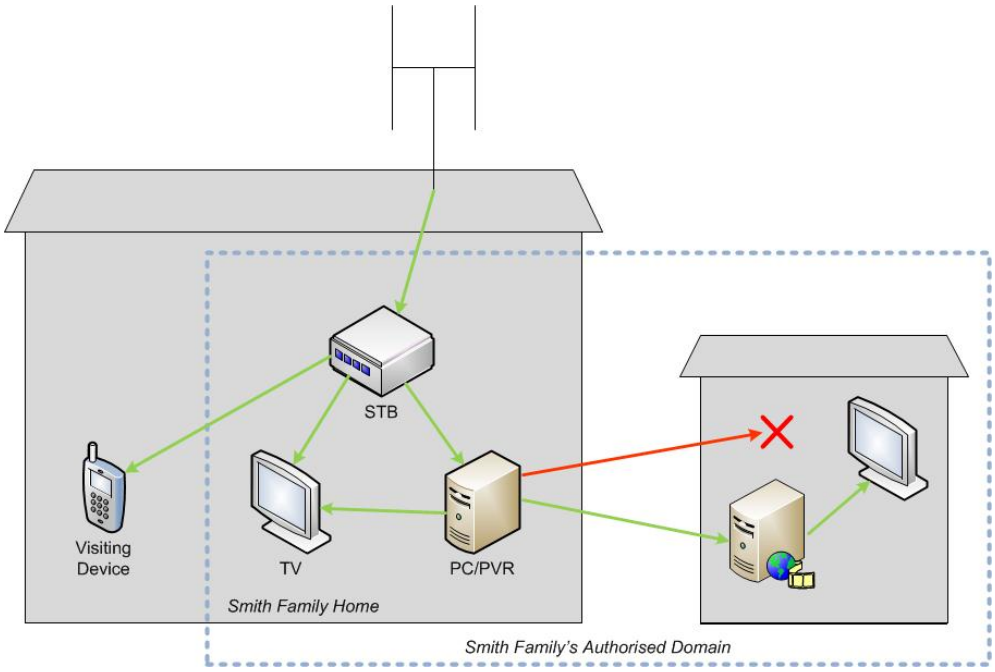

Figure 48: Viewing in Single Local Environment Content Flow

4.26.2 Usage State Information

The following USI settings support this scenario.

Table 27: Viewing in Single Local Environment USI

Type of Control	Propagation Control				Copy Control
	Movement		View		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	**MAD**	**Asserted**	**VLAD**	**Asserted**	C1/CNM

4.26.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

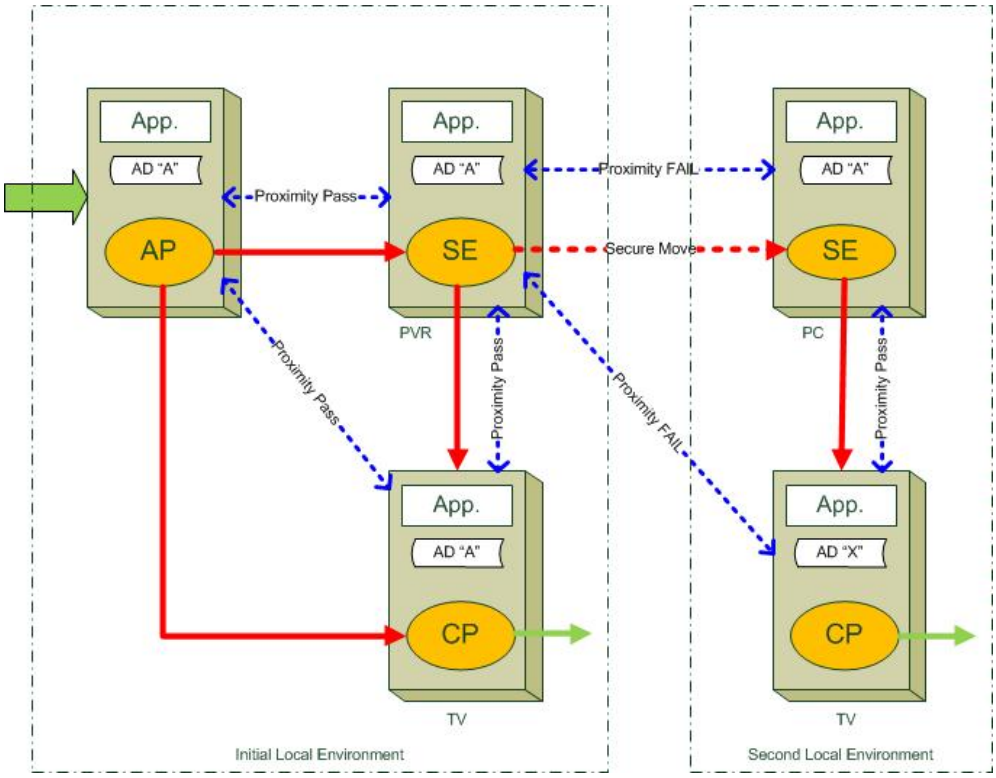

Figure 49: Viewing in Single Local Environment Operation

The normal operation of this scenario is as follows:

1) When the server acquires the content, it is bound to the AD as usual.

2) The server device checks the proximity of the destination device. If this is local the content is always allowed to flow due to MLocal/VLocal.

3) If the destination is not local and a request is made to view, this will be rejected.

4) If the destination is not local and a request is made to move the AD memberships of the two devices and the content are compared. If there is a match, the content can be securely moved to the new location, which means that that the original copy is removed or disabled.

5) Once in the new location, other devices local to that device can view the content as needed.

6) When content is securely moved to another device that is local but in a different domain, the single copy of the content is reassigned to the new domain because the ADID of the content is changed to match the ADID of the new device domain.

4.27 Scenario 27 - Movement of Content by MCPCM

4.27.1 Business Intent

This scenario covers content offered with permission to transfer it between all CPCM devices under one or more Compliance and Robustness Regimes.

NOTE 1: The primary benefit of this approach is to retain the content within the control of the C&R regime. For such content, the USI and C&R rules may also allow export to other technologies; however this export is out of scope for this scenario.

NOTE 2: This scenario raises certain implementation hurdles, because there is, by design, no global secret that can be used to protect the licences of such content.

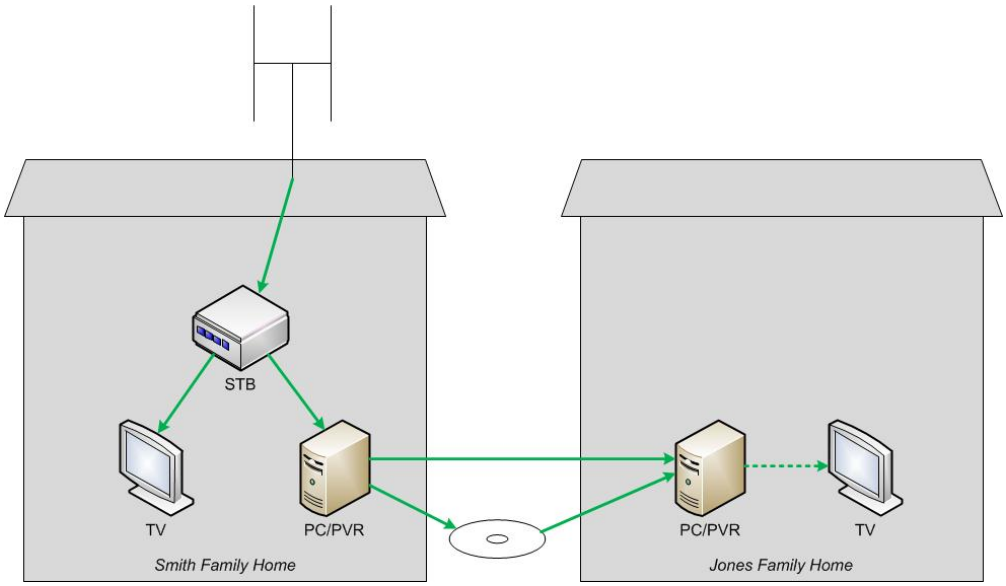

Figure 50: Movement of Content by MCPCM Content Flow

4.27.2 Usage State Information

The following USI settings support this scenario.

Table 28: Movement of Content by MCPCM USI

Type of Control	Propagation Control				Copy Control
	Movement		View		
USI Field	MCPI	MLocal	VPI	VLocal	CCI
Value	**MCPCM**	Asserted	**VCPCM**	Asserted	CCNA

4.27.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

1) Where content is moving directly from one device to another, be it local or remote, the content licence keys will be encrypted by the session key of the Secure Authenticated Channel between the two devices.

2) Where the content is being moved between two or more devices that belong to the same AD, the content keys can be protected with the AD key.

   EXAMPLE: if content is being put on a USB storage device for use by the same user in an AD member device at another location, or if the content is being multicast around a home network.

3) It is also permitted to store such content on a simple bit bucket when the DNCS flag is asserted to disable the CPCM scrambler. In such a case, the content licence is protected with the AD key.

4) If MCPCM content protected with an AD key is placed on a bit bucket store, or is sent over a multicast, and a device that does not belong to the same AD tries to access it, the content will need to be routed via a CPCM device that is a member of the original AD so as to access the content keys and replace the AD based encryption with SAC based encryption.

5) Once content arrives at a device, the MCPCM setting allows the device to change the AD identity and key, if any, and to use any of the other methods listed to move the content to yet another CPCM device.

NOTE: In all cases, despite the MCPCM setting, the content can ONLY be moved to a CPCM device that is certified under one or more of the same identified for the specific content item being moved.

5 Advanced Content Management Scenarios

The advanced scenarios discussed in this section involve some additions beyond the CPCM system specifications. In some cases this requires changes to broadcast signals. Others may be achieved using proprietary extensions or by future extension of the CPCM specifications.

5.1 Scenario 28 - Limited Plays

5.1.1 Business Intent

This scenario covers content which is delivered with permission to be viewed a limited number of times. Once these plays have been used, the content is no longer playable.

It may be possible to purchase additional plays as described in scenario 32.

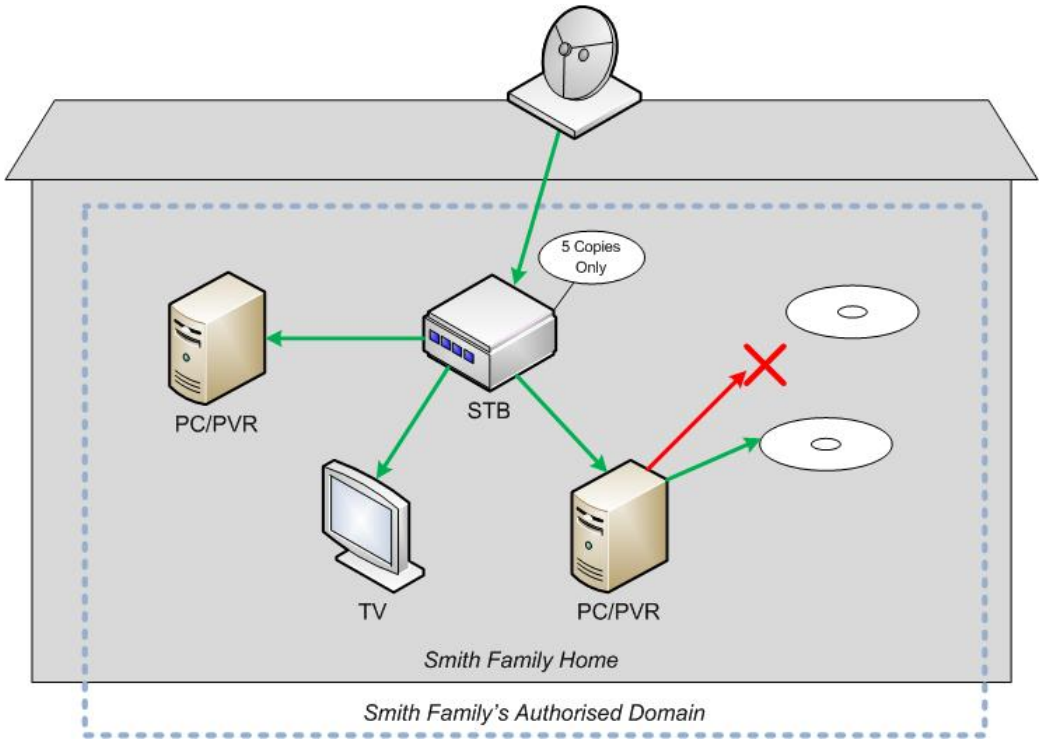

Figure 51: Limited Plays Content Flow

5.1.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 29: Limited Plays USI

Type of Control	Consumption Control	Propagation Control				Copy Control	Play Count Extension	
		Movement		View				
USI Field	Viewable	MCPI	MLocal	VPI	VLocal	CCI	Play Limit	Play Remain
Value	**Not Asserted**	MAD	Not Asserted	VAD	Not Asserted	**Copy Once**	**5**	**5**

NOTE 1: The USI setting of Not Viewable prevents legacy CPCM devices without the Play Count Extension from playing the content. The Play Count Extension provides an exception that overrides this setting. Care should be taken therefore, not to use the Play Count Extension when the content should truly not be viewable, such as when it requires a purchase transaction to enable it.

NOTE 2: The presence of the Play Limit value may allow more than one copy to be made, provided that the total number of permitted plays is not exceeded. The content licence for each derived copy will be updated with the Play Limit field changed to show the subset of plays assigned to each specific copy.

NOTE 3: The values of MAD and VAD are given as examples. Other values are possible. It is also possible to permit MLocal and/or VLocal, as the content will remain within CPCM and hence the limited plays will be enforced.

5.1.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

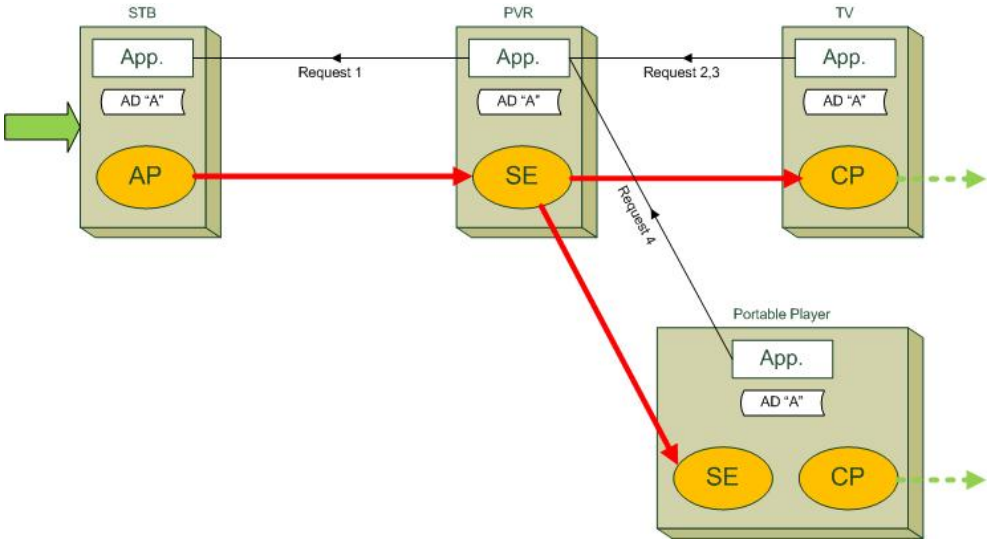

Figure 52: Limited Plays Operation

1) Request 1 causes the content to be recorded. The Acquisition Point includes the extension for limited plays, which indicates 5 plays are permitted.

2) Request 2 asks the PVR to stream the content to the TV. This constitutes the first play.

3) The PVR decrements the count of Play Remain in the Play Count Extension of the content licence, leaving 4 plays remaining.

4) Later, with Request 3 the TV requests a second playing, leaving 3 plays remaining.

5) Request 4 asks for a copy to be made on the portable player. The user decides to move a single play to the portable player.

   a) The PVR decrements the Play Remain of its own licence to 2.

   b) The content licence sent to the portable player has a Play Remain of 1.

6) The user plays the content on the portable player. The portable Play Remain decrements to 0, blocking further plays.

7) The user is still able to play the remaining 2 plays from the PVR, or he can move another play to the portable device.

8) When the Play Remain is decremented to zero, the content cannot be played and further copies cannot be made.

NOTE: It may not be appropriate to count a play if the play sequence is interrupted, which may happen if there is a network fault. Determining exactly what constitutes a valid countable play is the responsibility of the appropriate Compliance and Robustness Regime, as is any non-repudiation mechanism for such plays.

5.2 Scenario 29 - CA-based AAA

5.2.1 Business Intent

The CPCM specifications describe the use of an Authorised Authenticated Agent (AAA) to replace, modify or update a CPCM content licence.

This scenario covers a number of situations where it is possible or necessary to update, replace, or modify the CPCM content licence under the authority of the original Acquisition Point. This would be a suitable approach when CPCM is acquiring content being delivered under the control of a conditional access (CA) system.

See scenarios 31 and 32 for scenarios that can make use of this approach.

See scenario 30 for an alternative scenario where the AAA function resides at an internet web address.

5.2.2 Usage State Information

The following USI settings will support this usage of content.

Table 30: CA-based AAA USI

Type of Control	**Other Content Licence information**	
USI Field	CLC	Key Recovery Information
Value	**Acquisition Point Device ID**	**Proprietary information**
NOTE 1: The CLC field will tell devices the identity of the CPCM device where they can obtain an updated content licence, assuming all the pre-requisites are met. NOTE 2: The Acquisition Point provides Key Recovery Information that will enable an AAA function to regenerate the original content scrambling key for the content new licence.		

5.2.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

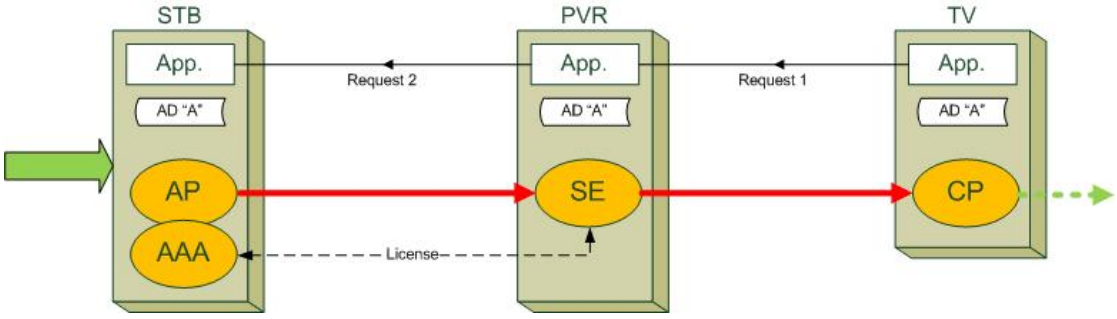

Figure 53: CA-based AAA Operation

1) The TV requests to play a stored content item; Request 1.

2) The PVR determines that the current content licence is not valid for the action that has been requested.

3) The PVR determines that the CLC field is populated with the identification of the STB, and that the STB is available for communication.

4) The PVR sends Request 2 to the STB, asking for a replacement content licence with the additional capability. The request includes the current content licence, auxiliary data, and content item identifier.

5) The CA function in the STB determines that the request is acceptable, and a new content licence is made available to this device.

6) The CA function may use the Key Recovery Information to obtain the correct content scrambling key, unless it already has a record of it. This is placed in the new content licence.

7) The CA function authorises the CPCM function to issue a new content licence to the PVR. This delivery may be protected using the SAC or, if both devices belong to the same AD, it may be protected using the AD key.

8) The PVR receives the new content licence, and stores it with the content item.

9) The PVR uses the new licence to display the content on the TV.

5.3 Scenario 30 - Web-based AAA

5.3.1 Business Intent

The CPCM specifications describe the use of an Authorised Authenticated Agent to replace, modify or update a CPCM content licence.

This scenario covers a number of situations where it is possible or necessary to update, replace, or modify the CPCM content licence under the authority of a server acting for the service provider or content provider. This would be a suitable approach for a web based authorisation system.

See scenarios 31, 32, and 33 for scenarios that can make use of this approach.

See scenario 29 for an alternative scenario where the AAA function resides at the original Acquisition Point.

5.3.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 31: Web-based AAA USI

Type of Control	**Other Content Licence information**	
USI Field	Rights Issuer URL	Key Recovery Information
Value	**URL**	**Proprietary information**
NOTE 1: The Rights Issuer URL field tells the device the internet, or home network, location from which a new content licence can be obtained. However, as explained below, this URL points to a service application which can authorise and identify an AAA, not to an AAA directly.		
NOTE 2: The Acquisition Point should provide Key Recovery Information that will enable an AAA function to regenerate the original content scrambling key for the new content licence.		

5.3.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

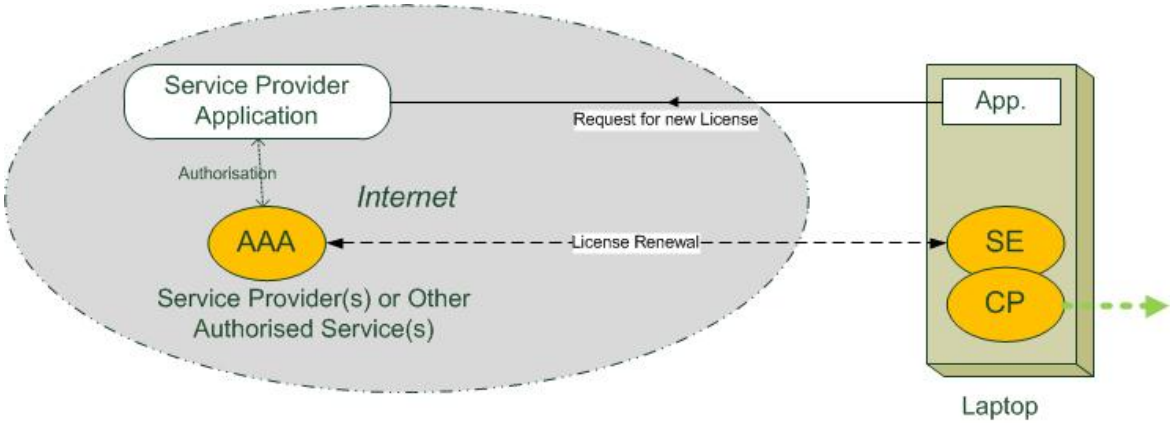

Figure 54: Web-based AAA Operation

1) The user asks the laptop to play a stored content item.

2) The laptop determines that the current content licence is not valid for the action that has been requested.

3) The laptop checks the Rights Issuer URL field, and passes this information to the appropriate function within the device application.

4) The laptop application communicates with the remote web service of the service provider application, identified by the URL.

NOTE: The protocol of this interaction is out of scope for CPCM.

5) The web service verifies, after some user interaction such as payment if applicable, that a new content licence can be issued and communicates this to the appropriate CPCM AAA running in the internet cloud or home network.

6) The web service sends a message back to the laptop application with the URL of the appropriate AAA function to contact.

7) The CPCM Instance in the laptop establishes a SAC with the remote AAA using the URL obtained at 6, and starts the content licence renewal protocol with the AAA.

8) The AAA function may use the Key Recovery Information to obtain the correct content scrambling key, unless it already has a record of it. This is placed in the new content licence.

9) The AAA issues the new content licence to the laptop's CPCM instance with the appropriate modified USI and or, auxiliary data. The licence delivery will employ SAC based protection of the content scrambling key, or keys, as the AAA is not a member of the AD and thus does not have a suitable AD key.

10) The new content licence is received and stored, and the content is played on the laptop.

5.4 Scenario 31 - Downloaded Subscription Content

5.4.1 Business Intent

This scenario covers content offered as a subscription service, where the content can be freely used as long as the subscription fee is paid.

See scenario 29 for a description of the approach when the AAA function resides at the Acquisition Point.

See scenario 30 for a description of the approach when the AAA function resides at an internet web address.

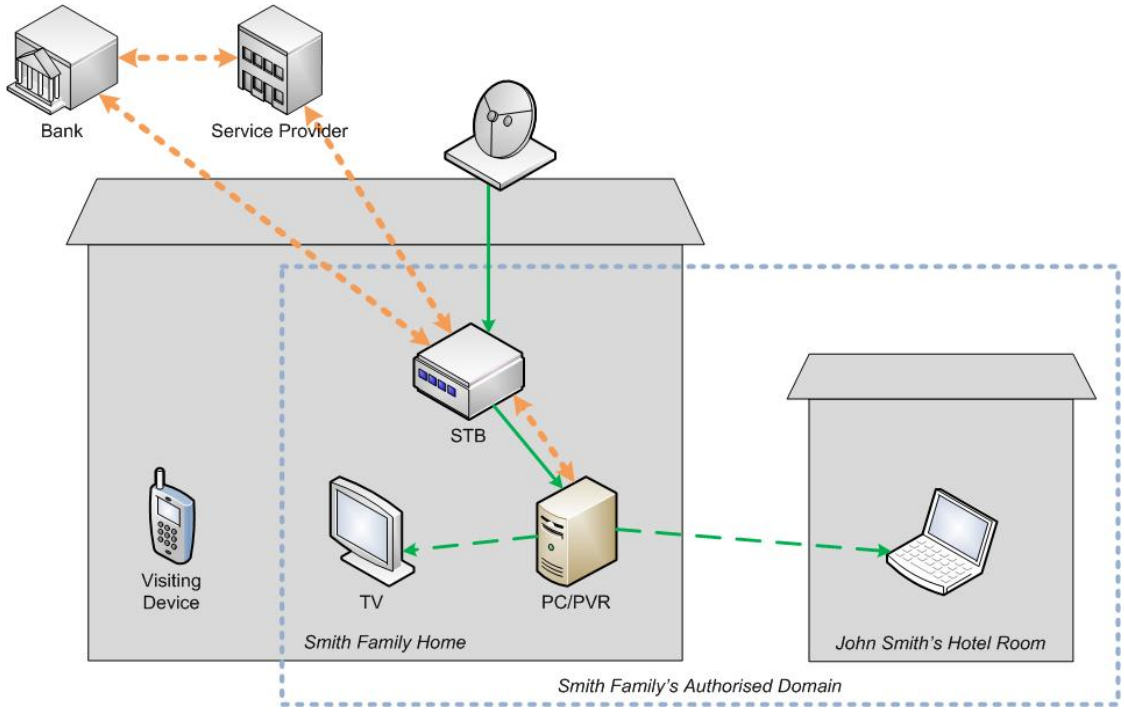

Figure 55: Downloaded Subscription Content Flow

5.4.2 Usage State Information

The following USI settings will enforce this usage of content.

Table 32: Downloaded Subscription Content USI

Type of Control	**Propagation Control**					**Copy Control**	**Other Content Licence information**
	Movement		**View**				
USI Field	MCPI	MLocal	VPI	VLocal	View Window End	CCI	**See scenarios 29 and 30**
Value	MAD	Not Asserted	VAD	Not Asserted	**Date/Time**	CCNA	
NOTE 1: The MCPI, MLocal, VPI and VLocal settings can be whatever is appropriate to the specific service. NOTE 2: The View Window End field would be set for a suitable expiry date after acquisition, such as two months for a monthly subscription service. There is a balance to be achieved between strictness of timing against usability for the consumer.							

5.4.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

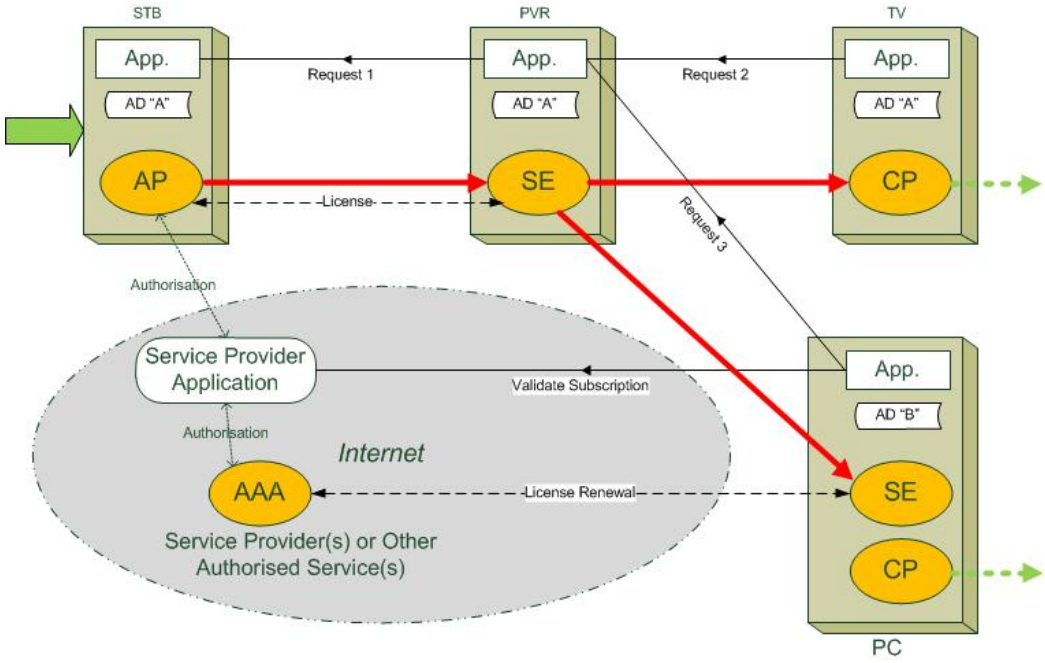

Figure 56: Downloaded Subscription Content Operation

1) When Request 1 is made, content is acquired in the conventional manner. The AP creates a content licence with USI as shown above, with a View Window End set for a suitable period.

2) Viewing, copying and movement of content are carried out as in accordance with USI settings.

3) Content licences for acquired content can be updated from time to time to provide additional viewing time in the View Window End. This could arise:

   a) When an attempt is made to use content for which the View Window is expired.

   b) When content is accessed and the View Window has a limited amount of time left to run.

   c) Periodically, when an implementation chooses to validate and renew licences proactively.

   d) At the user's request, when they anticipate using the content in a portable device and will not be able to renew content licences.

4) Request 2 is made to play content that is under a CA managed subscription service for which the current licence is expired.

5) The PVR checks the CLC field, and identifies the Acquisition Point.

6) The PVR requests a new content licence from the STB, as described in scenario 29.

7) The PVR passes a copy of the revised content licence to the TV and the content is played.

8) Request 3 is made to play content that is under a web-service-managed subscription service, and for which the current content licence is expired.

9) The PC checks the Rights Issuer URL field, and passes this information to the appropriate function within the device application.

10) The AAA issues a new content licence to the PC CPCM instance with an extended viewing period, as described in scenario 30.

11) The new content licence is received and stored, and the content is played on the PC.

5.5 Scenario 32 - Purchase of Additional Rights

5.5.1 Business Intent

This scenario covers content offered in such a way that additional rights can be purchased, as would be the case to extend an initial rental period.

See scenario 29 for a description of the approach when the AAA function resides at the Acquisition Point.

See scenario 30 for a description of the approach when the AAA function resides at an internet web address.

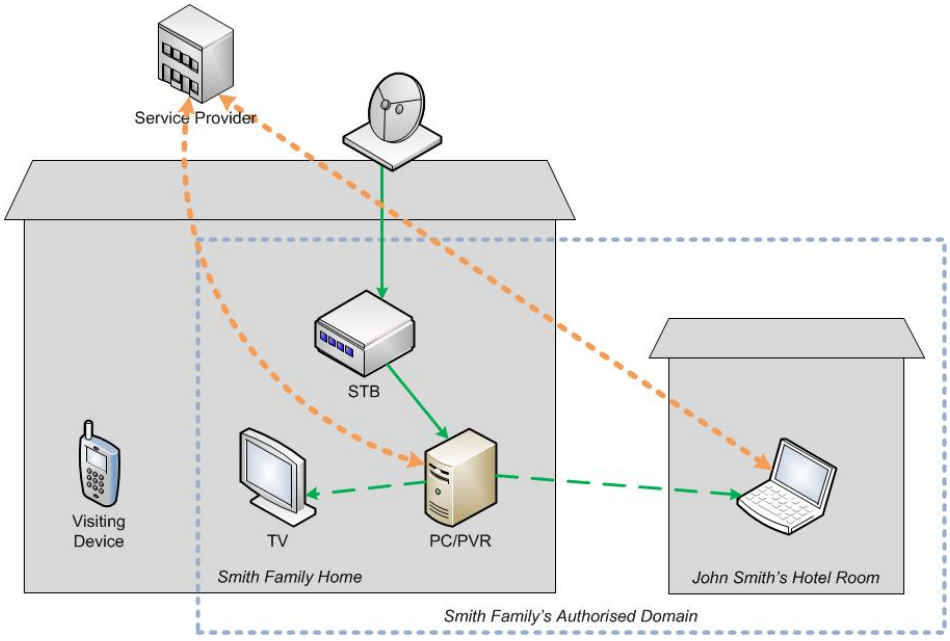

Figure 57: Purchase of Additional Rights Content Flow

5.5.2 Usage State Information

The following USI settings will enforce this usage of content:

Table 33: Purchase of Additional Rights USI

Type of Control	**Propagation Control**					**Copy Control**	**Other Content Licence information**
	Movement		**View**				
USI Field	MCPI	MLocal	VPI	VLocal	View Window End	CCI	**See scenarios 29 and 30**
Value	MAD	Asserted	VAD	Asserted	**Date/Time**	CCNA	
NOTE: In this scenario, the View Window End field would be set to indicate the end of the rental period, after which additional time can be purchased.							

5.5.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

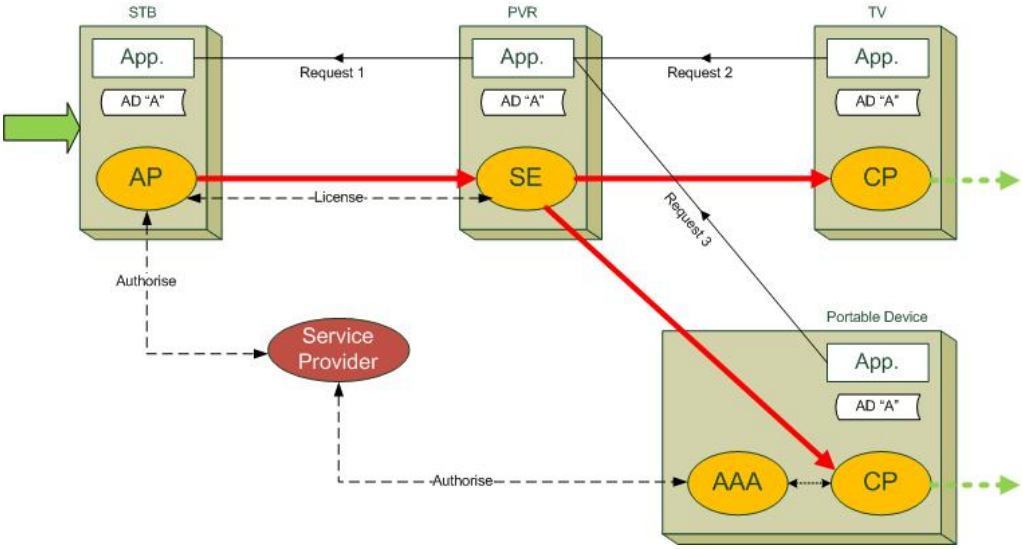

Figure 58: Purchase of Additional Rights Operation

The operation of this service is very similar to that in scenario 29. However, in this case, there is no automatic or periodic renewal of licences. Rather, each renewal is carried out as requested by the user.

Also, unlike the Downloaded Subscription Content scenario, the content licence can be adjusted in various ways not limited to extending the View Window End data.

EXAMPLE: Payment of a fee will allow Copy Once content to be made Copy Freely within the AD.

NOTE: There will be a need to provide user interaction for this service, typically including a menu of choices to the user with pricing information so that a decision can be made. This is out of scope of CPCM.

5.6 Scenario 33 - Superdistribution

5.6.1 Business Intent

This scenario covers content offered in a form that can be freely copied and shared, but where the some or all of the content item requires a payment, registration or other condition to be met by the user who receives the copy.

The initial free play period acts as an incentive to attract the purchase of authorisation to see the remainder.

Figure 59: Superdistribution Content Structure

NOTE 1: The content is acquired into CPCM by the first user. Subsequent users do not need to acquire the content again, but do need to obtain a revised content licence for the second section.

See scenario 30 for a description of the interactions between this service and the web-based AAA function.

NOTE 2: Because this content is designed to function outside the original home, there is no point in implementing the method described at scenario 29.

NOTE 3: The initial segment needs to be left in the clear (unscrambled), and with the USI set to indicate Do Not CPCM Scramble to ensure that the segment remains playable as it moves between domains.

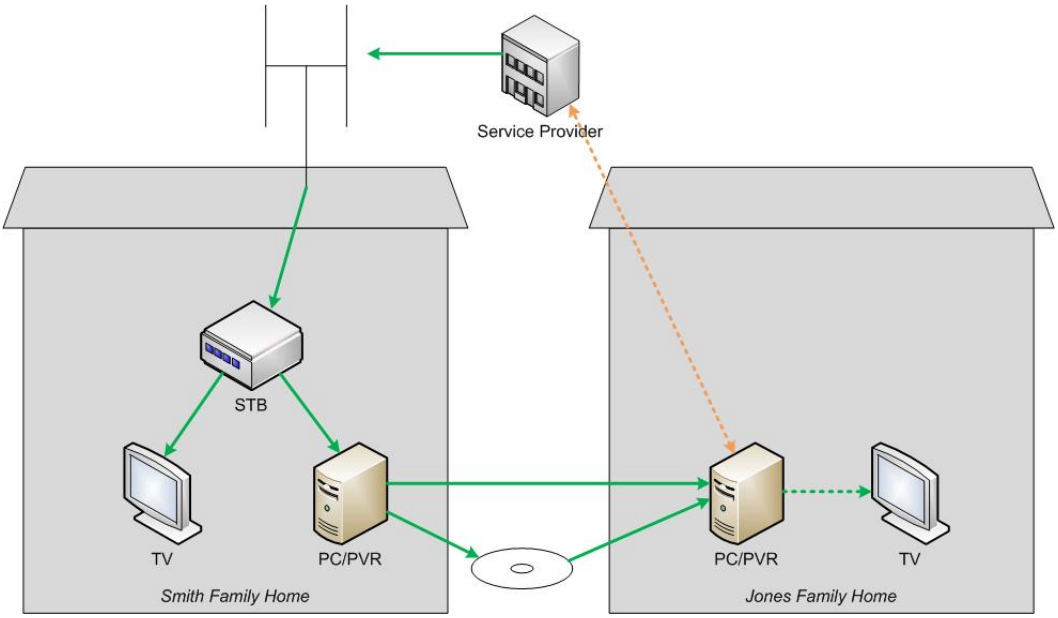

Figure 60: Superdistribution Content Flow

5.6.2 Usage State Information

This is another case of a content item being provided with multiple content licences. In this case, the service provides an initial content licence for the first period of the content item which is suitable for playing on any CPCM device. The section of content item associated with this content licence is not encrypted.

Table 34: Superdistribution initial USI

Type of Control	**Propagation Control**				**Copy Control**	**Ancillary Control**	**Auxilliary Data**
	Movement		**View**				
USI Field	MCPI	MLocal	VPI	VLocal	CCI	DNCS	Rights Issuer URL
Value	**MCPCM**	**Asserted**	**VCPCM**	**Asserted**	**CCNA**	**Asserted**	**URL**
NOTE: Where a SAC can be established between two CPCM devices in different domains, the content licence can be validated using the SAC protection. Where a SAC is not possible, such as when passing content via a bit bucket, the Rights Issuer URL allows the receiving device to both validate the original licence and obtain a new one. Hence the Rights Issuer URL should always be included although it may not always be needed.							

At some pre-determined time interval after the start of the content item, a content encryption key is created and a second content licence is provided that contains this key, with USI set as follows:

Table 35: Superdistribution modified USI

Type of Control	Propagation Control				Copy Control	Ancillary Control	Auxilliary Data
	Movement		View				
USI Field	MCPI	MLocal	VPI	VLocal	CCI	DNCS	Rights Issuer URL
Value	**MAD**	**Not Asserted**	**VAD**	**Not Asserted**	CCNA	**Not Asserted**	**URL**
NOTE 1: The Rights Issuer URL field tells devices where to go for additional rights. In this case, the source will require the use of additional client software to provide the necessary user interface. NOTE 2: The second content licence binds the main part of the content item to the original user AD, which is no longer valid for another user. The CPCM instance can use the auxiliary data to find the location where another user can acquire a content licence for their AD.							

5.6.3 CPCM System Operation

With the above USI settings, the CPCM system will operate as follows.

5.6.3.1 Content Scrambling Key management for Super-distribution

For this scenario, it is necessary to use a reusable content key that is known by the service provider application and AAA. This is because the service provider needs to be able to reconstruct a valid content licence for a device that may have no communication with the original Acquisition Point device.

These interactions between the player and the AAA are out of scope for CPCM.

NOTE 1: One possible approach is to protect the content scrambling key using a proprietary means and place it in the Key Recovery Information field of the auxiliary data, which can then be sent back with the original Content Licence to the service provider and, or, AAA where the scrambling key can be securely extracted to be used in the new content licence.

NOTE 2: Another possible approach is for the original Acquisition Point to request a scrambling key from the service provider for each content item, rather than generating random key as is usual; or for the original Acquisition Point to notify the service provider of the random key it has assigned to the specific content item identification. In this case, the Key Recovery Information field may be used to provide an index or similar means to help obtain the key record.

NOTE 3: An alternative approach would be for the main segment to be marked as MCPCM and not viewable. This would allow for movement of the content without loss of the content scrambling key, but it would require obtaining a new license marked MAD and viewable from the rights issuer. Both of these licenses would need to be retained with the content to allow further distribution.

5.6.3.2 Super-distribution using Streaming

In this case, the content is streamed with both content licences as generated by the original AP.

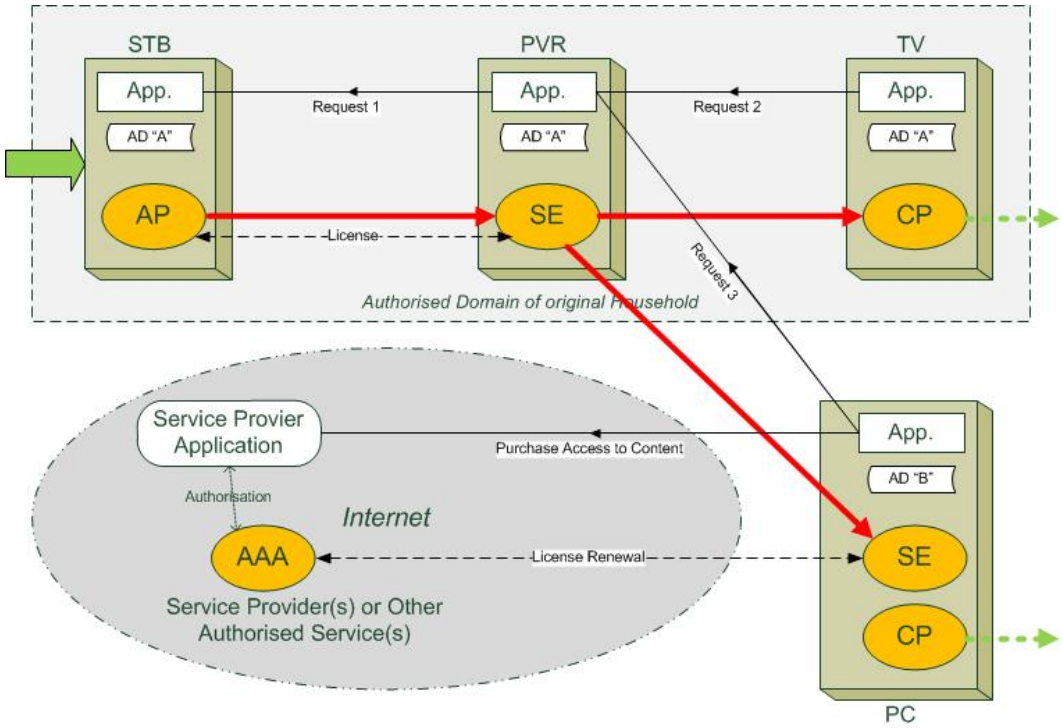

Figure 61: Superdistribution Operation - Streaming

1) Request 1 triggers the delivery of the super-distribution content to the PVR. This is stored with both content licences.

   a) The first segment and its associated licence are not bound to a domain.

   b) The remaining segment and its associated licence are bound to the Authorised Domain by the Acquisition Point.

2) Request 2 asks to play the content within the AD. Because the TV is a member of the same AD, both content segments can be played immediately.

3) Request 3 asks the PVR to stream the content to a PC belonging to another AD.

4) The PVR transfers the whole content item.

5) The PVR sends both content licences to the PC.

6) The first part of the content plays on the PC, as it is marked VCPCM and is not AD-bound.

   a) If the PVR transmitted the content licence via the SAC, the content licence will have been rebound to the new domain.

   b) Else the receiving device will be able to extract the Rights Issuer URL as described below.

   NOTE: Since the content is not scrambled, the key recovery information field does not need to be used.

7) When the PC attempts to use the second content licence, it is unable to do so as it does not belong to the same AD.

8) The PC identifies the Rights Issuer URL and passes this to a suitable device application, which communicates with the service provider.

9) The service provider offers the consumer a way to gain the right to play the rest of the content. This may be by payment, advertising, registration, or any other business transaction, which is out of scope for CPCM.

10) The service provider notifies the AAA function which prepares a new licence with the same USI, but with the AD identity of the new AD.

NOTE: Scenario 30 describes this process, during which the AAA needs to recover the content scrambling key using the Key Recovery Information field of the auxiliary data.

11) The AAA function sends the new content licence to the PC, which enables it to recover the content scrambling key, or keys.

12) The PC is now able to play the whole content item, or to share it with other devices in the same AD.

13) This process can be repeated in the same way as the content is further re-distributed from the first user or subsequent users.

5.6.3.3 Super-distribution using Removable Storage Media

In this case, the content is recorded to removable storage media with both content licences which are generated by the first AP.

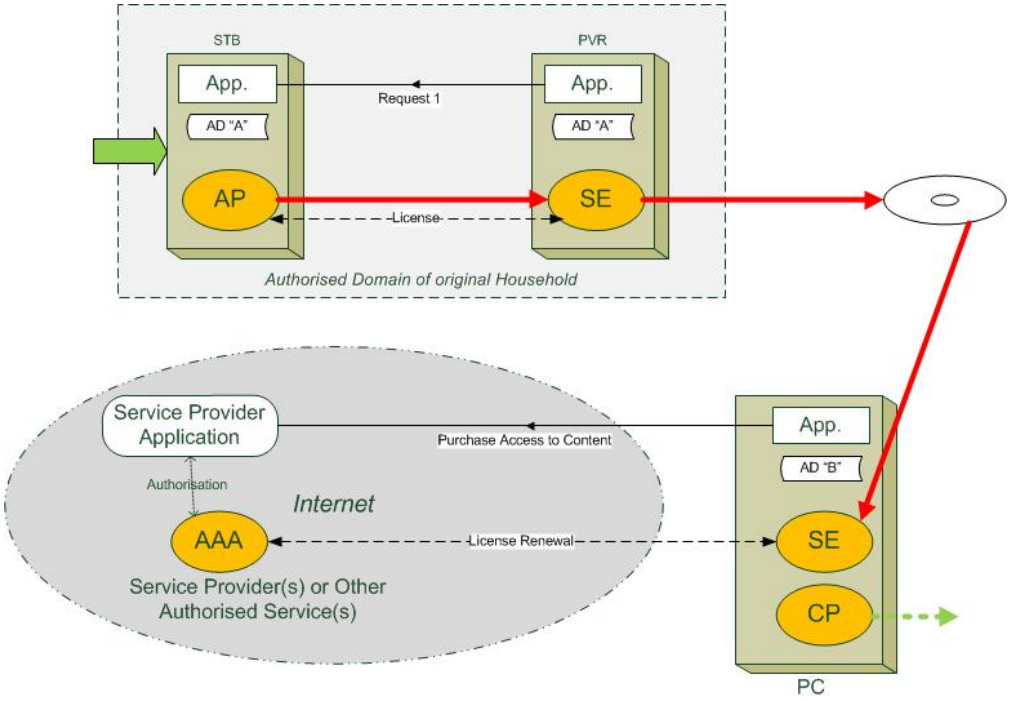

Figure 62: Superdistribution Operation - Removable Media

1) As in clause 5.6.3.2, the content is acquired and recorded by the PVR.

2) The user now makes an additional recording to a removable storage media.

3) The entire content item is written to the removable storage media, which in this case is a DVD, using the DVB File Format. The original content licences are both written to the file, protected by the AD secret.

NOTE: This is because there is no SAC available to communicate with removable storage media.

4) The user gives the DVD to a friend who attempts to play the content.

5) The Storage Entity of the PC starts to play the file from the DVD.

6) The first content licence cannot be used directly as it is protected by an unknown domain key. Therefore it is necessary to examine the Rights Issuer URL and to request a new licence with the correct AD binding.

7) The PC identifies the Rights Issuer URL and passes this to a suitable device application, which communicates with the service provider. A new playable licence is received automatically.

8) When the PC attempts to use the second content licence, it is unable to do so as it does not belong to the same AD.

9) The PC again checks the Rights Issuer URL (which is likely to be different from the first one) to request a playable licence for the main body of the file.

10) The service provider offers the consumer a way to gain the right to play the rest of the content. This may be by payment, advertising, registration, or any other business transaction, which is out of scope for CPCM.

11) The service provider notifies the AAA function which prepares a new content licence with the same USI, but with the AD identity of the new AD, as described in scenario 30, during which the Key Recovery Information field is used to obtain the correct content scrambling keys.

12) The AAA function sends the new content licence to the PC.

13) The PC is now able to play the whole content item directly from the DVD, or to copy it and share it with other devices within the AD.

This process can be repeated in the same way as the content is further re-distributed from the first user or subsequent users.

5.7 Scenario 34 - Hosted CPCM Service

5.7.1 Business Intent

This scenario covers content offered via a service that implements CPCM as a hosted function outside the user home, such as an internet based service. Unlike most CPCM scenarios, in this case content is acquired by an authorised service remote from, and not directly associated with, the home, but which itself includes a CPCM instance that belongs to the user's Authorised Domain.

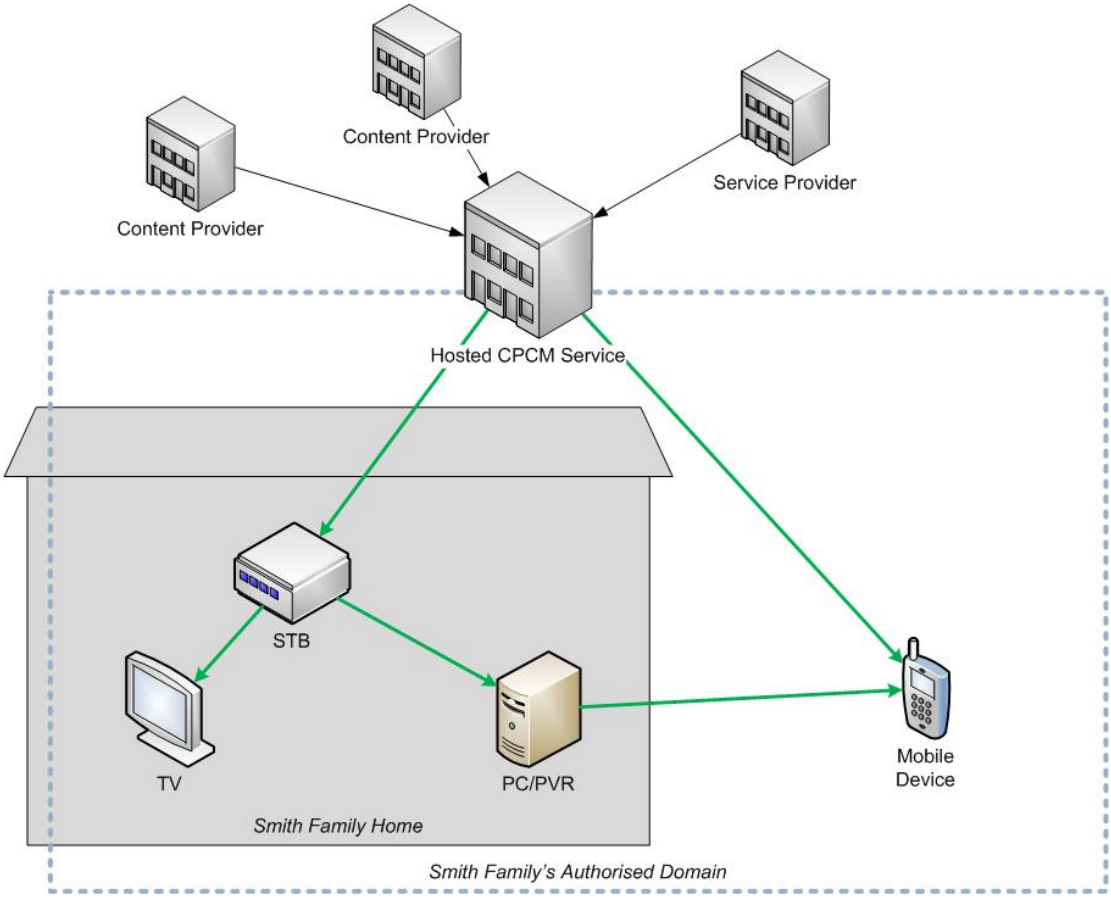

Figure 63: Hosted CPCM Service Content Flow

5.7.2 Usage State Information

This scenario is independent of all USI settings.

The C&R Regime will need to either avoid the use of, or provide some exceptions to, the use of local or geographic usage restrictions. Otherwise there is the risk that content marked as MLAD, VLAD, MGAD or VGAD will be unusable as it will be tied to the locality of the service provider data centre and will not be available in the user location, be it his home or a portable device.

An approach is for the C&R Regime to modify the use of proximity tests when sending content from the service to the consumer. This can be done by defining an additional proximity tool which automatically returns a successful check on the connection between the service and their registered device or devices.

5.7.3 CPCM System Operation

A Hosted CPCM system will operate as follows.

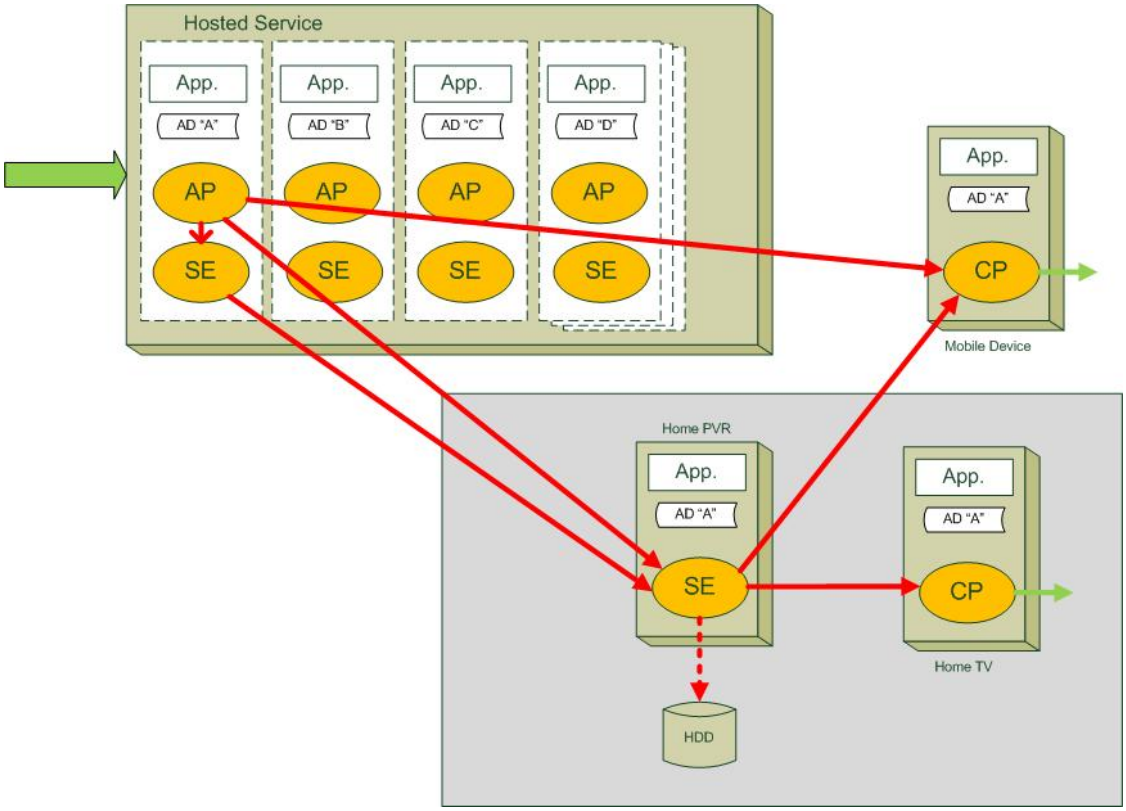

Figure 64: Hosted CPCM Service Operation

Each user making use of the service is assigned a dedicated CPCM instance within the service by means of unique AD identification. This instance cannot be shared with other users.

NOTE: The instance may be implemented as a record in a database of such instances, much like a bank account.

The hosted CPCM instance acts as AD controller. One or more of the user's CPCM Devices need to be configured to use this AD controller to make use of this service. Such devices would be able to function as Local Master for the AD (as described in TS 102 825-7 [i.8]). The definition of the special proximity test for the link between the service and the local master, combined with the use of standard proximity tests between the local master and device that wish to join the domain, will allow determination of proximity by association. Thus devices joining this type of remotely managed domain can still be treated as local upon joining, rather than the more restrictive remote joining. Such arrangements need to be approved by the C&R Regime.

5.7.3.1 Hosted CPCM Service

The Hosted CPCM Service implements the following functions:

- Authorised Domain Management.
- Acquisition Point.

It may additionally implement the following functions:

- Storage Entity, to enable network PVR functionality within the CPCM AD.
- Processing Entity, to enable manipulation of CPCM content.
- Export Point, to enable export of CPCM content via other technologies devices implementing trusted content protection systems, as defined by the relevant C&R Regime.

5.7.3.2 Client CPCM devices for the Hosted CPCM Service

A Client device for the Hosted CPCM Service implements the following functions:

- Authorised Domain Management, including at a minimum:
  - Domain membership.
  - A configuration mechanism to determine and set the address of the remote Domain Controller. This may be manual, automatic, or preconfigured.
  - Support for communicating with a remote Domain Controller.
  - Local Master to communicate between the Hosted Service and local CPCM Devices which are not configured as clients of the Hosted CPCM Service.
- Proximity tools.

It may additionally implement the following functions:

- Acquisition Point for acquisition of content from sources other than the Hosted CPCM Service.
- Storage Entity.
- Processing Entity.
- Consumption Point.
- Export Point.

Each CPCM Device configured as a client of the Hosted Service needs to join the AD governed by the hosted CPCM instance.

If the client device also implements one or more other content protection protocols, it may also join a native domain for the other protocol at the same time. Thus the device is known to be a member of the same user no matter which protocol is used for a given content item or transaction.

5.7.3.3 Non-Client CPCM devices

Devices that implement CPCM but are not fully equipped to act as described in clause 5.7.3.2 can still join the hosted AD via the Local Master function of the client and use content obtained from it, as long as they comply with the C&R Regime that governs the Hosted CPCM Service.

A non-client device that successfully joins the hosted AD may also be able to obtain content directly from the Hosted CPCM Service, as long as it is able to discover and download or stream the content, using standard CPCM protocols.

5.7.3.4 Sequence of operation

1) The user registers with the Hosted CPCM Service. This process is out of scope for CPCM.

   NOTE 1: This may be by visiting a website or other interactive application, or it may be preconfigured in a device when it is purchased.

2) The Hosted CPCM Service configures the associated device with the address of the Domain Controller, which resides within the logical CPCM instance assigned to this specific user.

3) The device joins the hosted AD using conventional CPCM ADM protocols. Once this is completed, the device will act as a Local Master for this AD within the home network.

4) Other devices join the new Authorised Domain via the Local Master device, as described in the CPCM ADM specification.

   NOTE 2: The Hosted CPCM Service obtains content from various authorised sources. This may be as a result of purchase, capture off air, or by other commercial means. Content is stored securely, along with the keys needed to descramble it.

   NOTE 3: The Hosted CPCM Service may choose to optimise content storage by using the CPCM local scrambling algorithm (LSA), as defined in CPCM specifications, with the same content descrambling key for all users. However, this approach will need to satisfy the CPCM C&R Regime, and the C&R Regime of the content source, that this does not reduce system security. Alternatively, the service may protect the content with their own encryption technology and re-scramble using LSA with individual scrambling keys for each user at the time of content delivery.

5) The service now advertises the content as being available and bound to the Authorised Domain.

6) When requested by the user, or based on previously configured delivery settings, the protected content is delivered to the user's device.

   NOTE 4: In some cases the service may block the delivery of content if the user does not have a current authorisation. In other cases the content may be delivered in expectation that the user will be authorised at a later time. In any case, no content item may be played without a valid content licence.

7) Once the user is authorised, the scrambling key for each content item is protected using the authorised domain key in a CPCM content licence and delivered to the user.

   NOTE 5: The content licence may be delivered with the content item, or at any time when requested by the user device, or pushed to the device by the service. As soon as both the content licence and the start of the content have been received, the receiving device can begin playing. There is no need to wait for the complete content item to be delivered before playback can begin.

List of Figures

List of Tables

History

Document history		
V1.1.1	March 2011	Publication