3GPP TR 33.844 V11.0.0 (2012-12)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security Study on IP Multimedia Subsystem (IMS) based peer-to-peer content distribution services;
Stage 2
(Release 11)

Keywords
3GPP, Security, IMS, P2P

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword 4
1 Scope 5
2 References 5
3 Definitions and abbreviations 5
3.1 Definitions 5
3.2 Abbreviations 5
4 System Architecture 5
4.1 Alternative Architecture 1 5
4.2 Alternative Architecture 2 6
4.3 Alternative Architecture 3 6
4.4 Alternative Architecture 4 7
4.5 Alternative Architecture 5 7
4.6 Security Architecture 8
5 Security threats 9
5.1 User Identity Privacy 9
5.2 Eavesdropping 9
5.3 Adversarial content announcement 9
5.4 Content Tampering and Replacement (Trojan Horse) 9
6 Security Requirements 9
6.1 Security requirement for User Identity Privacy 9
6.2 Security requirement for eavesdropping 9
6.3 Security requirement for adversarial content announcement 10
6.4 Security requirement for Content Tampering and Replacement (Trojan Horse) 10
7 Security Solutions 10
7.1 Security protection to prevent eavesdropping 10
7.2 Security solution against adversarial content announcement 12
7.3 Security protection on user identity privacy 12
7.4 Security protection against content tampering and replacement 13
8 Conclusions 15
Annex A: Change history 16

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document provides an analysis of security aspects of the enhancements of IMS to support Peer-to-Peer Content Distribution Services based on the requirements studied in TR 22.906 [2] and architecture studied in TR 23.844 [3]. This analysis focuses on both the network and terminal and includes security threats, requirements and solutions.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 22.906: "Study on IMS based peer-to-peer content distribution services".

[3] 3GPP TR 23.844: "Feasibility study on IP Multimedia Subsystem (IMS) based peer-to-peer content distribution services; Stage 2".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] apply.

4 System Architecture

4.1 Alternative Architecture 1

TR 23.844 [3] has introduced candidate architecture about signalling between user peer and other peers not traversing IMS core. The architecture is as follows:

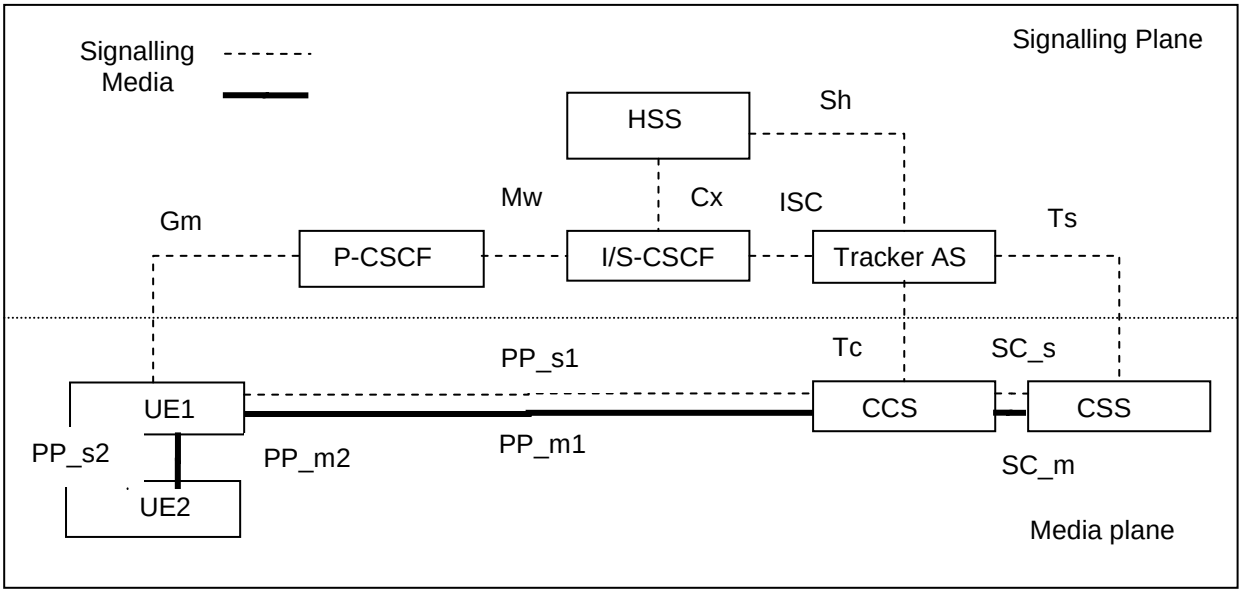

Figure 1: System Architecture Alternative 1 - signalling between user peer and other peers not traversing IMS core

4.2 Alternative Architecture 2

TR 23.844 [3] has introduced candidate architecture in which signalling between user peer and other peers traverses IMS core. The architecture is as follows:

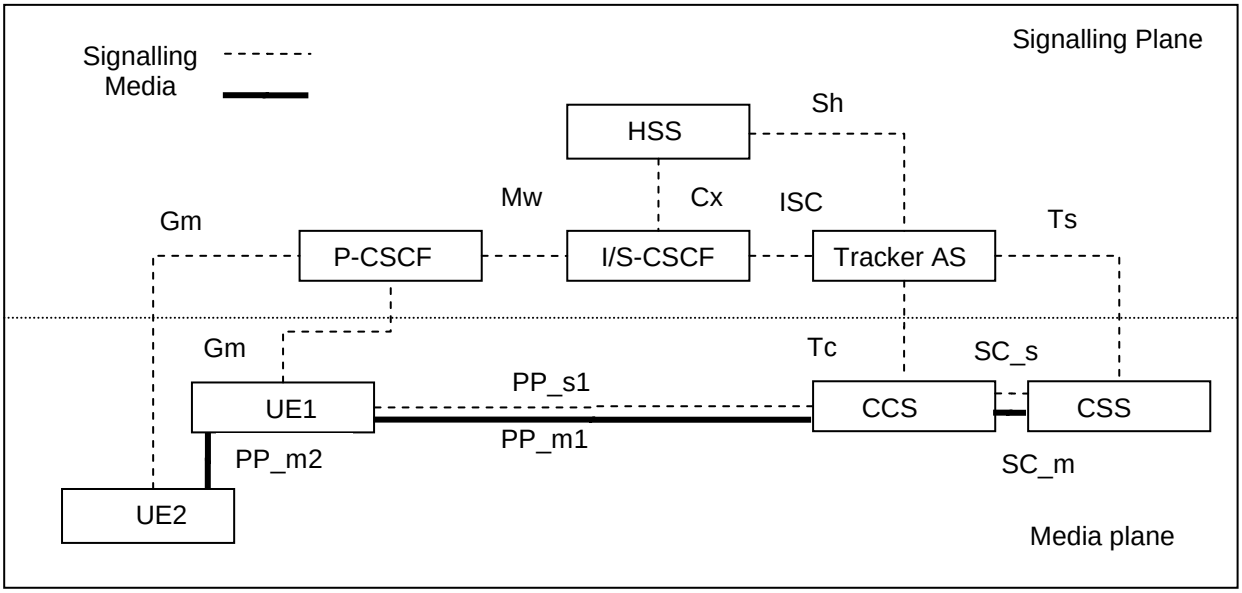

Figure 2: System Architecture Alternative 2 - signalling between user peer and other peers traversing IMS core

4.3 Alternative Architecture 3

TR 23.844 [3] has introduced candidate architecture that is using direct interface for signalling between user peer and Tracker AS. The architecture is as follows:

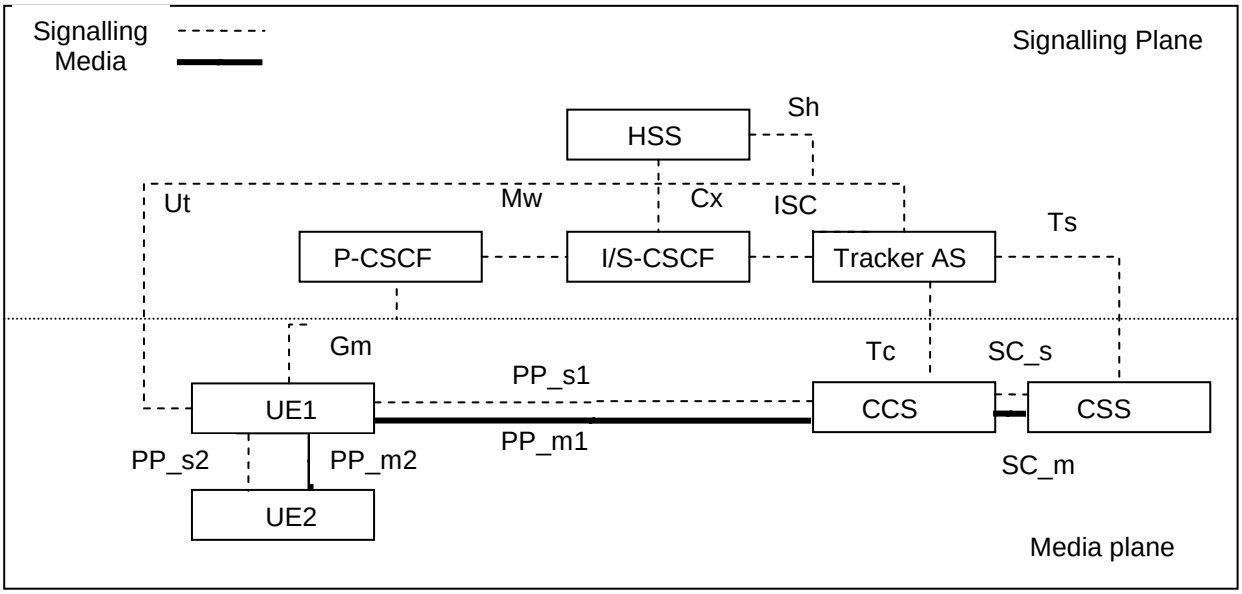

Figure 3: System Architecture Alternative 3 - direct interface for signalling between user peer and Tracker AS

4.4 Alternative Architecture 4

TR 23.844 [3] has introduced candidate architecture in which IMS P2P CDS is used in conjunction with CDN. The architecture is as follows:

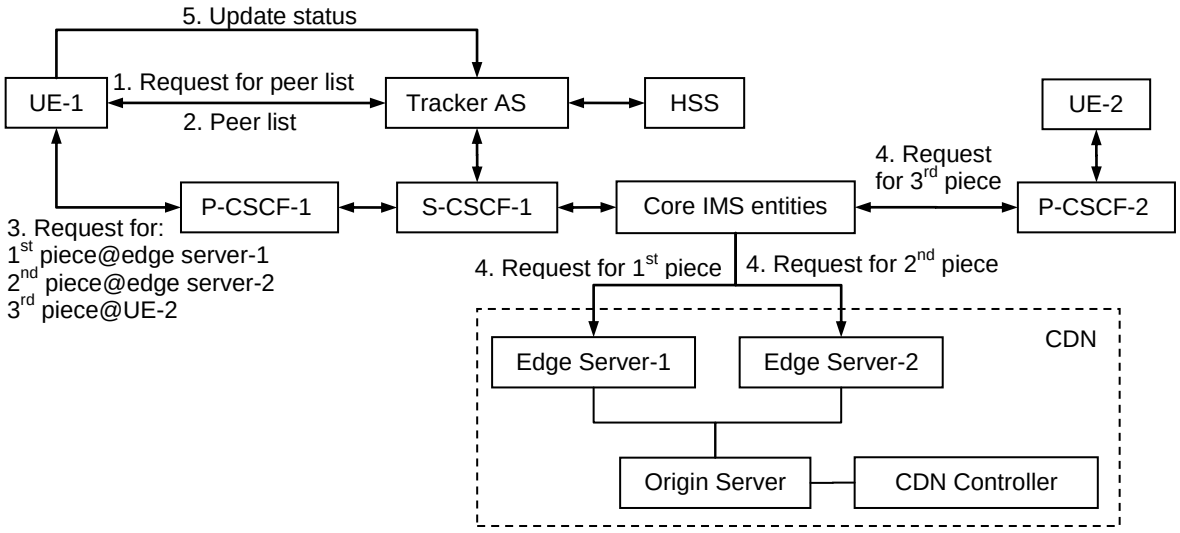

Figure 4: System Architecture Alternative 4 - IMS P2P CDS used in conjunction with CDN

4.5 Alternative Architecture 5

TR 23.844 [3] has introduced candidate architecture that includes ALTO(Application Layer Traffic Optimization) server in IMS P2P CDS. The architecture is as follows:

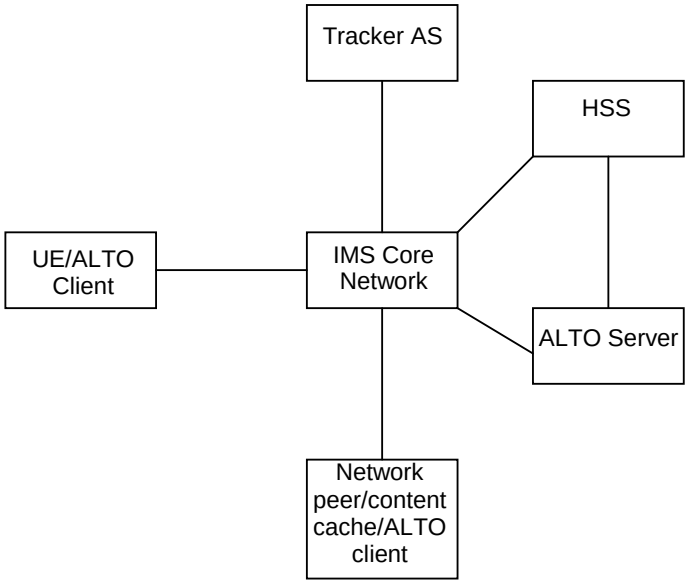

Figure 5: System Architecture Alternative 5- ALTO server in IMS P2P CDS

4.6 Security Architecture

All architectures contain three domains:

1. IMS core network domain: which is used to provide basic IMS P2P management service
2. Content service domain: which is used to provide original content for users and content distribution management
3. User(peer) domain: which accesses through IMS core network, and gets content from content service provider or other users under content service provider's control.

Based on these 3 domains, the security architecture can be divided into 3 security interfaces. Furthermore, as user can get content from other users, so there should be an addition security interface to indicate the security between users.

As a result, an IMS P2P security architecture described in Figure 6 is introduced.

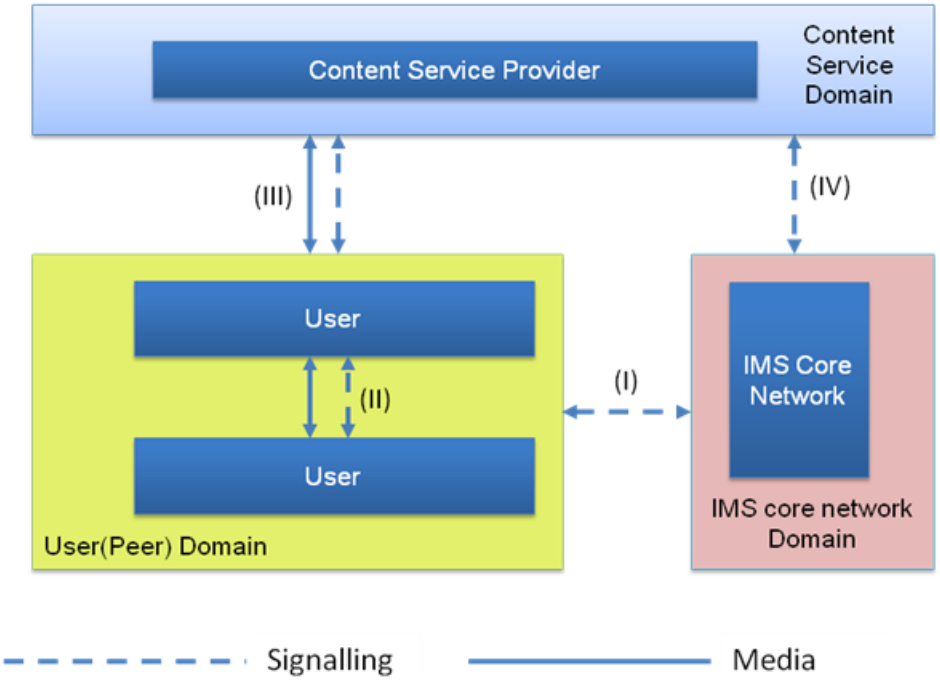

Figure 6: Security Architecture for IMS P2P

There are four security interfaces defined for IMS P2P:

I) Security about user access through IMS.

II) Security for User Peer to Peer communication interface.

III) Security between UE and content service provider.

IV) Security between IMS core network and content service provider

NOTE: The term user peer is used for UE peer.

5 Security threats

5.1 User Identity Privacy

In TR 23.844 [3] it is described that "The system shall support a mechanism to provide to user peers an optimal selection of user peers and network peers for obtaining requested media content from, based upon metrics including: network location information such as, proximity of peers, access type used by peers, peer IP addresses (including IPv4 and/or IPv6 types), and peer identities" And in Alt1 architecture, a peer can get this list from Tracker AS, as shown in clause 6.1.4.2.1 (Content Delivery Establishment Procedure) of TR 23.844 [3].

In this procedure, one user peer can get another user peer's identity. If the identity is permanent like IMSI, the user IMSI privacy protection is breached.

5.2 Eavesdropping

Two legitimate users may share content using IMS based P2P Content Distribution service. A malicious user may eavesdrop on the communication and obtain the content on PP_m2 interface in Alternative 1 architecture model. A malicious user may also eavesdrop on the communication and obtain the content on PP_m1 interface in Alternative 1 architecture when CCS shares content with a legitimate user.

5.3 Adversarial content announcement

In this attack a legitimate user announces a content list through PP_s2 or PP_s1 interface that she/he intends to provide to other peers, but this user does not actually possess the content.

5.4 Content Tampering and Replacement (Trojan Horse)

A legitimate user inserts into the content a malicious piece of software or replaces the content completely with something else and shares the replaced content with others. The other peers would obtain wrong or malicious content from PP_m2 interface.

6 Security Requirements

6.1 Security requirement for User Identity Privacy

The system shall not reveal permanent identity of peers when sharing peer lists containing identities.

6.2 Security requirement for eavesdropping

It shall be possible to protect content and associated metadata from eavesdropping on PP_m1 and PP_m2 interface in Alternative 1 architecture model.

6.3 Security requirement for adversarial content announcement

The network (e.g. Tracker AS) shall have the ability to verify whether the user truthfully announces content resources.

6.4 Security requirement for Content Tampering and Replacement (Trojan Horse)

- The network (e.g. CCS/Tracker AS) shall have the ability to verify whether the content shared by a legitimate user is tampered with.
- The receiver peer shall have the ability to verify whether the content shared by a legitimate user is tampered with.

7 Security Solutions

7.1 Security protection to prevent eavesdropping

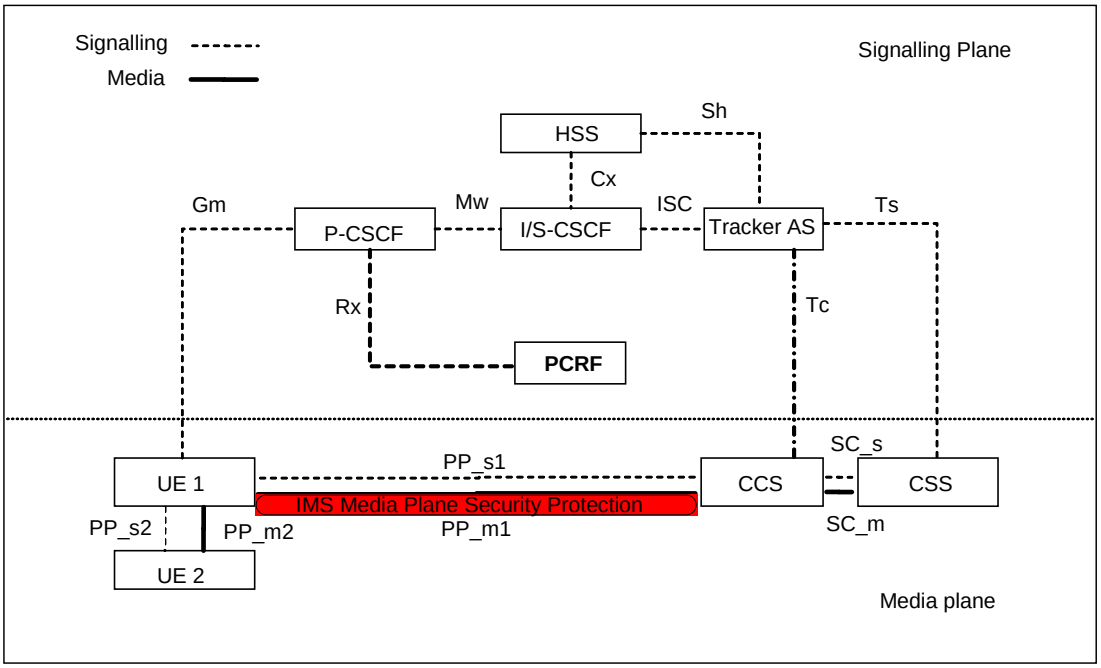

Figure 7: Session encryption protection between UE and CCS

Interface pp_m1 is the data interface between UE peer and cache server. To prevent eavesdropping attack on this interface, the simplest way is to provide encryption protection to data transportation. In this way, IMS media plane security can be applied as following. In IMS media plane security mechanism SDES, the encryption algorithm is defined as AES, and the key length is 128 bits.

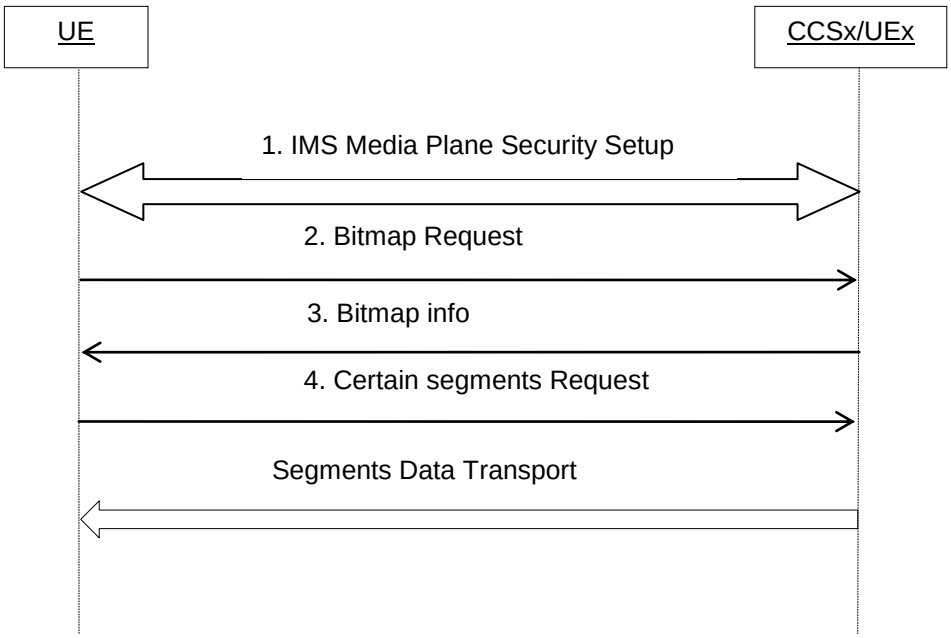

Figure 8: Message flow for session encryption protection

1. UE and CCSx/UEx establish security protection by using IMS Media Plane Security procedure.

2-4 UE get content information from CCSx/UEx as SA2 procedure described.

But it should be designed carefully on encryption algorithm, considering the huge volume of data.

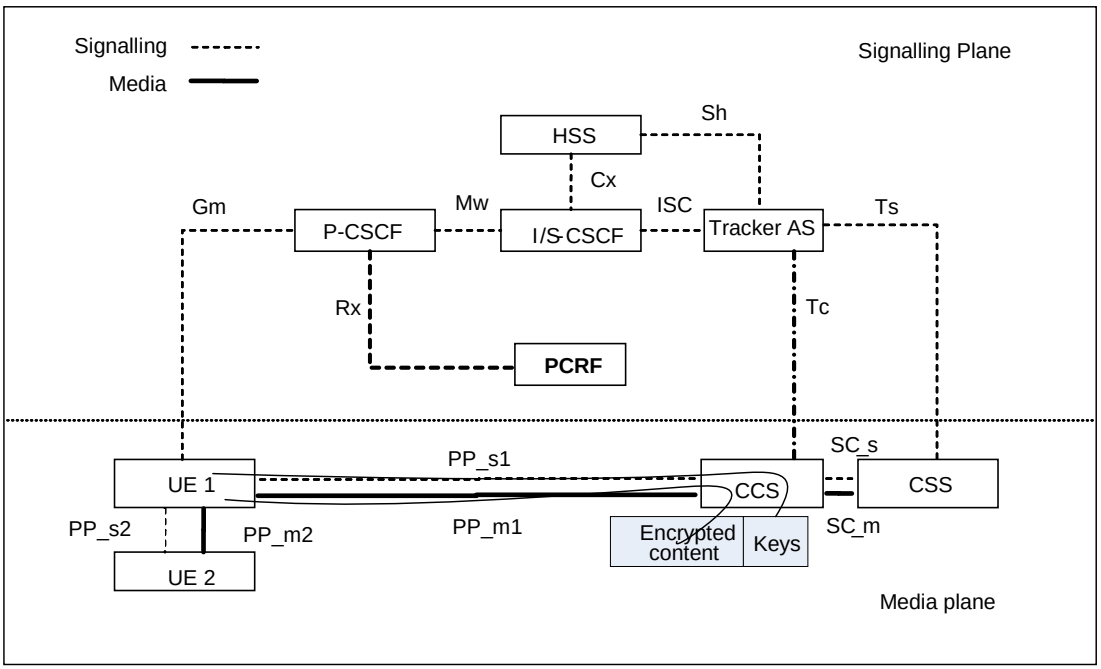

Figure 9: Key provisioning between UE and CCS

Another updated solution is to make pre-encryption on the data before it is issued, which is like DRM mechanism. The content is encrypted before it is imported to IMS P2P system, and the key would be stored in cache server by out-of-band methods. When UE peer wants to get content from cache server, the key related to such content can be sent from cache server to UE peer through IMS core network as following.

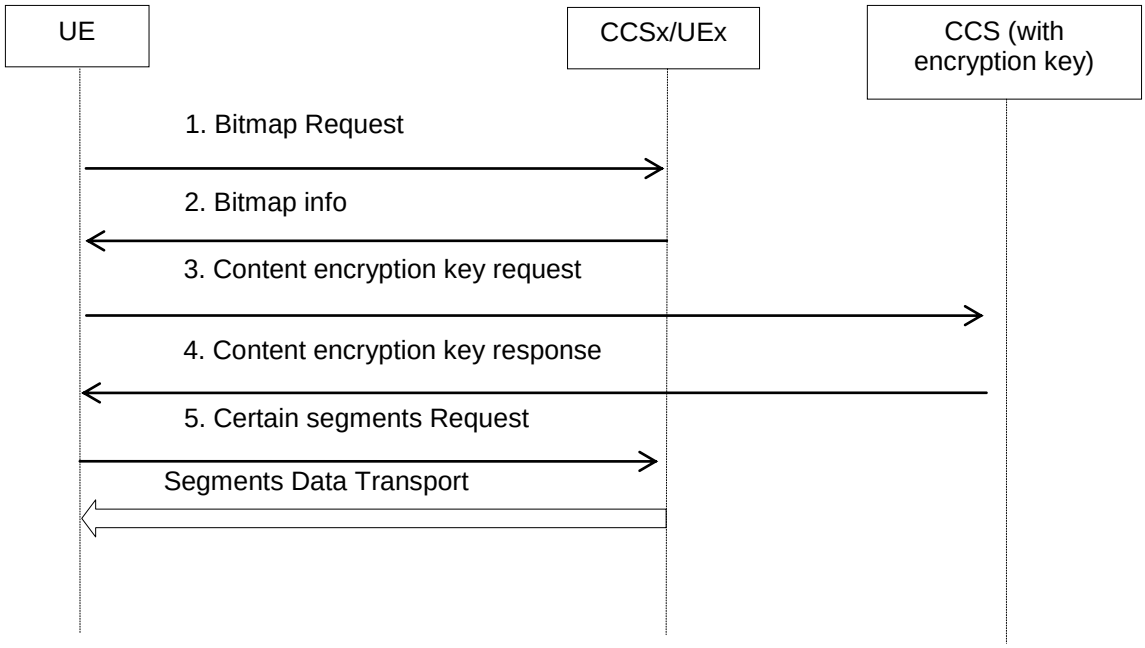

Figure 10: Message flow for Key provisioning

1-2 UE gets bitmap from CCSx/UEx for downloading preparation.

3. UE sends content encryption key request to the CCS with encryption key through PP_s1 interface based on bitmap info.

4. CCS sends content encryption key response to the UE.

5. UE requires contents from CCSx/UEx.

Interface pp_m2 is the data interface between UE peers. So the same mechanism mentioned above can be used in this interface, too.

7.2 Security solution against adversarial content announcement

As TR 23.844 described, the Tracker AS records and maintains the index of contents/content segments and where the contents/contents segments are cached. As a result, Tracker AS has the ability to know the real mapping information between segments and peers.

Under this fact, security solution against adversarial content announcement can be made in two ways:

1) The first way is to forbid UE announcement. When one peer who wants to download content, it should only connect to Tracker AS to get segment information, then the peer can get content from network peer or other user peers based on the segment information.

NOTE: It will increase Tracker AS burden and would cause DoS attack.

2) The second way is to allow UE announcement, but Tracker AS will check whether the content announcement is correct or not. To reduce the Tracker AS burden, the checking procedure can be executed periodically. Considering efficiency and cost, checking cycle should be carefully designed based on network deployment scale, amount of users, and data transfer frequency.

7.3 Security protection on user identity privacy

UE should generate an temporary peer ID when it connect to IMS P2P system. UE should bind its temporary peer ID and content information together and send it to Tracker AS with its permanent ID.

When Tracker AS received such update information, it should update bitmap information about specific content by using a cluster like {permanent ID, temporary ID, content information}. When some other peers want to get peer list

from Tracker AS, Tracker AS should send response with temporary ID instead of permanent ID. After that, the other peers can communicate with this peer by using its temporary ID.

The detail procedure is as following:

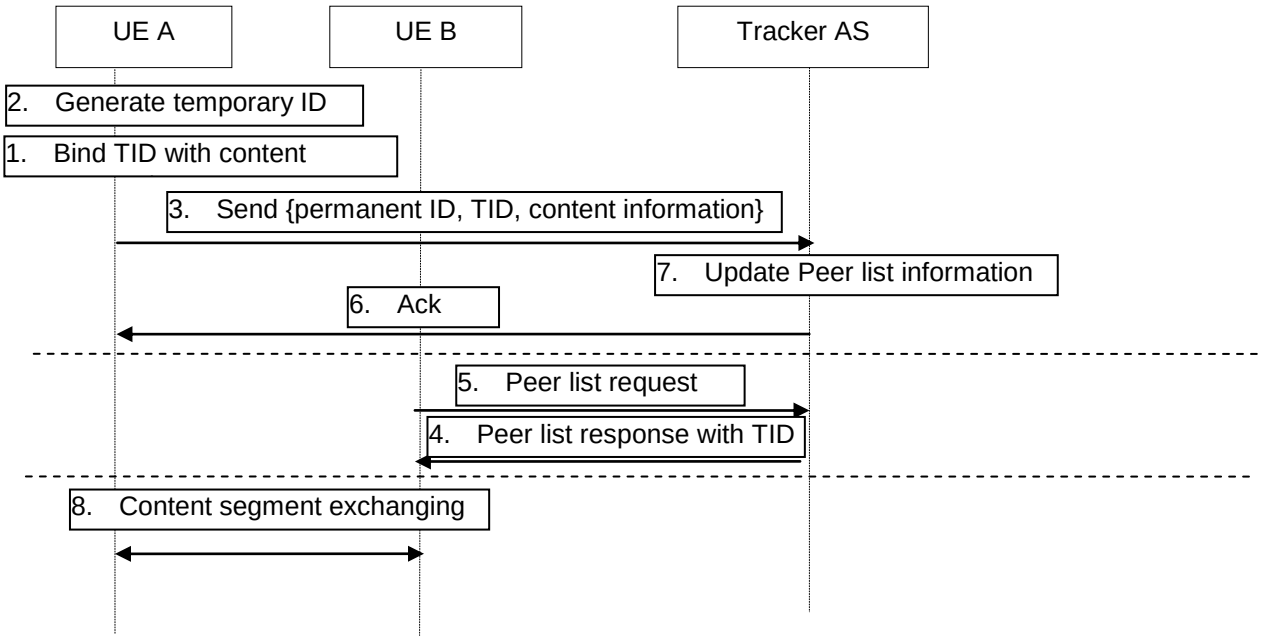

Figure 11

1. When UE A wants to update its own content information to Tracker AS, it generate an temporary ID first.
2. UE A binds TID with content segment.
3. It sends {permanent ID, TID, content information} to Tracker AS.
4. Tracker AS will update Peer list information based on received message.
5. Tracker AS send back an acknowledgment message to UE A.
6. When another UE B wants to get specific content, it should send peer list request to Tracker AS.
7. Tracker AS will send peer list response indexed by using TID to UE B.
8. UE B will setup communication with UE A by using its TID. Then they exchange content segment for each other.

7.4 Security protection against content tampering and replacement

When content is provisioned from provider into IMS P2P CDS system, IMS P2P CDS system will break content into several segments. Then these segments will be used to calculate their Hash values through some integrity algorithm. The Hash values could be stored in network and transferred to UE peers through PP_s1 interface when a integrity check request is received.

The detail procedure is as following:

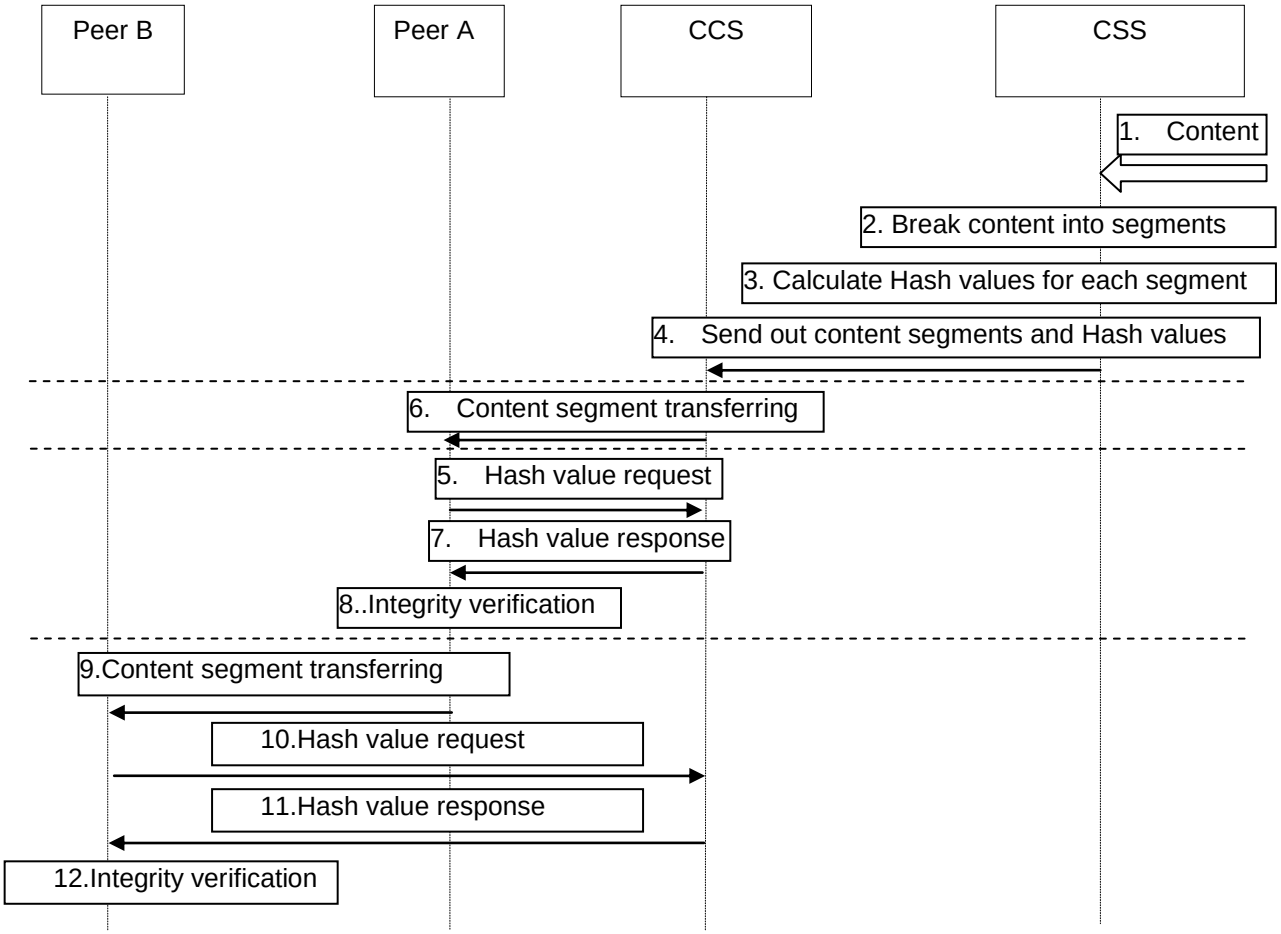

Figure 13

1. IMS P2P CDS system get content from provider. The content will be import to CSS.
2. CSS break content into several segments for P2P transferring preparation.
3. CSS calculate Hash value for each segment.
4. CSS sends content segments and Hash values to CCS. After that, the transferring preparation is finished.
5. When UE (named peer A) uses IMS P2P CDS, it can get content segment from CCS.
6. If peer A wants to verify the content integrity, it should send Hash values request to CCS through PP_s1 interface.

NOTE: PP_s1 interface is involved to protect Hash values value from tampering.

7. CCS will send Hash value response back through PP_s1 interface.
8. Peer A can use Hash values to verify the content segment integrity.
9. If the another UE (named peer B) is involved, it can get content segment from peer A.
10. If peer B wants to verify the content integrity, it should send Hash values request to CCS through PP_s1 interface.
11. CCS will send Hash value response back through PP_s1 interface to peer B.
12. Peer B can use Hash values to verify integrity of the content segment from Peer A.

8 Conclusions

This study has analyzed the security threats for the IMS based Peer-to-Peer Content Distribution Services based on SA1's requirement and SA2's architecture. IMS P2P CDS should follow the security requirements in clause 4 to prevent such threats.

What is more, specific security solutions are proposed to fulfil these security requirements. The study has concluded without any firm recommendations on a specific solution.

Lastly, security study is based on SA2 current architecture study; it would be possible to study further if SA2 wants to make future discussion on this subject.

Annex A:
Change history

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New
2012-11-09						Presentation to SA for approval	-	1.0.0
2012-12	SP-58	SP-120853	-	-	-	MCC Update	1.0.0	2.0.0
2012-12	SP-58						2.0.0	11.0.0