International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3612

(06/2011)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Service and session control protocols – supplementary services

Signalling requirements and protocol profiles for IP Centrex service

Recommendation ITU-T Q.3612

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3999
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	**Q.3600–Q.3649**
NGN applications	Q.3700–Q.3849
Testing for NGN networks	Q.3900–Q.3999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Q.3612

Signalling requirements and protocol profiles for IP Centrex service

Summary

The IP Centrex service, which is defined in Recommendation ITU-T Y.2211, can be provided over either IMS-based or call-server based components. This Recommendation provides the general architecture of the IP Centrex service, and specifies the signalling requirements and protocol profiles for the IP Centrex service. The signalling flows of the IP Centrex service are also provided in this Recommendation.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Q.3612	2011-06-29	11

Keywords

IP Centrex, NGN, SDP, SIP.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

The IP Centrex service is a PBX-like service, but it is provided by the central office rather than the customer's premises and is implemented over an IP-basic network, such as an NGN. The IP Centrex service is defined in [ITU-T Y.2211]. This Recommendation specifies the signalling requirements and protocol profiles for the IP Centrex service provided over an NGN. The signalling flows of the IP Centrex service are also provided in this Recommendation.

Recommendation ITU-T Q.3612

Signalling requirements and protocol profiles for IP Centrex service

1 Scope

This Recommendation specifies signalling requirements and protocol profiles of the IP Centrex service. The Recommendation also contains signalling flows.

The IP Centrex service can be provided over either IMS-based or call-server-based networks, as per [ITU-T Y.2211].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Q.3402] Recommendation ITU-T Q.3402 (2008), *NGN UNI signalling profile (Protocol set 1)*.

[ITU-T Y.2211] Recommendation ITU-T Y.2211 (2007), *IMS-based real-time conversational multimedia services over NGN*.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[IETF RFC 2401] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

[IETF RFC 2633] IETF RFC 2633 (1999), *S/MIME Version 3 Message Specification*.

[IETF RFC 3262] IETF RFC 3262 (2002), *Reliability of Provisional Responses in the Session Initiation Protocol (SIP)*.

[IETF RFC 3323] IETF RFC 3323 (2002), *A Privacy Mechanism for the Session Initiation Protocol (SIP)*.

[IETF RFC 3325] IETF RFC 3325 (2002), *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*.

[IETF RFC 3515] IETF RFC 3325 (2002), *The Session Initiation Protocol (SIP) Refer Method*.

[IETF RFC 3891] IETF RFC 3891 (2004), *The Session Initiation Protocol (SIP) "Replaces" Header*.

[IETF RFC 3892] IETF RFC 3892 (2004), *The Session Initiation Protocol (SIP) Referred-By Mechanism*.

[IETF RFC 4244] IETF RFC 4244 (2005), *An Extension to the Session Initiation Protocol (SIP) for Request History Information*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 picking-up endpoint/user [b-ITU-T H.450.5]: A user/endpoint that picks-up a parked call or an alerting call.

3.1.2 pickup group [b-ITU-T H.450.5]: A group of users that may be notified when one of the group members receives a call that can be picked up. Each group member is authorized to answer the call by using SS-PICKUP.

3.2 Terms defined within this Recommendation

This Recommendation defines the following terms:

3.2.1 Centrex service: A services package which provides an emulation of a private branch exchange (PBX) by using special programming software at the central office, instead of at the customer's premises.

NOTE – The typical feature is that users within the same group can communicate with each other by using the private number instead of the public number (i.e., full subscriber number).

3.2.2 communication pickup: A service that enables an IP Centrex user to pick up an alerting call within the same Centrex group when the alerted user is unavailable to answer the call.

3.2.3 group pickup: One of the two service features for communication pickup. Group pickup enables a pickup group user to pick up an alerting call within the same pickup group without dialling the picked-up user's private number.

3.2.4 IP Centrex service: A certain type of Centrex service which is provided over an IP-based network, such as an NGN. The typical service features included in the IP Centrex service are defined in [ITU-T Y.2211].

3.2.5 picked-up user: A user whose call is picked up by a picking-up user.

3.2.6 private number: A certain number only used within a given Centrex group. It is shorter than the user's local public number, and typically has only three, four or five digits, depending on how large the Centrex group is.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AGC-FE	Access Gateway Control Functional Entity
ASF	Application Service Function
AS-FE	Application Server Functional Entity
EUF	End-User Function
I-CSC-FE	Interrogating Call Session Control Functional Entity
IMS	IP Multimedia Subsystem
ISDN	Integrated Services Digital Network
MGC-FE	Media Gateway Control Functional Entity
PBX	Private Branch eXchange
P-CSC-FE	Proxy Call-Session-Control Functional Entity
SCF	Service Control Function

S-CSC-FE	Serving Call-Session-Control Functional Entity
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SUP-FE	Service User Profile Functional Entity
TLS	Transport Layer Security
UE	User Equipment
UNI	User Network Interface

5 Conventions

In this Recommendation:

The keyword "shall" indicates a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "shall not" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keyword "should" indicates a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "should not" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this Recommendation can still be claimed even if this requirement is present.

The keyword "may" indicates an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Service architecture

6.1 General architecture

The IP Centrex service as defined in [ITU-T Y.2211] can be provided over either an IMS-based or a call-server-based subsystem. Figure 6-1 depicts the general architecture [ITU-T Y.2211].

The IP Centrex service logic and service executing environments are provided by an application service function (ASF) within the service stratum. The originating and terminating IP Centrex service logics serving for a designated Centrex group are provided by one ASF. When serving the originating network, the ASF performs the originating IP Centrex service logic invoked by the originating service control function (SCF), which shall include internal communication and originating identification restriction service features. When serving the terminating network, the ASF performs the terminating IP Centrex service logic invoked by the terminating SCF, which shall include the internal communication, the originating identification presentation and the terminating identification restriction.

The SCF holds the service subscription profile for the NGN user and performs the service-trigger function. The end user who subscribes to the IP Centrex service may reside in the IMS component or in the call-server component. Both of these components can invoke the IP Centrex service.

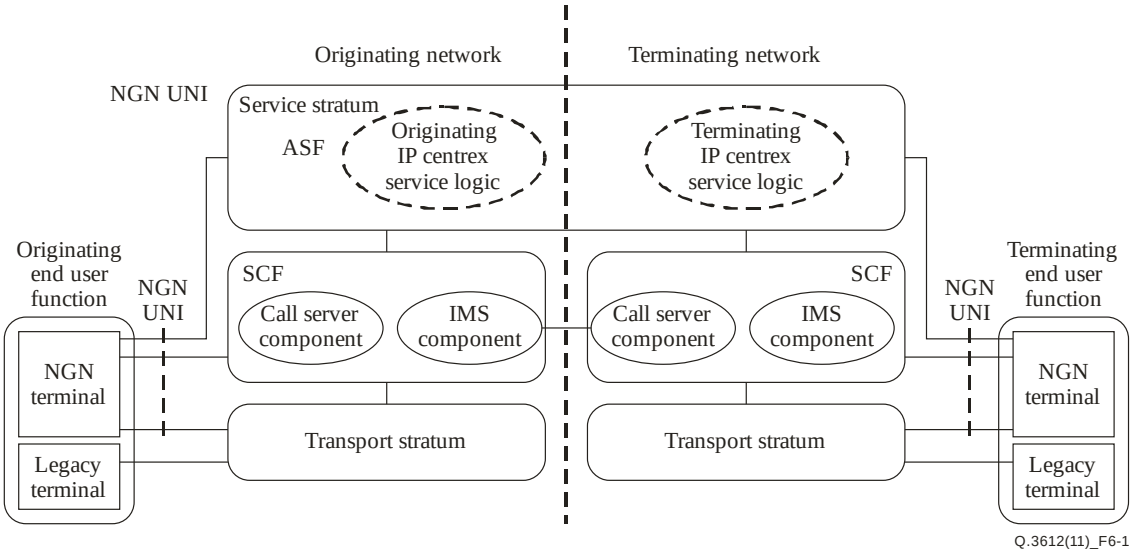

Figure 6-1 – The general architecture of IP Centrex service

6.2 Functional entities involved in IP Centrex service

Figure 6-2 illustrates the functional entities involved in the IP Centrex service.

In the originating network, the originating end-user function is the end user that originates the IP Centrex session. If the end-user function resides in the call-server-based component, the related functional entities shall be the call server, the service-user-profile functional entity (SUP-FE) and the application-server functional entity (AS-FE). When the end-user function resides in the IMS-based component, the related functional entities shall be the access gateway control functional entity (AGC-FE), the proxy/serving call-session-control functional entity (P/S-CSC-FE) and the application server functional entity (AS-FE).

In the terminating network, the terminating end-user function is the end user that terminates the IP Centrex session. When the end user resides in the call-server-based component, the related functional entities shall be the call server, the SUP-FE and the AS-FE. When the end user resides in the IMS-based component, the related functional entities shall be the AGC-FE, the P/S-CSC-FE, the interrogating call session control functional entity (I-CSC-FE) and the AS-FE.

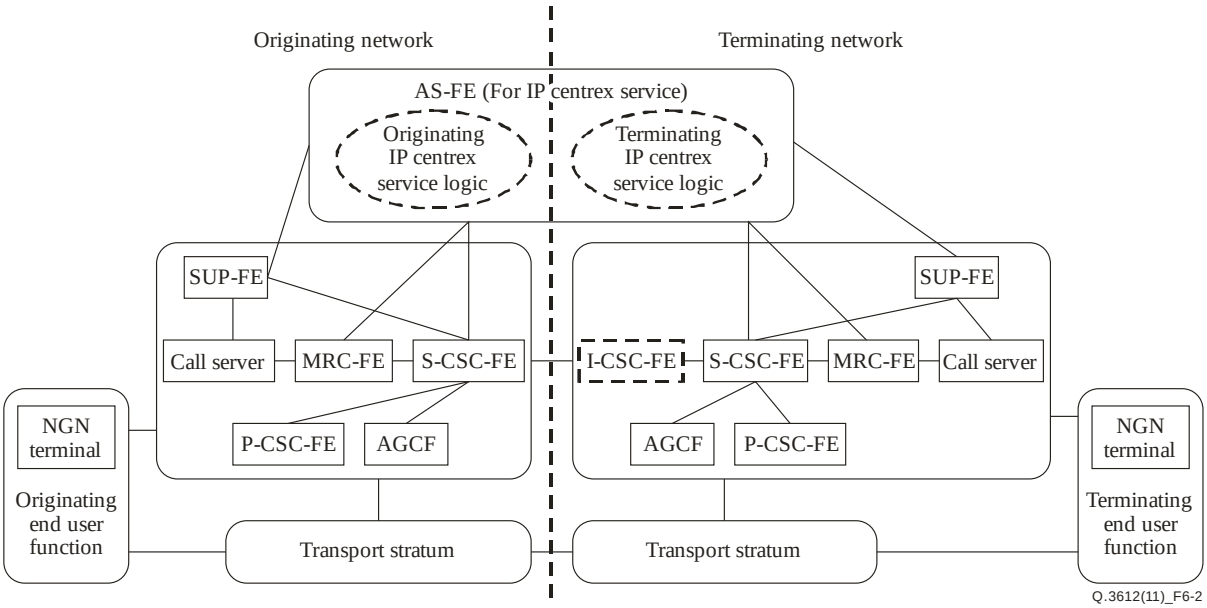

Figure 6-2 – The functional entities involved in the IP Centrex service

7 Signalling requirements

7.1 General description

According to [ITU-T Y.2211] and service features used in the current PBX service, this Recommendation defines the signalling requirements of the following service features:

1) Internal communication
2) Outgoing communication
3) Incoming communication
4) Originating identification presentation
5) Originating identification restriction
6) Terminating identification presentation
7) Terminating identification restriction
8) Communication transfer
9) Communication diversion
10) Communication pickup
11) Communication hold

7.2 Signalling requirements

7.2.1 Internal communication

The internal communication service feature enables a Centrex user to communicate with another user in the same Centrex Group with a private number.

When initiating a call, the originating party can directly dial the private number of the terminating party. Based on the terminating party's service profile, if the identities of the originating party can be presented to the terminating party, the private number of the originating party shall be presented.

7.2.1.1 Requirements for the originating user equipment (UE)

When the originating user equipment (UE) initiates an INVITE request, the private number of the terminating party shall be included in the Request-URI.

7.2.1.2 Requirements for the originating access gateway control functional entity (AGC-FE)

When the originating AGC-FE initiates an INVITE request, the private number of terminating party shall be included in the Request-URI.

7.2.1.3 Requirements for the originating proxy call-session-control functional entity (P-CSC-FE)

No special requirement for this FE.

7.2.1.4 Requirements for the originating serving call-session-control functional entity (S-CSC-FE)

No special requirement for this FE.

7.2.1.5 Requirements for the originating call server

No special requirement for this FE.

7.2.1.6 Requirements for the application server functional entity (AS-FE)

When sending an INVITE request to the terminating interrogating call-session-control functional entity (I-CSC-FE), the terminating S-CSC-FE or the terminating call server, the AS-FE shall:

1) include the private number of the originating party in the P-Asserted-identity header field.

2) include the public user identity of the terminating party in the Request-URI.

7.2.1.7 Requirements for the terminating call server

No special requirement for this FE.

7.2.1.8 Requirements for the terminating interrogating call session control functional entity (I-CSC-FE)

No special requirement for this FE.

7.2.1.9 Requirements for the terminating S-CSC-FE

No special requirement for this FE.

7.2.1.10 Requirements for the terminating P-CSC-FE

No special requirement for this FE.

7.2.1.11 Requirements for the terminating UE

If the identities of the originating party are allowed to be presented to the terminating party, the private number shall be presented.

7.2.1.12 Requirements for the terminating AGC-FE

If the identities of the originating party are allowed to be presented to the terminating party, the private number shall be presented.

7.2.2 Outgoing communication

The outgoing communication service feature enables a Centrex user to initiate the communication with a public user.

7.2.2.1 Requirements for the originating UE

No special requirement for this FE.

7.2.2.2 Requirements for the originating AGC-FE

No special requirement for this FE.

7.2.2.3 Requirements for the originating P-CSC-FE

No special requirement for this FE.

7.2.2.4 Requirements for the originating S-CSC-FE

No special requirement for this FE.

7.2.2.5 Requirements for the originating call server

No special requirement for this FE.

7.2.2.6 Requirements for the AS-FE

When the AS-FE sends an INVITE request to the originating S-CSC-FE or the originating call server, the public user identity of the terminating party shall be included in the Request-URI header field.

7.2.2.7 Requirements for the terminating call server

No special requirement for this FE.

7.2.2.8 Requirements for the terminating I-CSC-FE

No special requirement for this FE.

7.2.2.9 Requirements for the terminating S-CSC-FE

No special requirement for this FE.

7.2.2.10 Requirements for the terminating P-CSC-FE

No special requirement for this FE.

7.2.2.11 Requirements for the terminating UE

No special requirement for this FE.

7.2.2.12 Requirements for the terminating AGC-FE

No special requirement for this FE.

7.2.3 Incoming communication

The incoming communication service feature enables a public user to initiate the communication with a Centrex user.

7.2.3.1 Requirements for the originating UE

No special requirement for this FE.

7.2.3.2 Requirements for the originating AGC-FE

No special requirement for this FE.

7.2.3.3 Requirements for the originating P-CSC-FE

No special requirement for this FE.

7.2.3.4 Requirements for the originating S-CSC-FE

No special requirement for this FE.

7.2.3.5 Requirements for the originating call server

No special requirement for this FE.

7.2.3.6 Requirements for the AS-FE

When the AS-FE sends an INVITE request to the terminating I-CSC-FE, or the terminating S-CSC-FE, or the call server, the originating party's identities contained in the P-Asserted-Identity header field can be used by the terminating party to call back directly.

If the outgoing communication needs a prefix, the public user identity with the prefix shall be presented to the terminating party in the incoming communication.

7.2.3.7 Requirements for the terminating call server

No special requirement for this FE.

7.2.3.8 Requirements for the terminating I-CSC-FE

No special requirement for this FE.

7.2.3.9 Requirements for the terminating S-CSC-FE

No special requirement for this FE.

7.2.3.10 Requirements for the terminating P-CSC-FE

No special requirement for this FE.

7.2.3.11 Requirements for the terminating UE

No special requirement for this FE.

7.2.3.12 Requirements for the terminating AGC-FE

No special requirement for this FE.

7.2.4 Originating identification presentation

The originating identification presentation service feature enables the originating party's identification to be presented to the terminating party.

1) The private number of the originating party shall be presented to the terminating party in the internal communication scenario.
2) The public user identity of the originating party shall be presented to the terminating party in the incoming communication scenario.

This service feature can be activated by the terminating party.

7.2.4.1 Requirements for the originating UE

No special requirement for this FE.

7.2.4.2 Requirements for the originating AGC-FE

When sending an INVITE request to the originating S-CSC-FE, the AGC-FE shall insert a P-Asserted-Identity header field. The P-Asserted-Identity header field shall be set to the public user identity which has been registered in the network by the originating party.

7.2.4.3 Requirements for the originating P-CSC-FE

When sending an INVITE request to the originating S-CSC-FE, the P-CSC-FE shall insert a P-Asserted-Identity header field. The P-Asserted-Identity header field shall be set to the public user identity which has been registered in the network by the originating party.

7.2.4.4 Requirements for the originating S-CSC-FE

No special requirement for this FE.

7.2.4.5 Requirements for the originating call server

When sending an INVITE request to the originating AS-FE, the call server shall insert a P-Asserted-Identity header field. The P-Asserted-Identity header field shall be set to the public user identity which has been registered in the network by the originating party.

7.2.4.6 Requirements for the AS-FE

When AS-FE receives an INVITE request from the terminating S-CSC-FE or call server, the terminating party AS-FE shall:

1) verify whether the terminating party has activated the originating identification presentation service. If not, the AS-FE shall add the Privacy header field, if it is not contained in the INVITE request, and set the value to "id", then set the From header field to "Anonymous" and send the INVITE request to the terminating S-CSC-FE or the call server.

   NOTE – The value of the Privacy header field refers to [IETF RFC 3323] and [IETF RFC 3325].

2) verify whether the originating party and the terminating party are in the same Centrex group. If they are, then the AS-FE shall change the public user identity of the originating party in the P-Asserted-Identity header field into Private number.

7.2.4.7 Requirements for the terminating call server

When receiving an INVITE request,

1) if the Privacy header field is contained with the value unequal to "none", the terminating call server shall delete the P-Asserted-Identity header field if it is contained in the INVITE request before forwarding the message to the terminating party.

2) otherwise, the P-Asserted-Identity header field shall be forwarded to the terminating party.

7.2.4.8 Requirements for the terminating I-CSC-FE

No special requirement for this FE.

7.2.4.9 Requirements for the terminating S-CSC-FE

No special requirement for this FE.

7.2.4.10 Requirements for the terminating P-CSC-FE

When receiving an INVITE request,

1) if the Privacy header field is contained with the value unequal to "none", the P-CSCF-FE shall delete the P-Asserted-Identity header field if it is contained in the INVITE request before forwarding the INVITE request to the terminating party.

2) otherwise, the P-Asserted-Identity header field shall be forwarded to the terminating party.

7.2.4.11 Requirements for the terminating UE

If a P-Asserted-Identity header field is included in an INVITE request, the originating identification in the header field shall be presented to the terminating party. If more than one P-Asserted-Identity header field is received, the identity that is presented will be decided by a local policy.

If the P-Asserted-Identity header field is not contained in the INVITE request, the information about the FROM header field shall be presented to the terminating party.

7.2.4.12 Requirements for the terminating AGC-FE

When receiving an INVITE request,

1) if a P-Asserted-Identity header field is contained in the INVITE request, and the Privacy header field is not contained or is contained with the value setting at "none", the information about the P-Asserted-Identity shall be presented to the terminating party.

2) otherwise, the information about the FROM header field shall be presented to the terminating party.

7.2.5 Originating identification restriction

The originating identification-restriction-service feature restricts the calling party's identities to be presented to the called party, even when the called party has activated the originating identification presentation.

This service feature shall be activated by the calling party.

7.2.5.1 Requirements for the originating UE

No special requirement for this FE.

7.2.5.2 Requirements for the originating AGC-FE

No special requirement for this FE.

7.2.5.3 Requirements for the originating P-CSC-FE

No special requirement for this FE.

7.2.5.4 Requirements for the originating S-CSC-FE

No special requirement for this FE.

7.2.5.5 Requirements for the originating call server

No special requirement for this FE.

7.2.5.6 Requirements for the AS-FE

When the AS-FE receives an INVITE request from the originating S-CSC-FE or call server and executes the originating IP Centrex service logic, the INVITE request sent from the AS-FE shall:

1) include the Privacy header field with the value setting at "id";
2) set the From header field to "Anonymous".

7.2.5.7 Requirements for the terminating call server

When receiving an INVITE request, the terminating call server shall delete the P-Asserted-Identity header field before forwarding the message to the called party if the Privacy header field is contained with the value unequal to "none".

7.2.5.8 Requirements for the terminating I-CSC-FE

No special requirement for this FE.

7.2.5.9 Requirements for the terminating S-CSC-FE

No special requirement for this FE.

7.2.5.10 Requirements for the terminating P-CSC-FE

When receiving an INVITE request, the P-CSC-FE shall delete the P-Asserted-Identity header field before forwarding the message to the called party if the Privacy header field is contained with the value unequal to "none".

7.2.5.11 Requirements for the terminating UE

When receiving an INVITE request, the information about the FROM header field shall be presented to the called party.

7.2.5.12 Requirements for the terminating AGC-FE

When receiving an INVITE request, if a Privacy header field is contained with the value unequal to "none", the information of the FROM header field shall be presented to the called party.

7.2.6 Terminating identification presentation

7.2.6.1 Requirements for the originating UE

If a 200 (OK) response for the INVITE request includes more than one P-Asserted-Identity header field, the UE shall select one and present it to the originating party.

7.2.6.2 Requirements for the originating AGC-FE

When receiving a 200 (OK) response to the INVITE request, if the Privacy header field is not included in this response or the Privacy header field which is included with a value of "none", the AGC-FE shall provide the information extracted from P-Asserted-Identity to the Originating UE.

NOTE – If more than one P-Asserted-Identity header field is received, the identity that is presented to the originating party will be decided by a local policy.

7.2.6.3 Requirements for the originating P-CSC-FE

When receiving a 200 (OK) response to the INVITE request, if the Privacy header field is not included in this response or the Privacy header field which is included in this response has a value of "none", the P-CSC-FE shall provide the P-Asserted-Identity to the originating UE.

7.2.6.4 Requirements for the originating S-CSC-FE

No special requirement for this FE.

7.2.6.5 Requirements for the originating call server

When receiving a 200 (OK) response to the INVITE request, if the Privacy header field is not included in this response or the Privacy header field which is included in this response has a value of "none", the originating call server shall provide the information extracted from the P-Asserted-Identity to the originating UE.

NOTE – If more than one P-Asserted-Identity header field is received, the identity that is presented to the originating party will be decided by a local policy.

7.2.6.6 Requirements for the AS-FE

When AS-FE receives a 200 (OK) response to the INVITE request from the originating S-CSC-FE or call server, AS-FE shall:

a) verify whether the originating party has activated the terminating identification presentation service. If not, the AS-FE shall add the Privacy header field if it is not contained in the 200 (OK) response and set the value to "id", then send this response to the originating S-CSC-FE or the originating call server, and

b) verify whether the originating party and the terminating party are in the same Centrex. If they are, then the AS-FE shall change the public user identity of the terminating party in the P-Asserted-Identity into private number.

7.2.6.7 Requirements for the terminating call server

When the terminating party answers the call, the terminating call server shall insert a P-Asserted-Identity header field into a 200 (OK) response to the INVITE request before forwarding this 200 OK. The P-Asserted-Identity shall be set to the public user identity of the terminating party which has been registered in the network by the terminating party.

7.2.6.8 Requirements for the terminating I-CSC-FE

No special requirement for this FE.

7.2.6.9 Requirements for the terminating S-CSC-FE

No special requirement for this FE.

7.2.6.10 Requirements for the terminating P-CSC-FE

When the terminating P-CSC-FE receives a 200 (OK) response to the INVITE request from the terminating UE. The Terminating P-CSC-FE shall then insert a P-Asserted-Identity header field into the 200 (OK) response before forwarding it to the terminating S-CSC-FE. The P-Asserted-Identity shall be set to the public user identity which has been registered in the network by the terminating party.

7.2.6.11 Requirements for the terminating UE

No special requirement for this FE.

7.2.6.12 Requirements for the terminating AGC-FE

When the terminating party answers the call, the terminating AGC-FE shall insert a P-Asserted-Identity header field into a 200 (OK) response to the INVITE request before forwarding this 200 (OK) response to the terminating S-CSC-FE. The P-Asserted-Identity shall be set to the public user identity which has been registered in the network by the terminating party.

7.2.7 Terminating identification restriction

The terminating identification restriction service feature restricts the terminating party's identities to be presented to the originating party.

NOTE – In this case, the terminating party means the party who answers the call.

This service feature shall be activated by the terminating party.

7.2.7.1 Requirements for the originating UE

No special requirement for this FE.

NOTE – If there is no P-Asserted-Identity in a received 200 (OK) response to the INVITE request, it is recommended that the originating UE does not present any information about the terminating party's identity, not even that contained in the To header field to the originating party.

7.2.7.2 Requirements for the originating AGC-FE

When receiving a 200 (OK) response to the INVITE request, if the Privacy header field is set to "id", "header" or "user", the originating AGC-FE shall not present the terminating party's identity to the originating party.

7.2.7.3 Requirements for the originating P-CSC-FE

When receiving a 200 (OK) response to the INVITE request, if the Privacy header field which has a value of "id", "header" or "user" is included in the response, the originating P-CSC-FE shall delete the P-Asserted-Identity header field before forwarding this response to the originating UE.

7.2.7.4 Requirements for the originating S-CSC-FE

No special requirement for this FE.

7.2.7.5 Requirements for the originating call server

When receiving a 200 (OK) response to the INVITE request, and the Privacy header field which has a value of "id", "header" or "user" is included in the response, the originating call server shall not provide the originating party with the terminating party's identity.

7.2.7.6 Requirements for the AS-FE

When the AS-FE receives a 200 (OK) response to the INVITE request from the terminating S-CSC-FE or call server, the AS-FE shall add the Privacy header field in the 200 (OK) response to the INVITE request and set the value to "id", then send this response to the terminating S-CSC-FE or call server.

7.2.7.7 Requirements for the terminating call server

When the terminating party answers the call, the terminating call server shall insert a P-Asserted-Identity header field into a 200 (OK) response to the INVITE request before forwarding this 200 (OK) response. The P-Asserted-Identity shall be set to the public user identity which has been registered in the network by the terminating party.

7.2.7.8 Requirements for the terminating I-CSC-FE

No special requirement for this FE.

7.2.7.9 Requirements for the terminating S-CSC-FE

No special requirement for this FE.

7.2.7.10 Requirements for the terminating P-CSC-FE

When the terminating P-CSC-FE receives a 200 (OK) response to the INVITE request from the terminating UE, the terminating P-CSC-FE shall insert a P-Asserted-Identity header field into the 200 (OK) response before forwarding this 200 OK to the terminating S-CSC-FE. The P-Asserted-Identity shall be set to the public user identity which has been registered in the network by the terminating party.

7.2.7.11 Requirements for the terminating UE

No special requirement for this FE.

7.2.7.12 Requirements for the terminating AGC-FE

When the terminating party answers the call, the terminating AGC-FE shall insert a P-Asserted-Identity header field into a 200 (OK) response to the INVITE request before forwarding it to the terminating S-CSC-FE. The P-Asserted-Identity shall be set to the public user identity which has been registered in the network by the terminating party.

7.2.8 Communication transfer

When user A and user B are in the same Centrex group, and they have set up a call, user B can transfer this call to user C which can be a Centrex user or a public user.

When user B successfully transfers the call to user C, user A and user C will establish a call and the call between user A and user B will be released.

If user B fails to transfer the call for some reason, for example, network congestion, or user C is busy, or user C gives no reply, then the call between user A and user B shall remain unchanged.

In this service, user A is a transferee, user B is a transferor, and user C is a transfer target.

7.2.8.1 Requirements for the transferee UE (user A)

No special requirement for this FE.

7.2.8.2 Requirements for the transferee AGC-FE (user A)

No special requirement for this FE.

7.2.8.3 Requirements for the transferee P-CSC-FE (user A)

No special requirement for this FE.

7.2.8.4 Requirements for the transferee S-CSC-FE (user A)

No special requirement for this FE.

7.2.8.5 Requirements for the transferee call server (user A)

No special requirement for this FE.

7.2.8.6 Requirements for the transferor UE (user B)

The UE shall send a REFER request when user B wants to transfer the call.

When the UE receives a NOTIFY message sent by the AS-FE, which indicates that the call has been transferred successfully to user C, the UE shall send a BYE message to the AS-FE to release the call between user A and user B.

If the NOTIFY message sent by AS-FE indicates that the call has not been transferred successfully to user C, the UE shall not send the BYE message.

7.2.8.7 Requirements for the transferor AGC-FE (user B)

The AGC-FE shall send a REFER request when user B wants to transfer the call.

When the AGC-FE receives a NOTIFY message, which indicates that the call has been transferred successfully to user C, the AGC-FE shall send a BYE message to the AS-FE to release the call between user A and user B.

If the NOTIFY message sent by AS-FE indicates that the call has not been transferred successfully to user C, the AGC-FE shall not send the BYE message.

7.2.8.8 Requirements for the transferor P-CSC-FE (user B)

No special requirement for this FE.

7.2.8.9 Requirements for the transferor S-CSC-FE (user B)

No special requirement for this FE.

7.2.8.10 Requirements for the transferor call server (user B)

No special requirement for this FE.

7.2.8.11 Requirements for the AS-FE

When the AS-FE receives a REFER request sent from user B and the AS-FE confirms that user B wants to transfer the call to user C, the AS-FE shall:

1) send a 202 (Accepted) response to user B
2) create an INVITE request based on the REFER message, and the Request-URI shall be the URI of user C.

When the AS-FE receives a 200 (OK) responses for the re-INVITE sent to user C, the AS-FE shall:

1) send a re-INVITE message with the SDP information of user C to user A
2) send a NOTIFY message to user B to indicate the successful transfer of the call to user C.

When the AS-FE receives a BYE message sent by user B that wants to release the call between user A and user B, the AS-FE shall send a 200 (OK) response to user B. The BYE message shall not be forwarded to user A.

7.2.8.12 Requirements for the transfer target UE (user C)

No special requirement for this FE.

7.2.8.13 Requirements for the transfer target AGC-FE (user C)

No special requirement for this FE.

7.2.8.14 Requirements for the transfer target P-CSC-FE (user C)

No special requirement for this FE.

7.2.8.15 Requirements for the transfer target S-CSC-FE (user C)

No special requirement for this FE.

7.2.8.16 Requirements for the transfer target call server (user C)

No special requirement for this FE.

7.2.9 Communication diversion

When the communication diversion service is activated for Centrex user B, the service is triggered and the call shall be forwarded to user C automatically. The service-triggered condition can be unconditional, busy or no reply. User C can be a Centrex user or a public user.

7.2.9.1 Requirements for the UE of user A

No special requirement for this FE.

7.2.9.2 Requirements for the AGC-FE of user A

No special requirement for this FE.

7.2.9.3 Requirements for the P-CSC-FE of user A

No special requirement for this FE.

7.2.9.4 Requirements for the S-CSC-FE of user A

No special requirement for this FE.

7.2.9.5 Requirements for the call server of user A

No special requirement for this FE.

7.2.9.6 Requirements for the UE of user B

No special requirement for this FE.

7.2.9.7 Requirements for the AGC-FE of user B

No special requirement for this FE.

7.2.9.8 Requirements for the P-CSC-FE of user B

No special requirement for this FE.

7.2.9.9 Requirements for the S-CSC-FE of user B

No special requirement for this FE.

7.2.9.10 Requirements for the call server of user B

No special requirement for this FE.

7.2.9.11 Requirements for the AS-FE

When the AS-FE confirms that the call shall be forwarded, the AS-FE shall create a new INVITE request, and:

1) the Request-URI shall be the information of user C.
2) a History header field shall be included.

7.2.9.12 Requirements for the UE of user C

No special requirement for this FE.

7.2.9.13 Requirements for the AGC-FE of user C

No special requirement for this FE.

7.2.9.14 Requirements for the P-CSC-FE of user C

No special requirement for this FE.

7.2.9.15 Requirements for the S-CSC-FE of user C

No special requirement for this FE.

7.2.9.16 Requirements for the call server of user C

No special requirement for this FE.

7.2.10 Communication pickup

7.2.10.1 Service description

There are two scenarios for communication pickup.

a) Explicitly identified pickup

A call is alerting user A. User B, who is in the same Centrex group as user A, is aware of the alerting call and willing to retrieve the call. User B shall identify the number of user A and connect to the calling user, typically by dialling "Pickup Access Code + picked-up user number #".

b) Group pickup

In the group pickup scenario, users in the same Centrex group can be divided into several pickup groups. Each user in the pickup group can pick up any alerting call within the same pickup group. When a call is alerting a user belonging to a pickup group, any other group member willing to retrieve the call may connect to the calling user, typically by dialling a specific pickup access code.

In this scenario, the picking-up user is not required to explicitly identify the phone number of the picked-up user. If multiple calls are alerting, the first altering call may be picked up first.

7.2.10.2 Requirements for the UE of calling user

No special requirement for this FE.

7.2.10.3 Requirements for the AGC-FE of calling user

No special requirement for this FE.

7.2.10.4 Requirements for the P-CSC-FE of calling user

No special requirement for this FE.

7.2.10.5 Requirements for the S-CSC-FE of calling user

No special requirement for this FE.

7.2.10.6 Requirements for the call server of calling user

No special requirement for this FE.

7.2.10.7 Requirements for the UE of picked-up user

No special requirement for this FE.

7.2.10.8 Requirements for the AGC-FE of picked-up user

No special requirement for this FE.

7.2.10.9 Requirements for the P-CSC-FE of picked-up user

No special requirement for this FE.

7.2.10.10 Requirements for the S-CSC-FE of picked-up user

No special requirement for this FE.

7.2.10.11 Requirements for the call server of picked-up user

No special requirement for this FE.

7.2.10.12 Requirements for the AS-FE

When the AS-FE confirms that the alerting call can be picked up by the picking-up user, the AS-FE shall:

1) cancel the INVITE request sent to the picked-up user,
2) update the dialogue between the AS-FE and the calling user by the newly received SDP from the picking-up user, and
3) send the SDP answer which is based on the updated SDP received from the calling user to the picking-up user.

7.2.10.13 Requirements for the UE of the picking-up user

When the picking-up user is willing to pick up an alerting call and request the communication pickup service, the UE of the picking-up user shall send an INVITE request with a specific pickup access code to the AS-FE.

7.2.10.14 Requirements for the AGC-FE of the picking-up user

No special requirement for this FE.

7.2.10.15 Requirements for the P-CSC-FE of the picking-up user

No special requirement for this FE.

7.2.10.16 Requirements for the S-CSC-FE of the picking-up user

No special requirement for this FE.

7.2.10.17 Requirements for the call server of the picking-up user

No special requirement for this FE.

7.2.11 Communication hold

When user A and user B have established a call, both users can place the call on hold. The user that places the call on hold is called the served user. The other user who is being put on hold is called the held user.

As an enhanced function, the served user of the hold service can make a new call to user C, and it can be switched between the new call and the original call.

7.2.11.1 Requirements for the UE (served user)

If a UE places a call on hold and the media stream is a bi-directional media stream, it shall send a re-INVITE request containing a SDP with "a=" line set to "sendonly".

7.2.11.2 Requirements for the AGC-FE (served user)

If a user under the control of the AGC-FE places a call on hold and the media stream is a bi-directional media stream, AGC-FE shall send a re-INVITE request containing a SDP with "a=" line set to "sendonly".

7.2.11.3 Requirements for the P-CSC-FE (served user)

No special requirement for this FE.

7.2.11.4 Requirements for the S-CSC-FE (served user)

No special requirement for this FE.

7.2.11.5 Requirements for the call server (served user)

No special requirement for this FE.

7.2.11.6 Requirements for the AS-FE

When the AS-FE receives a re-INVITE request containing an SDP with "sendonly" media, if the AS-FE wants to supply the service announcement, the AS-FE shall modify the "c=" line of the SDP to indicate the address which shall supply the service announcement.

7.2.11.7 Requirements for the UE (held user)

No special requirement for this FE.

7.2.11.8 Requirements for the AGC-FE (held user)

No special requirement for this FE.

7.2.11.9 Requirements for the P-CSC-FE (held user)

No special requirement for this FE.

7.2.11.10 Requirements for the S-CSC-FE (held user)

No special requirement for this FE.

7.2.11.11 Requirements for the call server (held user)

No special requirement for this FE.

8 Protocol profiles

The protocol profiles for the IP Centrex service shall be based on [ITU-T Q.3402] identified in Table 8.1.

Table 8.1 – Base Recommendation for IP Centrex protocol profiles

Profile	Interface	Protocol	Recommendation
NGN UNI	Between the originating end user function and the service control function in the Originating network. Between the terminating end user function and the service control function in the terminating network.	SIP/SDP	[ITU-T Q.3402]

In terms of the IMS-based IP Centrex service, some special requirements needed for the SIP are provided in Table 8.2, as follows:

- M indicates "mandatory"
- C indicates "conditionally mandatory"
- For the "mandatory" case, the EUF or SCF implementing the IP Centrex shall comply with the listed RFCs
- For the "conditionally mandatory" case, the EUF or SCF implementing the IP Centrex shall comply with the listed RFCs when the stated conditions have been met.

Table 8.2 – RFCs to be supported for the IMS-based IP Centrex service

Category	RFC	RFC Title	EUF	SCF
SIP and Extension	[IETF RFC 3262]	Reliability of Provisional Responses in Session Initiation Protocol (SIP)	M	M
SIP and Extension	[IETF RFC 3515]	The Session Initiation Protocol (SIP) Refer Method	C1	C1
	[IETF RFC 3892]	The Session Initiation Protocol (SIP) Referred-By Mechanism	C1	C1
	[IETF RFC 3891]	The Session Initiation Protocol (SIP) "Replaces" Header	C1	C1
SIP and Extension	[IETF RFC 4244]	An Extension to the Session Initiation Protocol for Request History Information	C2	C2
C1: [IETF RFC 3515], [IETF RFC 3891] and [IETF RFC 3892] are conditionally mandatory when an explicit communication transfer service feature is required. C2: [IETF RFC 4244] is conditionally mandatory when communication diversion is required and communication diversion related information is transferred over the UNI.				

9 Security considerations

The IP Centrex service shall use the appropriate security mechanisms to meet the general security requirements of the NGN [ITU-T Y.2701].

Also, as the IP Centrex service provides media transport and signalling messages, the NGN network infrastructure for the IP Centrex service should ensure the confidentiality and integrity of the signalling messages transported on it. For this purpose, security mechanisms of different layers, such as transport layer security (TLS), IPSec and S/MIME, should be used when implementing the IP Centrex service.

The TLS should be used for providing transport layer security over connection-oriented protocols (such as TCP). The TLS is specified in [IETF RFC 2246].

IPSec should be used for providing security at network layer. IPSec is a set of network-layer protocol tools that collectively can be used as a secure replacement for traditional IP (Internet Protocol). IPSec is specified in [IETF RFC 2401].

S/MIME should also be used to provide mechanisms for securing message bodies. S/MIME can provide end-to-end confidentiality and integrity for MIME contents, as well as mutual authentication. S/MIME is specified in [IETF RFC 2633].

Appendix I

IMS-based signalling flows for the IP Centrex service

(This appendix does not form an integral part of this Recommendation.)

I.1 Internal communication

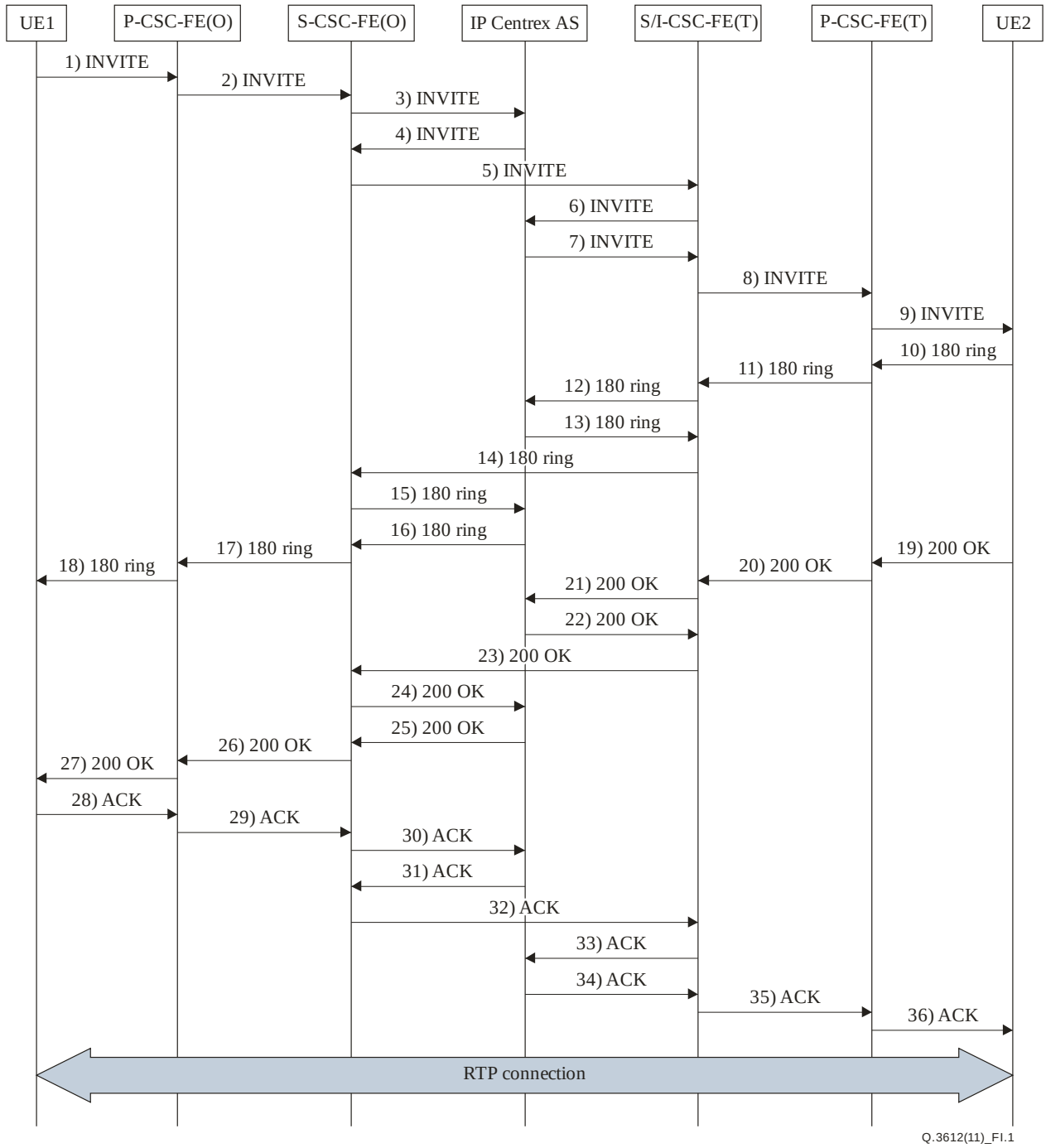

Figure I.1 – Internal communication call flow

1) UE1 sends an INVITE request to the originating P-CSC-FE. Based on the originating party's dial plan, the Request-URI may be the terminating party's private number or public user identity.

2) The INVITE request is forwarded to the S-CSC-FE serving for the originating party.

3) Based on the originating party's subscription, the INVITE request is forwarded to the IP Centrex AS.

4) Based on the originating party's identities and the terminating party's identities, the IP Centrex AS confirms that it is an internal communication. If the terminating party identity is a private number in step 1), the IP Centrex AS shall transform it into a public user identity and include it in the Request-URI header field. The IP Centrex AS forwards the INVITE request to the originating S-CSC-FE.

5) After invoking all the services subscribed to by the originating party, the originating S-CSC-FE will locate the terminating party and based on the normal procedure, the INVITE request will be sent to the terminating S-CSC-FE.

6) The terminating S-CSC-FE analyses the terminating party's service subscription and sends the INVITE request to the IP Centrex AS.

7) Based on the originating party's identities and terminating party's identities, the IP Centrex AS confirms that it is an internal communication. The originating party's identities will be transformed to the private number and included in the P-Asserted-Identity header field. The INVITE request is sent to the terminating S-CSC-FE.

8) After invoking all the services subscribed to by the terminating party, the terminating S-CSC-FE sends the INVITE message to the terminating P-CSC-FE.

9) The terminating P-CSC-FE sends the INVITE request to the UE2.

10)-18) The terminating party is alerted and a 180 message is sent by the UE2. The 180 message is forwarded to the UE1.

NOTE – If the SIP Precondition procedure is used, a message such as 183 PRACK UPDATE shall be shown.

19)-27) The terminating party answers and a 200 (OK) response for the INVITE request is sent by the UE2. The 200 (OK) message is forwarded to the UE1.

28)-36) The UE1 sends an ACK message after receiving the 200 (OK). The ACK message is forwarded to the UE2. The RTP connection is established between the UE1 and UE2.

I.2 Outgoing communication

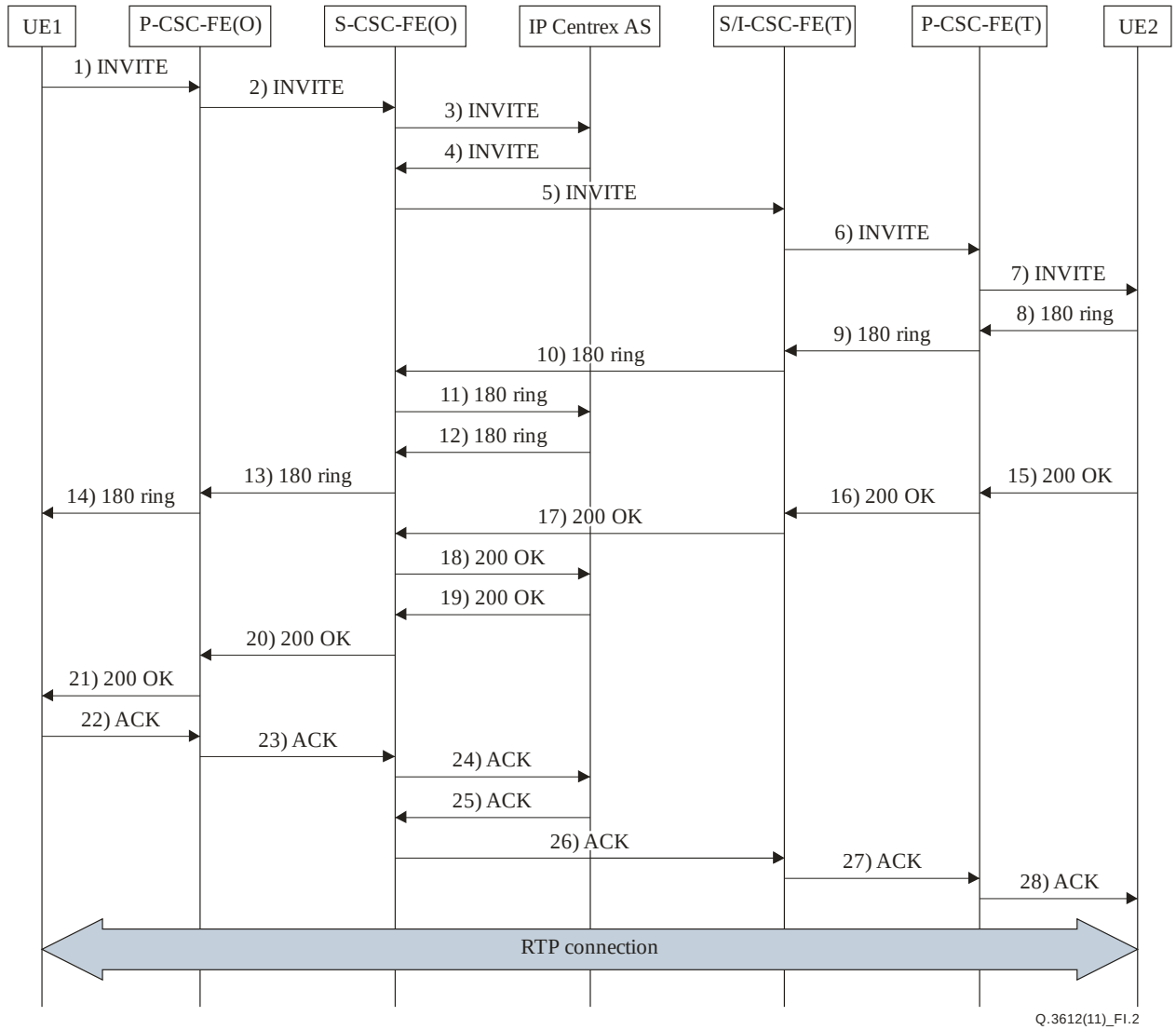

Figure I.2 – Outgoing communication call flow

1) UE1 sends an INVITE request to the originating P-CSC-FE. The Request-URI is the information about the terminating party's public identity.

2) The INVITE request is forwarded to the S-CSC-FE serving for the originating party.

3) Based on the originating party's subscription, the INVITE request is forwarded to the IP Centrex AS.

4) Based on the originating party's public identity and the terminating party's identity, the IP Centrex AS confirms that it is an outgoing communication. When the AS-FE sends the INVITE request to the originating S-CSC-FE, the public user identity of the terminating party shall be included in the Request-URI header field.

5) After invoking all the service subscribed by the originating party, the Originating S-CSC-FE will locate the terminating party and based on the normal procedure, the INVITE request will be sent to the terminating S-CSC-FE.

6) After invoking all the services subscribed to by the terminating party, the terminating S-CSC-FE sends the INVITE message to the terminating P-CSC-FE.

7) The terminating P-CSC-FE sends the INVITE request to the UE2.

8)-14) The terminating party is alerted and a 180 message is sent by the UE2. The 180 message is forwarded to the UE1.

NOTE – If the SIP Precondition procedure is used, a message such as 183 PRACK UPDATE shall be shown.

15)-21) The terminating party answers and a 200 (OK) response for the INVITE request is sent by the UE2. The 200 (OK) response is forwarded to the UE1.

22)-28) The UE1 sends an ACK message after receiving the 200 (OK). The ACK message is forwarded to the UE2. The RTP connection is established between the UE1 and UE2.

I.3 Incoming communication

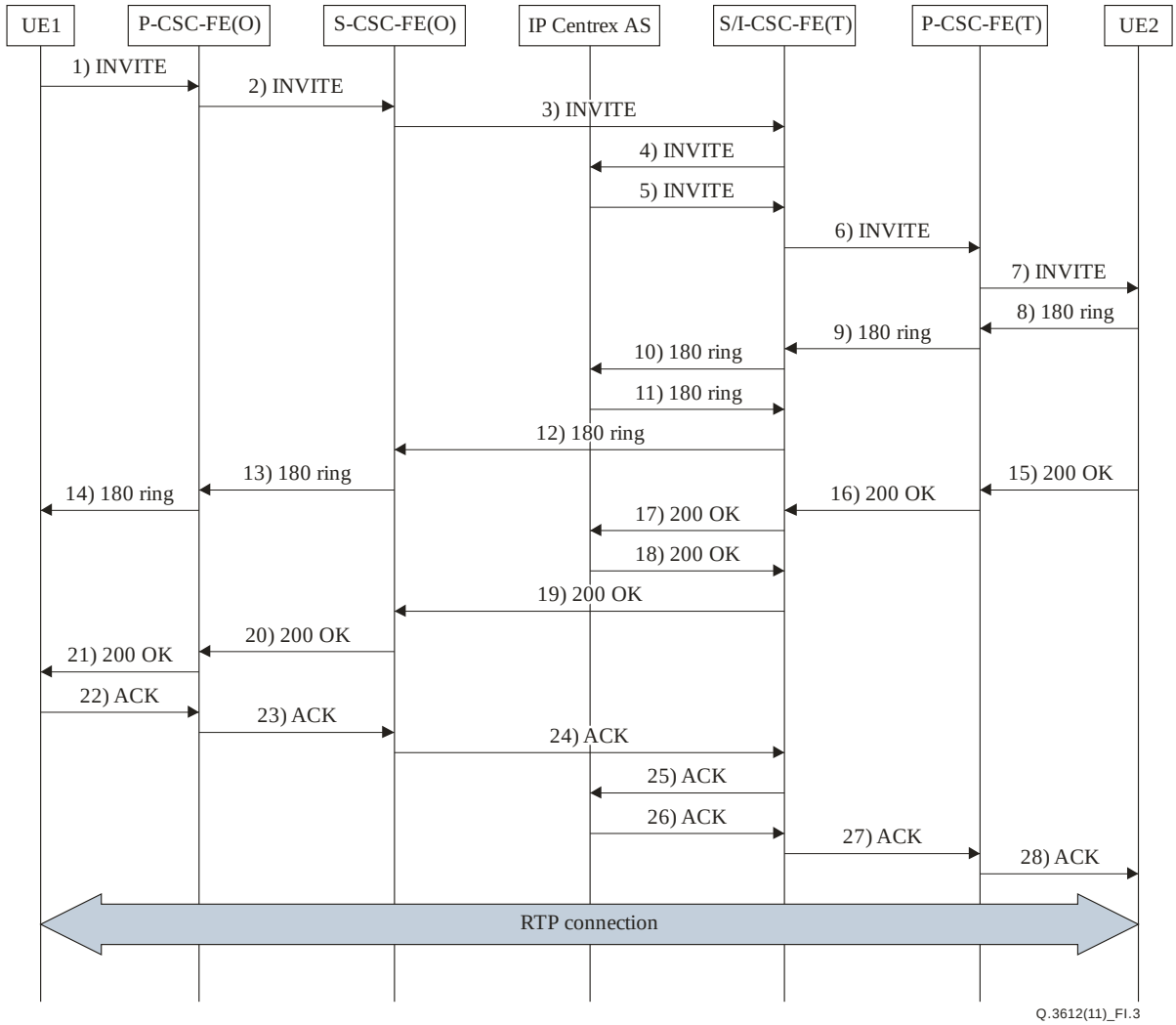

Figure I.3 – Incoming communication call flow

1) UE1 sends an INVITE request to the originating P-CSC-FE. The Request-URI is the information on the terminating party's public user identity.

2) The INVITE request is forwarded to the S-CSC-FE serving for the originating party.

3) After invoking all the services subscribed to by the originating party, the originating S-CSC-FE will locate the terminating party and, based on the normal procedure, the INVITE request will be sent to the terminating S-CSC-FE.

4) The terminating S-CSC-FE analyzes the terminating party's service subscription and sends the INVITE request to the IP Centrex AS.

5) Based on the originating party's public identity and the terminating party's public identity, the IP Centrex AS confirms that it is an incoming communication. When the AS-FE sends the INVITE request to the terminating I-CSC-FE, or the terminating S-CSC-FE, the originating party's identities contained in the P-Asserted-Identity header field can be used for call back directly by the terminating party.

6) After invoking all the services subscribed to by the terminating party, the terminating S-CSC-FE sends the INVITE request to the terminating P-CSC-FE.

7) The terminating P-CSC-FE sends the INVITE request to the UE2.

8)-14) The terminating party is alerted and a 180 message is sent by the UE2. The 180 message is forwarded to the UE1.

NOTE – If the SIP Precondition procedure is used, a message such as 183 PRACK UPDATE shall be shown.

15)-21) The terminating party answers and a 200 (OK) response for the INVITE request is sent by the UE2. The 200 (OK) response is forwarded to the UE1.

22)-28) The UE1 sends an ACK message after receiving the 200 (OK). The ACK message is forwarded to the UE2. The RTP connection is established between the UE1 and UE2.

I.4 Originating identification presentation

The following diagram describes the call flow of the originating identification presentation service. It is assumed that UE1 and UE2 belong to the same Centrex group and that UE2 has activated the originating identification presentation service.

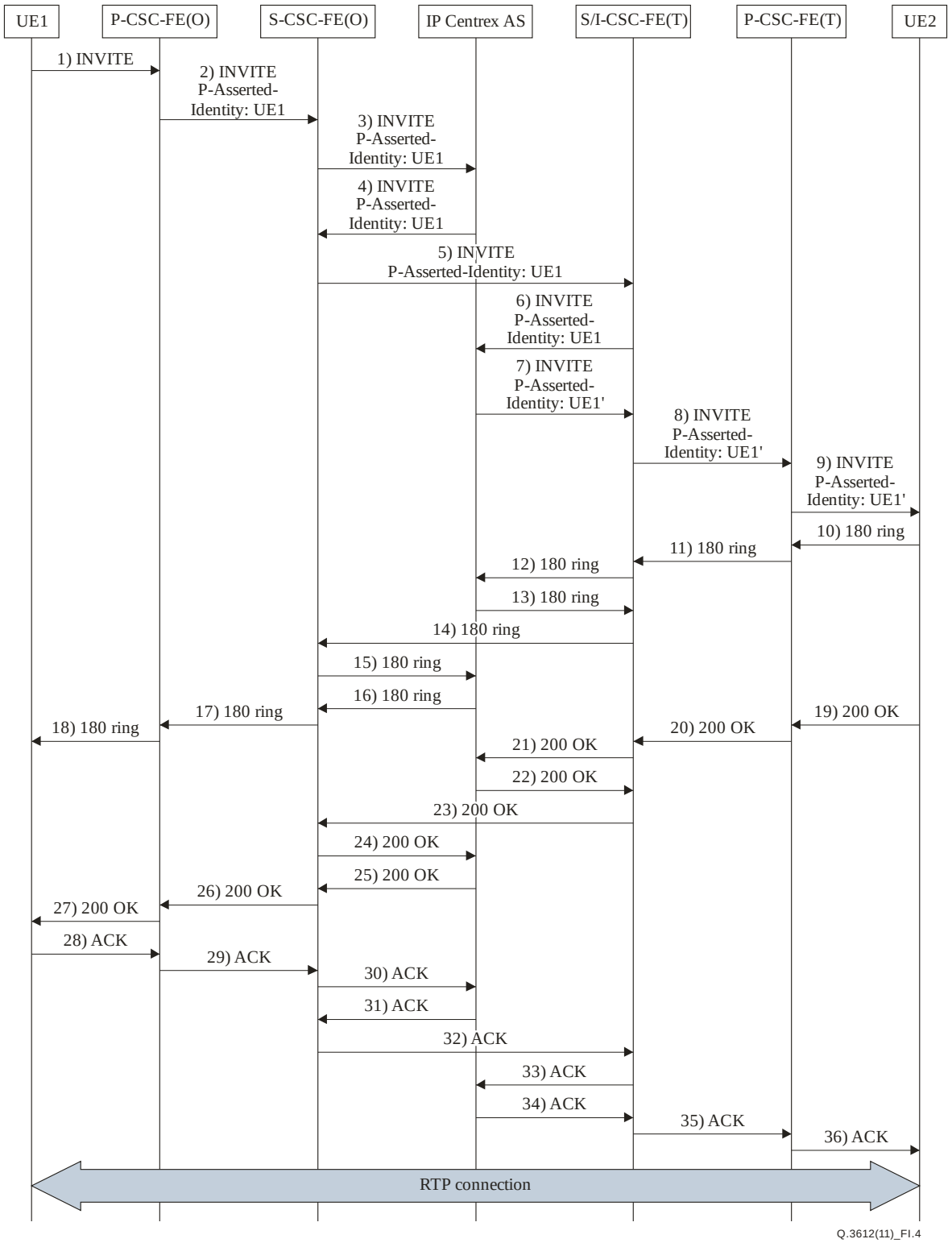

Figure I.4 – Originating identification presentation call flow

1) UE1 sends an INVITE request to the originating P-CSC-FE. The originating P-CSC-FE inserts a P-Asserted-Identity header field into the INVITE request before forwarding it to the S-CSC-FE. The P-Asserted-Identity shall be set to the public user identity of the originating party which has been registered in the network by the originating party.

2) The INVITE request is forwarded to the S-CSC-FE serving for the originating party.

3) Based on the originating party's subscription, the INVITE request is forwarded to the IP Centrex AS.

4) The IP Centrex AS forwards the INVITE request to the originating S-CSC-FE.

5) After invoking all the services subscribed to by the originating party, the originating S-CSC-FE will locate the terminating party and, based on the normal procedure, the INVITE request will be sent to the terminating S-CSC-FE.

6) The terminating S-CSC-FE analyzes the terminating party's service subscription and sends the INVITE request to the IP Centrex AS.

7) The IP Centrex AS confirms that the terminating party has activated the originating identification presentation service, before sending the received INVITE request to the terminating S-CSC-FE. IP Centrex AS can either add a Privacy header field into the INVITE request with the value set to "none", or just leave the INVITE request without the Privacy header field, and change the public user identity (UE1) of the originating party in the P-Asserted-Identity into a private number (UE1'). The INVITE request is then sent to the terminating S-CSC-FE.

   NOTE – The public user identity (UE1) can be changed to a private number (UE1') in step 4) or step 7), depending on the operators' policy.

8) After invoking all the service subscribed to by the terminating party, the terminating S-CSC-FE sends the INVITE request to the terminating P-CSC-FE.

9) If the Privacy header field is contained in the INVITE request with the value unequal to "none", the P-CSC-FE shall delete the P-Asserted-Identity header field before forwarding the INVITE request to UE2. If there is no Privacy header field in the INVITE request, or the Privacy header field is set to "none", then P-Asserted-Identity has to be provided to UE2.

10)-18) The terminating party is alerted and a 180 message is sent by the UE2. The 180 message is forwarded to the UE1.

   NOTE – If the SIP Precondition procedure is used, a message such as 183 PRACK UPDATE shall be shown.

19)-27) The terminating party answers and a 200 (OK) response for the INVITE request is sent by the UE2. The 200 (OK) response is forwarded to the UE1.

28)-36) The UE1 sends an ACK message after receiving the 200 (OK). The ACK message is forwarded to the UE2. The RTP connection is established between the UE1 and UE2.

I.5 Originating identification restriction

The following diagram describes the call flow of the originating identification restriction service. It is assumed that UE1 has subscribed to the IP Centrex service and has activated the originating identification restriction service.

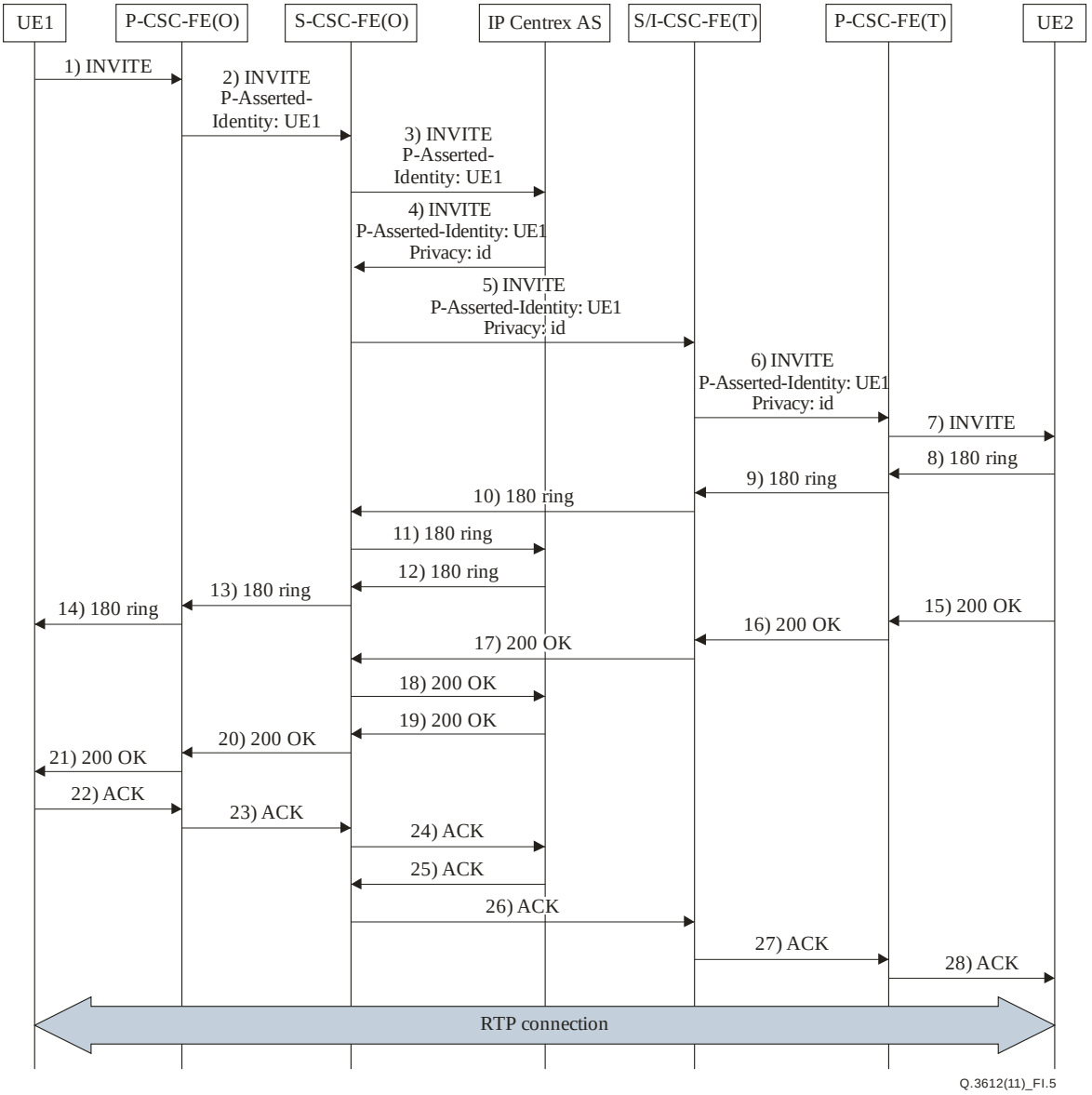

Figure I.5 – Originating identification restriction call flow

1) UE1 sends an INVITE request to the originating P-CSC-FE. The originating P-CSC-FE inserts a P-Asserted-Identity header field into the INVITE request before forwarding it to the S-CSC-FE. The P-Asserted-Identity shall be set to the public user identity of the UE1 which has been registered in the network by the originating party.

2) The INVITE request is forwarded to the S-CSC-FE serving for the originating party.

3) Based on the originating party's subscription, the INVITE request is forwarded to the IP Centrex AS.

4) In this case, since the originating party has activated the originating identification restriction service, the IP Centrex AS shall add the Privacy header field in the INVITE request and set the value to "id", then set the From header field to "Anonymous" and send the INVITE request to the originating S-CSC-FE.

5) After invoking all the services subscribed to by the originating party, the originating S-CSC-FE will locate the terminating party and, based on the normal procedure, the INVITE request will be sent to the terminating S-CSC-FE.

6) After invoking all the services subscribed to by the terminating party, the terminating S-CSC-FE sends the INVITE request to the terminating P-CSC-FE.

7) The P-CSC-FE shall delete the P-Asserted-Identity header field before forwarding the INVITE request to UE2.

8)-14) The terminating party is alerted and a 180 message is sent by the UE2. The 180 message is forwarded to the UE1.

NOTE – If the SIP Precondition procedure is used, a message such as 183 PRACK UPDATE shall be shown.

15)-21) The terminating party answers and a 200 (OK) response for the INVITE request is sent by the UE2. The 200 (OK) response is forwarded to the UE1.

22)-28) The UE1 sends an ACK message after receiving the 200 (OK). The ACK message is forwarded to the UE2. The RTP connection is established between the UE1 and UE2.

I.6 Terminating identification presentation

The following diagram describes one of the scenarios of the terminating identification presentation service. In this case, it is assumed that both the UE1 and UE2 are in the same IP Centrex group and that UE1 has activated the terminating identification presentation service.

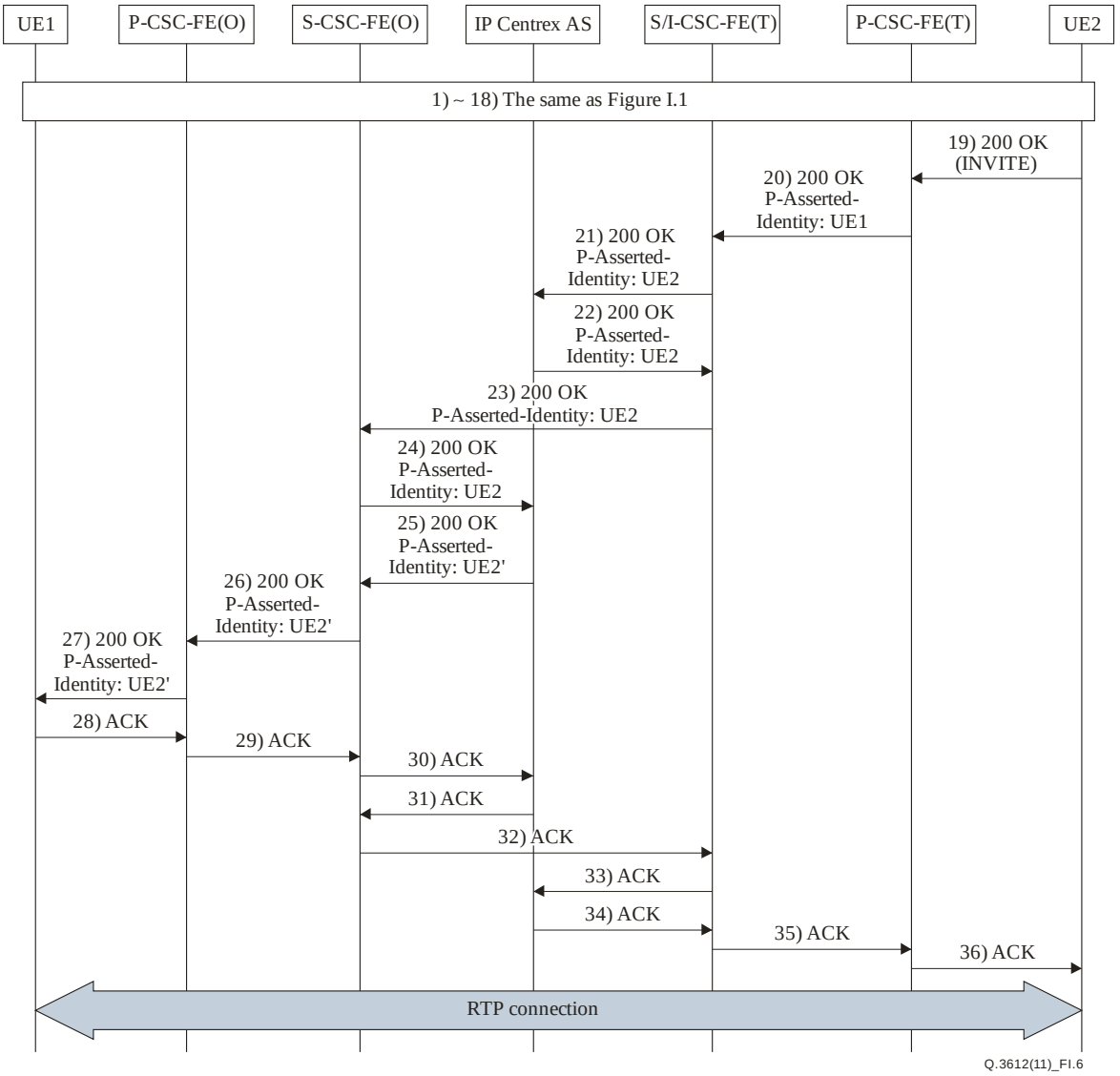

Figure I.6 – Terminating identification presentation call flow

1)~18) UE1 initiates a call to UE2, and UE2 is alerting. Up to this point, it is almost the same as the first 18 steps depicted in Figure I.1.

19) The terminating party answers the call and a 200 (OK) response to the INVITE request is sent by the UE2 to the terminating P-CSC-FE.

20) The terminating P-CSC-FE inserts a P-Asserted-Identity header field into the 200 (OK) response before forwarding the 200 (OK) response to the terminating S-CSC-FE. The P-Asserted-Identity shall be set to the public user identity of the terminating party.

21) The terminating S-CSC-FE forwards the 200 (OK) response with P-Asserted-Identity to IP Centrex AS.

22) IP Centrex AS forwards the 200 (OK) response to the terminating S-CSC-FE.

23) The terminating S-CSC-FE forwards the 200 (OK) response with P-Asserted-Identity to the originating S-CSC-FE.

24) The originating S-CSC-FE forwards the 200 (OK) response to IP Centrex AS.

25) In this case, since the originating party has activated the terminating identification presentation service, before forwarding the received 200 (OK) response to the originating S-CSC-FE, IP Centrex AS can either add a Privacy header field into the 200 (OK) response to the INVITE request with the value setting to "none", or just leave the 200 (OK) response without a Privacy header field, and change the public user identity of the terminating party in the P-Asserted-Identity into a private number.

26) The originating S-CSC-FE forwards the 200 (OK) response to the originating P-CSC-FE.

27) In this case, since there is no Privacy header field within the 200 (OK) response or the value of the Privacy is "none", then P-Asserted-Identity has to be provided to UE1.

28)-36) The UE1 sends an ACK message after receiving the 200 (OK). The ACK message is forwarded to the UE2. The RTP connection is established between the UE1 and UE2.

I.7 Terminating identification restriction

The following diagram describes one of the scenarios of the terminating identification restriction service. In this case, it is assumed that both UE1 and UE2 are in the same IP Centrex group and that UE2 has activated the terminating identification restriction service.

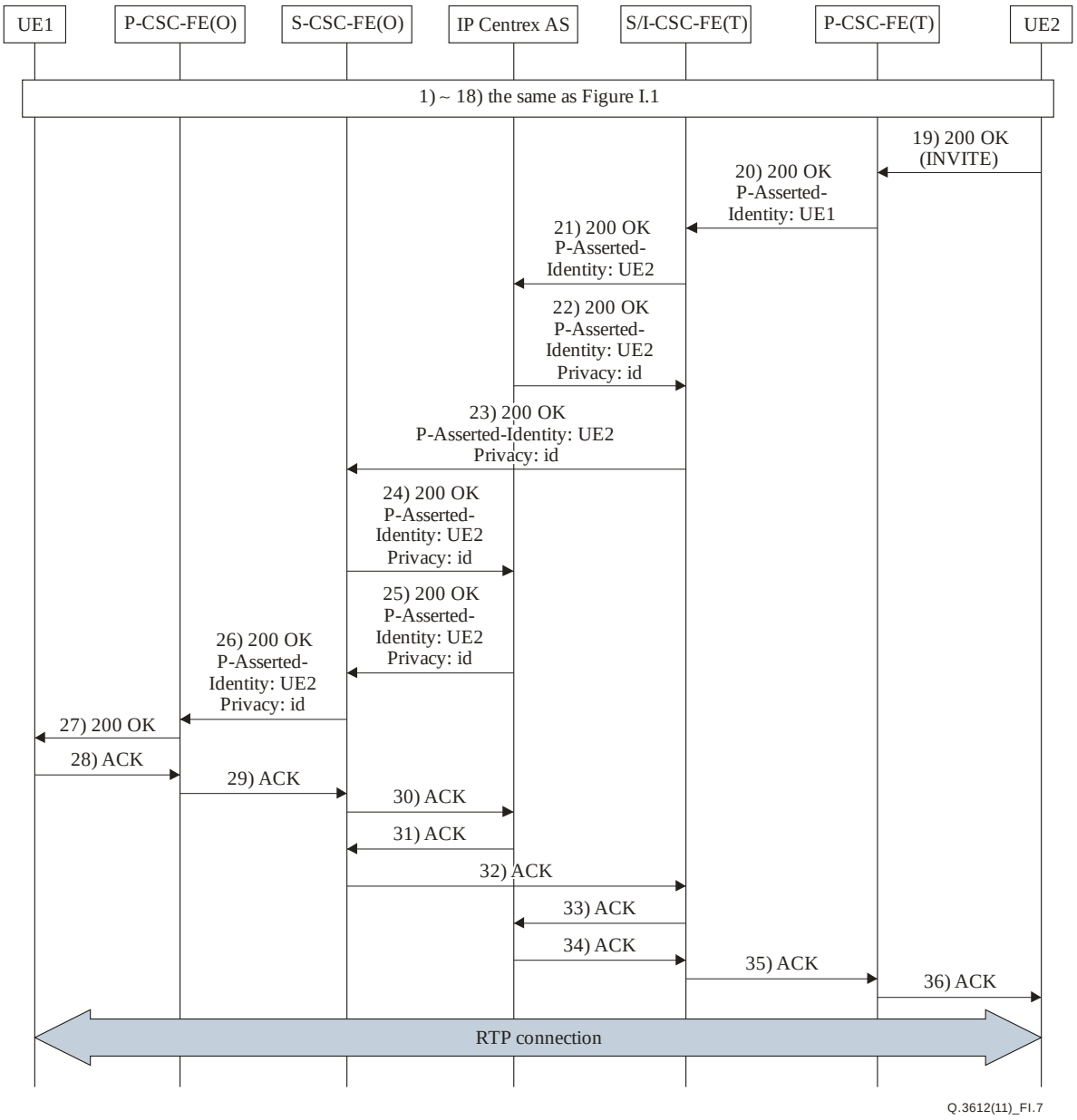

Figure I.7 – Terminating identification restriction call flow

1)-18) UE1 initiates a call to UE2, and UE2 is alerting. Up to this point, it is almost the same as the first 18 steps depicted in the Figure I.1.

19) The terminating party answers the call and a 200 (OK) response to the INVITE request is sent by the UE2 to the terminating P-CSC-FE.

20) The terminating P-CSC-FE inserts a P-Asserted-Identity header field into the 200 (OK) response before forwarding the message to the terminating S-CSC-FE. The P-Asserted-Identity shall be set to the public user identity of the terminating party.

21) The terminating S-CSC-FE forwards the 200 (OK) response with P-Asserted-Identity to IP Centrex AS.

22) In this case, since the terminating party has activated the terminating identification restriction service, the IP Centrex AS shall add the Privacy header field into the 200 (OK) response to the INVITE request and set the value to "id", and send this response to the terminating S-CSC-FE.

23) The terminating S-CSC-FE forwards the 200 (OK) response with P-Asserted-Identity and Privacy header fields to originating S-CSC-FE.

24) The originating S-CSC-FE forwards the 200 (OK) response to IP Centrex AS.

25) IP Centrex AS forwards the 200 (OK) response to the originating S-CSC-FE.

NOTE – Since UE1 and UE2 are in the same IP Centrex group, IP Centrex AS may change the public user identity of the terminating party into a private number in the P-Asserted-Identity header field in the 200 (OK) response.

26) The originating S-CSC-FE forwards the 200 OK received from the IP Centrex AS to the originating P-CSC-FE.

27) The P-CSC-FE shall delete the P-Asserted-Identity header field before forwarding the 200 (OK) response to UE1.

28)-36) The UE1 sends an ACK message after receiving the 200 (OK). The ACK message is forwarded to the UE2. The RTP connection is established between the UE1 and UE2.

I.8 Communication transfer

The following diagram describes the call flow of the communication transfer service. It is assumed that UE2 is a Centrex user and that it has activated the communication transfer service.

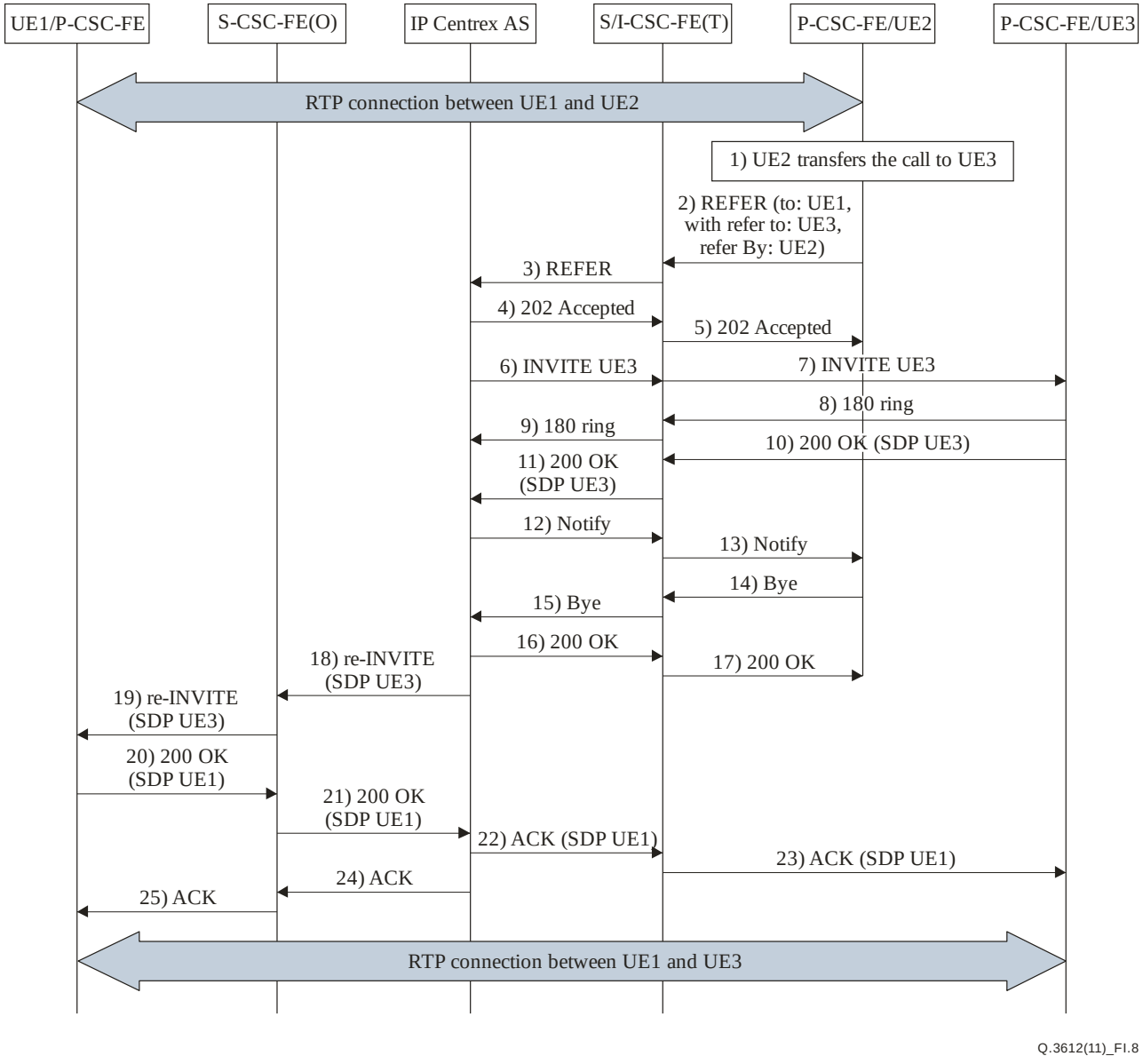

Figure I.8 – Communication transfer call flow

1) The RTP connection is established between the UE1 and UE2. The UE2 transfers the call to UE3 which can be a Centrex user or a public user.

2), 3) The UE2 sends a REFER request to IP Centrex AS.

4)-7) The AS confirms that UE2 wants to transfer the call to UE3. The AS sends a 202 (Accepted) response to UE2 and creates an INVITE request based on the REFER message. In the INVITE request, The Request-URI shall be set to the public user identity of UE3. The INVITE request is forwarded to UE3.

8), 9) The terminating party is alerted and a 180 message is sent by the UE3. The 180 message is forwarded to the AS.

10), 11) The terminating party answers and a 200 (OK) response for the INVITE request is sent by the UE3. The 200 (OK) response is forwarded to the AS.

12), 13) The AS sends a NOTIFY message to UE2 to indicate the successful transfer of the call to UE3.

14)-17) UE2 sends a BYE message to the AS-FE to release the connection between UE1 and UE2.

18), 19) The AS sends a re-INVITE message to UE1 to indicate the capability of UE3.

20), 21) UE1 sends a 200 (OK) response for the reINVITE request with the SDP information of UE1.

22)-25) The AS sends an ACK message after receiving the 200 (OK). The RTP connection is established between the UE1 and UE3.

I.9 Communication diversion

The following diagram describes the call flow of the communication diversion service. It is assumed that UE2 is a Centrex user and that it has activated the communication forwarding service on the condition of no reply. UE1 and UE3 are public users.

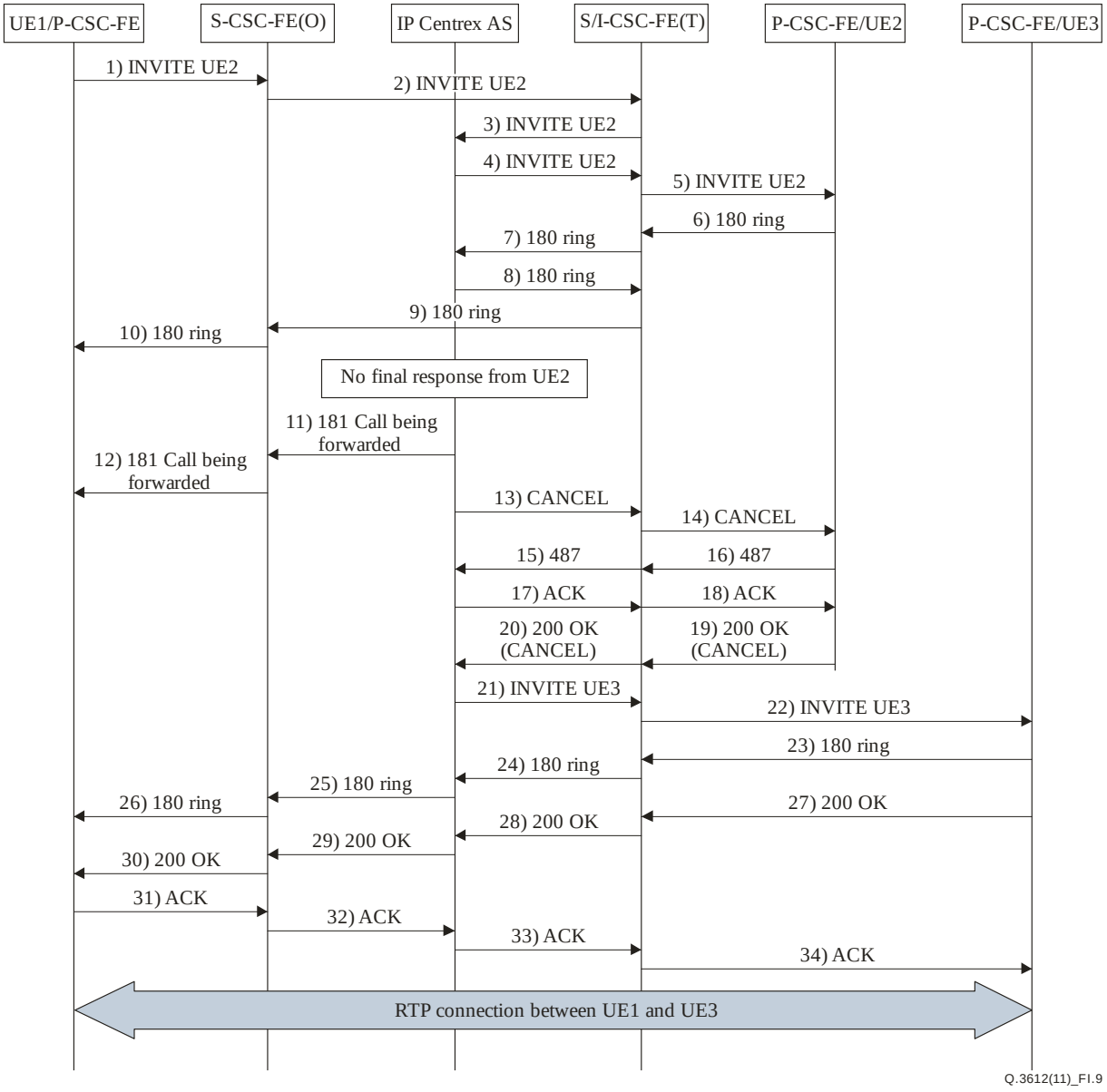

Figure I.9 – Communication diversion call flow

1)-10) The UE1 initiates a call to UE2, and UE2 is alerting.

11)-20) The IP Centrex AS does not receive any final response from UE2, and then triggers call-forwarding on the no-reply service. IP Centrex AS informs UE1 that the call is being forwarded, and cancels the INVITE request sent to UE2.

21), 22) Based on UE2's subscription, the call shall be forwarded to UE3. The IP Centrex AS sends an INVITE request to UE3. In the INVITE request, the Request-URI shall be set to the public user identity of UE3 and the History header field shall be set to the public user identity of UE2.

23)-26) the UE3 is alerted and a 180 message is sent by the UE3. The 180 message is forwarded to the UE1.

NOTE – If the SIP Precondition procedure is used, a message such as 183 PRACK UPDATE shall be shown.

27)-30) The UE3 answers and a 200 (OK) response for the INVITE request is sent by the UE3. The 200 (OK) response is forwarded to the UE1.

31)-34) The UE1 sends an ACK message after receiving the 200 (OK). The ACK message is forwarded to the UE2. The RTP connection is established between the UE1 and UE3.

I.10 Communication pickup

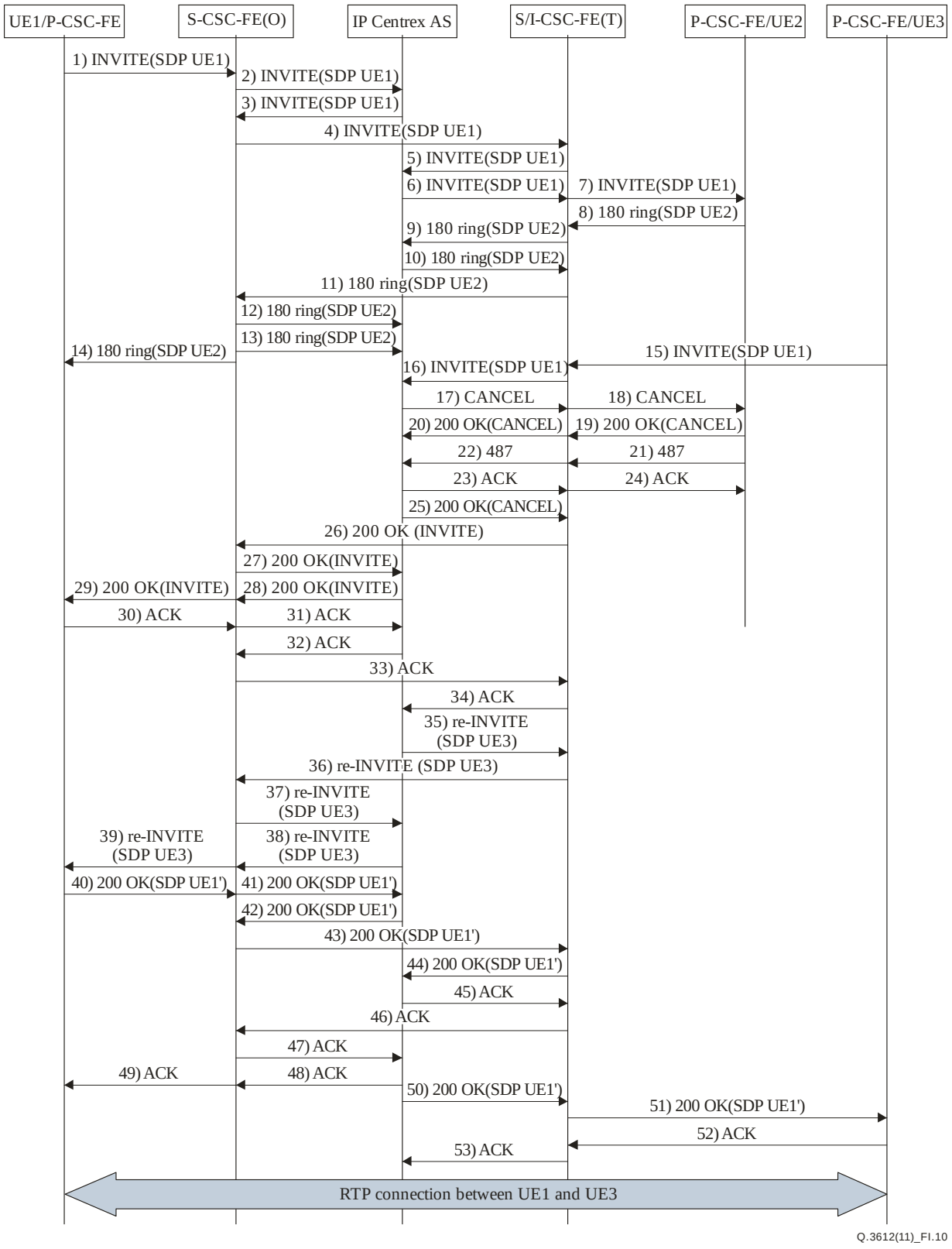

Figure I.10 – Communication pickup call flow

1)-14) UE1 initiates a call to UE2, and UE2 is alerting. Up to this point, it is almost the same as the first 18 steps depicted in Figure I.1.

15) UE3 picks up the alerting call by using a specific pickup access code. UE3 sends an INVITE request with the pickup access code to S-CSC-FE of UE2. The SDP UE3 is provided in the INVITE request.

16) Based on UE3's subscription, the INVITE request is forwarded to IP Centrex AS.

17)-24) The AS confirms that UE3 is picking up the call to UE2 by analysing the phone number followed by the access code for the explicitly identified pickup scenario, or based on the fact that UE2 and UE3 are in the same pickup group for the group pickup scenario. The AS then decides to cancel the INVITE request sent to UE2.

NOTE – The AS is now in back-to-back user agent (B2BUA) mode.

25)-29) The AS sends a 200 (OK) response upstream to the UE1 so that it can establish the confirmed dialogue with UE1.

30)-34) UE1 sends an ACK to AS. Now, AS has established a call leg (SIP dialogue) for UE1.

35)-39) AS uses the SDP UE3 received in the INVITE request from UE3 to generate an INVITE (re-INVITE) to UE1.

40)-44) UE1 responds with an SDP Answer to AS. The SDP Answer in 200 (OK) response may be different from the one sent in Step 1), and it is therefore denoted as SDP UE1'.

45)-49) AS sends an ACK towards UE1.

50), 51) AS sends a 200 (OK) response, including the newly received SDP UE1' from UE1, towards UE3.

52), 53) UE3 sends an ACK towards AS. Now, AS has established two call-legs, one for UE1, the other for UE3, and the RTP connection is established between UE1 and UE3.

I.11 Communication hold

The following diagram describes the call flow of the communication hold service. It is assumed that UE1 is a Centrex user and that it has activated the communication hold service.

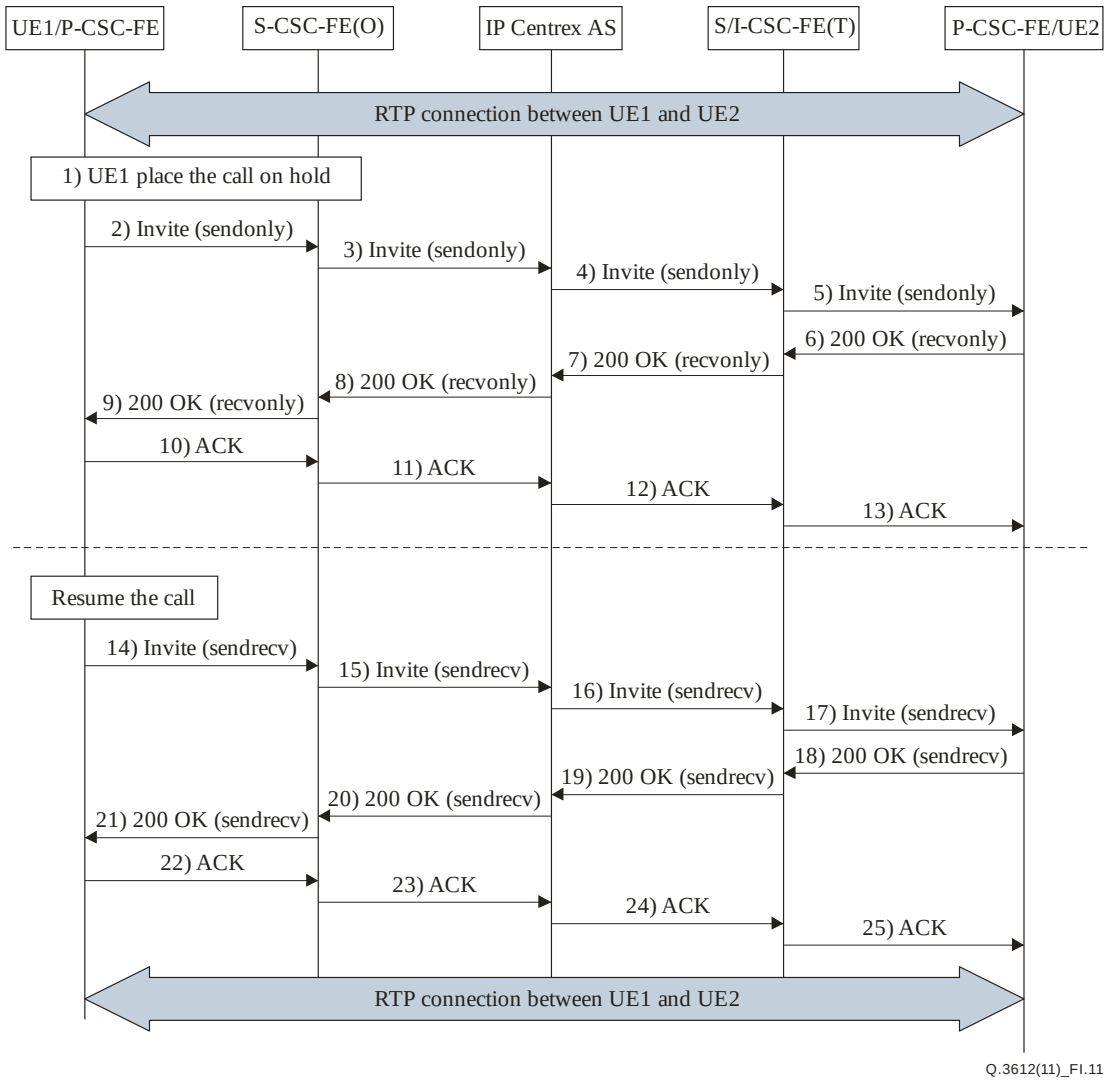

Figure I.11 – Communication hold call flow

1) The RTP connection is established between the UE1 and UE2. UE1 places the call on hold.

2)-5) The UE1 sends a re-INVITE request containing a SDP with "a=" line set to "sendonly". The re-INVITE request is forwarded to UE2.

NOTE – The AS can play the service announcement to UE2 in step 5), which depends on operators' policy.

6)-9) The UE2 sends a 200 (OK) response containing a SDP with "a=" line set to "recvonly". The 200 (OK) response is forwarded to UE1.

10)-13) The UE1 sends an ACK message after receiving the 200(OK).

14)-17) The UE1 wants to resume the call. The UE1 sends a re-INVITE request containing a SDP with "a=" line set to "sendrecv". The re-INVITE request is forwarded to UE2.

18)-25) The UE2 sends a 200 (OK) response containing a SDP with "a=" line set to "sendrecv". The 200 (OK) response is forwarded to UE1. The ACK message is forwarded to the UE2. The RTP connection between the UE1 and UE2 is resumed.

Appendix II

Call server based signalling flows for the IP Centrex service

(This appendix does not form an integral part of this Recommendation.)

For call server based IP Centrex, the access protocol between UE and the call server can be ISDN, ISUP, or ITU-T H.248, etc. The access protocol in the signalling flow given in Figure II.1 just illustrates the message sequence. In the actual implementation, it could be any of the protocols mentioned above. Figure II.1 gives an example of internal communication in the call server based context, i.e., UE1 and UE2 are in the same IP Centrex group.

UEs in Figure II.1 refer to legacy terminals.

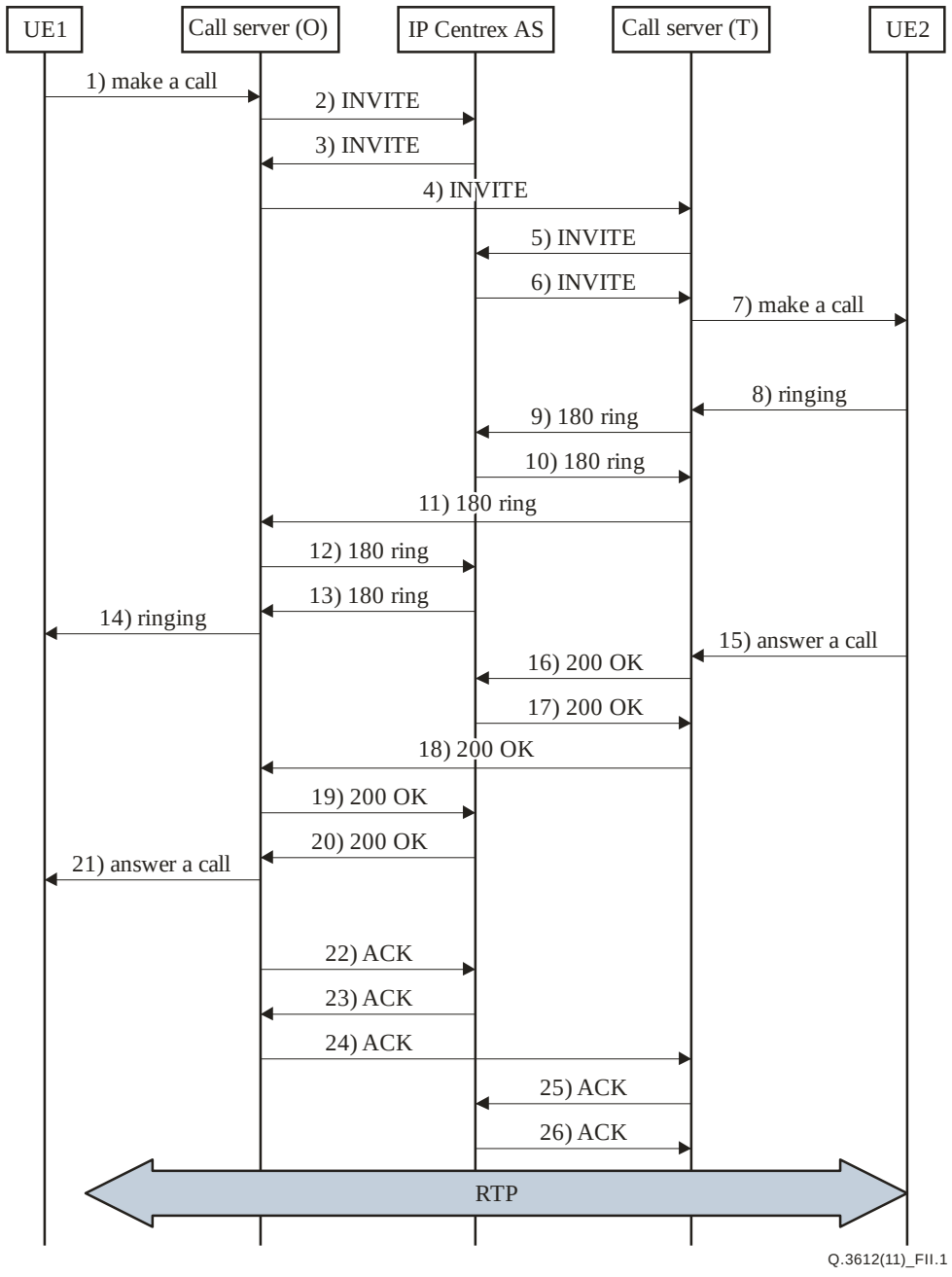

Figure II.1 – Internal communication call flow

1) UE1 initiates a call to UE2. The originating party can either dial the private number or the public user identity of the terminating party. The corresponding number information shall be sent to the call server.

2) The originating call server sends an INVITE request to IP Centrex AS with the dialled digits in the request-URI, according to the originating party's subscription.

3) Based on the originating party's identities and the terminating party's identities, the IP Centrex AS confirms that it is an internal communication. If the digits in the request-URI represent the private number in step 1), the IP Centrex AS shall transform it into a public user identity. The IP Centrex AS forwards the INVITE request to the originating call server.

4) The originating call server will route the call to the terminating call server and forward the INVITE request to the terminating call server.

5) The terminating call server analyzes the terminating party's service subscription and forwards the INVITE request to the IP Centrex AS.

6) IP Centrex AS confirms that it is an internal communication. The originating party's identities in the P-Asserted-Identity header field in the INVITE request need to be transformed into the private number of the originating party. The INVITE request is sent to the terminating call server.

7) The terminating call server then routes the call to the UE2.

8) If the UE2 is free, it will ring at this time.

9)-14) A 180 response is forwarded along to the originating call server. Then the alerting information of the terminating party is provided to UE1.

NOTE – If the SIP Precondition procedure is used, a message such as 183 PRACK UPDATE shall be shown.

15)-21) The terminating party answers the call and related information is transmitted to UE1 by appropriate messages, e.g., 200 (OK), to the INVITE request.

22)-26) To complete the INVITE transaction, an ACK request is needed in order to comply with the basic SIP protocol. After that, RTP connection between UE1 and UE2 is established.

Bibliography

[b-ITU-T H.450.5] Recommendation ITU-T H.450.5 (1999), *Call park and call pickup supplementary services for H.323.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012