PacketCable™ 2.0

HSS Technical Report

PKT-TR-HSS-V01-060914

RELEASED

Notice

Document Status Sheet

Document Control Number:	PKT-TR-HSS-V01-060914
Document Title:	HSS Technical Report
Revision History:	V01 – Released 09/14/06
Date:	September 14, 2006

Abstract

PacketCable is a CableLabs specification effort designed to extend cable's real-time IP communication service architecture and to accelerate the convergence of voice, video, data, and mobility technologies.

This technical report describes the Home Subscriber Server (HSS) requirements to support the PacketCable architecture, applications and services. It contains the following information:

- The reference points related to the HSS.
- Enhancements to the HSS as defined by the 3rd Generation Partnership Project (3GPP) IP Multimedia Subsystem (IMS) Release 6 (R6) specifications to support PacketCable requirements.
- For each of the necessary enhancements, the technical requirements for PacketCable along with the list of impacted components and IMS delta specifications is provided.

Contents

Figures

Tables

This page left blank intentionally.

1 SCOPE

1.1 Introduction and Purpose

The purpose of this technical report is to provide an overview of the reference points for the Home Subscriber Server (HSS) and related components. In addition, this technical report describes the specific HSS related enhancements to the 3GPP IMS Release 6 specifications to support the PacketCable requirements.

1.2 Document Scope

The PacketCable Architecture Framework TR [ARCH TR FRM] describes the overall document organization plan for PacketCable. Since the PacketCable HSS is closely aligned with 3GPP Release 6 IMS, the PacketCable HSS normative requirements are defined in the delta specifications, which are enhanced versions of 3GPP specifications and accommodate cable-specific requirements.

The PacketCable HSS requirements are documented in the following IMS Delta specifications: [PKT 23.008], [PKT 29.229], [PKT 29.228] and [PKT 29.109].

Note 1: The IMS Delta specifications listed above may also contain requirements related to other portions of the PacketCable architecture.

Note 2: In the presence of any contradictions, the PacketCable specifications take precedence over this technical report.

1.2.1 Relationship to PacketCable Features and Services

This Technical Report and its associated IMS delta specifications serve as a base for the handling of subscriber related data within PacketCable. This foundation provides for the support of a wide variety of communication services, ranging from legacy telephony features to new and enhanced communication applications and services.

This foundation is service independent and, therefore, requirements specific to each PacketCable service and feature are out-of-scope for this document, and defined separately in PacketCable service specifications. Any requirements that are deemed to be non-service specific are included and are addressed within this document.

1.2.2 Relationship to Other PacketCable Documents

The PacketCable HSS specifications together define the generic HSS requirements for the following general capabilities:

- Identification Handling
- User Profile Management (Cx and non-Transparent Data)
- Application Specific User Profile Management (Transparent Data)
- Service Profile Provisioning
- Call/Session Establishment Support
- User Security Support
- Registration State Management

The PacketCable Architecture uses these general capabilities, and, to fulfill service specific requirements, may document additional capabilities in PacketCable service specifications.

1.3 Document Organization

Section 5 of this document describes the PacketCable HSS architecture, including the main functional elements and reference points.

Section 6 of this document describes the PacketCable HSS enhancements to the 3GPP Release 6 IMS specifications motivated by the PacketCable architecture or service requirements.

Appendices in this document summarize requirements considered that do not impact the HSS.

2 REFERENCES

2.1 Informative References

This Technical Report uses the following informative references.

[ARCH TR FRM] PacketCable Architecture Framework Technical Report PKT-TR-ARCH-FRM-V01-060406, April 6, 2006, Cable Laboratories, Inc.

[E.164] ITU-T Recommendation E.164, The international public telecommunication numbering plan, February 2005.

[ID DIAMETER SIP] IETF draft, Diameter Session Initiation Protocol (SIP) Application, draft-ietf-aaa-diameter-sip-app-12, April 2006.

[ID GRUU] IETF draft, Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP), draft-ietf-sip-gruu-10, July 2006.

[PKT 23.008] PacketCable Organization of Subscriber Data Specification 3GPP TS 23.008, PKT-SP-23.008-I01-060914, September 14, 2006, Cable Laboratories, Inc.

[PKT 29.109] PacketCable Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3 Specification 3GPP TS 29.109, PKT-SP-29.109-I01-060914, September 14, 2006, Cable Laboratories, Inc.

[PKT 29.228] PacketCable Cx and Dx Interfaces Specification 3GPP TS 29.288, PKT-SP-29.228-I01-060914, September 14, 2006, Cable Laboratories, Inc.

[PKT 29.229] PacketCable Cx/Dx Interfaces based on Diameter Protocol Specification 3GPP TS 29.229, PKT-SP-29.229-I01-060914, September 14, 2006, Cable Laboratories, Inc.

[PKT 33.220] PacketCable Generic Bootstrapping Architecture Specification 3GPP TS 33.220 PKT-SP-33.220-I01-060406, April 4, 2006, Cable Laboratories, Inc.

[RFC 2617] IETF RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, June 1999.

[RFC 3261] IETF RFC 3261, SIP: Session Initiation Protocol, June 2002.

[RFC 3310] IETF RFC 3310, Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA), September 2002.

[RFC 3966] IETF RFC 3966, The tel URI for Telephone Numbers, December 2004.

[SEC TR] PacketCable Security Technical Report, PKT-TR-SEC-V01-060406, April 6, 2006, Cable Laboratories, Inc.

[SIP TR] PacketCable SIP Signaling Technical Report, PKT-TR-SIP-V01-060406, April 6, 2006, Cable Laboratories, Inc.

2.1 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
  Phone 303-661-9100; Fax 303-661-9199; Internet: http://www.cablelabs.com
- Internet Engineering Task Force (IETF), Internet: http://www.ietf.org
- Third Generation Partnership Project (3GPP), Internet: http://www.3gpp.org
- Internet Assigned Number Authority (IANA), http://www.iana.org
- International Telecommunication Union (ITU), http://www.itu.int/home/index.html

3 TERMS AND DEFINITIONS

PacketCable Specifications and Technical Reports use the following terms and definitions:

E.164	An ITU-T Recommendation that defines the international public telecommunication numbering plan used in the PSTN and other data networks.
IMS Delta specifications	A suite of 3GPP IMS specifications modified to reflect cable-specific deltas necessary to comply with PacketCable.
Public User Identity	Used by any user for requesting communications to other users.
Server	A network element that receives requests in order to service them and sends back responses to those requests. Examples of servers are proxies, User Agent servers, redirect servers, and registrars.
Subscriber	An entity (comprising one or more users) that is engaged in a Subscription with a service provider.
Subscription	A contract for service(s) between a user and a service provider.
User	A person who, in the context of this document, uses a defined service or invokes a feature on a UE.

4 ABBREVIATIONS AND ACRONYMS

PacketCable Specifications and Technical Reports use the following abbreviations and acronyms:

3GPP	3rd Generation Partnership Project
AKA	Authentication and Key Agreement
AS	Application Server
AVP	Attribute-Value Pair
BSF	Bootstrapping Server Function
CNAM	Calling NAMe
CSCF	Call Session Control Function
GBA	Generic Bootstrapping Architecture
GUSS	GBA User Security Setting
HSS	Home Subscriber Server
I-CSCF	Interrogating Call Session Control Function
IM CN	IP Multimedia Core Network
IMPI	IM Private Identity
IMPU	IM Public Identity
ISIM	IMS SIM
MAA	Multimedia-Auth-Answer
MAR	Multimedia-Auth-Request
P-CSCF	Proxy Call Session Control Function
PACM	Provisioning, Activation, Configuration, and Management
S-CSCF	Serving Call Session Control Function
SAA	Server-Assignment-Answer
SAR	Server-Assignment-Request
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
UAR	User-Authorization-Request
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
XML	Extensible Markup Language

5 PACKETCABLE HOME SUBSCRIBER SERVER (HSS)

The Home Subscriber Server (HSS) is the master database containing the subscription related information for a particular user. There may be one or more HSSs in the network. When multiple HSSs are in the network, a Subscription Locator Function (SLF) is used to locate the proper HSS.

5.1 PacketCable HSS Architecture and Reference Points

The reference points associated with the HSS are illustrated in Figure 1. These reference points are as defined in the 3GPP IMS, with appropriate enhancements identified by PacketCable.

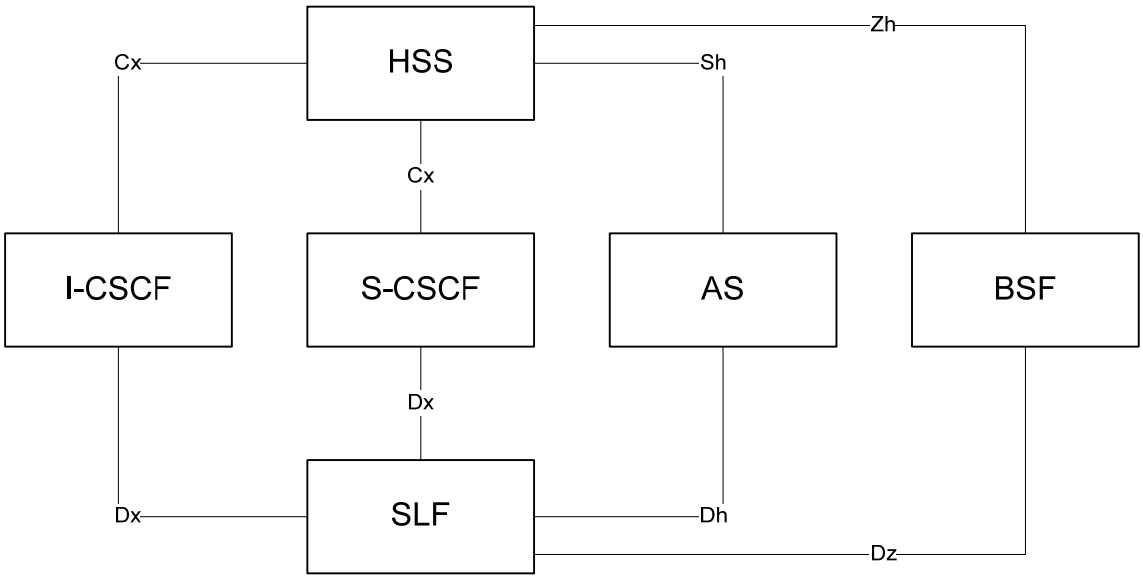

Figure 1 – HSS Reference Points

The HSS provides several logical functions needed by the various entities throughout the network in order to support session handling. Here is a list of some of the logical functions provided by the HSS:

- Registration State Management: This function supports the management of the user's registration state.
- Session Establishment Support: The HSS supports the session establishment procedures in the IP Multimedia Core Network (IM CN) subsystem. For terminating traffic, it provides information on which session control entity currently hosts the user.
- User Security Information Generation: The architecture supports the storage and generation of User security credentials and parameters required for authentication. This task may be handled by the HSS or other elements in the network depending on the authentication method and network architecture being used.
- User Security Support: The HSS supports the authentication procedures to access the IM CN subsystem services by storing the generated data for authentication, integrity, and ciphering, and by providing these data to the appropriate entity in the CN.
- User Identification Handling: The HSS provides the appropriate relations among all the identifiers that uniquely determine the user in the system (private identity and public identities for IM CN subsystem).

- Access Authorization: The HSS authorizes the user for access when requested by the Call Session Control Function (CSCF) by checking that the user is allowed to roam in a given visited network.
- Service Authorization Support: The HSS provides basic authorization for terminating call/session establishment and service invocation. The HSS updates the appropriate serving entities (i.e., CSCF) with the relevant information related to the services to be provided to the user.
- Service Profile Provisioning Support: The HSS provides access to the service profile data for use within the IM CN subsystem.

5.1.1 HSS Functional Components

5.1.1.1 Home Subscriber Server (HSS)

The HSS is the master database for a given user. It is the entity containing the subscription-related information to support the network entities managing sessions.

A Home Network may contain one or more HSSs depending on the number of subscribers, the capacity of the network elements, and the organization of the network.

The HSS provides support to the call control servers in order to complete the routing/roaming procedures by solving authentication, authorization, naming/addressing resolution, location dependencies, etc.

The HSS is responsible for holding the following user related information:

- User Identification, Numbering and addressing information.
- User Security information: Network access control information for authentication and authorization.
- User Location information at inter-system level: the HSS supports the user registration, and stores inter-system location information, etc.
- User profile information.

The HSS may generate User Security information for mutual authentication, communication integrity check and ciphering, depending on the authentication mechanism and the chosen architecture being used.

5.1.1.2 Subscription Locator Function (SLF)

When more than one independently addressable HSS is utilized by a network operator, there is a need to associate a given subscriber with the HSS that contains the subscriber's data. This functionality is provided by the SLF, which is a Diameter redirect agent.

The SLF is:

- Queried by the Interrogating Call Session Control Function (I-CSCF) during the Registration and Session Setup to retrieve the address of the HSS that contains the subscriber specific data. Furthermore, the SLF is also queried by the S-CSCF during Registration.
- Queried by the AS in conjunction with the Sh interface operation to retrieve the address of the HSS that contains the subscriber specific data.
- Accessed via the Dx interface by the CSCF and via the Dh interface by the AS.

A single HSS environment can still be achieved when there are physically multiple HSSs by using techniques such as server farms or clustering. The SLF is not required when such techniques are used to provide a logical single HSS environment.

5.1.2 HSS Reference Points

The reference points depicted in Figure 1 are described in Table 1. All reference points are DIAMETER-based.

Table 1 - Call Signaling Reference Points

Reference Point	PacketCable Network Elements	Reference Point Description
Cx	I-CSCF - HSS S-CSCF - HSS	The Cx reference point supports information transfer between CSCF and HSS. The main procedures that require information transfer between CSCF and HSS are: • Procedures related to Serving CSCF assignment. • Procedures related to routing information retrieval from HSS to CSCF. • Procedures related to authorization (e.g., checking of roaming agreement). • Procedures related to authentication: transfer of security parameters of the subscriber between HSS and CSCF. • Procedures related to filter control: transfer of filter parameters of the subscriber from HSS to CSCF.
Dx	I-CSCF - SLF S-CSCF - SLF	This interface between CSCF and SLF is used to retrieve the address of the HSS which holds the subscription for a given user. This interface is not required in a single HSS environment. An example for a single HSS environment is a server farm architecture.
Sh	AS - HSS	The Application Server (SIP Application Server and/or the OSA Service Capability Server) may communicate to the HSS. The Sh interface is used for this purpose. The Sh interface is between the HSS and the "SIP Application Server" and between the HSS and the "OSA service capability server". The HSS is responsible for policing what information is provided to each individual Application Server. The Sh interface transports transparent data for service related data, user related information, etc. In this case, the term transparent implies that the exact representation of the information is not understood by the HSS or the protocol. The Sh interface also supports mechanisms for transfer of user related data stored in the HSS
Dh	AS - SLF	This interface between AS and SLF is used to retrieve the address of the HSS that holds the subscription for a given user. This interface is not required in a single HSS environment. An example for a single HSS environment is a server farm architecture.

Reference Point	PacketCable Network Elements	Reference Point Description
Zh	BSF - HSS	The reference point Zh used between the BSF and the HSS allows the BSF to fetch the required authentication information and all Generic Bootstrapping Architecture (GBA) user security settings from the HSS.
Dz	BSF - SLF	The reference point Dz used between the BSF and the SLF allows the BSF to obtain the name of the HSS containing the required subscriber specific data. This interface is not required in a single HSS environment. An example for a single HSS environment is a server farm architecture.

6 PACKETCABLE HSS ENHANCEMENTS

This section describes the areas in which PacketCable has made enhancements to the 3GPP IMS Release 6 HSS. Each subsection provides a description of the change and the requirement that motivated that change. Additionally, the affected components and reference points are described.

6.1 Support for SIP Digest

6.1.1 Support for SIP Digest in an IMS Network

6.1.1.1 Background

In the IMS architecture, the User Equipment (UE) contains a UICC (Universal Integrated Circuit Card) with an IM Service Identity Module (ISIM) application. The ISIM application is aware of one or more IM Private Identities (IMPIs) and associated credentials (keys) that are also provisioned in the HSS. These credentials are used during the registration process for authentication.

Authentication in IMS utilizes mechanisms defined in [RFC 3310], "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)". AKA is a 3GPP defined challenge response based mechanism that uses symmetric cryptography.

Since not all PacketCable UEs are expected to contain UICCs, alternate authentication mechanisms are needed. One such authentication mechanism is SIP-Digest, as specified in [RFC 3261], and is leveraged by PacketCable. SIP Digest is based on HTTP Digest [RFC 2617] and [ID DIAMETER SIP] defines a general architecture that allows a Diameter client to request authentication and authorization information from a Diameter Server for SIP-based services.

In [ID DIAMETER SIP], the role of the Server used for HTTP-Digest authentication (as specified in [RFC 2617]) is taken on by both the SIP-Server and Diameter Server (in the IMS, the S-CSCF fulfills the role of a SIP-Server and the HSS fulfills the role of a Diameter Server).

Support for SIP Digest in a PacketCable network requires determination of the network elements responsible for:

- Generation of the nonce.
- Authentication of the User.

The draft [ID DIAMETER SIP] provides multiple options with regards to which network elements can be responsible for the generation of the nonce and performs the authentication of the user. However, this version of the document is based on the following:

- Nonce Generated in the SIP-Server (S-CSCF), SIP-Server (S-CSCF) authenticates the user.

Note: In this version of the document, the only algorithm parameter supported is "MD5" for the Digest-Algorithm AVP.

6.1.1.2 Nonce Generated in the S-CSCF, S-CSCF Authenticates the User

This option aligns closely with the existing messaging sequence used for IMS AKA. The S-CSCF still acts as the Authenticator, but the role of the Authentication Service is split between the HSS and the S-CSCF. Further, this option does not incur an extra round-trip between the S-CSCF and HSS.

Figure 2 shows the message flow related to this option.

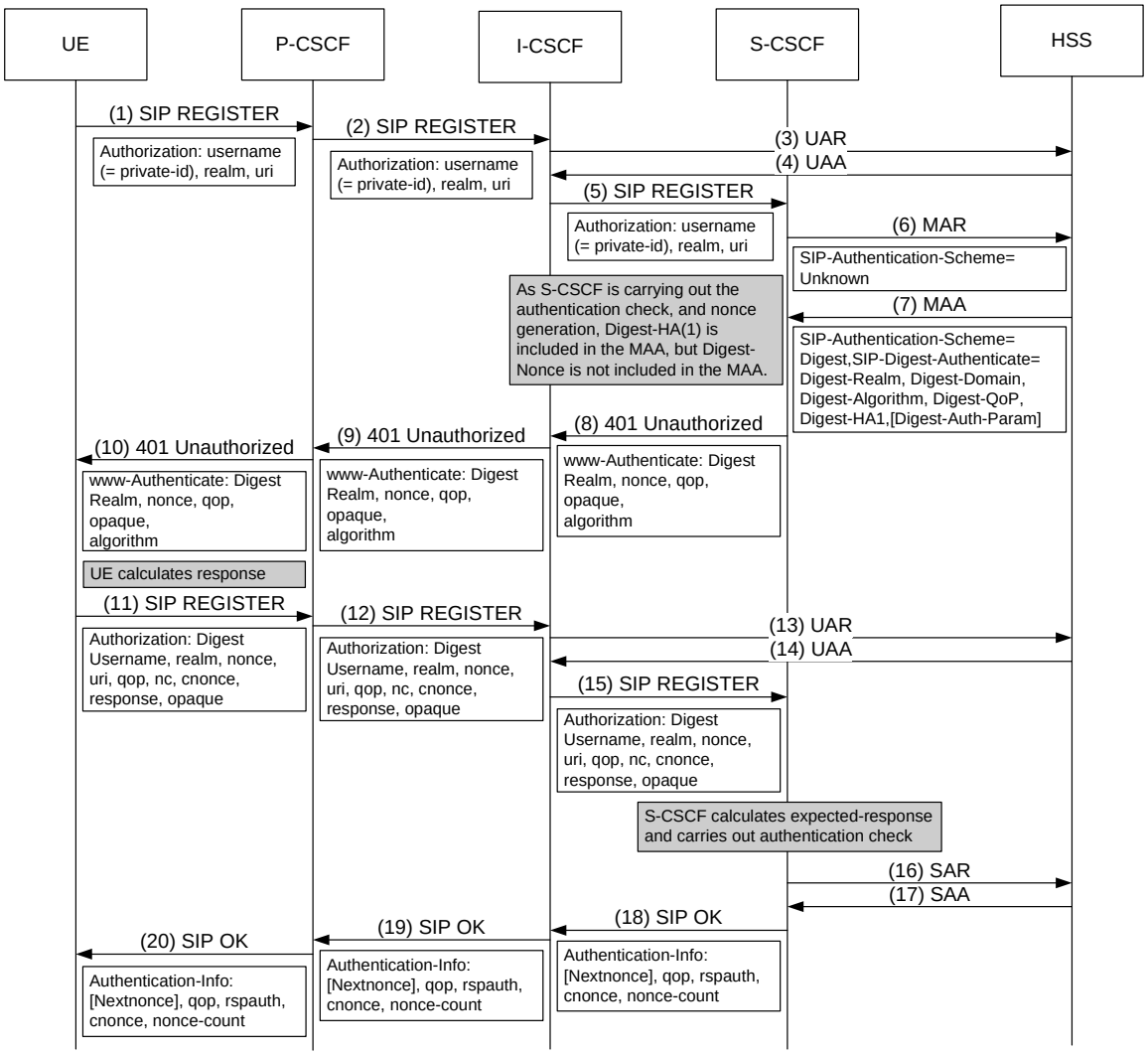

Figure 2 – Nonce Generated in S-CSCF, S-CSCF Authentications the User

[Step 1] The UE sends a register request to the P-CSCF. The message includes an authorize header that includes the private identity of the subscriber. An example authorization header is shown below:

```
REGISTER sip:home.mobile.biz SIP/2.0
      Authorization: Digest
            username="jon.dough@mobile.biz",
            realm="RoamingUsers@mobile.biz",
            nonce="",
            uri="sip:home.mobile.biz",
            response=""
            algorithm="MD5"
```

[Step 2] The P-CSCF forwards the register request to the appropriate I-CSCF.

[Step 3] The I-CSCF sends a User-Authorization-Request (UAR) request asking the HSS to carry out Authorization of the subscriber.

[Step 4] The HSS responds back with a User-Authorization-Answer (UAA) answer (which may include capabilities or server-names to allow the I-CSCF to choose an appropriate S-CSCF).

[Step 5] The I-CSCF selects an appropriate S-CSCF in the home network and forwards the Register request to this S-CSCF.

[Step 6] The S-CSCF contacts the HSS using a MAR message towards the HSS on the Cx interface. The MAR message contains the following authentication Attribute-Value Pairs (AVPs):

- SIP-Number-Auth-Items
- SIP-Auth-Data-Item
- SIP-Authentication-Scheme – Set to "Unknown"

This information is to inform the HSS that a user is authenticating to the IMS network and is requesting HTTP-Digest (MD5) authentication. Note: At this stage, the HSS records the S-CSCF name and sets the Not-Registered-Authentication-Pending flag.

[Step 7] The HSS looks up the user in its database and reads/calculates the necessary data required by the client in support of HTTP-Digest. The HSS returns a Multimedia-Auth-Answer (MAA), containing the following data authentication elements:

- SIP-Number-Auth-Items
- SIP-Auth-Data-Item
- SIP-Authentication-Scheme – Set to "Digest"
- SIP-Digest-Authenticate – New grouped AVP used for passing the www-authenticate header
    - Digest-Realm
    - Digest-Domain
    - Digest-Algorithm
    - Digest-QoP
    - Digest-HA1
    - Digest-Auth-Param

For a definition of the above parameters, see [RFC 2617].

[Step 8] The S-CSCF creates a SIP 401 (Unauthorized) response, which includes the challenge (nonce) in the www-authenticate header field and sends it back to the I-CSCF. An example header is shown below:

```
SIP/2.0 401 Unauthorized
      WWW-Authenticate: Digest
              realm="RoamingUsers@mobile.biz",
              nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==",
              opaque="5ccc069c403ebaf9f0171e9517f40e41",
              stale=false,
              algorithm=MD5,
              qop="auth,auth-int"
```

[Step 9] The I-CSCF sends the SIP 401 (Unauthorized) response back to the P-CSCF.

[Step 10] The P-CSCF routes the response back to the UE.

[Step 11] The UE chooses the strongest value of "qop" it supports and uses the nonce to create the response (RES) as per [RFC 2617] (termed request-digest). The UE also calculates a client-nonce (cnonce) and nonce-count (nc) and sends a second register request to the P-CSCF, with an Authorization header. An example Authorization header is shown below:

```
REGISTER sip:home.mobile.biz SIP/2.0
      Authorization: Digest
              username="jon.dough@mobile.biz",
              realm="RoamingUsers@mobile.biz",
              nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==",
              uri="sip:home.mobile.biz",
              qop=auth,
              nc=00000001,
              cnonce="0a4f113b",
              response="6629fae49393a05397450978507c4ef1",
              opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

[Step 12] The P-CSCF sends the Register request onto the I-CSCF.

[Step 13] As the I-CSCF is stateless, it sends a UAR request to the HSS to find the address of the S-CSCF to route the request to.

[Step 14] The HSS returns the S-CSCF address in a UAA response.

[Step 15] The I-CSCF sends the Register request to the S-CSCF.

[Step 16] The S-CSCF completes the registration procedure by sending a Server-Assignment-Request (SAR) to the HSS.

[Step 17] The HSS sets the registration state to "Registered", clears the "Authentication-Pending" flag and downloads the profile down to the S-CSCF in a Server-Assignment-Answer (SAA).

[Step 18] The S-CSCF formulates a 200 OK response with an Authentication-Info header and sends this to the I-CSCF. An example is shown below:

```
SIP/2.0 200 OK
      Authentication-Info:
              qop=auth-int,
              rspauth="6629fae49393a05397450978507c4ef1",
              cnonce="0a4f113b",
              nc=00000001
```

[Step 19] The I-CSCF forwards the 200 OK response (with Authentication-Info header) to the P-CSCF

[Step 20] The P-CSCF forwards the 200 OK response (with Authentication-Info header) to the UE. The UE validates the rspauth in the Authentication-Info header to authenticate the network.

6.1.2 Support for SIP Digest within the Generic Bootstrapping Architecture (GBA)

Supporting SIP Digest (or HTTP digest, [RFC 2617]) as explained earlier in Section 6.1.1.1, allows for authentication of non-UICC clients. This flexibility is also needed for the bootstrapping process since it also requires authentication involving the UE - authentication between the Bootstrapping Server Function (BSF) and the UE. Hence the bootstrapping process must be enhanced so it can use SIP Digest authentication in addition to existing mechanisms.

- [PKT 33.220] provides a general overview and write-up of the SIP Digest authentication function for bootstrapping. It does not address any specific requirements for SIP Digest on the Zh interface (BSF to HSS interface).

The Zh interface is a subset of the Cx interface, re-using the MAR/MAA message definitions [PKT 29.228] to exchange authentication information between the HSS and BSF. Following the Cx authentication model in this document the Zh interface should support authentication and nonce generation in the BSF for support of SIP Digest.

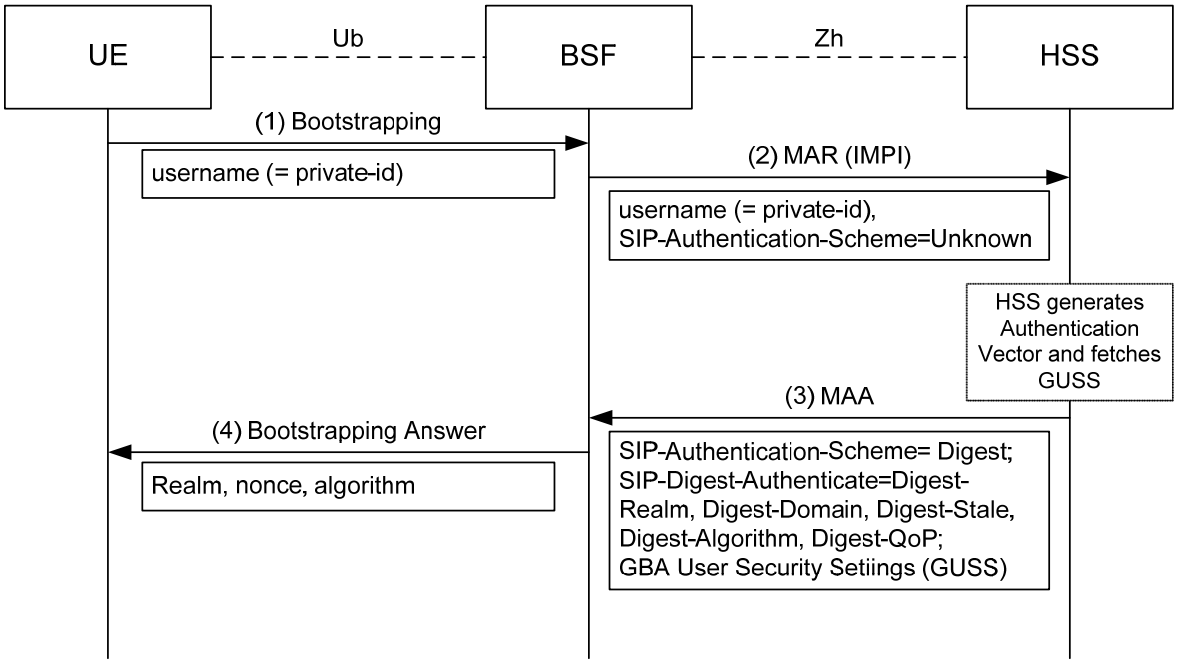

Figure 3 – Partial Bootstrapping Messaging Flow

The overall MAR/MAA exchange is described in Section 6.1.1.2. GBA User Security Setting (GUSS) is included in the MAA if available in the HSS for the requested PrivateID.

6.1.3 Impacted Components

This section describes the component impacts needed to support SIP Digest.

6.1.3.1 HSS

Support for SIP Digest in the HSS requires support of the new SIP-Digest-Authenticate AVP. Additionally, changes have been made to some of the existing AVPs that were previously only used for AKA authentication. The changes to the AVPs are documented in [PKT 29.228].

6.1.3.2 S-CSCF

The S-CSCF is acting as the Authenticator and as a partial Authentication-Service. It is now doing more work as it has to generate the expected-response and the nonce. As with the HSS, support of the new SIP-Digest-Authenticate AVP and handling of the changes to the existing AVPs is required.

6.1.3.3 BSF

The BSF needs to support the SIP Digest Authentication message extensions as well as the corresponding authentication calculations. The BSF also needs to support the generation of the nonce.

6.2 Support for Display Name associated with an IM Private Identity (IMPU) for Calling NAMe (CNAM) Service

6.2.1 Overview

PacketCable requires support for the CNAM (Calling NAMe) service. To support this requirement, the originating P-CSCF inserts the Display Name of the Calling Party in the P-Asserted-Identity Header of the SIP INVITE message. Figure 4 illustrates the role of the P-CSCF in support of the CNAM service.

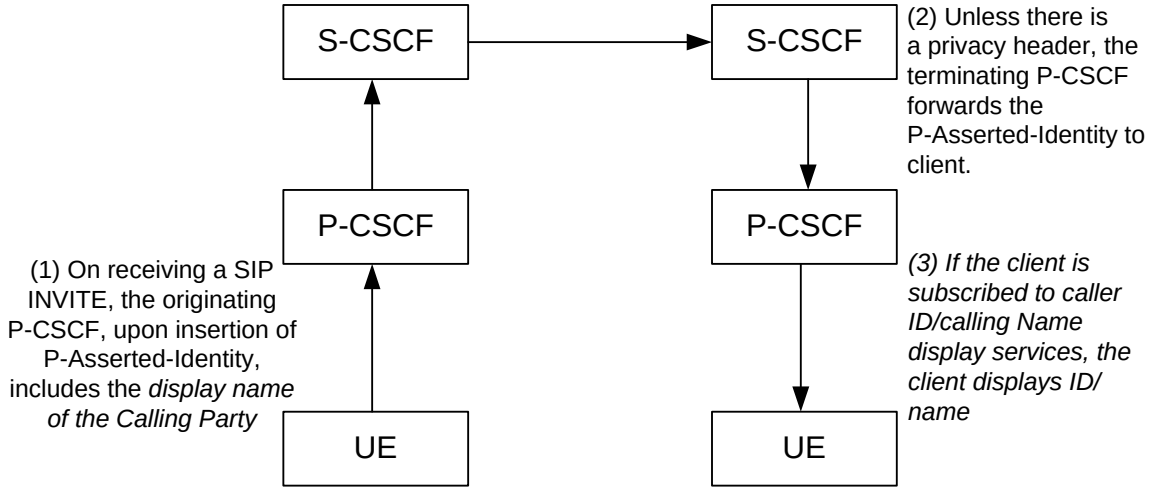

Figure 4 – Actions on Receipt of a SIP-Invite in Support of the CNAM Service

6.2.2 Solution

The solution addresses two main requirements:

- Determination of the authoritative source for the Display Name information
- Acquisition of the Display Name for a given IMPU by the P-CSCF

To solve them, this technical report proposes that the HSS store a Display Name against each IMPU in the user-profile and facilitate retrieval of the Display Name over the Cx interface to the S-CSCF. Thus, upon registration, the HSS provides the Display Name associated with each IMPU included in the same Implicit Registration Set (IRS) to the S-CSCF. The S-CSCF can then proceed to forward all the IMPUs and their associated Display Name in the P-Associated-URI (as part of registration) to the P-CSCF. The P-CSCF is required to store the obtained Display Names and the associated IMPUs until UE or network deregistration occurs. Figure 5 illustrates this process.

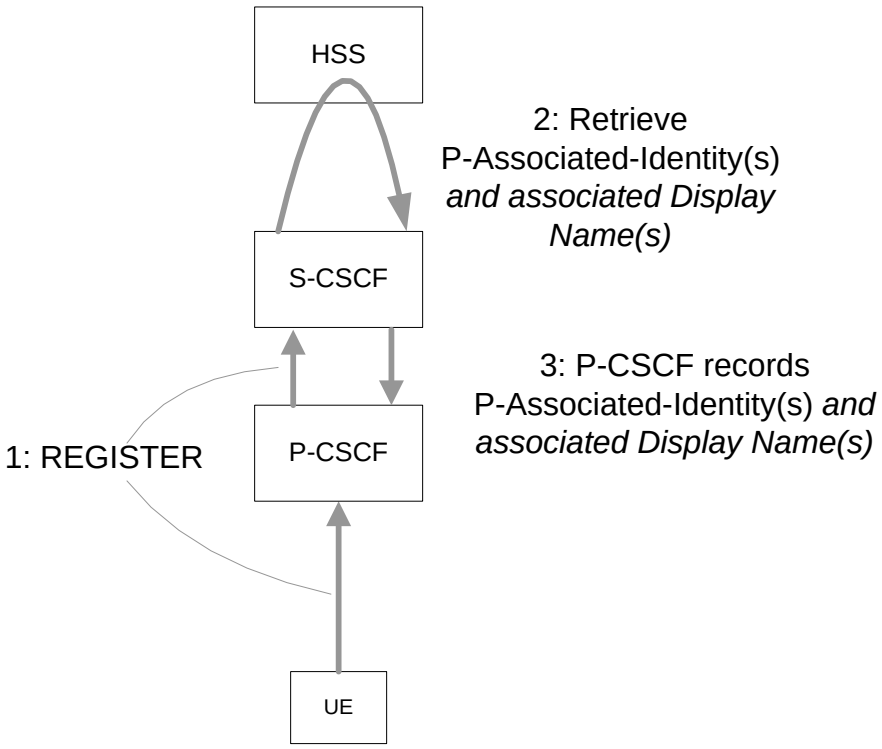

Figure 5 – Actions on Receipt of a SIP-Register in Support of the CNAM Service

The proposed solution makes the following assumptions:

- It is assumed that the operator treats CNAM as an optional server capability, i.e., the operator configures the HSS to return capabilities that enable the I-CSCF to select an S-CSCF that understands the Display Name when sent over the Cx interface; an S-CSCF that does not support the proposed extension, ignores it.
- There exists exactly one Display Name associated with one IMPU, i.e., irrespective of IMPI used for registration, the same Display Name is used for a particular IMPU.
- If Display Names are configured in the HSS, then they are downloaded to the S-CSCF when the S-CSCF transmits an SAR for:
    - Unregistration (SAT=UNREGISTERED_USER),
    - Registration (SAT=REGISTRATION), or
    - Re-registration (SAT=RE_REGISTRATION),
- Upon registration, following the existing implicit registration rules, the HSS provides the Display Names for all IMPUs in the same IRS in SAA and PPR messages,

- If a Display Name changes post-registration, the HSS provides the new Display Name (the whole IRS) in the user-profile sent in a PPR message,
- The Display Name is never sent over the Sh reference point,
- The following PacketCable IMS delta specifications are affected as a result of the modifications:
    - [PKT 29.228]
    - [PKT 23.008]

6.2.3 Impacted Components

6.2.3.1 HSS

The HSS data model is enhanced to store a "Display Name" against each IMPU belonging to a Subscription. To avoid modifications to the Cx interface (e.g., new AVPs), the proposal is to take advantage of the XML extensions mechanism in 3GPP and define a backwards compatible change to the XML schema to transport the Display Name.

This proposal is illustrated in Figure 6 as an enhancement to the Public-Identification Base Class of [PKT 29.228], to include a "Display Name".

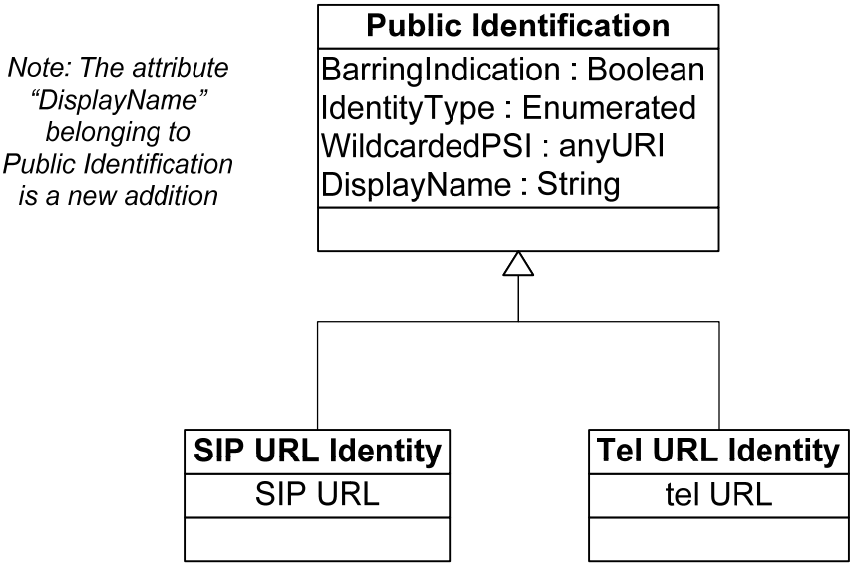

Figure 6 – XML changes required in support of the CNAM Service

6.2.3.2 S-CSCF

During the registration process, the S-CSCF parses the user-data AVP and extracts the Display Name associated with each IMPU. It includes the Display Names along with the IMPUs (in the same implicit registration set) into the P-Associated-URI Header of the SIP REGISTER (response) and sends the P-Associated-URI in a 200 OK response back to the P-CSCF.

Post-registration changes to the Display Name are obtained by the S-CSCF in a PPR message (along with other details belonging to the same implicit registration set).

6.2.3.3 P-CSCF

The P-CSCF receives the Display Names in the P-Associated-URI Header as part of a successful registration response (200 OK), and stores them, along with the associated IMPUs.

When the originating party initiates a session, the originating P-CSCF receives the SIP INVITE, matches the P-Preferred-ID header with a list of valid IDs from the stored P-Associated ID list, and replaces the P-Preferred-ID header with a P-Asserted-Identity header containing the matched ID and the stored Display Name. Unless there is a privacy header, the terminating P-CSCF forwards the P-Asserted-Identity to the destination client.

6.2.3.4 UE

If the UE subscribes to Caller ID/Calling Name display services, the UE displays the Caller ID/Calling Name to the user.

6.3 Matching of tel URI

The Public User Identity sent to the HSS by the various network entities is the index for finding the user profile, and is only used for user identification. For SIP URIs, the guidelines for the canonical form defined in [RFC 3261] are applied before sending the Public User Identity to the HSS. For tel URIs, however, the guidelines are not as clear, particularly in the presence of a context parameter.

In [RFC 3966] the canonical form for a tel URI is defined as follows:

> The telephone number is understood here as the canonical address-of-record or identifier for a termination point within a specific network. For the public network, these numbers follow the rules in [E.164], while private numbers follow the rules of the owner of the private numbering plan.

This passage indicates that for global numbers, the E.164 number is the canonical form. For private (or local) numbers, the elements necessary to form the canonical form are not specified. By piecing together other portions of [RFC 3966] it should be possible to define a canonical form for private tel URIs. For example, the last paragraph in section 5.1.5 of [RFC 3966] gives a hint at the possible canonical form:

> If the recipient of a "tel" URI uses it simply for identification, the receiver does not need to know anything about the context descriptor. It simply treats it as one part of a globally unique identifier, with the other being the local number.

Here it is implied that for identification purposes (i.e., the canonical form) is the combination of the local number plus the context. From an HSS perspective there are two items that must be determined:

- The canonical form for private network tel URIs.
- The network elements (i.e., HSS, I-CSCF, S-CSCF, etc) that are responsible for performing canonicalization of the tel URI when accessing the user profile from the HSS.

The recommendation is that canonicalization be performed prior to querying the HSS, treating the public identity that is sent as an index into the HSS.

6.3.1 Impacted Components

Since this is a clarification to the usage of tel URIs in the context of user identification, the impacts largely depend on the existing vendor implementations. Therefore, this section attempts to describe some of the potential impacts.

6.3.1.1 HSS

For SIP URIs, the normalization to the canonical form takes place outside of the HSS by the elements that interact with the HSS, such as the I-CSCF (Cx/Dx), S-CSCF (Cx/Dx) and Application Servers (Sh/Dh). If it is decided that the normalization of tel URIs be performed by the HSS, then this requires changes to the HSS to accommodate this requirement. Otherwise, it is anticipated that there would be little to no impact to the HSS to support the canonical form that is defined.

6.3.1.2 S-CSCF

Since the S-CSCF handles canonical forms for managing its local user state information, it is anticipated that impacts to the S-CSCF would be limited to discrepancies between current implementations of a canonical tel identity and the form that is being defined.

Furthermore, it is assumed that current S-CSCF implementations already perform canonicalization prior to sending the identity to the HSS. Therefore, it will have little to no impact on the S-CSCF regardless of where the canonicalization takes place.

6.3.1.3 I-CSCF

Since the I-CSCF does not store user state information, the only potential impacts to the I-CSCF depend on the decision of where to perform canonicalization. It is assumed that current I-CSCF implementations already perform canonicalization prior to sending the identity to the HSS. Therefore it will have little to no impact on the I-CSCF regardless of where the canonicalization takes place.

6.3.1.4 Application Server

An Application Server may or may not store user state information that is indexed on the canonical form of the user identity. For those Application Servers that store user state information, it has little to no impact on the Application Server regardless of where the canonicalization takes place. For those Application Servers that do not store user state information, it is assumed that they already perform canonicalization prior to sending the identity to the HSS. Therefore, these Application Servers also experience little to no impact regardless of where the canonicalization takes place.

Appendix I Non-HSS Impacting Requirements Considered

This section documents issues that were discussed by the HSS Focus Team and were eventually deemed to be non-issues from an HSS perspective.

I.1 Dynamic Filter Criteria

I.1.1 Background

In an attempt to optimize the signaling traffic in the network, a general requirement to limit the amount of session signaling that reaches an application server has been considered. Filter criteria determine when an application server is invoked as part of the session. Manipulation of the filter criteria based on the features that a subscriber has activated, could potentially reduce the need to invoke an application server as part of a basic session. This manipulation of the filter criteria was termed Dynamic Filter Criteria.

There were four options considered during the discussions:

- Option 1: Use HSS provisioning interface to update filter criteria in real time.
- Option 2: Use AS-HSS Sh interface to update filter criteria as needed.
- Option 3: Use AS-HSS Sh interface to update an on/off switch for each combination of Subscriber Public Identity and AS.
- Option 4: Make no Changes to the IMS Architecture.

The final decision was to go with Option 4.

The remainder of this section briefly describes the four options that were considered.

I.1.2 Option 1: Use HSS Provisioning Interface to Update Filter Criteria in Real Time

This option is based on the premise that the existing north bound provisioning interface could be used to dynamically update the filter criteria.

- Advantages:
    - No IMS changes required.
- Disadvantages:
    - The north bound HSS provisioning interface was not intended for real time traffic use.
    - The north bound HSS provisioning interface is not currently specified.
    - Updating Filter Criteria may require an update of additional data elements in the User Profile for the subscriber, making this update an "expensive transaction".
    - The Filter Criteria is a part of the Service Profile data structure in the HSS and Service Profiles are designed to be shared across many different users. Creating many different service profiles so that filter criteria can be customized for each user reduces the optimal sharing of service profiles across many users.

I.1.3 Option 2: Use Sh Interface to Update Filter Criteria

This option is based on the concept that the application server already uses the Sh interface to communicate with the HSS and could reuse this interface to update filter criteria targeted to that specific application server.

- Advantages:
    - Avoids use of non-real-time HSS provisioning interface.
- Disadvantages:
    - Requires a modification of the Sh interface to allow the AS to update Filter Criteria.
    - Updating Filter Criteria may require an update of additional data elements in the User Profile for the subscriber, making this update an "expensive transaction" on the Cx interface as the HSS updates the S-CSCF.
    - The Filter Criteria is a part of the Service Profile data structure in the HSS, and Service Profiles are designed to be shared across many different users. Creating many different service profiles so that filter criteria can be customized for each user will reduce the optimal sharing of service profiles across many users.

I.1.4 Option 3: Use Sh Interface to Update On/Off Switch for each Public Identity and AS Combination

This option uses the same underlying principle that the application server can communicate with the HSS using the Sh interface. Rather than manipulating the actual filter criteria, however, this option uses the concept of an on/off switch for each Public Identity and application server combination.

- Advantages:
    - Avoids use of non-real-time HSS provisioning interface.
    - Avoids expensive filter-update transactions.
    - Does not break the shared service profile model.
- Disadvantages:
    - Requires a modification of the Sh interface to allow the AS to create the new on/off switch.
    - Requires a modification of the Cx interface to create the new on/off switch.
    - Requires a change to the S-CSCF filter processing logic to include a check of the new on/off switch.

I.1.5 Option 4: Make no Changes to the IMS Architecture

This option is really just the existing architecture and imposes no changes.

- Advantages:
    - Avoids IMS changes, maintaining the clean separation of routing logic and application logic within the architecture.
    - Avoids expensive filter update transactions at the HSS/S-CSCF.
    - Does not break the shared service profile model.

- Disadvantages:
    - Requires application servers to be invoked for services even in situations where they may have been able to be optimized out of the call path through the use of a dynamic filter criteria mechanism.

I.2 Architectural Guidelines Regarding Storage of Service Data in the HSS

The question of where to store service data has resulted in numerous lengthy discussions and covered a multitude of topics including CNAM and "cic" codes, to name two examples. A big part of the discussion really boils down to the decision of what is service specific data and what should be static user profile data. Although the decision as to whether data is service specific or status user profile data needs to take place on a case-by-case basis, it was generally agreed that service specific data will be provisioned either at the UE or the application server. The application server can then use the Sh interface to store this data if desired.

I.3 Triggering Based on Presence of Globally Routable UA URIs (GRUU)

GRUUs allow a specific UA instance to be addressed with a URI that specifically targets that UA. This can be useful for services where addressing a specific UA instance may enhance the user experience, such as call transfer.

A requirement has been expressed to allow application server triggering based on the presence (or absence) of a GRUU. This can be used to selectively invoke services based on whether a GRUU is included. For example, an operator may decide to only invoke voicemail if a GRUU is not being addressed.

The discussion surrounding this topic took place during the period when the GRUU requirements and format were still changing. With the release of draft-ietf-sip-gruu-07, a new URI parameter (gruu) was introduced that allows for a GRUU to be easily identified. This development allowed this issue to be laid to rest.

During the discussion, there were two alternatives that were debated. The first alternative involves making changes to the Service Point Triggers, whereas the second alternative is based on the assumption that the existing Service Point Triggers are sufficient to perform any desired triggering. With the introduction of the new URI parameter it was determined that no changes are needed to the Service Point Triggers in order to support the identification of a GRUU.

The remainder of this section describes the two alternatives that were considered prior to the change to the [ID GRUU] and is provided simply for informational purposes.

I.3.1 Alternatives

I.3.1.1 GRUU Trigger support requiring changes to Service Point Triggers (SPT)

This approach is based on modifying the Choice attribute of the Service Point Trigger class, which is part of the User Profile. The proposed change for this approach is to add an additional Choice. The new SPT returns TRUE if, and only if, the Request-URI is a GRUU associated with a Public User Identity for which the S-CSCF is responsible [SIP TR].

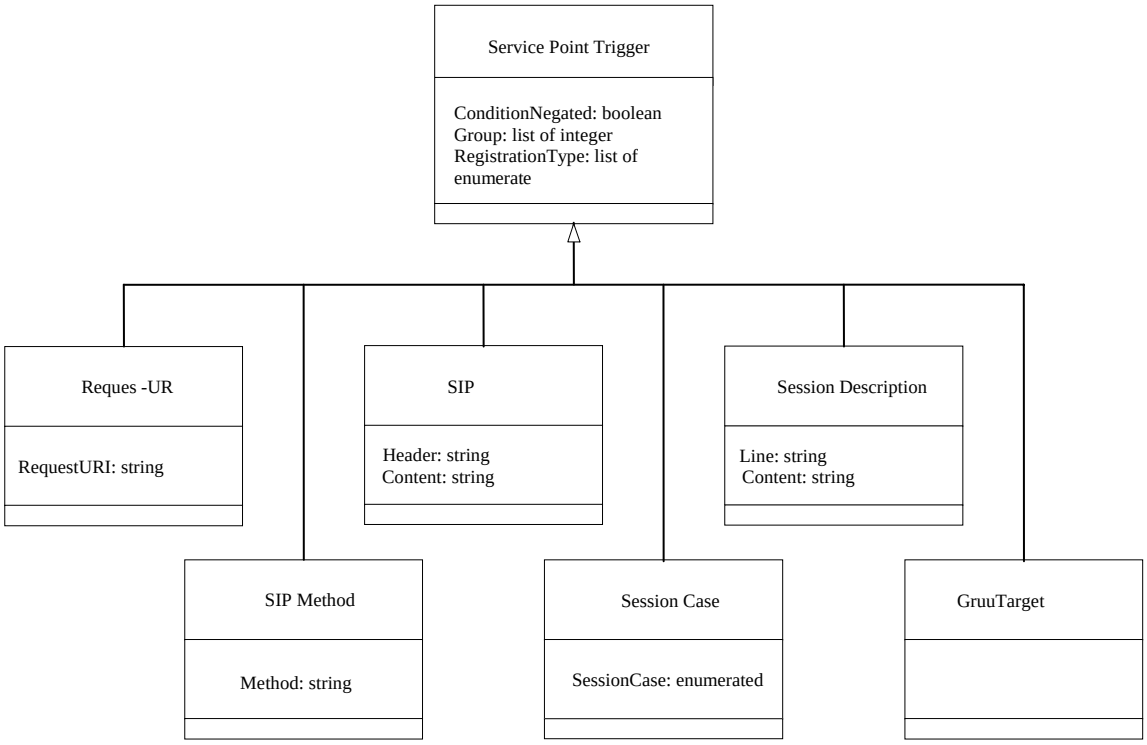

Figure 7 – GRUU Target addition to Service Point Triggers (SPT)

I.3.1.1.1 Pros

- Changes to the GRUU format in the future would not require changes to the already defined iFC stored for users within the HSS.
- This would continue to work even if the GRUU format changed in a way that was no longer detectable by using the existing SPT types.

I.3.1.1.2 Cons

- Requires changes to User Profile on the HSS will:
    - Impact existing provisioning systems (North Bound Interface).
    - Impact the data structure stored in the HSS.
    - Impact the data sent over the Cx interface (minimal impact).
    - Impact the data sent over the Sh interface (minimal impact).
    - Impact the XML schemas for Cx and Sh in a way that is not backwards compatible (because the Choice option is currently not extensible).
- Requires changes to Application Servers that use iFC provided via Sh:
    - The AS now needs to understand how the GRUU is constructed in order to evaluate the iFC that it receives over the Sh interface.
- Requires changes to the S-CSCF iFC handling:
    - Although it could be argued that the S-CSCF already needs changes in order to support GRUU anyway, those changes are not related to the iFC handling.

I.3.1.2 Impacted Components

I.3.1.2.1 HSS

The Schema for the User Profile, which is stored in the HSS, needs to be changed in a non-backwards compatible manner. This new schema impacts the data sent over both the Cx and Sh interfaces.

I.3.1.2.2 S-CSCF

The S-CSCF needs to understand the updated schema for the User Profile in order to recognize the new Service Point Trigger. If the GruuTarget Service Point Trigger is present, the S-CSCF must determine if the Request-URI is a GRUU associated with a Public User Identity for which the S-CSCF is responsible. If (and only if) this condition is true, the SPT returns TRUE.

I.3.1.2.3 Application Server

The Application Server needs to understand the updated schema for the User Profile in order to recognize the new Service Point Trigger. The Application Server needs to be able to evaluate whether the Request-URI is a GRUU if it wishes to analyze the iFC. The Application Server, however, has no means of determining any association with a particular S-CSCF for a given GRUU.

I.3.1.3 GRUU Trigger support using existing Service Point Triggers (SPT)

This approach is based on using the existing SPTs to be able to identify that a GRUU is involved. It is based on the assumption that it is possible to identify whether a GRUU is present based on an included URI parameter.

I.3.1.3.1 Pros

- No impact to existing User Profile:
- No changes to the existing provisioning systems/interfaces
- No changes to HSS data
- No changes to the Cx interface
- No changes to the Sh interface
- No impact to existing iFC implementations (including CSCF and AS)

I.3.1.3.2 Cons

- Would require changing existing iFC for users that are already defined if the GRUU format were to change in such a way that the URI parameter is no longer sufficient to identify that a GRUU is being used.

I.3.1.3.3 Impacted Components

This solution is based on the status quo and, therefore, has no impacts.

I.3.1.3.4 Example

```
<?xml version="1.0" encoding="UTF-8"?>
<IMSSubscription xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="C:\Documents and Settings\user\Local
Settings\Temp\CxDataType_Rel6.xsd">
             <PrivateID>IMPI1@homedomain.com</PrivateID>
             <ServiceProfile>
```

```
                    <PublicIdentity>
                          <BarringIndication>1</BarringIndication>
                          <Identity> sip:IMPU1@homedomain.com </Identity>
                    </PublicIdentity>
                    <PublicIdentity>
                          <Identity> sip:IMPU2@homedomain.com </Identity>
                    </PublicIdentity>
                    <InitialFilterCriteria>
                          <Priority>0</Priority>
                          <TriggerPoint>
                                <ConditionTypeCNF>1</ConditionTypeCNF>
                                <SPT>
                                      <ConditionNegated>0</ConditionNegated>
                                      <Group>0</Group>
                                      <RequestURI>*;gruu*</RequestURI>
                                </SPT>
                          </TriggerPoint>
                          <ApplicationServer>

      <ServerName>sip:AS1@homedomain.com</ServerName>
                                <DefaultHandling>0</DefaultHandling>
                          </ApplicationServer>
                    </InitialFilterCriteria>
              </ServiceProfile>
</IMSSubscription>
```

I.4 Support for SIP Digest

I.4.1 Support for SIP Digest in an IMS Network

I.4.1.1 Background

Multiple solutions for dealing with SIP Digest support in IMS were identified when the initial HSS investigation for this requirement took place. In [ID DIAMETER SIP], the role of the Server used for HTTP-Digest authentication (as specified in [RFC 2617]) is taken on by both the SIP-Server and Diameter Server (in the IMS, the S-CSCF fulfills the role of a SIP-Server and the HSS fulfills the role of a Diameter Server).

Support for SIP Digest in a PacketCable network requires the determination of the network elements responsible for:

- Generation of the nonce
- Authentication of the User

The IETF draft [ID DIAMETER SIP] provides multiple options with regards to the above. Based on the technical evaluation of the options available, the following two options were recommended:

- Option 1: Nonce Generated in the Diameter Server (HSS), Diameter Server (HSS) authenticates the user. This option allows the user credentials to be centralized within the HSS, and these credentials do not need to be sent to the S-CSCF during the authentication process.
- Option 2: Nonce Generated in the SIP-Server (S-CSCF), SIP-Server (S-CSCF) authenticates the user. This option minimizes the number of needed message roundtrips between the S-CSCF and HSS but requires the user credentials to be passed to the S-CSCF and stored during the authentication process.

The rest of this section describes the technical evaluation and information related to Option 1.

I.4.1.2 Nonce Generated in HSS, HSS Authenticates the User

This option requires an additional Multimedia-Auth-Request (MAR) sequence to deliver the necessary parameters for the HSS to calculate the expected-response and perform the final authentication check. Figure 8 illustrates this scheme as part of the IMS registration process.

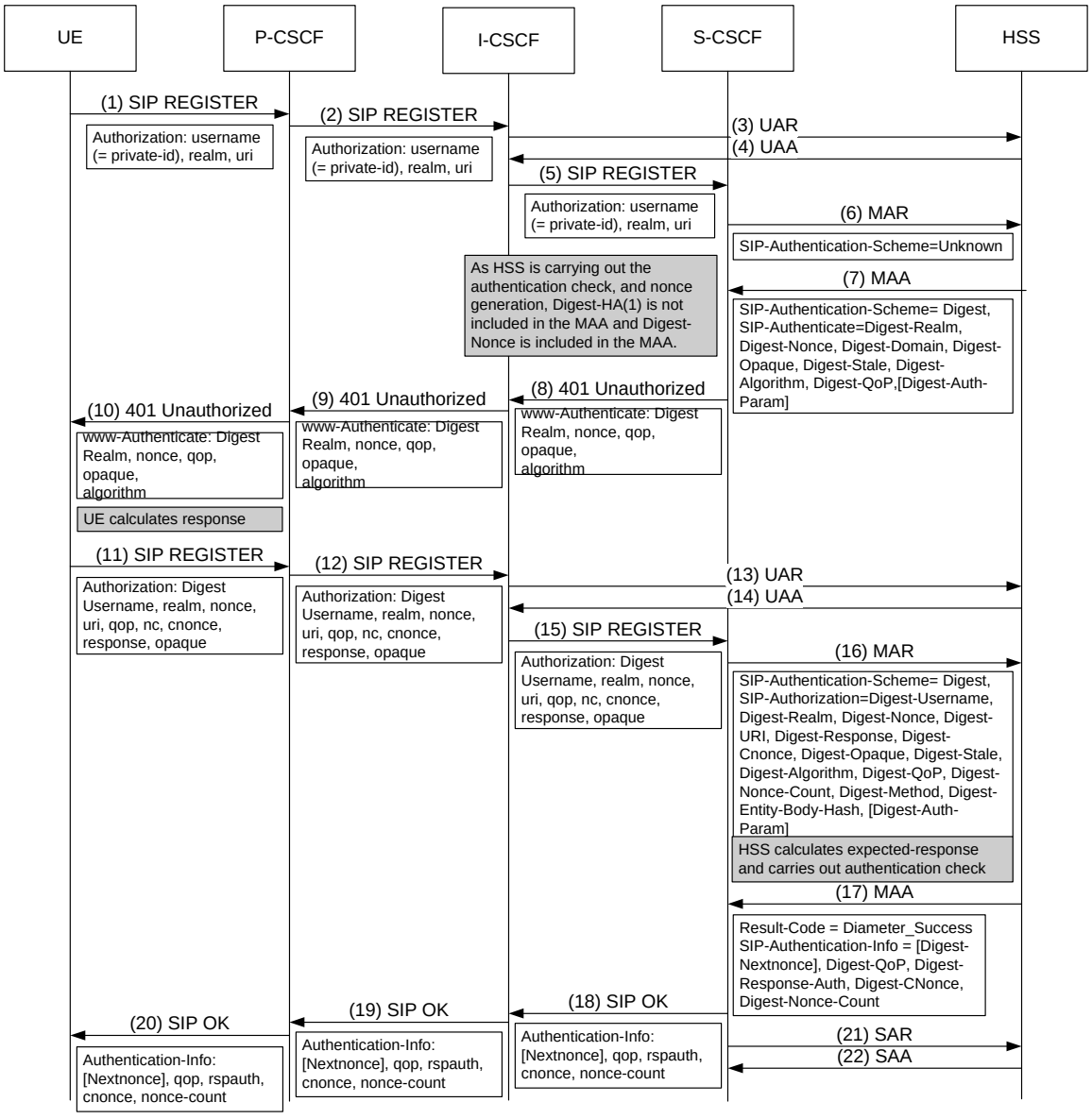

Figure 8 – Nonce Generated in HSS, HSS Authenticates the User

[Step 1] The UE sends a register request to the P-CSCF. The message includes an authorize header, which includes the private identity of the subscriber. An example authorization header is shown below:

```
REGISTER sip:home.mobile.biz SIP/2.0
       Authorization: Digest
              username="jon.dough@mobile.biz",
              realm="RoamingUsers@mobile.biz",
              nonce="",
              uri="sip:home.mobile.biz",
              response=""
              algorithm="MD5"
```

[Step 2] The P-CSCF forwards the register request to the appropriate I-CSCF.

[Step 3] The I-CSCF sends a User-Authorization-Request (UAR) request asking the HSS to carry out Authorization of the subscriber.

[Step 4] The HSS responds back with a User-Authorization-Answer (UAA) answer (which may include capabilities or server-names to allow the I-CSCF to choose an appropriate S-CSCF).

[Step 5] The I-CSCF selects an appropriate S-CSCF in the home network and forwards the Register request to this S-CSCF.

[Step 6] The S-CSCF contacts the HSS using a MAR message towards the HSS on the Cx interface. The MAR message contains the following authentication Attribute-Value Pairs (AVPs):

- SIP-Number-Auth-Items
- SIP-Auth-Data-Item
- SIP-Authentication-Scheme – Set to "Unknown"

This information is to inform the HSS that a user is authenticating to the IMS network and is requesting HTTP-Digest (MD5) authentication. Note: At this stage, the HSS records the S-CSCF name and sets the Not-Registered-Authentication-Pending flag.

[Step 7] The HSS looks up the user in its database and reads/calculates the necessary data required by the client in support of HTTP-Digest. The HSS returns a Multimedia-Auth-Answer (MAA) containing the following data authentication elements:

- SIP-Number-Auth-Items
- SIP-Auth-Data-Item
- SIP-Authentication-Scheme – Set to "Digest"
- SIP-Digest-Authenticate – New grouped AVP used for passing the www-authenticate header
- Digest-Realm
- Digest-Nonce
- Digest-Domain
- Digest-Opaque
- Digest-Stale
- Digest-Algorithm

- Digest QOP
- Digest-Auth-Param

For a definition of the above parameters, see [RFC 2617].

[Step 8] The S-CSCF creates a SIP 401 (Unauthorized) response, which includes the challenge (nonce) in the www-authenticate header field and sends it back to the I-CSCF. An example header is shown below:

```
SIP/2.0 401 Unauthorized
      WWW-Authenticate: Digest
              realm="RoamingUsers@mobile.biz",
              nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==",
              opaque="5ccc069c403ebaf9f0171e9517f40e41",
              stale=false,
              algorithm=MD5,
              qop="auth,auth-int"
```

[Step 9] The I-CSCF sends the SIP 401 (Unauthorized) response back to the P-CSCF.

[Step 10] The P-CSCF routes the response back to the UE.

[Step 11] The UE chooses the strongest value of "qop" it supports and uses the nonce to create the response (RES) as per [RFC 2617] (termed request-digest). The UE also calculates a client-nonce (cnonce) and nonce-count (nc) and sends a second register request to the P-CSCF, with an Authorization header. An example Authorization header is shown below:

```
REGISTER sip:home.mobile.biz SIP/2.0
      Authorization: Digest
              username="jon.dough@mobile.biz",
              realm="RoamingUsers@mobile.biz",
              nonce="CjPk9mRqNuT25eRkajM09uTl9nM09uTl9nMz5OX25PZz==",
              uri="sip:home.mobile.biz",
              qop=auth,
              nc=00000001,
              cnonce="0a4f113b",
              response="6629fae49393a05397450978507c4ef1",
              opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

[Step 12] The P-CSCF sends the Register request onto the I-CSCF.

[Step 13] As the I-CSCF is stateless, it sends a UAR request to the HSS to find the address of the S-CSCF to route the request to.

[Step 14] The HSS returns the S-CSCF address in an UAA response.

[Step 15] The I-CSCF sends the Register request to the S-CSCF.

[Step 16] The S-CSCF formulates a second MAR with the following AVPs:

- SIP-Number-Auth-Items
- SIP-Auth-Data-Item
- SIP-Authentication-Scheme – Set to "Digest"
- SIP-Digest-Authorization – New grouped AVP used for passing the Authorization header.
- Digest-Username
- Digest-Realm

- Digest-Nonce
- Digest-URI
- Digest-Response
- Digest-Algorithm
- Digest-Cnonce
- Digest-Opaque
- Digest-QoP
- Digest-Nonce-Count
- Digest-Method
- Digest-Entity-Body-Hash
- Digest-Auth-Param

For a definition of the above parameters, see [RFC 2617].

[Step 17] The HSS creates the expected-response using the parameters that were sent in the MAR together with H(A1) that is generated/stored on the HSS. The HSS then checks the response that came in the MAR against the expected-response (which it generated) to decide whether authentication is allowed or not. If authentication succeeds, the HSS sends back the following data to the S-CSCF.

- Result-Code = Diameter-Success
- SIP-Number-Auth-Items
- SIP-Auth-Data-Item
- SIP-Authentication-Scheme – Set to "Digest"
- SIP-Digest-Authentication-Info
- Digest-NextNonce – the next nonce that the UE uses for authentication to prevent the need for the first SIP-Register round-trip. It is an HSS implementation option over whether this is supported.
- Digest-QoP – the selected value of QoP used to calculate Digest-Response-Auth.
- Digest-Response-Auth – the response from the HSS (server) used to provide mutual authentication (i.e., client can authenticate the server).
- Digest-CNonce – Contains the Client Nonce value used to calculate the response and rspauth.
- Digest-Nonce-Count – Contains the Nonce Count value used to calculate the response and rspauth.

[Step 18] The S-CSCF formulates a 200 OK response with an Authentication-Info header and sends this to the I-CSCF. An example is shown below:

```
SIP/2.0 200 OK
      Authentication-Info:
              qop=auth-int,
              rspauth="6629fae49393a05397450978507c4ef1",
              cnonce="0a4f113b",
              nc=00000001
```

[Step 19] The I-CSCF forwards the 200 OK response (with Authentication-Info header) to the P-CSCF.

[Step 20] The P-CSCF forwards the 200 OK response (with Authentication-Info header) to the UE. The UE validates the rspauth in the Authentication-Info header to authenticate the network.

[Step 21] The S-CSCF completes the registration procedure by sending a Server-Assignment-Request (SAR) to the HSS.

[Step 22] The HSS sets the registration state to "Registered", clears the "Authentication-Pending" flag and downloads the profile down to the S-CSCF in a Server-Assignment-Answer (SAA).

I.4.2 Support for SIP Digest within the Generic Bootstrapping Architecture (GBA)

Supporting SIP Digest (or HTTP digest, [RFC 2617]) as explained earlier in Section 6.1.1.1 allows for authentication of non-UICC clients. This flexibility is also needed for the bootstrapping process since it also requires authentication involving the UE - authentication between the Bootstrapping Server Function (BSF) and the UE. Hence the bootstrapping process must be enhanced so it can use SIP Digest authentication in addition to existing mechanisms.

The Zh interface is a subset of the Cx interface, re-using the MAR/MAA message definitions [PKT 29.228] to exchange authentication information between the HSS and BSF. Following the Cx authentication model in this document, the Zh interface should support authentication in the BSF and the nonce to be generated either in the HSS or the BSF.

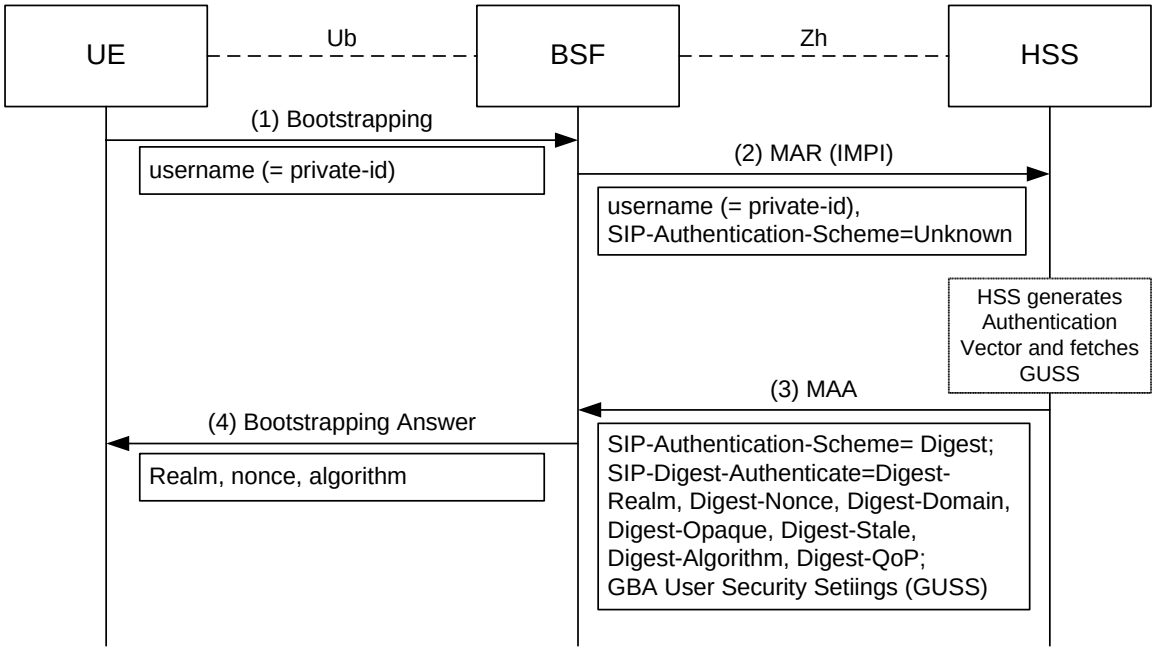

Figure 9 – Partial Bootstrapping Messaging Flow

If the nonce is generated in the HSS, the SIP-Authenticate AVP in the MAA will contain the generated nonce, if the nonce is to be generated in the BSF it will not be included in the SIP-Authenticate AVP in the MAA. The overall MAR/MAA exchange is as described in Section 6.1.1.2. GBA User Security Setting (GUSS) is included in the MAA if available in the HSS for the requested PrivateID.

I.4.3 Impacted Components

This section describes the impacts if both options are included.

I.4.3.1 HSS

The impacts to the HSS depend on the option(s) chosen by the operator. All options defined require changes to the Cx interface, Option 1 requires the support of three new Grouped AVPs within the SIP-Auth-Data-Item:

- SIP-Digest-Authenticate
- SIP-Digest-Authorization
- SIP-Digest-Authentication-Info

It is assumed that the HSS "Authentication Engine" needs to be modified to take on the extra work required to implement SIP-Digest, the amount of work required being dependent on the option(s) chosen for implementation.

Additionally, there are various parts of functionality that can be supported on the HSS in support of HTTP-Digest (as specified in [RFC 2617]) and (depending on the option chosen) this functionality may have an impact on the HSS, S-CSCF or both components. For example:

- Support of qop-value of "auth-int"
- Support of nextnonce
- Support of stale
- Support of auth-param

I.4.3.2 S-CSCF

Option 1 does not require the S-CSCF to act as an Authenticator nor Authentication Service. However, the S-CSCF has to support the AVPs described in the previous section. The S-CSCF does not need to perform any computationally intensive calculations for the Option 1. For Option 2, the S-CSCF is acting as the Authenticator and as a partial Authentication-Service. It is now doing more work as it has to generate the expected-response and (optionally) the nonce.

I.4.3.3 BSF

The BSF needs to support the SIP Digest Authentication message extensions as well as the corresponding authentication calculations. The BSF may also need to support generation of the nonce.

Appendix II Acknowledgements

CableLabs wishes to thank the following PacketCable focus team participants for authoring various sections that led to the development of this technical report:

- Klaus Hermanns (Cisco)
- Sean Schneyer (Ericsson)
- Ricky Kaura (Nortel)
- Ajay Gupta (Verisign)

Special thanks are extended to Sean Schneyer for being the primary editor of the technical report and other reviewers who provided valuable feedback.

Sumanth Channabasappa and the PacketCable Architecture team, CableLabs.