IP Multimedia Subsystem (IMS)

Definition: IP Multimedia Subsystem

IMS is a global, access-independent and standard-based IP connectivity and service control architecture that enables various types of multimedia services to end-users using common Internet-based protocols.

aus:

Miika Poikselkä, Georg Mayer, Hisham Khartabil and Aki Niemi: The IMS: IP multimedia concepts and services.
John Wiley & Sons, 2006
ISBN: 0-470-01906-9

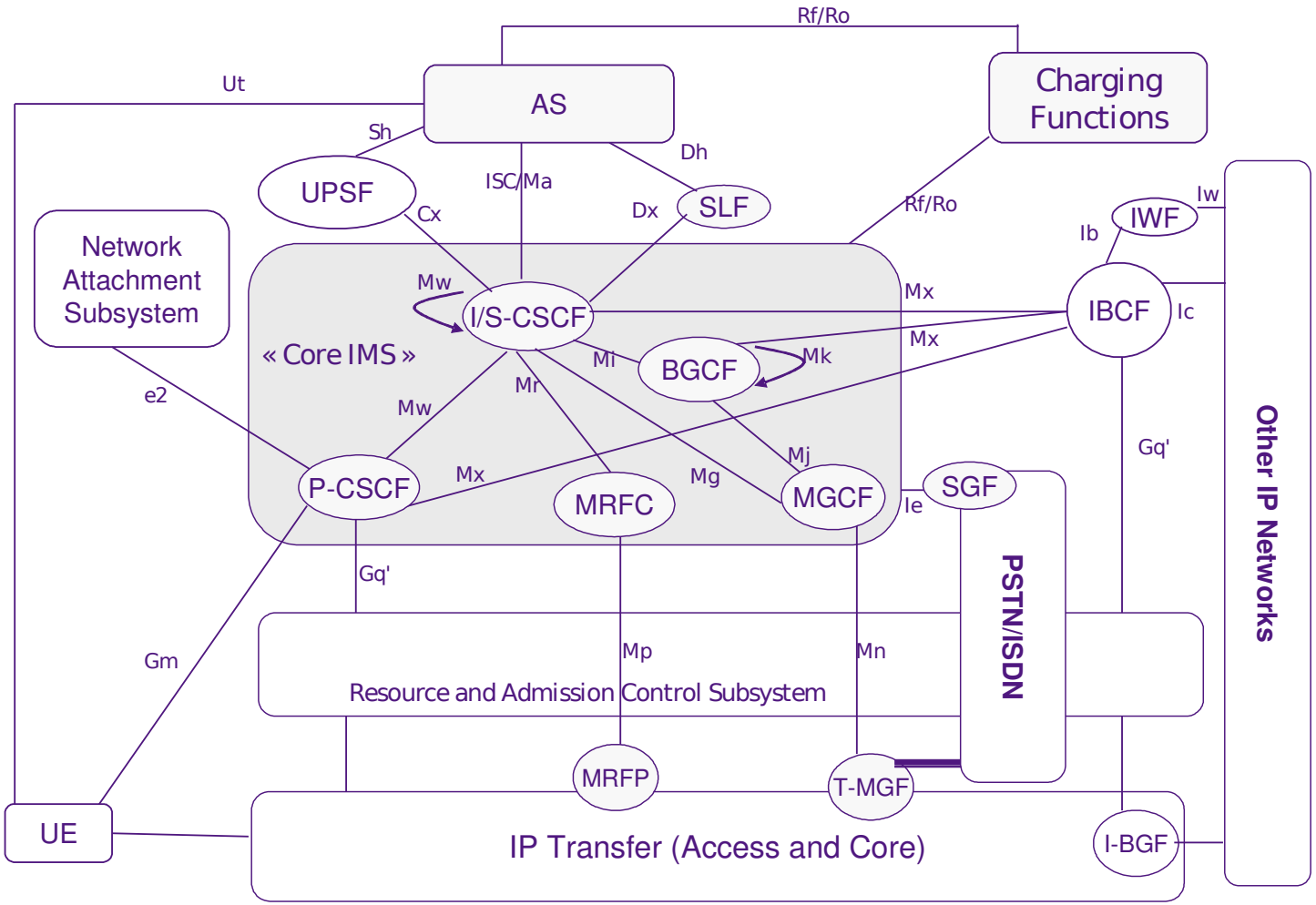
Geschichte

- **2001**: Arbeit an 3GPP Release 4 wurde fertig gestellt, es enthält IP Core Transport und Media Gateways
- **2002**: 3GPP Release 5 enthält Benutzerdatenbank (HSS, Home Subscriber Server), SIP Routing Systeme, Digest AKA Authentifizierung, SIP basierte Diensteplattform
- **2004**: 3GPP Release 6 bietet zusätzlich Interworking von IMS mit Circuit Switched Netzen und anderen IP Netzen
- **2006**: Release 7 ergänzt SIP SMS, Handover zwischen CS und IP, Festnetz IP Telefonie

Ziele

- Zusammenwachsen von Sprachdiensten und Datendiensten
- Zusammenwachsen von Festnetz und Mobiltelefonie (Fixed to Mobile Convergence / FMC)
- Sicherheit
- Möglichkeit zur Abrechnung

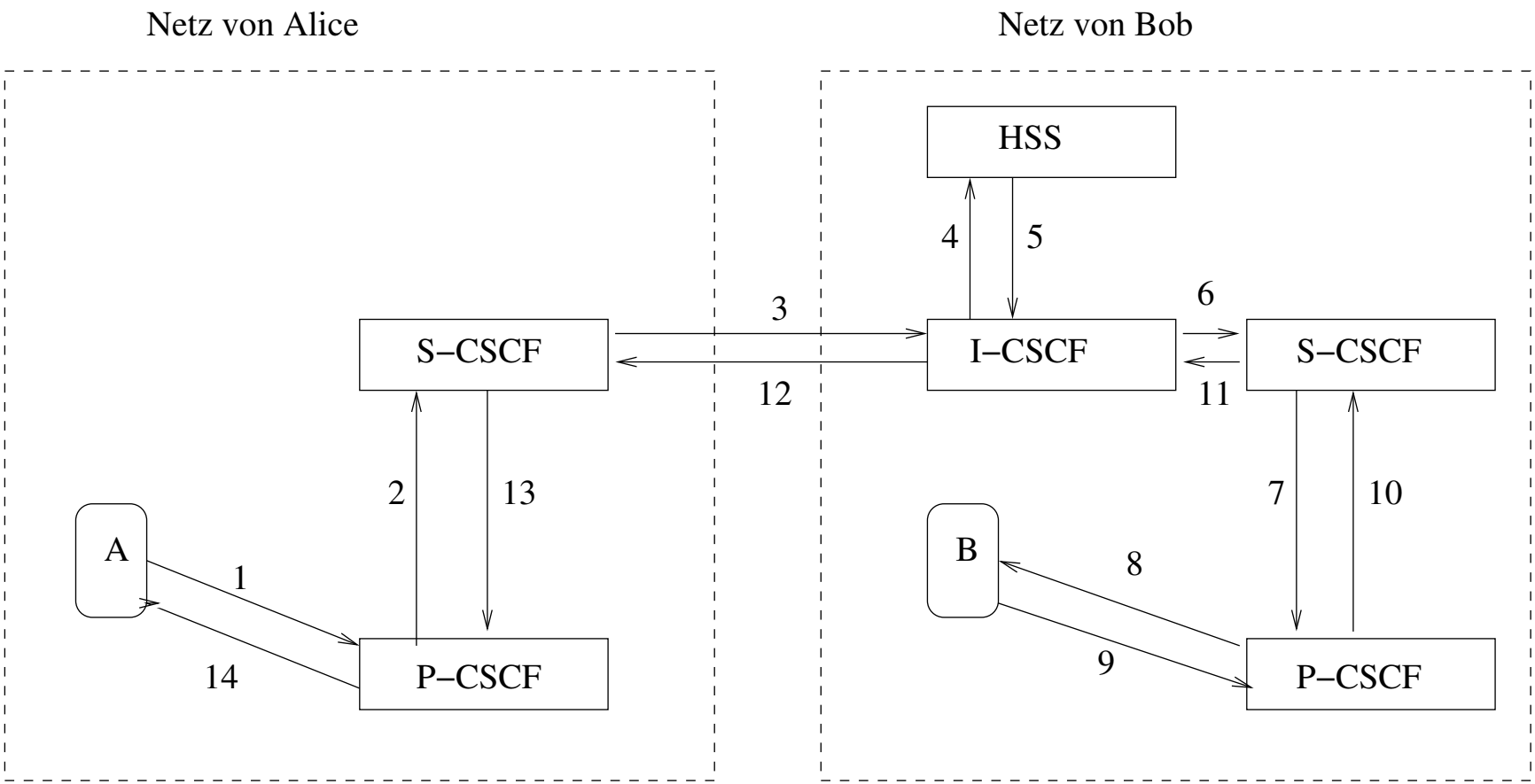
3GPP TS 23.417-700



Abkürzungen

CSCF	Call Session Control Function (P-Proxy, S-Serving, I-Interrogating)
UE	User Equipment (Endgerät)
BGCF	Breakout Gateway Control Function
MGW	Media Gateway
MGCF	Media Gateway Control Function
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
IWF	Interworking Function
IBCF	Interconnect Border Control Function
SGF	Signaling Gateway Function
AS	Appilication Server
UPSF	User Profile Server Function
SLF	Subscription Locator Function

Beispiel: Sitzungsaufbau in IMS



1. Alice schickt `INVITE` via Gm Interface zu ihrer P-CSCF
2. P-CSCF prüft den Absender und leitet das Paket (ggfs. nach weiteren Verarbeitungsschritten) über das Mw Interface an die S-CSCF weiter.
3. Die S-CSCF führt die für Alice konfigurierten Verarbeitungsschritte aus, bestimmt anhand der URI von Bob die zugehörige I-CSCF und leitet das Paket über das Mw Interface weiter.
4. Die I-CSCF erfragt beim HSS/UPSF die Adresse der für Bob konfigurierten S-CSCF.
5. Das HSS liefert die URI der S-CSCF über das Cx Interface.

6. Die I-CSCF leitet den `INVITE` über das Mw Interface an die S-CSCF weiter.
7. Die S-CSCF verarbeitet die Anforderung, wobei ggfs. konfigurierte Dienste abgearbeitet werden. In diesem Fall wird der Request über das Mw Interface an die P-CSCF weitergeschickt.
8. Die P-CSCF konvertiert das Paket für die Übertragung auf der Luftschnittstelle und leitet es über das Gm Interface an das Endgerät (UE B) weiter.

9.-14. Das Endgerät erzeugt eine Antwort (z.B. 183 Session Progress), die auf dem umgekehrten Weg an UE A zurückgeschickt wird.

Call Session Control Function (CSCF)

Jede CSCF ist ein SIP Proxy, der

- Routingentscheidungen trifft.
- dem Netzbetreiber Kontroll- und Abrechnungsfunktionen bietet.
- Integration mit anderen Netzelementen (z.B. Media Gateways) sicherstellt.

Im IMS werden folgende CSCF unterschieden:

- **P-CSCF/Proxy CSCF**: Einstiegspunkt für UE in das aktuelle IMS Netz
- **S-CSCF/Serving CSCF**: Session Control für eingehende und ausgehende Sessions
- **I-CSCF/Interrogating CSCF**: Einstiegspunkt für Fremdnetze in das Heimnetz des UE

S-CSCF

Die S-CSCF bietet folgende Funktionen:

- Registrar (vgl. RFC3261), speichert die physikalische Adresse zur **Public User ID**
- Holt das Dienstprofil und Triggerlisten (Initial Filter Criteria) des Kunden vom UPSF/HSS (Cx Interface)
- Sessionkontrolle und Routing für registrierte UE
- Prüft Medienbeschreibungen im SDP (Service Delivery Profile) gegen das Dienstprofil
- Bindet Application Server (AS) anhand der Triggerlisten in die Session ein

Initial Filter Criteria

Die Initial Filter Criteria bestehen aus einer Liste von

- Application Servern beschrieben durch deren URI.
- Bedingungen, unter denen eine Nachricht an diesen Application Server weitergeleitet wird. Mögliche Kriterien sind:
  - jede bekannte SIP Methode
  - eine unbekannte Methode
  - jeder HTTP/SIP Header der Nachricht, aber auch deren Fehlen
  - Richtung der Nachricht, d.h. vom UE (Mobile Originated) oder zum UE (Mobile Terminated)
  - SDP Anteil einer Nachricht

Erst wenn die Liste abgearbeitet ist, wird die Nachricht von der S-CSCF zu ihrem vorgesehenen Ziel weitergeleitet.

Routing der S-CSCF

Routingentscheidungen unterscheiden sich für MO und MT Nachrichten:

- Mobile Originated (MO):
  - Benutze einen DNS Server zur Bestimmung des IP Endpunktes, der im Netzwerk des Empfängers für den Kunden zuständig ist.
  - Im Erfolgsfall kann die S-CSCF die Nachricht an die I-CSCF im Zielnetz weiterleiten.
  - War die Zieladresse eine TEL-URI für die keine SIP-URI im DNS hinterlegt war, wird die Nachricht über die Breakout Gateway Control Function weitergeleitet.
- Mobile Terminated (MT):
  - Für registrierte Kunden sende die Nachricht zur P-CSCF
  - Für nicht registrierte Kunden sende die Nachricht zu einem Ersatzziel (z.B. Anrufbeantworter).

I-CSCF

Die I-CSCF ist ein zustandsloser SIP Proxy mit folgenden Funktionen:

- versteckt die Topologie des Zielnetzes
- wählt die S-CSCF aus, die für den Kunden zuständig ist
  - erfragt die S-CSCF vom HSS
  - ist im HSS keine S-CSCF eingetragen, d.h. der Kunde zur Zeit nicht registriert, weist mittels lokaler Konfiguration eine S-CSCF zu
- Bedient als SIP Client oder Server
  - die S-CSCF eines Fremdnetzes
  - die MGCF (Media Gateway Control Function) nach einem `INVITE` vom MGCF

P-CSCF

Die P-CSCF ist ein zustandsbehafteter SIP Proxy. Aufgaben sind:

- Terminiert alle SIP Transaktionen eines UE
- Leitet `REGISTER` Requests an die I-CSCF des Heimnetzes des Kunden weiter
- Leitet alle weiteren Requests des UE an die S-CSCF weiter, die von der I-CSCF bestimmt worden ist
- Fügt die Public User Identity in Requests des UE ein
- Komprimiert Nachrichten zur Übertragung über die Luftschnittstelle
- Reserviert bei Bedarf Bandbreite anhand der Daten in der SDP Nachricht.
- Terminiert verschlüsselte Verbindungen (z.B. IPSEC)

Breakout Gateway Control Function (BGCF)

Ein BGCF eines Netzes hat folgende Aufgaben:

- Ist ein PSTN das Ziel, bestimmt das BGCF das Netzwerk, in dem der Übergang stattfindet.
- Wählt bei lokalem Übergang die MGCF, andernfalls das BGCF eines anderen Netzes.
- Authentifiziert das Netz, in das weitergeleitet wird

Auswahlkriterien für die Stelle des Netzübergangs sind nicht spezifiziert, mögliche Kriterien sind:

- Aktuelle Position des Anrufers (Quellnetz)
- Heimatnetz des Angerufenen
- Lokale Konfiguration, Absprachen zwischen den beteiligten Netzbetreibern

Media Gateway Control Function (MGCF)

Die MGCF ist für folgende Funktionen zuständig:

- Protokollkonversion zwischen ISUP (ISDN User Part) und SIP
- Sie verwaltet den Zustand des Media Gateways im Rahmen eines Anrufs, d.h.
  - sie empfängt SIP Requests von S-CSCF, BGCF und I-CSCF und erzeugt daraus Kommandos des Media Gateways.
  - sie verarbeitet Signalisierungsinformation des PSTN und sendet sie an Media Gateway und I-CSCF/S-CSCF weiter.

Media Gateway (MGW)

Das Media Gateway dient der Konversion der Medienströme zwischen verschiedenen Netzen:

- kontrolliert die Datenströme getrieben durch die MGCF
- terminiert Datentransport eines CS Netzes und erzeugt daraus einen RTP Datenstrom
- erkennt Probleme im Datenstrom (z.B. Verbindungsabbruch) und informiert die MGCF
- unterstützt möglicherweise DiffServ für QoS
- DTMF Umsetzung (RFC2844 nach G.711)

Media Resource Function Controller (MRFC)

Der MRFC steuert den Media Resource Function Processor (MRFP):

- Er nimmt Kommandos der Application Server entgegen (via S-CSCF) und steuert damit den MRFP.
- Informiert einen AS (via S-CSCF) über Daten, die ein MRFP empfangen hat.

Media Resource Function Processor (MRFP)

Der MRFP kann Medienströme aufzeichnen, abspielen, konvertieren und ggfs. interpretieren.

- Auf dem MRFP sind Ansagetexte, Signaltöne und andere statische Medienströme gespeichert.
- Gespeicherte Daten können anhand von konfigurierbaren Kriterien (z.B. Sprache, Land) selektiert werden.
- Der MFRP kann verschiedene Medienströme zusammenmischen (z.B. für Telefonkonferenzen).
- Er kann Medienströme transkodieren und extrahieren (z.B. nur Ton aus einer Videokonferenz).
- Er informiert einen Application Server (via MRFC, S-CSCF) über eingegangene DTMF Ziffern.

P-Header

IMS definiert einige private Header, die von IMS Knoten eingesetzt bzw. interpretiert werden:

- **P-Asserted-Identity**: Wird üblicherweise von der P-CSCF eingesetzt, wenn der Nutzer über das Netzwerk sicher identifiziert ist.
- **P-Called-Party-ID**: Da die S-CSCF in die URI des Requests die registrierte Adresse des UEs einsetzt, geht die ursprüngliche Public User ID verloren. Diese wird daher in den P-Called-Party-ID kopiert.
- **P-Access-Network-Info**: In diesen Header setzt der UE, über welchen Typ von Netz er mit der P-CSCF verbunden ist, z.B.: `P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=123`
  UTRAN = UMTS Terrestrial Radio Access Network

P-Header

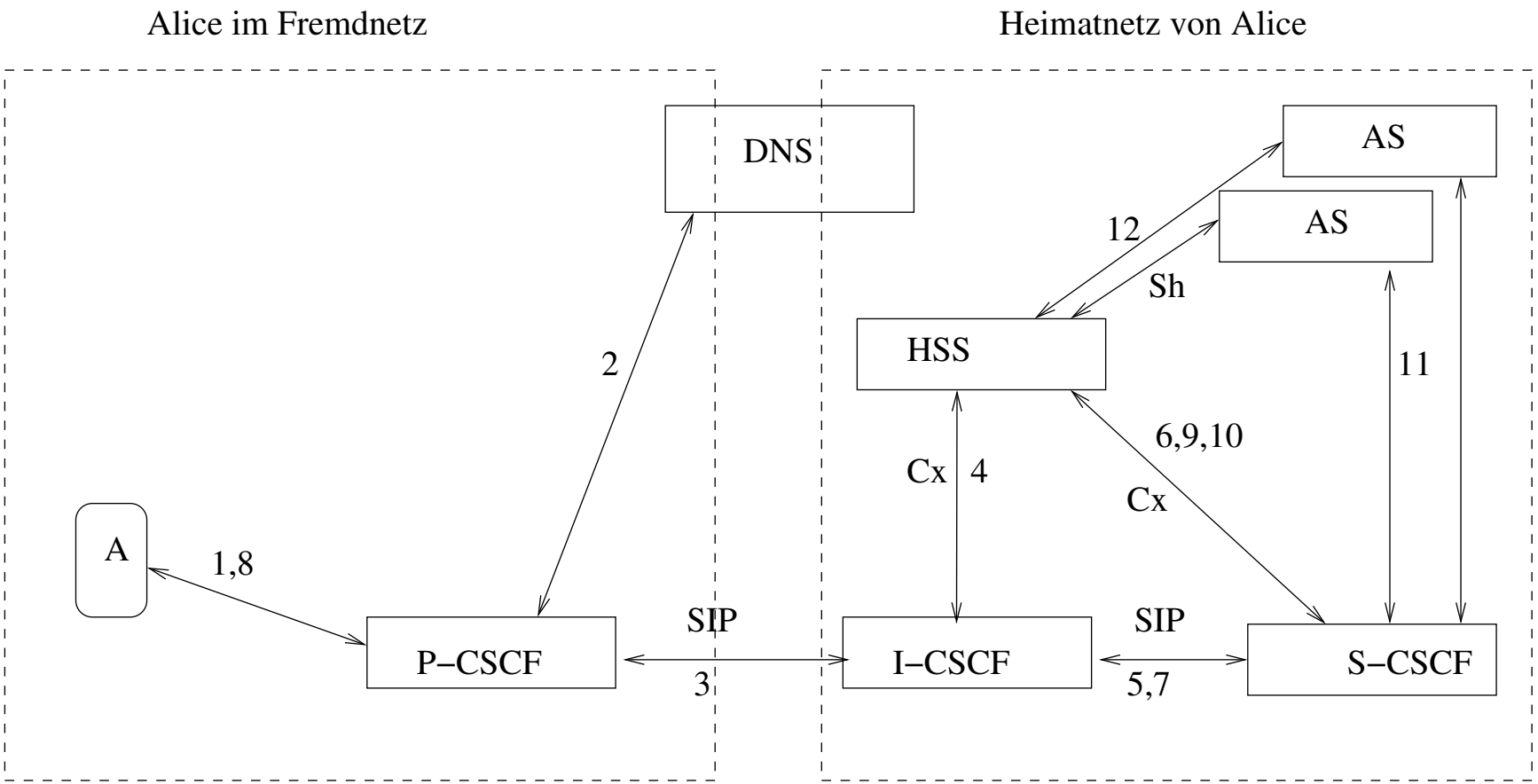
- **P-Visited-Network-ID**: Name des aktuellen Netzes, eingesetzt durch die P-CSCF
- **P-Associated-URI**: Liste von Public User IDs, die dem Nutzer ebenfalls zugeordnet sind, gesendet in einer Antwort auf ein `REGISTER`.
- **P-Charging-Function-Address**: Enthält die Adresse (z.B. IP) eines Abrechnungsknotens, sie wird von der S-CSCF eingesetzt und beim Verlassen des Heimnetzes wieder entfernt.
- **P-Charging-Vector**: Dient zur Korrelation zwischen Abrechnungsdaten, wird von der P-CSCF beim initialen `REGISTER` erzeugt.

Verwendung von SDP (Session Description Protocol)

Die Verwendung von SDP unterliegt bei IMS einigen Einschränkungen, die eine Kontrolle durch den Netzbetreiber ermöglichen:

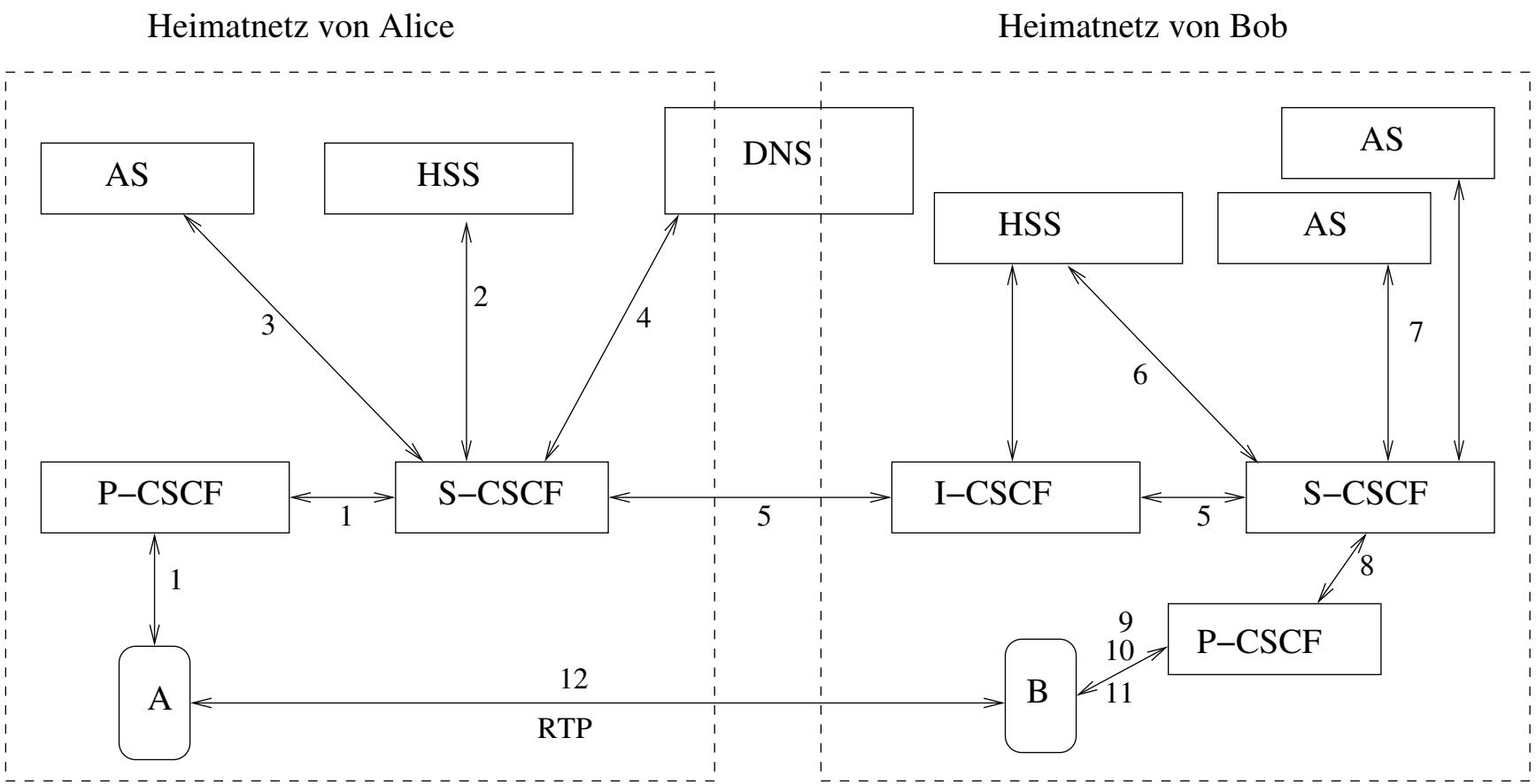
- SDP Daten dürfen nicht verschlüsselt werden.
- Die SDP Daten sollen die Fähigkeiten der Endgerätes angeben, d.h. die unterstützten Codecs in der Reihenfolge ihrer Priorität.
- Bandbreitenangaben für Audio und Video sollen enthalten sein (b= Header).

Registrierung aus einem Fremdnetz



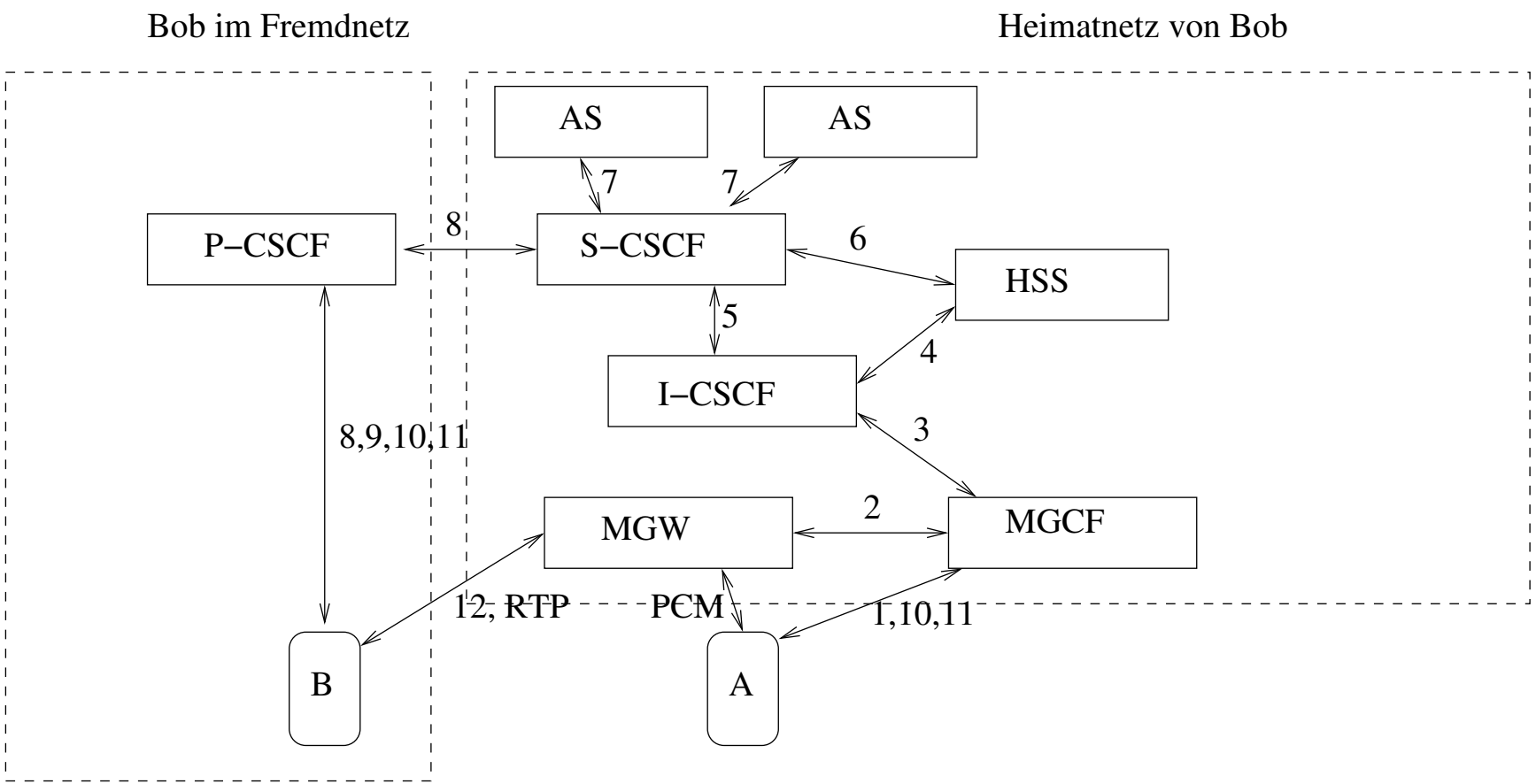
1. Starte SIP `REGISTER`
2. Bestimme IP/Port der I-CSCF des Heimatnetzes
3. Sende SIP `REGISTER` an I-CSCF des Heimatnetzes
4. Bestimme S-CSCF für den Kunden
5. Sende SIP `REGISTER` an die ausgewählte S-CSCF
6. Hole Authentifizierungsdaten (Authenication Vector, Vorstufe der Challenge vom HSS)
7. Weise den `REGISTER` ab (407 Proxy Auth Required)
8. Erneuter `REGISTER`, diesmal mit Response zur Challenge
9. Lege S-CSCF URI im HSS ab.
10. Hole Profil und Triggerlisten vom HSS
11. Sende `REGISTER` an Application Server, die das benötigen (s. Triggerlisten)
12. AS holen bei Bedarf Teile des Kundenprofils vom HSS

Telefonat IMS zu IMS



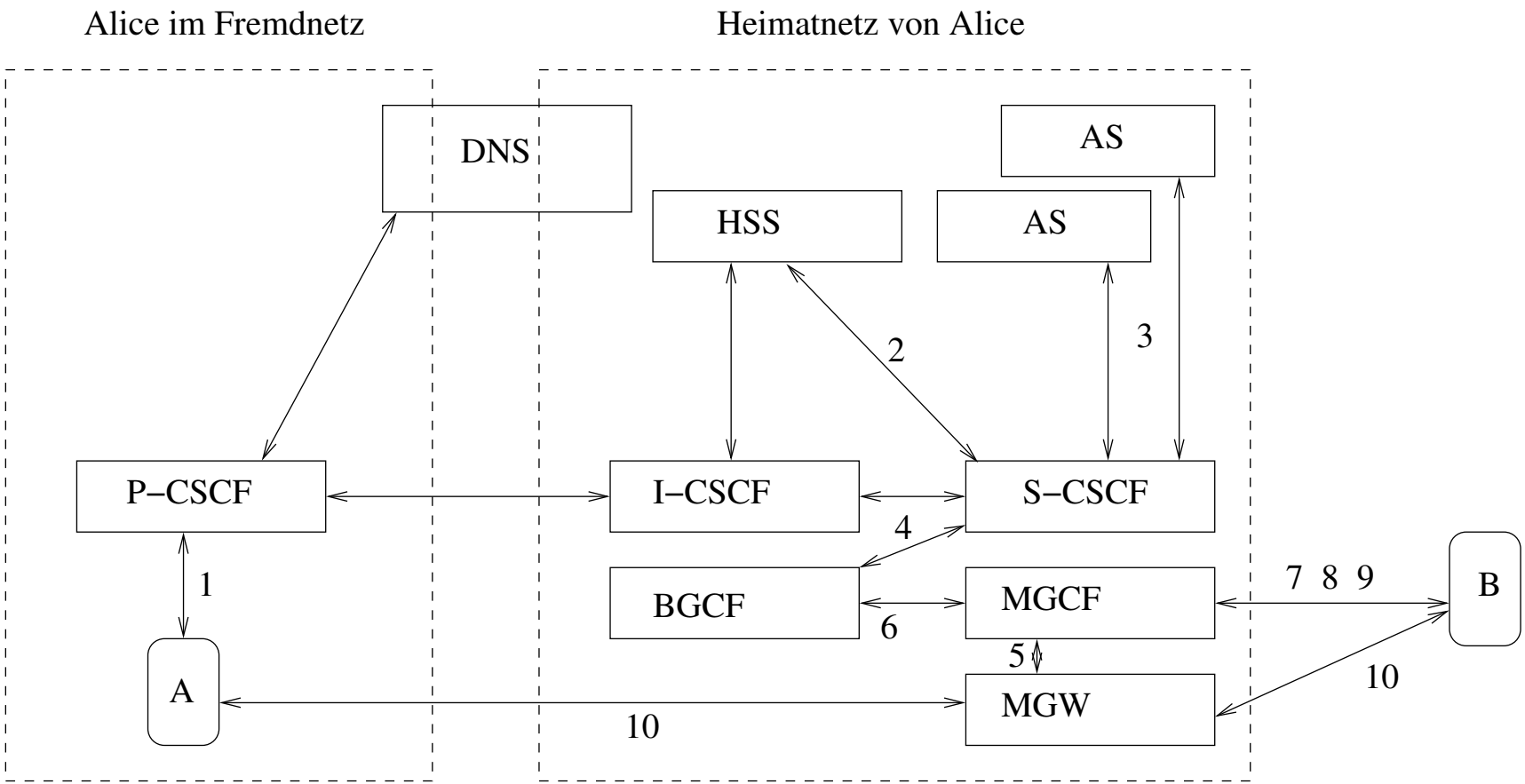
1. Alice sendet `INVITE` an Bob (URI mit Public User ID).
2. Die S-CSCF bestimmt Profil und Triggerlisten von Alice.
3. Bei Bedarf werden Application Server eingebunden.
4. Per DNS wird die Adresse der I-CSCF von Bobs Heimatnetz bestimmt.
5. Der `INVITE` wird über die I-CSCF an die zuständige S-CSCF weitergereicht.
6. Die S-CSCF bestimmt Profil und Triggerlisten von Bob.
7. Bei Bedarf werden Application Server eingebunden.
8. Der `INVITE` wird via P-CSCF an Bobs UE geschickt.
9. Das Endgerät interpretiert den SDP Anteil des `INVITE`
10. Das Endgerät klingelt (`180 RINGING`)
11. Bob akzeptiert den Anruf (`200 Ok`)
12. RTP Datenstrom

Telefonat PSTN an IMS



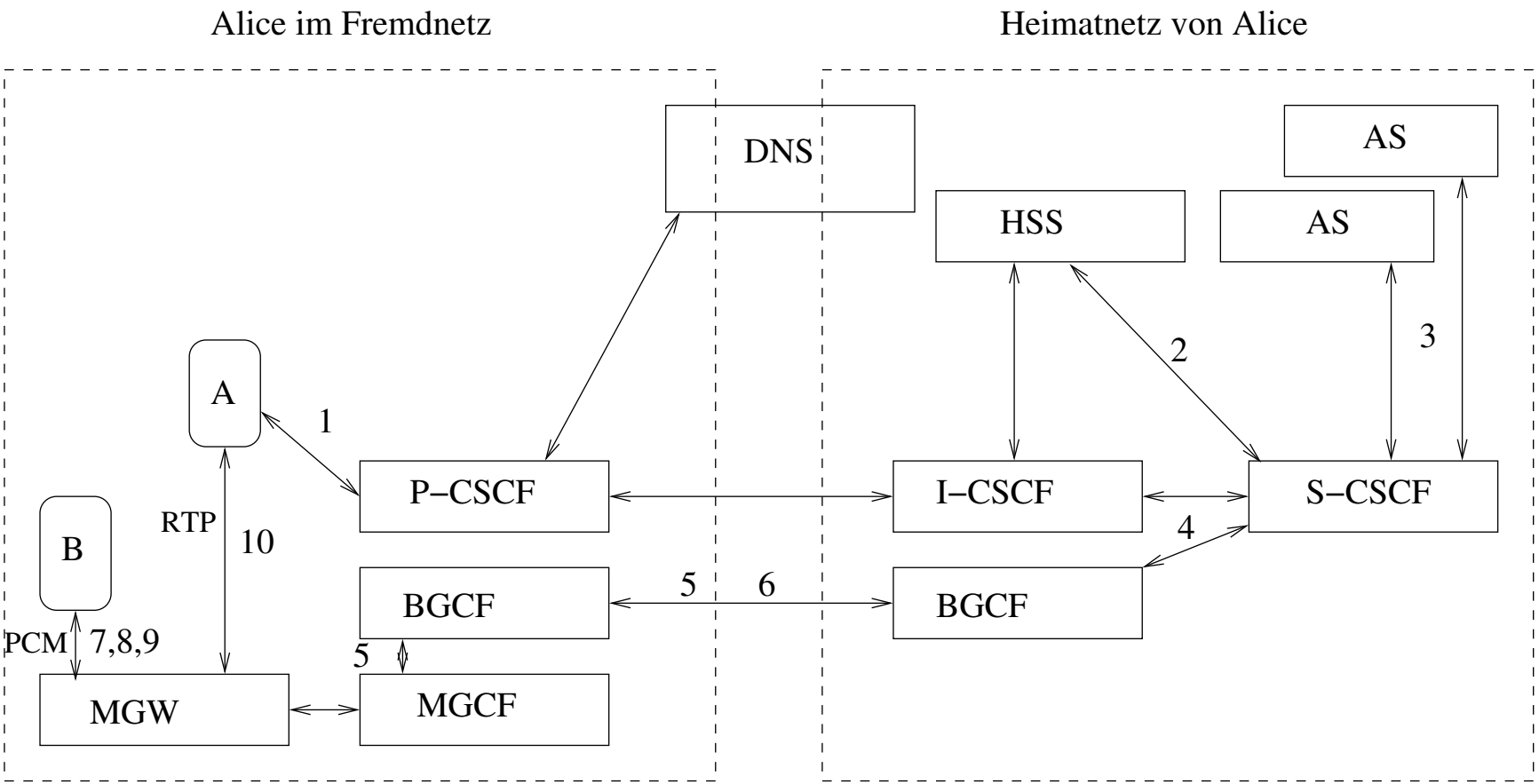
1. Anruf wird per ISUP (ISDN User Part) an der MGCF signalisiert
2. Das Media Gateway wird über den ISDN (PCM) Datenstrom informiert. Der ausgehende Port für den RTP Strom wird festgelegt.
3. Die MGCF erzeugt ein SIP `INVITE`.
4. Bestimme die zuständige S-CSCF.
5. Sende das `INVITE` zur S-CSCF.
6. Hole Profil und Triggerlisten für Bob vom HSS.
7. Binde bei Bedarf AS ein.
8. Sende `INVITE` an die P-CSCF des Netzes, in dem Bob eingebucht ist.
9. Bobs UE wertet SDP Nachricht aus.
10. UE sendet `180 Ringing`.
11. UE sendet `200 Ok`.
12. RTP Strom zum MGW auf dem gegebenen Port.

Telefonat IMS an PSTN (Variante 1)



1. Sende SIP `INVITE`
2. Hole Profil und Triggerlisten vom HSS
3. Arbeite Triggerlisten ab
4. Bestimme BGCF und MGCF
5. Konfiguriere MGW, lege Port für RTP Strom fest
6. Bilde SDP Antwort (Auswahl des Codecs)
7. ISUP Signalisierung zum PSTN Telefon
8. SIP `180 RINGING`
9. SIP `200 Ok`
10. RTP - PCM Datenstrom

Telefonat IMS an PSTN (Variante 2)



DIAMETER Base Protocol (RFC3588)

DIAMETER kontrolliert authentication, authorization und accounting (AAA). Benutzt für die Kommunkation zwischen HSS und anderen Entities (S-CSCF, AS,...)
DIAMETER ist eine (nicht rückwärtskompatible) Fortentwicklung des RADIUS Protokolls (Remote Authentication Dial In User Service, RFC2865). Die wichtigsten Unterschiede sind:

- Es benutzt einen zuverlässigen Transport (z.B. TCP)
- DNS SRV und NAPTR zum Auffinden eines Servers
- Unterstützt verschiedenen Nachrichtentypen auf einem Transport
- leicht erweiterbar
- bidirektional (Push - Pull Dienste)
- Länge von Attributen ist auf 16kB begrenzt, nicht 253B

DIAMETER Rahmen

0 32

Version	Message Length
Flags	Command–Code
Application ID	
Hop–by–Hop ID	
End–to–End ID	
AVPs	

Felder im DIAMETER Rahmen

- **Version**: 1 für Diameter nach RFC3588
- **Message Length**: Länge in Byte inklusive der Header
- **Flags**: 8Bit, von denen 0-3 benutzt werden:
  0. 1 für Request, 0 für Response
  1. Nachricht kann von Proxies weitergeleitet werden.
  2. Error Message, darf nicht in Requests gesetzt werden.
  3. Erneute Übertragung nach einem Link Fehler
- **Command-Code**: Typ der Nachricht, die Werte werden durch die IANA verwaltet.

Felder im DIAMETER Rahmen

- **Application-ID**: Identifiziert die Anwendung, muß mit einem Application-ID Attribut übereinstimmen.
- **Hop-by-Hop ID**: 32Bit, dienen dazu, Request und Response einander zuzuordnen, muß in einem gewissen Zeitfenster eindeutig sein (auch nach Neustart).
- **End-to-End ID**: 32Bit, um Doubletten erkennen zu können, muß im Zeitfenster von 4 Minuten eindeutig sein (auch nach Neustart).
- **AVPs**: Folge von Attribut-Wert Paaren

DIAMETER AVP

<table>
<tr><td colspan="2">AVP Code</td></tr>
<tr><td>Flags</td><td>AVP Length</td></tr>
<tr><td colspan="2">Vendor ID</td></tr>
<tr><td colspan="2">Data</td></tr>
</table>

Felder im DIAMETER AVP

- **AVP Code**: Identifiziert (zusammen mit der Vendor-ID) den Typ des Attributes
- **Flags**: Nur Bits 0-2 werden benutzt:
  0. Vendor-ID ist im Rahmen
  1. Attribut muß vorhanden sein (bei dieser Nachricht)
  2. Attribut ist verschlüsselt
- **AVP Length**: Länge des Attributes in Bytes vom AVP-Code bis zum Ende der Daten
- **Vendor-ID**: Namensraum, in dem der AVP-Code interpretiert wird.
- **Data**: Daten, die je nach AVP-Code interpretiert werden.

XML Beispiel

```
<?xml version=”1.0” encoding=” UTF-8”?>
<presence>
xmlns=” urn:ietf:params:xml:ns:pidf”
entity=” sip:test@10.1.195.159”>
<tuple id=”udupwd”>
<status>
<basic>busy</basic>
</status>
</tuple>
</presence>
```

XPath, `http://www.w3.org/TR/xpath`

Sprache, um Teile eines XML Dokumentes zu adressieren:

- `text()`: Zugriff auf Textknoten
- `[Name="Wert"]`: Test auf Textknoten, z.B.: `status[basic="busy"]`
- `.../@Name`: Zugriff auf Wert eines Attributes
- `[@Name="Wert"]`: Test auf Wert eines Attributes
- `.../Name1/Name2`: Abstieg im Dokumentbaum
- `.../Name1[n]`: *n*-te Instanz von Name1

Beispielimplementation in Python

```
from xml.xpath import Evaluate
from xml.dom import minidom

path =
'/presence[@entity="sip:test@10.1.195.159"]//status/basic'

doc = minidom.parse("test.xml").documentElement
x = Evaluate(path, doc)
print x[0].toxml()

# ergibt:
<basic>busy</basic>
```

XML Configuration Access Protocol (XCAP, RFC4825)

XCAP dient dazu, in hierarchisch strukturierten Daten (XML Dateien), Einträge einzufügen, zu verändern oder zu löschen.

- XCAP basiert auf HTTP, die URL ist ein XPath Ausdruck, der ein Teildokument referenziert.
- `GET` liest den referenzierten Teil.
- `PUT` fügt den Nachrichtenkörper an der angegebenen Stelle in das Dokument ein.
- `DELETE` löscht den referenzierten Teilbaum des Dokumentes.

XDMS (vgl. OMA-ERELD-XDM-V1_0_1-20061128-A.pdf)

Ein XML Document Management Server dient dazu, ein XML Dokument in einer SIP/IMS Infrastruktur zugreifbar zu machen.

- XCAP dient dazu, Teile eines Dokumentes zu bearbeiten
- SUBSCRIBE wird benutzt, damit ein Kunde automatisch über Änderungen von Teilen des XML Dokumentes informiert wird.
- NOTIFY wird vom XDMS gesendet, wenn sich ein Teil des Dokumentes geändert hat und der Kunde darauf subscribiert ist.