PHS MoU Document
B-IF4.50-02-TS

Title: **Public Personal Handy-phone System : Network-Network Interface for SCP Exchange Public PHS Roaming Protocol**

Version: 02

Date: May 15, 1998

PHS MoU Classification: Unrestricted

List of contents:

Number of pages: 53

PHS MoU Group

c/o Association of Radio Industries and Businesses (ARIB)
14F, Nittochi Bldg., 4-1, Kasumigaseki 1-choume, Chiyoda-ku, Tokyo 100, Japan
TEL +81-3-5510-8599 FAX +81-3-3592-1103

PHS MoU Document
B-IF4.50-02-TS

History of Revised Versions

Version	Date	Outline
01		Established
02	May 15,1998	

B-IF4.50-02-TS

Public Personal Handy-Phone System:
Network - Network interface for SCP Exchange
Public PHS Roaming Protocol

< Summary>

1. Relationship with International Standards

This specifications specifies public PHS roaming interface based on TTC Standard JT-Q1218-a (PHS roaming capability set 2) which is based on the study results of IN-CS2 in ITU-T SG11.

2. Differences to/from International Recommendations

The description of this portion is not provided because the study results of IN-CS2 in ITU-T SG11 have not been officially published yet.

3. Others

3.1 References to ITU-T Recommendations

X.501, X.509, X.511

3.2 References to TTC Standards

JT-Q771, JT-Q772, JT-Q773, JT-Q774,
JT-Q1218, JT-Q1218-a
JT-X500, JT-X520

4. Items for Further Study

None

B-IF4.50-02-TS

Public Personal Handy-Phone System:
Network - Network interface for SCP Exchange
Public PHS Roaming Protocol

Contents

1. Scope of public PHS inter-network protocol standardization

This part describes the protocol for roaming between public PHS networks, based on the service definition (B-SV5.00) and the information flow of PHS basic roaming capability set (B-IF0.50).

2. Physical plane architecture

The physical plane architecture described in this part is based on the architecture defined in NW1.00-02-TS.

3. Information model

3.1 General

In the PHS basic roaming capability set, various types of data are stored in the SDF. Data for PHS basic roaming capability set is specified in the following data model. The aim of the model is primarily to provide an exhaustive list of all the data needed to support the PHS basic roaming capability set, and secondary to present the data as generally as possible so that they can be used as parameters for database operations.

Due to the amount of information contained in the data model, the model needs to be organized. The information and its associated structure construct the PHS information base.

3.2 PHS roaming information base

3.2.1 Information base

The information model is structured as object classes. Each object class is a general symbol of a telecommunication object (service provider, subscriber, etc.). An object is an instance of object class in which it is involved. Each object class is characterized by attributes. The attributes contain the data required to perform the service.

Several object classes can be identified as same as their attributes. All the object classes are subclasses under the top class. The top class is an abstract class of which all the other classes are subclasses. Under the top class, three types of object classes are identified;

- country

- public PHS ISPT service provider

- public PHS ISPT subscriber profile

- public PHS roaming number pool

3.2.1.1 Country

This object class is defined in ITU-T Recommendation X.521.

```
country OBJECT-CLASS::={
  SUBCLASS OF       top
  MUST CONTAIN  {countryName}
  MAY CONTAIN   {description|
                searchGuide}
  ID            {id-oc-country}}
```

The meanings of the attributes indicated by the above object class definition is as follows.

The ‘countryName’ attribute indicates the country. The relative distinguished name of this attribute type is described as, for example, “country=JP”, when it is used as the element of the directory name.

3.2.1.2 Public PHS ISPT service provider

This object class defines a PHS roaming service provider which realizes ISPT. The definition includes:

(1) identifying the service provider.

The following ASN.1 description is used to define the public PHS ISPT service provider.

```
phsISPTServiceProvider OBJECT-CLASS::={
  SUBCLASS OF       top
  MUST CONTAIN      {phsISPTServiceProviderId}
  ID                {ttc-objectClass 4}}

phsISPTServiceProviderId ATTRIBUTE::={
  WITH SYNTAX               NumericString(SIZE(1..ub-phsProviderId))
  EQUALITY MATCHING RULE            numericStringMatch
  SUBSTRINGS MATCHING RULE          numericStringSubstringsMatch
  SINGLE VALUE                      TRUE
  ID                                {ttc-attributeType 21}}
```

The meanings of the attributes indicated by above the object class definitions are as follows;

The ‘phsISPTServiceProviderId’ attribute identifies the public PHS ISPT service provider. The ‘phsISPTServiceProviderId’ is composed of digits, which may be a part of a numbering plan. In all cases, the value of the ‘phsISPTServiceProviderId’ can be obtained by the PHS number.

3.2.1.3 Public PHS ISPT subscriber profile

This object class defines a public PHS ISPT service subscriber. The definition includes:

(1) identifying the PHS number;

(2) giving the service provision conditions;

(3) giving the routing destination for call termination;

(4) giving the information to indicate the accessing network; and

(5) giving the information necessary for terminal authentication.

The following ASN.1 description is used to define the public PHS ISPT subscriber profile.

```
phsISPTSubscriberProfile OBJECT-CLASS::={
   SUBCLASS OF       top
   MUST CONTAIN   {    phsNumber|
                       providedRoamingService|
                       phsRoamingNumber|
                       accessingNetworkId|
                        routingType|
                       locationRegistrationAuthenticationInformation|
                       callSetupAuthenticationInformation}
   ID             {ttc-objectClass 5}}

phsNumber ATTRIBUTE::={
  WITH SYNTAX      OCTET STRING
   EQUALITY MATCHING RULE          octetStringMatch
   SINGLE VALUE                    TRUE
   ID                              {ttc-attributeType 14}}

providedRoamingService ATTRIBUTE::={
  WITH SYNTAX          OCTET STRING
   EQUALITY MATCHING RULE          octetStringMatch
   SINGLE VALUE                    TRUE
   ID                              {ttc-attributeType 22}}

phsRoamingNumber ATTRIBUTE::={
  WITH SYNTAX          OCTET STRING
   EQUALITY MATCHING RULE          octetStringMatch
   SINGLE VALUE                    TRUE
   ID                              {ttc-attributeType 23}}

accessingNetworkId ATTRIBUTE::={
WITH SYNTAX          NumericString(SIZE(1..ub-accessingNetworkId))
  EQUALITY MATCHING RULE          numericStringMatch
  SUBSTRINGS MATCHING RULE        numericStringSubstringsMatch
  SINGLE VALUE                    TRUE
  ID                              {ttc-attributeType 24}}

routingType ATTRIBUTE::={
WITH SYNTAX          ENUMERATED
  SINGLE VALUE                    TRUE
  ID                              {ttc-attributeType 25}}
```

```
locationRegistrationAuthenticationInformation ATTRIBUTE::={
  WITH SYNTAX          OCTET STRING
    SINGLE VALUE                    TRUE
    ID                              {ttc-attributeType 26}}

callSetupAuthenticationInformation ATTRIBUTE::={
  WITH SYNTAX          OCTET STRING
    SINGLE VALUE                    TRUE
    ID                              {ttc-attributeType 27}}
```

The meanings of the attributes indicated by the above object class definitions are as follows;

The ‘phsNumber’ attribute identifies a PHS number. The type of this attribute is Octet String, and in it, the information is set to be as same format as the called number parameter specified by B-IF3.03 Document.

The ‘providedRoamingService’ attribute indicates the services that can be provided in each visited network.

The ‘phsRoamingNumber’ attribute indicates the public PHS roaming number. The type of this attribute is Octet String, and in it, information is set to be same format as the called number parameter specified by B-IF3.03 Document.

The ‘accessingNetworkId’ attribute indicates information of the network that is executing the first location registration and the state of the registration. The type of this attribute is NumericString, and the ‘accessingNetworkId’ attribute contains accessing state and information to identify the public PHS service provider. This standard defines three states, ‘Idle’ , ‘registering location’ and ‘location registration failed’.

The ‘routingType’ attribute identifies the method for the usage of the public PHS roaming number in the visited network. This attribute enables to identify whether the PHS roaming number identifies the visited network or the Public PS. When the ‘RoamingNumber’ identifies the Public PS, it also identifies the valid period of the public PHS roaming number.

The ‘locationRegistrationAuthenticationInformation’ attribute is the information used for Public PS authentication when the location is registered in the visited network. This information contains set of authentication information each of which is used for each location registration.

The ‘callSetupAuthenticationInformation’ attribute is the information used for Public PS authentication for call origination/termination in the visited network. This information contains a set of setup authentication information each of which is used for each call origination/termination. Each series of authentication information can be used for several handover.

3.2.1.4 Public PHS roaming number pool

This object class defines a PHS roaming number pool which is to be prepared for roaming number assignment method No.2 (detailed explanation for roaming number assignment method is described

in B-NW0.00). The definition includes:

(1) relating a PHS roaming number with a PHS number; and

(2) managing the PHS roaming number condition (i.e., assignable or not).

```
phsRoamingNumberPool OBJECT-CLASS::={
   SUBCLASS OF       top
   MUST CONTAIN      {phsRoamingNumber}
   MAY CONTAIN       {phsNumber}
   ID                {X}}
```

(Note) Object identifier X is to be decided. New object identifiers to this PHS MoU Technical Specifications have not yet been assigned. At present PHS MoU Group itself has no right to assign object identifiers to PHS MoU Technical Specifications and so PHS MoU Group looking for organizations who are eligible and willing to assign object identifiers.

```
phsRoamingNumber ATTRIBUTE::={
   WITH SYNTAX              OCTET STRING
   EQUALITY MATCHING RULE   octetStringMatch
   SINGLE VALUE             TRUE
   ID                       {ttc-attributeType 23}}

phsNumber ATTRIBUTE::={
   WITH SYNTAX              OCTET STRING
   EQUALITY MATCHING RULE   octetStringMatch
   SINGLE VALUE             TRUE
   ID                       {ttc-attributeType 14}}
```

The meanings of the attributes indicated by the above object class definitions are as follows;

The ‘phsRoamingNumber’ attribute indicates the public PHS roaming number. The type of this attribute is Octet String, and in it, information is set to be same format as the called number parameter specified by B-IF3.03 Document.
To realize the efficient management of PHS roaming numbers, it is needed to associate a time-stamp with each roaming number so that the number whose timer has expired can be reassigned for another incoming call. For this purpose, CONTEXT indicating temporal validity of an attribute value (temporalContext defined in X.520) may be attached to the phsRoamingNumber attribute in the following way:

```
phsDITContextUse DIT-CONTEXT-USE-RULE::={
  ATTRIBUTE TYPE     {ttc-attributeType 23}
  OPTIONAL CONTEXTS  {temporalContext}}
```

The ‘phsNumber’ attribute identifies a PHS number. The type of this attribute is Octet String, and in it, the information is set to be as same format as the called number parameter specified by B-IF3.03 Document.

3.2.2 public PHS roaming information model

3.2.2.1 Relation between object classes

Figure 3-1 • B-IF4.50 shows the DIT model used to define the public PHS roaming service data model. The lines between object classes indicate existence of relation between two object classes. An existence of relation shows that an object class does not exist by itself. It requires a higher direction in the figure for an object class to have a meaning. For example, a 'phsISPTSubscriberPlofile' object class is not a standalone object class, it subordinates to a 'phsISPTServiceProvider' object class.
The existence of relation is not a one to one relation. The instance of a superior object class can be associated with several instances of an inferior object class. For example, a 'phsISPTServiceProvider' associates with several 'phsISPTSubscriberProfile's. All these relations have one to n relations.

The use of the terms "superior" and "inferior" does not imply any class relation. These terms only mean that an instance of an inferior class has no meaning if an instance of the superior class does not exist.

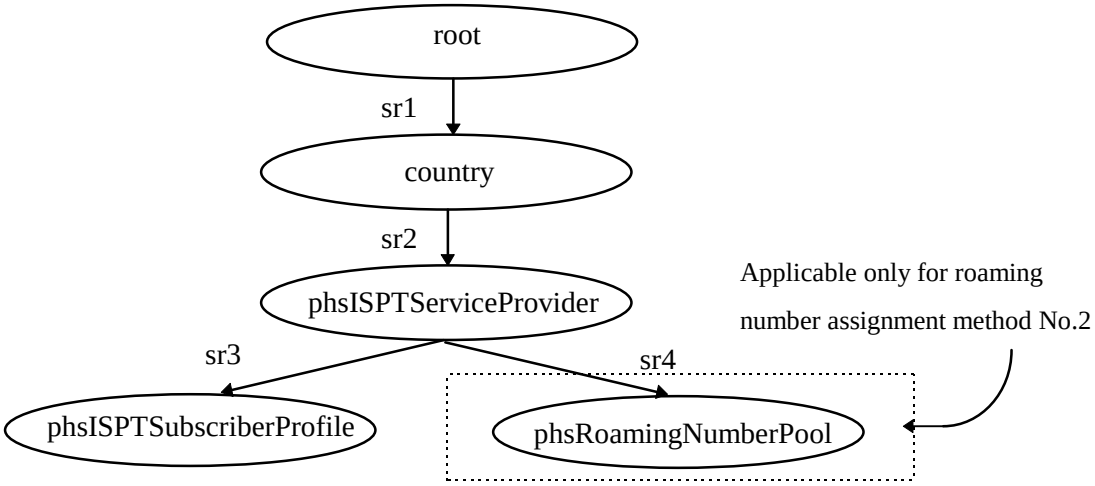


Figure 3.1 B-IF4.50 DIT structure for public PHS roaming service

3.2.2.2 Name forms

For each object class, the name forms define the attributes that will be included in the named object class. The naming attribute is used to uniquely identify the instances of the object class. The naming attribute should be a mandatory attribute of the object class.

```
countryNameForm NAME-FORM::={
  NAMES                 country
  WITH ATTRIBUTES       {countryName}
  ID                    {id-nf-countryNameForm}}

phsISPTServiceProviderNameForm NAME-FORM::={
```

NAMES phsISPTServiceProvider
WITH ATTRIBUTES {phsISPTServiceProviderId}
ID {ttc-nameForm 3}}

phsISPTSubscriberProfileNameForm NAME-FORM::={
NAMES phsISPTSubscriberProfile
WITH ATTRIBUTES {phsNumber}
ID {ttc-nameForm 4}}

phsRoamingNumberPoolNameForm NAME-FORM::={
NAMES phsRoamingNumberPool
WITH ATTRIBUTES {phsRoamingNumber}
ID {X}}

The 'phsRoamingNumberPoolNameForm' is applied only for roaming number assignment method No.2.
(Note) Object identifier X is to be decided. New object identifiers to this PHS MoU Technical Specifications have not yet been assigned. At present PHS MoU Group itself has no right to assign object identifiers to PHS MoU Technical Specifications and so PHS MoU Group looking for organizations who are eligible and willing to assign object identifiers.
Instances of the 'phsISPTServiceProvider' object class will be uniquely identified by the 'phsISPTServiceProviderId' attribute value. An instance of the 'phsISPTSubscriberProfile' object class will be identified by the 'phsNumber' attribute value. An instance of the 'phsRoamingNumberPool' object class will be identified by the 'phsRoamingNumber' attribute value.

3.2.2.3 Structure rules

In the database, the stored location of a data item is specified by the object class to which it belongs. The name of the object class is concatenated to the names of object classes superior to it in the structure rule. This implies that a hierarchical structure exists between the objects in order to create the object class.

sr1 STRUCTURE-RULE::={
NAME FORM countryNameForm
ID 1}

sr2 STRUCTURE-RULE::={
NAME FORM phsISPTServiceProviderNameForm
SUPERIOR RULES {sr1}
ID 2}

sr3 STRUCTURE-RULE::={
NAME FORM phsISPTSubscriberProfileNameForm
SUPERIOR RULES {sr2}
ID 3}

sr4 STRUCTURE-RULE::={

NAME FORM phsRoamingNumberPoolNameForm
SUPERIOR RULES {sr2}
ID 4}

sr4 is applied only for roaming number assignment method No.2.The relationships between the object classes are indicated by lines in Figure 3-1•B-IF4.50.
This Figure shows the structure of the Directory Information Tree.

To access an targeted object, it is necessary to follow a path defined in the Figure.

3.3 Access control

The access to attribute of the 'phsISPTSubscriberProfile' object class is controlled by access control information which is represented as a set of the 'ACIItems' parameters. Each component grants or denies access right of the PHS service network and the protected items of information.

The actual access control information is allocated for the value of the 'ACIItem' parameter.

The following access control information is specified in PHS basic roaming capability set. It is possible to modify the 'accessingNetworkId', the 'phsRoamingNumber', and the 'routingType' attributes in the 'phsISPTSubscriberProfile' entry. Search and modification to other attributes are not possible (See Appendix).

3.4 Agreement related model

Attributes of the 'phsISPTSubscriberProfile' object class are copied to the visited network and deleted from the home network by 'updateShadow'. The attributes allowed to be manipulated by shadowing are defined by the shadowing agreement. In public PHS basic roaming capability set, following two types of agreements are implicitly established:

(1) Unit of agreement is all users potentially roamable.

(2) Unit of agreement is the individual public PHS number that roams.

4. PHS roaming procedure

This clause provides the procedure for basic PHS roaming capability set described in B-IF0.50. Three following procedures are described in this clause.
-Basic procedure
-Mobility procedure
-Call handing procedure

The capability of Network performing the PHS roaming procedure is assumed the following items.
(1) A visited network is able to distinguish a public PS
(2) The visited network is able to distinguish the roaming public PS using PHS number.
(3) The PHS roaming service providing networks share the information of the DIT structure, and the agreement if signed for the shadowing service profile of all the roamable PHS users.

4.1 Protocol providing conditions

This protocol conforms B-IF4.28. Service provided by TCAP is described in clause 2 of B-IF4.28 document.

4.1.1 Correspondence between the SDF-SDF interface and TC service

The correspondence between below operations and TC service is regulated as follows:
(1) dSABind, dSAShadowBind, dSAUnbind, dSAShadowUnbind are provided by Conversation Part on TC. In dSABind and dSAShadowBind, each response (dSABindResult and dSAShadowBindResult) and error (dSABindError , dSAShadowBindError) also are provided by Conversation Part on TC . Parameters required in each operation are set in "User Information" part.
(2) inChainedModifyEntry, inCoordinateShadowUpdate, inRequestShadowUpdate, inUpdateShadow, chainedExecute, are provided by Component Part on TC . Each response and error are provided by ReturnResult and ReturnError that are kinds of component.

4.2 Basic procedure

4.2.1 PHS roaming service profile copying on the first location registration

4.2.1.1 Outline

PHS roaming service profile copying on the first location registration procedure is for the visited network from the home network to copy the PHS service profile included information for authentication, in order for visited network to check the validity and service providing conditions for public PS. This procedure is provided by following performances.
(1) Receiving request from SDF data manager, SDF on visited network updates accessingNetworkId attribute in SDF(H).
(2) After (1), from SDF(H) to SDF on visited network, inUpdateShadow is performed, and service profile is copied to SDF(Vnew).

4.2.1.2 Detailed procedure

(1) Updating 'accessingNetworkId' attribute

Receiving 'ModifyEntry' request from the SDF data manager, The SDF(Vnew) enters 'Wait for Subsequent Request' state from 'Idle' state. After that, the SDF(Vnew) send 'dSABind to SDF(H) to bind with it, and SDF(Vnew) enters 'Wait for Bind Result'. The SDF(H) enters 'Bind Pending' state from 'Idle' state on reception of 'dSABind'. For indicating to bind completely, the SDF(H) send 'dSABindResult' to the SDF(Vnew)., and enters 'SDF Bound' state. Upon receipt of 'dSABindResult', the SDF(Vnew) enters 'SDF Bound' state. If the bind is failed, the SDF(H) sends 'dSABindError' to the SDF(Vnew). Each SDF does not bind and enters 'Idle' state. In this case, the following procedures are not performed.

If the dSABind is finished successfully, the SDF(Vnew) sends 'inChainedModifyEntry' operation to the SDF(H).

Upon receipt of 'inChainedModifyEntry', the SDF(H) updates the accessing state of accessingNetworkId to 'Location Registration', and updates the part indicating PHS ISPTservice provider to the number indicating new visited network. The SDF(H) updates the attribute values of accessingNetworkId completely sends 'inChainedModifyEntryResult' to the SDF(Vnew).
When the operations are not provided as, for example, the requested data is not allowed to update, and is not existed in the SDF and others, the SDF(H) formulates one of the 6 error messages shown below:
Attribute Error
Name Error
Service Error
IN-dsa Referral Error
Security Error
Update Error
The SDF(Vnew) sends 'dSAUnbind' operation to the SDF(H) on reception of 'inChainedModifyEntryResult'. After this, the SDF(Vnew) does not bind to the SDF(H), and enters 'Idle' state.

If the same authenticated association is able to be used in the subsequent procedures, it is unnecessary to send 'dSAUnbind' operation.

(2) Copying PHS roaming service profile

The data manager on the SDF(H) requests to perform 'inUpdateShadow'' from the SDF(H) to the SDF(Vnew), if updating accessingNetworkId is finished successfully. Upon receipt of a request from the SDF data manager, the SDF(H) enters 'Wait for Subsequent Request' from 'Idle' state. After this, the SDF(H) sends 'dSAShadowBind' operation to the SDF(Vnew) and enters 'Wait for Bind Result'. The SDF(Vnew) enters 'Wait for Bind Result' state from 'Idle' state on reception of 'dSAShadowBind'. For indicating to bind completely, the SDF(Vnew) sends 'dSAShadowBindResult' and enters 'SDF Bound' state. The SDF(H) enters 'SDF Bound' state on reception of 'dSAShadowBindResult'. If 'dSAShadowBind' operation is failed, the SDF(Vnew) sends 'dSAShadowBindError' to the SDF(H). After this, each SDF enters 'Idle' state and the bind between the home and visited networks is not established. In this case, the following procedures are not performed.

If 'dSAShadowBind' operation is performed successfully, the SDF(H) formulates 'inCoordinateShadowUpdate' operation and sends it to the SDF(Vnew), and the SDF(H) enters 'Wait

for Coordination Result' state. 'inCoordinateShadowUpdate' operation is used for the shadow-provider to indicate the agreements of the data shadowing. Upon the receipt of 'inCoordinateShadowUpdate' operation, the SDF(Vnew) enters 'Wait for Coordination Result' state, and returns 'inCoordinateShadowUpdateResult' to the SDF(H), after this, the SDF(Vnew) enters 'Wait for Update' state. The SDF(H) enters 'Wait for Update' on the reception of 'inCoordinateShadowUpdate' operation. If the SDF(H) is able to provide the shadowing, then it sends 'inCoordinateShadowUpdate' operation to the SDF(Vnew), and it enters 'Wait for Update Confirmation' state. 'inUpdateShadow' operation sets the attribute values of the phsNumber, the providedRoamingService, the locationRegistrationAuthenticationInformation and the callSetupAuthenticationInformation. The SDF(Vnew) enters 'Wait for Update Confirmation'. When 'inUpdateShadow' operation is performed successfully, the SDF(Vnew) sends 'inUpdateShadowResult' operation and enters 'Wait for Update' state. The SDF(H) received 'inUpdateShadowResult' sends 'dSAShadowUnbind' operation to the SDF(Vnew). When this, the SDF(H) unbinds association to the SDF(Vnew), and enters 'Idle' state. The SDF(Vnew) unbinds association to the SDF(H), and enters 'Idle' state.

4.2.2 PHS roaming service additional copying

4.2.2.1 Outline

The PHS roaming service additional copying procedure is used to copy additionally the PHS roaming profile from the home network for the visited network to verify the public PS, if necessary. When this procedure is performed, it is necessary that implicit agreement between the SDF's exists. The SDF(Vnew) requests 'inUpdateShadow' operation to the SDF(H).

4.2.2.2 Detailed procedure

Receiving a indication from the SDF data manager, the SDF(Vnew) enters 'Wait for Subsequent Request' state from 'Idle' state. After this, the SDF(Vnew) sends 'dSAShadowBind' operation to the SDF(H), and enters 'Wait for Bind Result' state. The SDF(H) enters 'Wait for Bind Result' state from 'Idle' state. If the association between SDF(H) and the SDF(Vnew) is established successfully, the SDF(H) sends 'dSAShadowBindResult' for indicating to bind successfully, and enters 'SDF Bound' state. If the binding is failed with any causes, the SDF(H) sends 'dSAShadowBindError' to the SDF(Vnew). In this case, each SDF enter 'Idle'' state, and does not bind to the other. If 'dSAShadowBind' operation is performed successfully, the SDF(Vnew) sends 'inRequestShadowUpdate' operation, and enters 'Wait for Request Shadow Result' state. Upon receipt of 'inRequestShadowUpdate', the SDF(H) enters 'Wait for Request Shadow Result' state, and sends 'inRequestShadowUpdateResult' operation in response to received 'inRequestShadowUpdate' operation, and enters 'Wait for Update' state. The SDF(H) can provided 'Shadow', the SDF(H) sends 'inUpdateShadow' and enters 'Wait for Update Confirmation' state. The SDF(H) sends 'inUpdateShadow' operation containing the locationRegisterAuthenticationInformation attribute and the callSetupAuthenticationInformation attribute for the AgreementID. Upon the receipt of 'inRequestShadowUpdateResult' operation, the SDF(Vnew) enters 'Wait for Update' state, and enters 'Wait for Update Confirmation' state on reception of inUpdateShadow' operation indicated 'inUpdateShadow' operation.

The SDF(Vnew) retrieves the requesting information sends 'inUpdateShadowResult' to the SDF(H) and enters 'Wait for Update' state. After this, the SDF(Vnew) sends 'dSAShadowUnbind' operation to the SDF(H). The SDF(Vnew) unbinds to the SDF(H), and enters 'Idle' state. The SDF(H) unbinds to

the SDF(Vnew), and enters 'Idle' state.

4.3 Mobility procedure

This procedure is the PHS roaming procedure to assure the public PS mobility. The purpose of the mobility procedure is to assure to receive incoming call. The mobility procedure does not include the behavior for outgoing call and incoming call.

4.3.1 Inter-network location registration

4.3.1.1 Outline

The inter-network location registration procedure is used by the SDF(Vnew) for updating the information that identifies the visited network for the PHS number. The number that identifies the visited network is represented by the phsRoamingNumber. When the inter-network location registration from the SDF(Vnew) is performed, the phsRoamingNumber is overwritten.

The inter-network location registration procedure is performed at the first location registration. This procedure is performed only after both the attribute value of providedRoamingService for the PHS number indicates serviceAvailable, this attribute is received from the SDF(H) by the Service profile retrieval procedure at first location registration, and the authentication for the public PS shall be finished successfully.

4.3.1.2 Detailed procedure

When the SDF data manager requests the SDF(Vnew), it enters 'Wait for Subsequent Request' state from 'Idle' state. Then the SDF(Vnew) sends 'dSABind' operation to the SDF(H) for requesting to bind with the SDF(H). The SDF(H) enters 'Wait for Bind Result' state form 'Idle' state on reception of 'dSABind' operation. If the operation is performed successfully, the SDF(H) sends 'dSABindResult' for indicating to bind successfully, and enters 'SDF Bound' state. The SDF(Vnew) enters 'SDF Bound' state on reception of 'dSABindResult'. If the 'dSABind' operation is failed, the SDF(H) sends 'dSABindError' to the SDF(Vnew). When this, the SDF's on home and visited networks enter 'Idle' state. In this case, the following procedures are not performed.

If 'dSABind' operation is finished successfully, the SDF(Vnew) sends 'inChainedModifyEntry' operation to the SDF(H).

Upon receipt of 'inChainedModifyEntry' operation, the SDF(H) updates the attribute values of phsRoamingNumber and routingType. When the updating is finished completely, it sends 'inChainedModifyEntryResult' to the SDF(Vnew).

If the SDF(H) can not perform 'inChainedModifyEntry' operation (e.g. requested data is not allowed to be updated and nor exist), the SDF(H) sends one of the 6 error shown in subclause 4.2.1.2 to the SDF(Vnew).

The SDF(Vnew) sends 'dSAUnbind' operation to the SDF(H) on reception of 'inChainedModifyEntryResult'. Then the SDF(Vnew) unbinds to the SDF(H), and enters 'Idle' state. The SDF(H) also unbinds to the SDF(Vnew), and enters 'Idle' state on reception of 'dSAUnbind'

operation.

Then the SDF data manager on home network modifies 'roamingStatus' attribute value to the attribute value 'Idle'.

If the usable authenticated association is already established, it is unnecessary to send 'dSAUnbind' operation.

4.3.2 Deletion of service profile copied at the previously visited network

4.3.2.1 Outline

This procedure is used by the home network to delete the information for public PS in the pre-visited network.

This procedure uses 'inUpdateShadow' operation, and is performed when the phsRoamingNumber is updated in the inter-network location registration procedure. This procedure always is performed after the inter-network location registration.

When the public PS moves to a new-visited network from a pre-visited network or home network, and requests to register the location information for the first time.

4.3.2.2 Detailed procedure

Updating 'phsRoamingNumber' successfully, the SDF data manager on home network requests to perform 'inUpdateShadow' on the SDF on visited network (so-called pre-visited network). The SDF(H) enters 'Wait for Subsequent Request' state from 'Idle' state on reception of request from the SDF data manager. Then the SDF(H) sends 'dSABind' operation to the SDF on visited network and enters 'Wait for Bind Result'. The SDF on visited network enters 'Wait for Bind Result' state from 'Idle' state. If this operation is performed successfully, the SDF on visited network sends 'dSAShadowBindResult' operation for indicating to bind completely, and enters 'SDF Bound' state. The SDF(H) enters 'SDF Bound' state on reception of 'dSAShadowBindResult'. If 'dSAShadowBind' operation is failed, the SDF on visited network sends 'dSAShadowBindError' to the SDF(H). The SDF's enters 'Idle' state and not bind. In this case, the following procedures are not performed.

When 'dSAShadowBind' operation is performed successfully, the SDF(H) sends 'inCoordinateShadowUpdate' operation, and enters 'Wait for Coordination Result' state. 'inCoordinateShadowUpdate' operation indicates the agreement the shadowing that is intended by the shadow provider. The SDF on visited network enters 'Wait for Coordination Result' state, and sends 'inCoordinateShadowUpdateResult' to the SDF(H) and enters 'Wait for Update' state. Upon receipt of 'inCoordinateShadowUpdateResult', the SDF(H) enters 'Wait for Update' state, and sends 'inUpdateShadow' operation and enters 'Wait for Update Confirmation' state if possible. 'inUpdateShadow' operation deletes the copy existing in the visited network. Upon receipt of 'inUpdateShadow' operation, the SDF on visited network enters 'Wait for Update Confirmation' state, if 'inUpdateShadow' operation is performed completely, sends 'inUpdateShadowResult' operation to the SDF(H) and enters 'Wait for Update' state. The SDF(H) sends 'dSAUnbind' operation to the SDF on visited network on reception of 'inUpdateShadowResult'. Then the SDF(H) unbinds to the SDF on visited network, and enters 'Idle' state. The SDF on visited network unbinds to the SDF(H), and enters

'Idle' state on reception of 'dSAUnbind' operation.

4.4 Call handling procedure

4.4.1 PHS roaming number assignment

This procedure is the Call handling procedure requests to get the PHS roaming number to the visited network. The ’PHS roaming number assignment’is used only in chained execute operation for roaming number assignment method No.2.

4.4.1.1 Outline

The PHS roaming number assignment procedure is used by the SDF(H) for sending request to the visited network in order to get appropriate phsRoamingNumber, when the origination of a call to roamed public PS is informed to the visited network. The phsRoamingNumber assignment is performed by ‘chainedExecute’ operation which requests an Execute operation according to a predefined method, as a method represents a sequence of DAP operations which is performed under the control of the DSA.
SDF(Vnew) assigns the phsRoamingNumber whose timer already expired or the timer is active for a certain amount of second, and sets the present time as a time-stamp. SDF(Vnew) correlates the PHS number with available phsRoamingNumber, and then returns the phsRoamingNumber to SDF(H).

4.4.1.2 Detailed procedure

When the SDF data manager requests the SDF(H), it enters 'Wait for Subsequent Request' state from 'Idle' state. Then the SDF(H) sends 'dSABind' operation to the SDF(Vnew) for requesting to bind with the SDF(Vnew). The SDF(Vnew) enters 'Wait for Bind Result' state form 'Idle' state on reception of 'dSABind' operation. If the operation is performed successfully, the SDF(Vnew) sends 'dSABindResult' for indicating to bind successfully, and enters 'SDF Bound' state. The SDF(H) enters 'SDF Bound' state on reception of 'dSABindResult'. If the 'dSABind' operation is failed, the SDF(Vnew) sends 'dSABindError' to the SDF(H). When this, the SDF's on home and visited networks enter 'Idle' state. In this case, the following procedures are not performed.

If 'dSABind' operation is finished successfully, the SDF(H) sends 'ChainedExecute' operation to the SDF(Vnew).

The definition of method for assignment of temporal PHS roaming number shows as follows for example.

```
phsRoamingNumberAssignment METHOD ::={
SPECIFIC-INPUT   OCTET STRING --- PHS number of terminating PS
OUTPUT-ATTRIBUTE phsRoamingNumber
BEHAVIOUR        "This method performs following actions:
                  (1) selects a value of phsRoamingNumber attribute in entities of
                    phsRoamingNumberPool object class, which has no context
                    associated with it or has the expired temporal context associated with
                    it.
                  (2) if necessary, adds phsNumber attribute to entity, which stores the
                    selected value as the value of phsRoamingNumber attribute, of
                    phsRoamingNumberPool object class.
```

(3)stores a value of special input as a value of the phsNumber attribute
(4)attaches temporalContext value which is current time to the selected value.
(5) return the selected value without context values. "
ID {X}}

(Note) The 'phsRoamingNumberAssignment' method is used only in chained execute operation for roaming number assignment method No.2. Object identifier X is to be decided. New object identifiers to this PHS MoU Technical Specifications have not yet been assigned. At present PHS MoU Group itself has no right to assign object identifiers to PHS MoU Technical Specifications and so PHS MoU Group looking for organizations who are eligible and willing to assign object identifiers.

Upon receipt of 'ChainedExecute' operation, the SDF(Vnew) updates the attribute values of phsRoamingNumber and routingType. When the updating is finished completely, it sends 'ChainedExecuteResult' to the SDF(H).

If the SDF(Vnew) can not perform 'ChainedExecute' operation (e.g. the method fails to complete correctly), the SDF(Vnew) sends one of the 6 errors shown in subclause 4.2.1.2 or 'executionError' to the SDF(H).

The SDF(H) sends 'dSAUnbind' operation to the SDF(Vnew) on reception of 'ChainedExecuteResult'. Then the SDF(H) unbinds to the SDF(Vnew), and enters 'Idle' state. The SDF(Vnew) also unbinds to the SDF(H), and enters 'Idle' state on reception of 'dSAUnbind' operation.

If the usable authenticated association is already established, it is unnecessary to send 'dSAUnbind' operation.

4.4.2 Call termination to the roaming public PS

4.4.2.1 Outline

This section describes characteristics of the method No.2. In the method No.2, all calls are routed to the visited network by the temporary phsRoamingNumber. Then the visited network identifies which public PS terminates the call by phsRoamingNumber.
The method No.2 is specified in PHS MoU Document B-NW0.00.

4.4.2.2 Detailed procedure

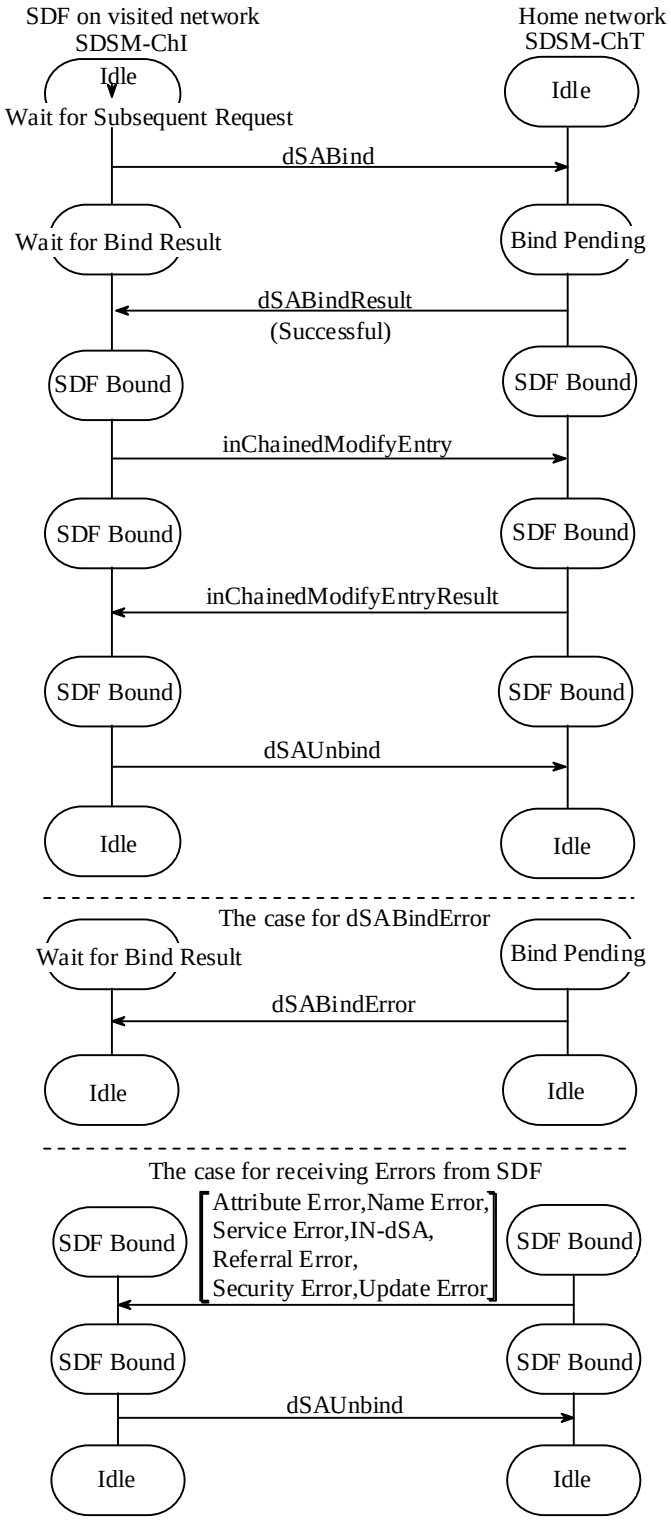
Handling of phsRoamingNumber applies either method No.1 or method No.2 by routingType. The method No.2 does not use the phsRoamingNumber in SDF(H), when a call to be terminated to roaming public PS to the visited network, SDF(Vnew) receives the phsRoamingNumber as called party number. SDF(Vnew) uses it as a search key for PHS number reference.

They may be the case of alternative selecting route, therefore some countermeasures such as an additional guard timer or a alternative number assignment might be necessary.

5. Signalling Sequence

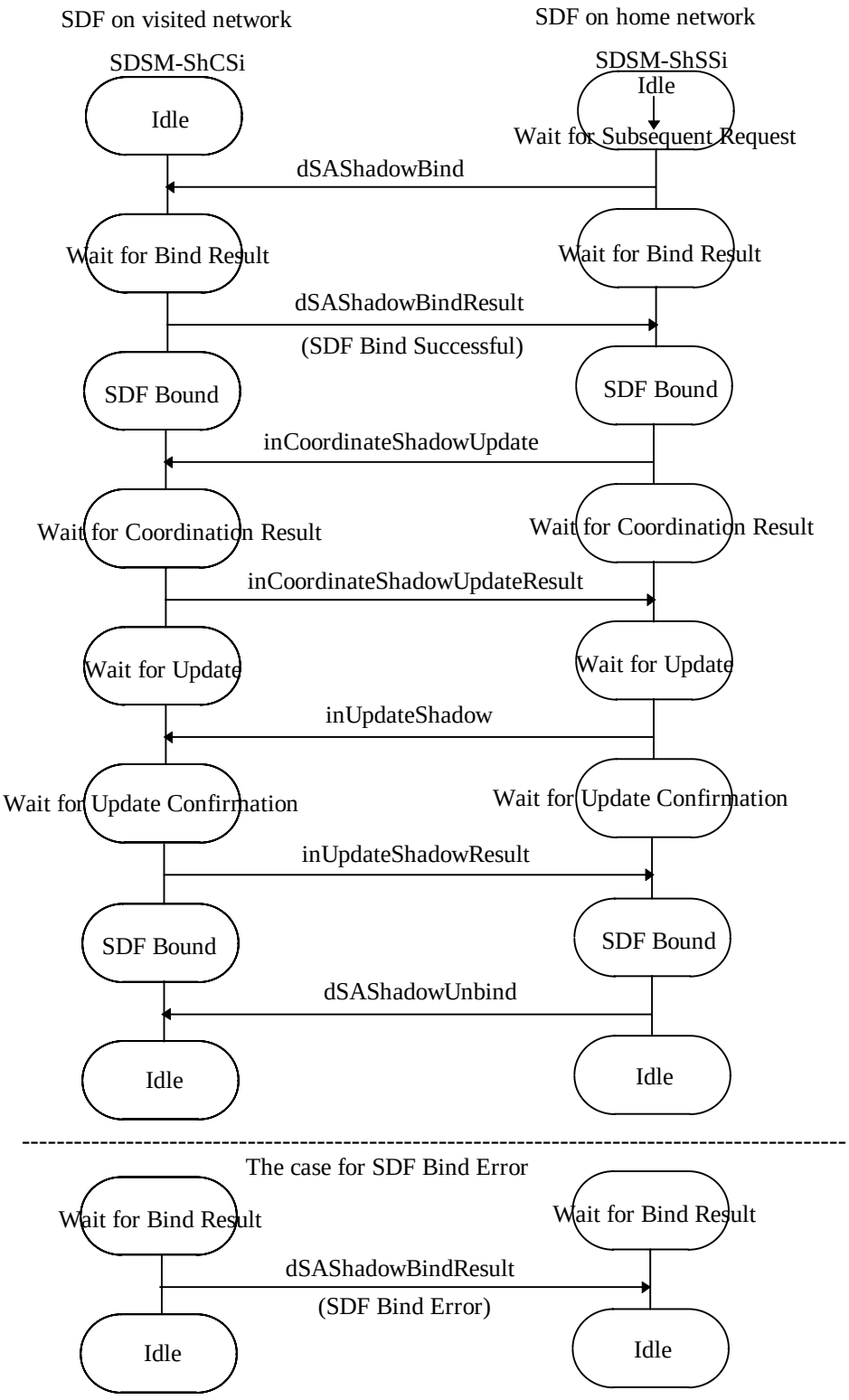
This clause shows signalling sequence between SDF on the visited network and SDF on the home network as follows:

Figure 5-1/B-IF4.50	PHS roaming service profile copying on the first location registration (1)
Figure 5-2/B-IF4.50	PHS roaming service profile copying on the first location registration (2)
Figure 5-3/B-IF4.50	PHS roaming service profile additional copying
Figure 5-4/B-IF4.50	Inter-network location registration
Figure 5-5/B-IF4.50	Deletion of service profile copied at the previously visited network
Figure 5-6/B-IF4.50	PHS roaming number assignment method No.2



In the following procedure, it is unnecessary to send 'dSAUnbind' if the use of the identical authentication association is suitable.

Figure 5-1/B-IF4.50 PHS roaming service profile copying on the first location registration(1)


SDF on visited network
SDF on home network
SDSM-ShCSi
SDSM-ShSSi
Idle
Idle
Wait for Subsequent Request
dSAShadowBind
Wait for Bind Result
Wait for Bind Result
dSAShadowBindResult
(SDF Bind Successful)
SDF Bound
SDF Bound
inCoordinateShadowUpdate
Wait for Coordination Result
Wait for Coordination Result
inCoordinateShadowUpdateResult
Wait for Update
Wait for Update
inUpdateShadow
Wait for Update Confirmation
Wait for Update Confirmation
inUpdateShadowResult
SDF Bound
SDF Bound
dSAShadowUnbind
Idle
Idle
The case for SDF Bind Error
Wait for Bind Result
Wait for Bind Result
dSAShadowBindResult
(SDF Bind Error)
Idle
Idle

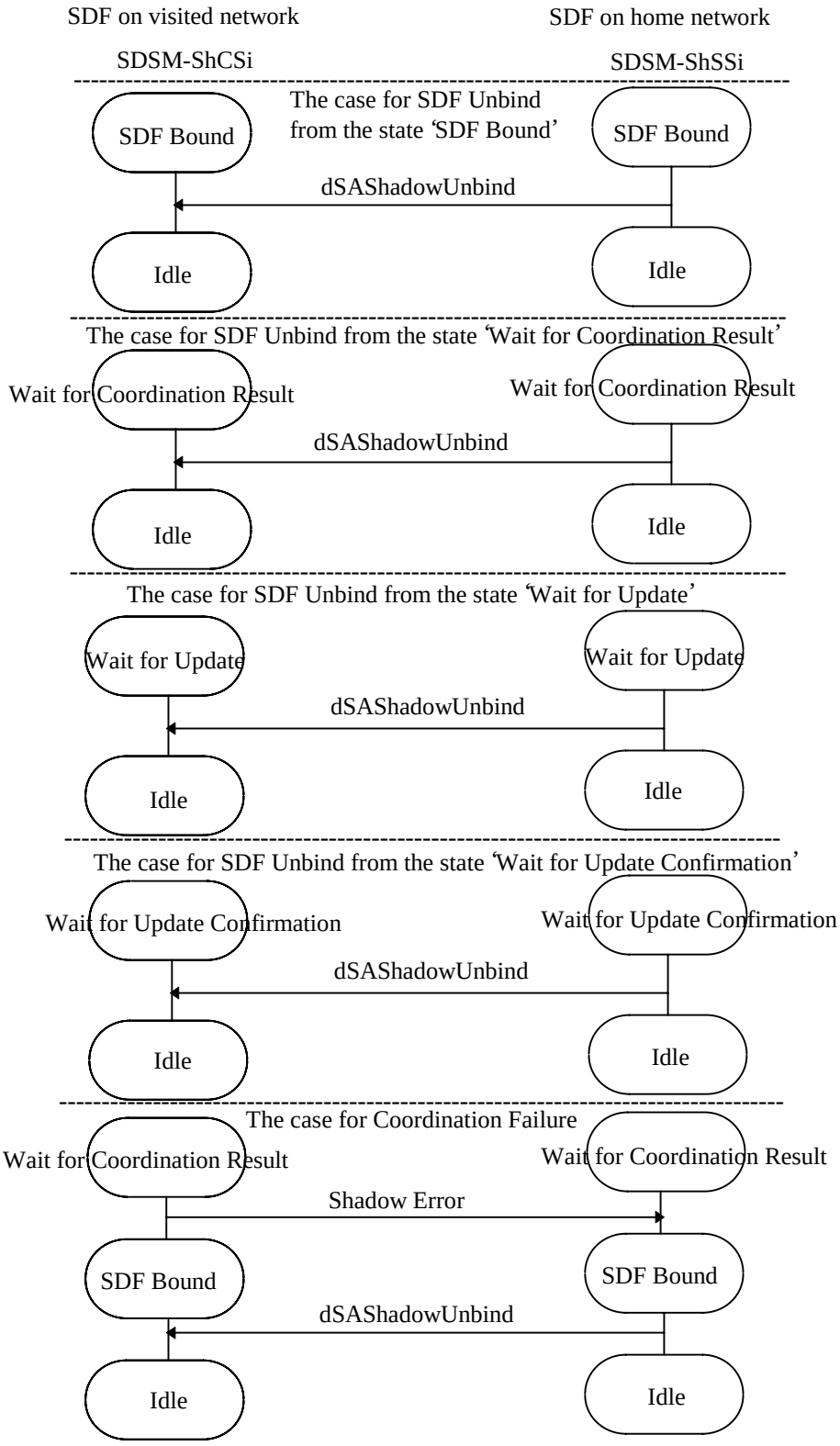
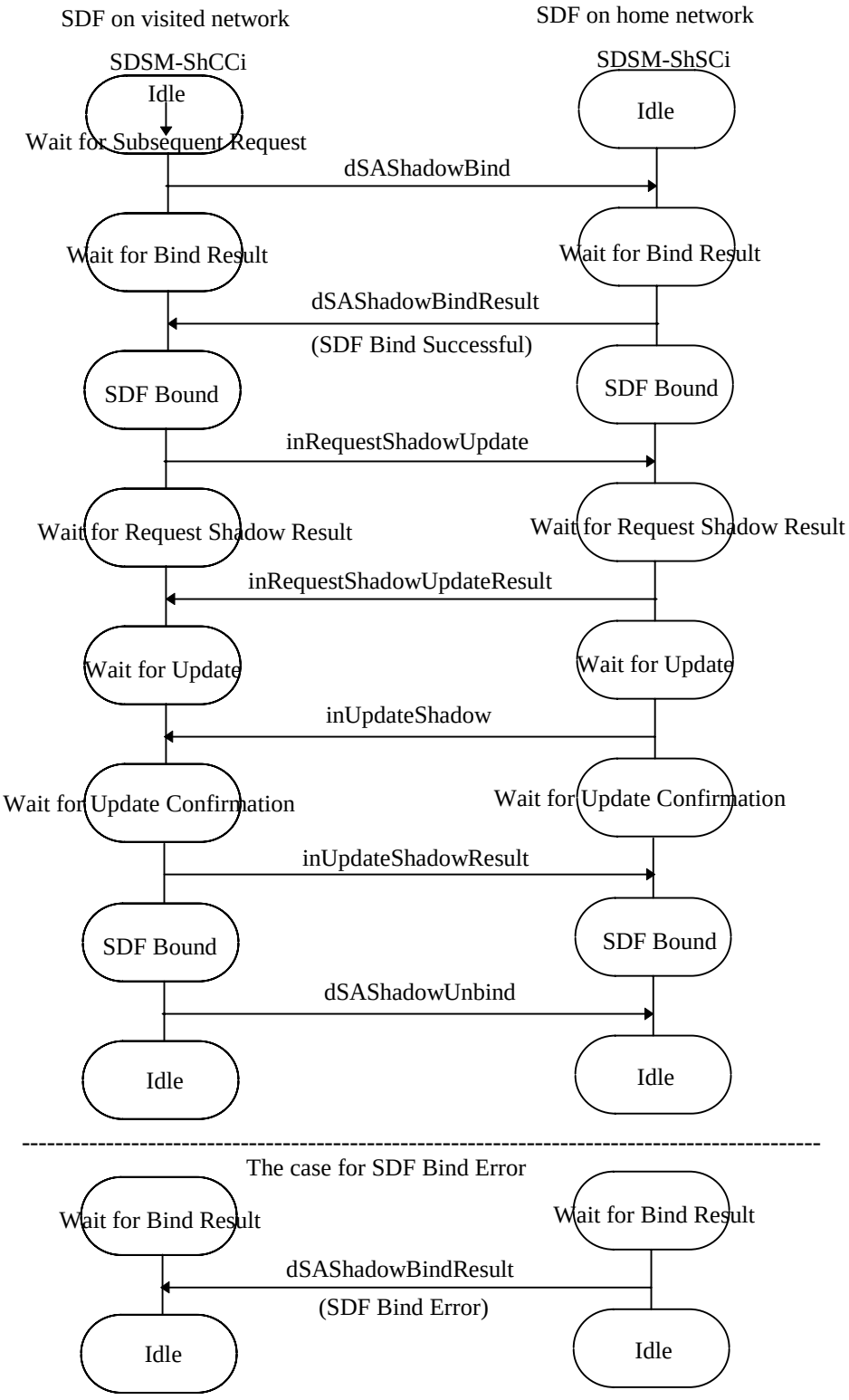


Figure 5-2/B-IF4.50 PHS roaming service profile copying on the first location registration(2)


SDF on visited network
SDF on home network
SDSM-ShCCi
SDSM-ShSCi
Idle
Idle
Wait for Subsequent Request
dSAShadowBind
Wait for Bind Result
Wait for Bind Result
dSAShadowBindResult
(SDF Bind Successful)
SDF Bound
SDF Bound
inRequestShadowUpdate
Wait for Request Shadow Result
Wait for Request Shadow Result
inRequestShadowUpdateResult
Wait for Update
Wait for Update
inUpdateShadow
Wait for Update Confirmation
Wait for Update Confirmation
inUpdateShadowResult
SDF Bound
SDF Bound
dSAShadowUnbind
Idle
Idle
The case for SDF Bind Error
Wait for Bind Result
Wait for Bind Result
dSAShadowBindResult
(SDF Bind Error)
Idle
Idle

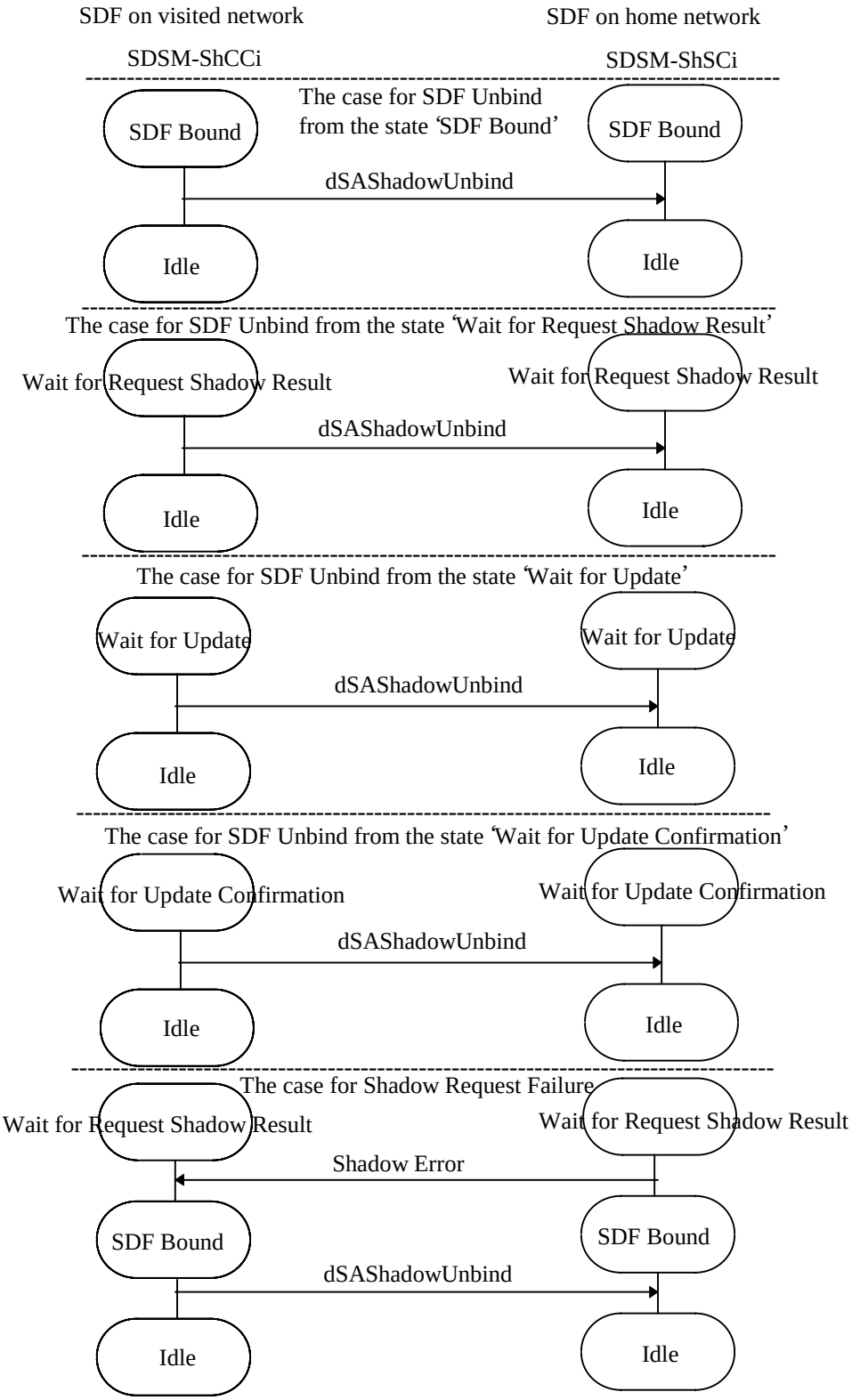
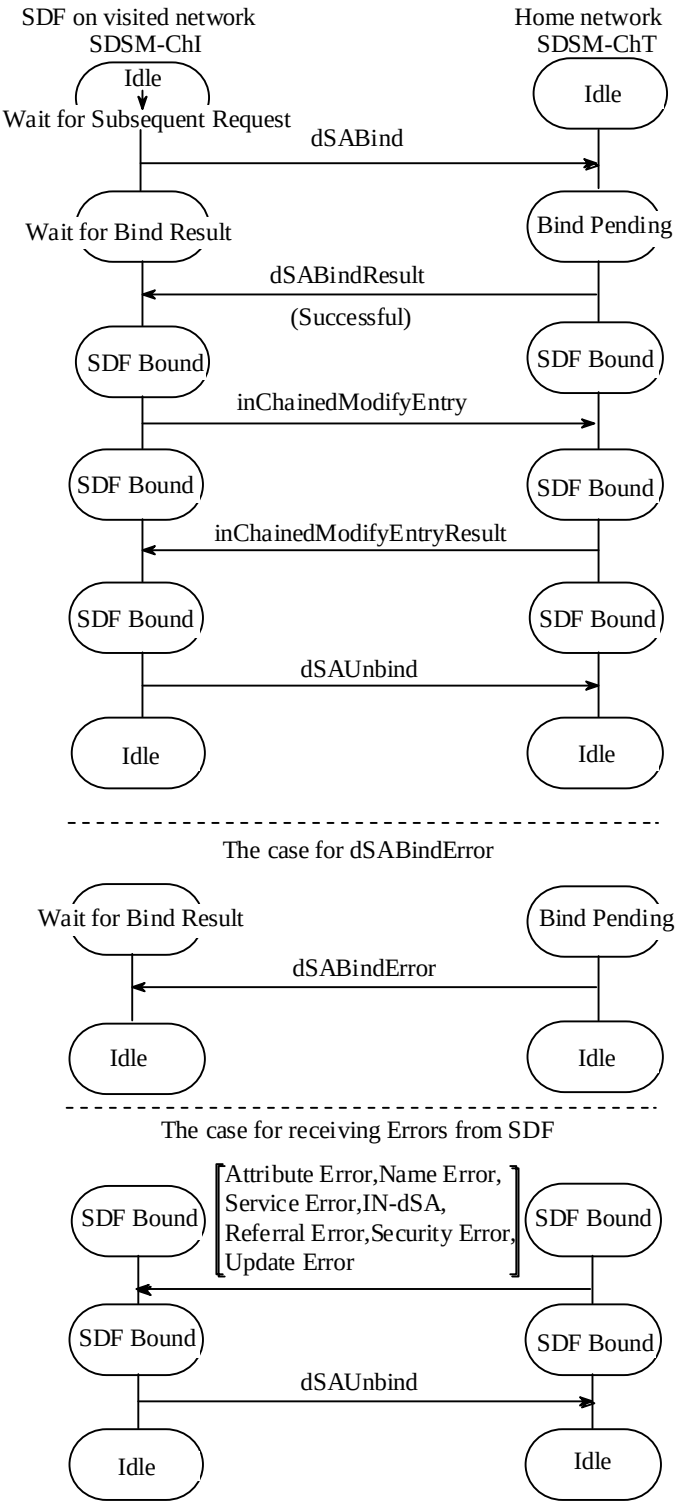
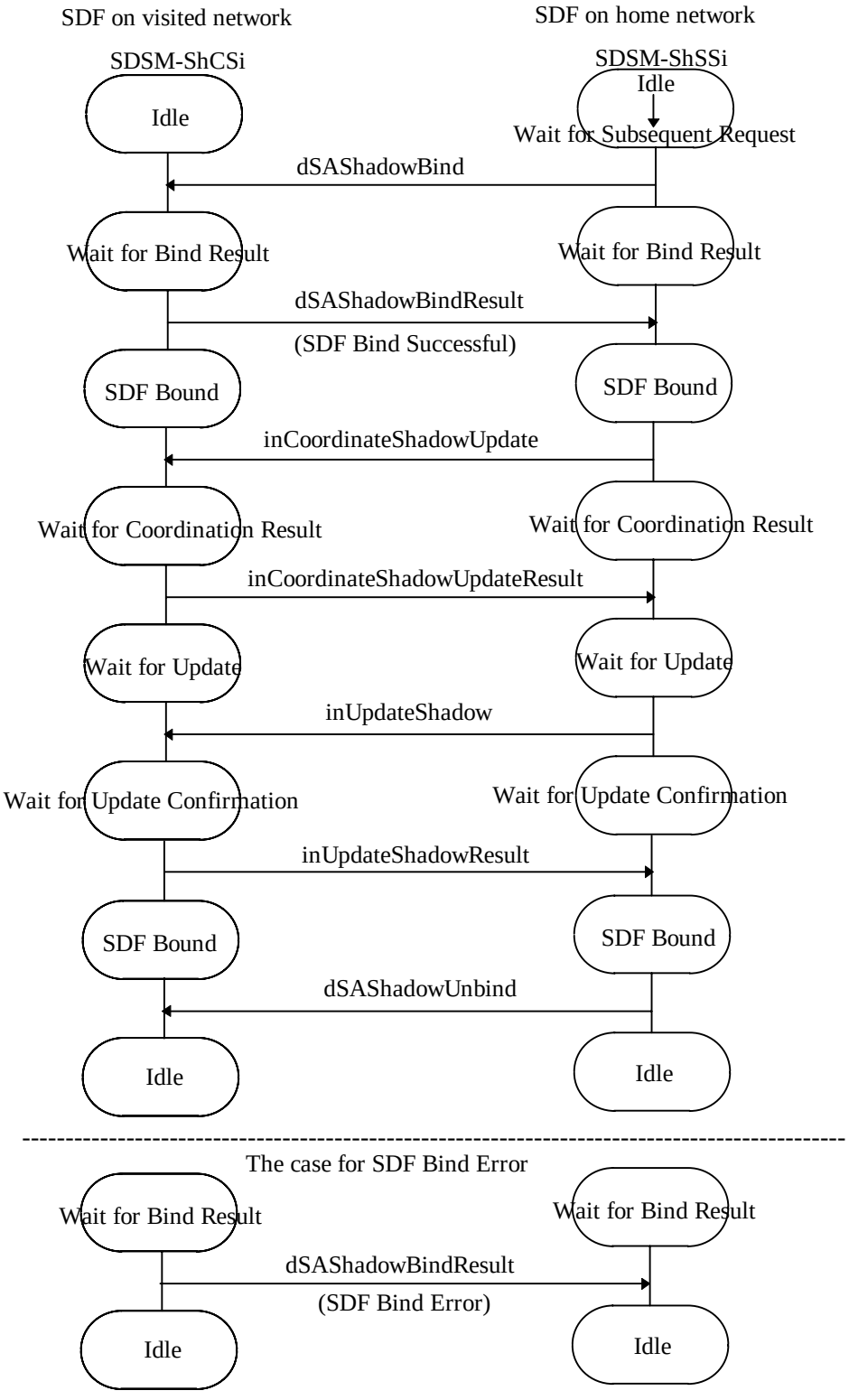


Figure 5-3/B-IF4.50 PHS roaming service profile additional copying



In this procedure, it is unnecessary to send ’dSABind' if the previously authenticated association which is available is established.

Figure 5-4/B-IF4.50 Inter-network location registration


SDF on visited network
SDF on home network
SDSM-ShCSi
SDSM-ShSSi
Idle
Idle
Wait for Subsequent Request
dSAShadowBind
Wait for Bind Result
Wait for Bind Result
dSAShadowBindResult
(SDF Bind Successful)
SDF Bound
SDF Bound
inCoordinateShadowUpdate
Wait for Coordination Result
Wait for Coordination Result
inCoordinateShadowUpdateResult
Wait for Update
Wait for Update
inUpdateShadow
Wait for Update Confirmation
Wait for Update Confirmation
inUpdateShadowResult
SDF Bound
SDF Bound
dSAShadowUnbind
Idle
Idle
The case for SDF Bind Error
Wait for Bind Result
Wait for Bind Result
dSAShadowBindResult
(SDF Bind Error)
Idle
Idle

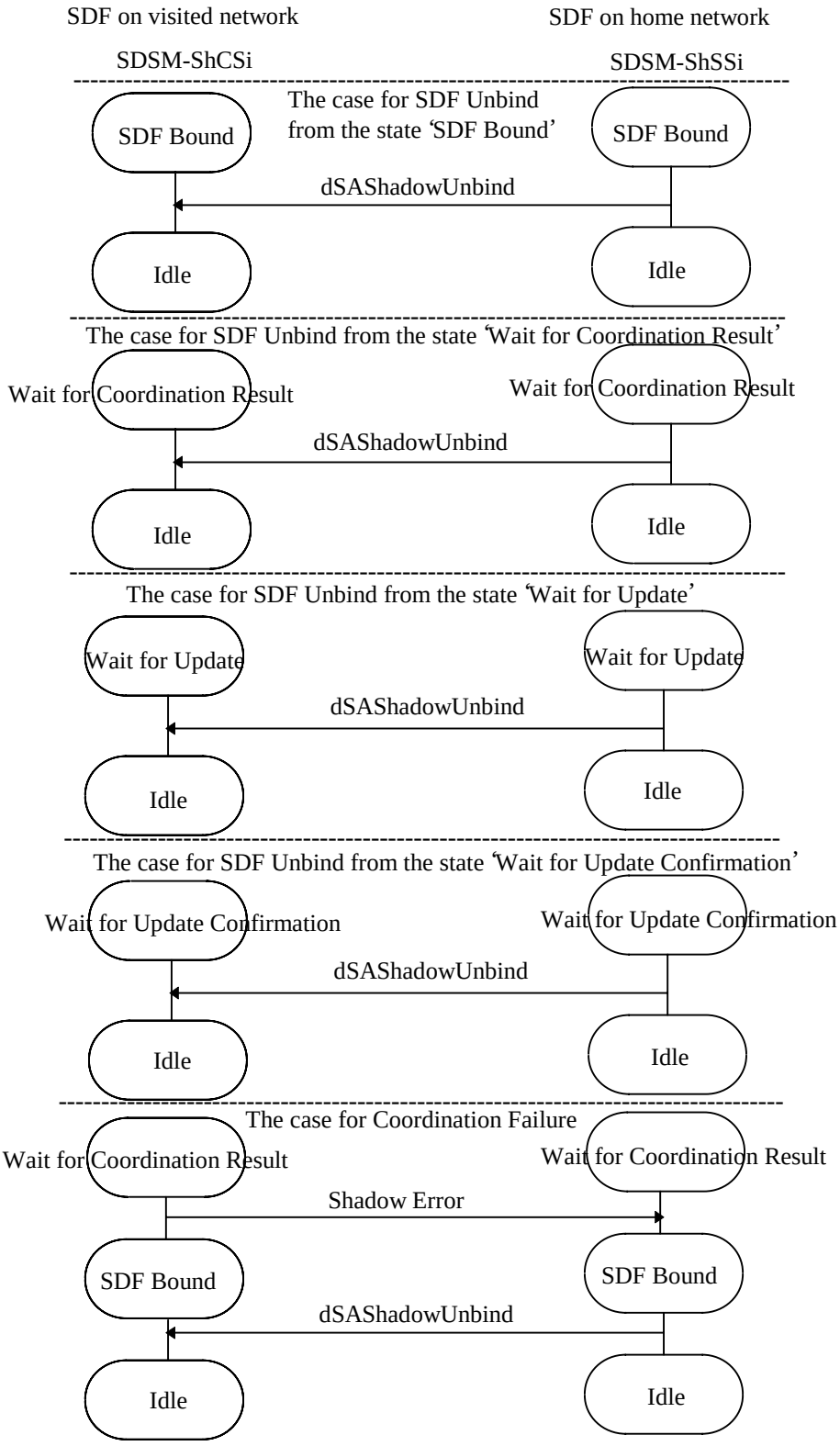
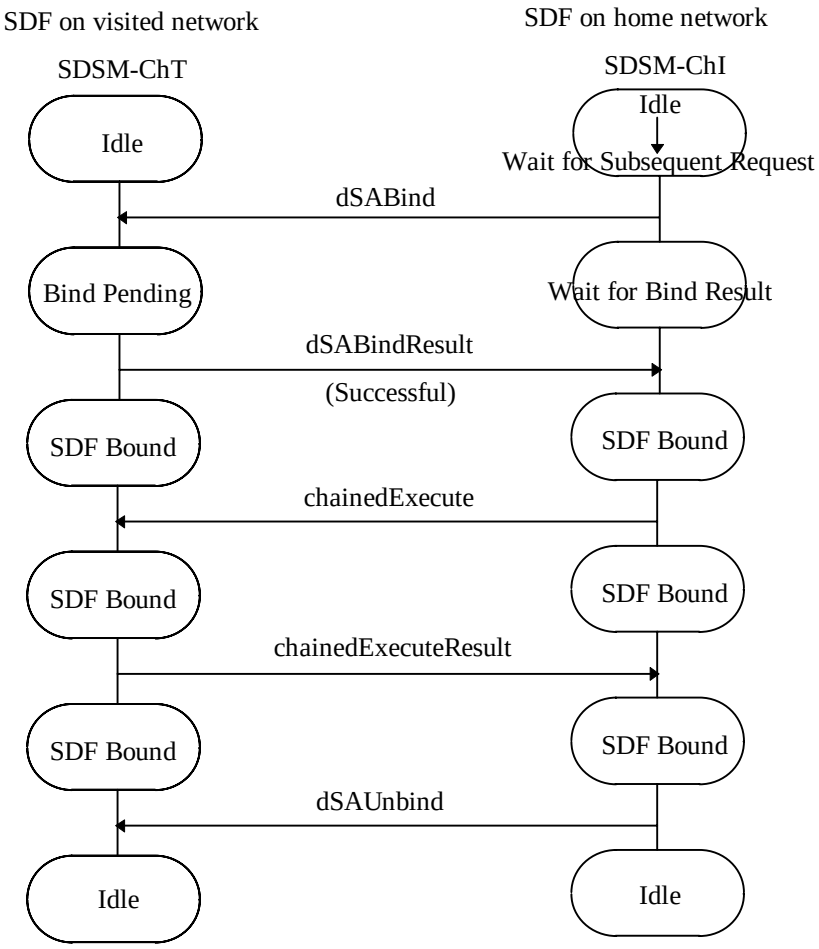
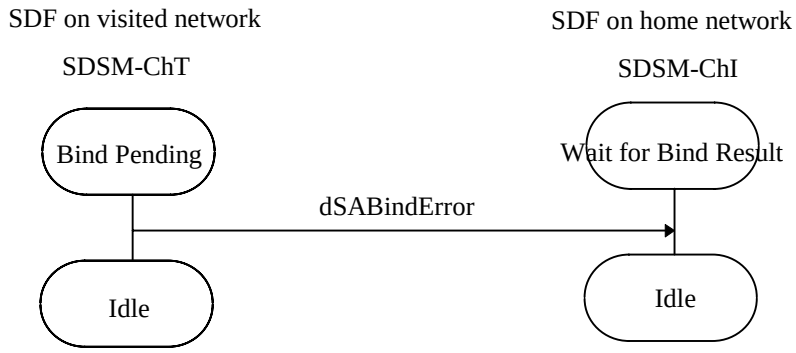


Figure 5-5/B-IF4.50 Deletion of service profile copied at the previously visited network



In this procedure, it is unnecessary to send ‘dSABind’ if the previously authenticated association which is available is established

The case for dSABindError



The case for receiving Errors from SDF

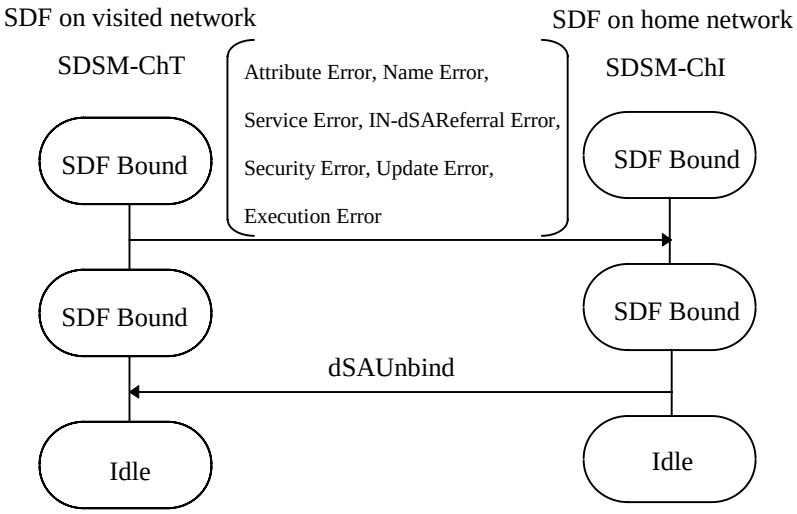


Figure 5-6/B-IF4.50 PHS roaming number assignment method No.2

Annex A

The ASN.1 description of the Attribute type, Object class, Name form, etc. for the basic PHS roaming capability set

This annex shows below ASN.1 descriptions such as PHS specific Attribute types, object classes, name forms, object identifiers, and upper bounds which are specifically defined for PHS in the main body of this document.

```
--Attribute types--

phsISPTServiceProviderId ATTRIBUTE::={
  WITH SYNTAX                    NumericString(SIZE(1..ub-phsProviderId))
    EQUALITY MATCHING RULE       numericStringMatch
    SUBSTRINGS MATCHING RULE     numericStringSubstringsMatch
    SINGLE VALUE                 TRUE
    ID                           {ttc-attributeType 21}}

phsNumber ATTRIBUTE::={
  WITH SYNTAX                    OCTET STRING
    EQUALITY MATCHING RULE       octetStringMatch
    SINGLE VALUE                 TRUE
    ID                           {ttc-attributeType 14}}

providedRoamingService ATTRIBUTE::={
  WITH SYNTAX                    OCTET STRING
    EQUALITY MATCHING RULE       octetStringMatch
    SINGLE VALUE                 TRUE
    ID                           {ttc-attributeType 22}}

phsRoamingNumber ATTRIBUTE::={
  WITH SYNTAX                    OCTET STRING
    EQUALITY MATCHING RULE       octetStringMatch
    SINGLE VALUE                 TRUE
    ID                           {ttc-attributeType 23}}

accessingNetworkId ATTRIBUTE::={
  WITH SYNTAX                    NumericString(SIZE(1..ub-accessingNetworkId))
    EQUALITY MATCHING RULE       numericStringMatch
    SUBSTRINGS MATCHING RULE     numericStringSubstringsMatch
    SINGLE VALUE                 TRUE
    ID                           {ttc-attributeType 24}}

routingType ATTRIBUTE::={
  WITH SYNTAX              ENUMERATED
    SINGLE VALUE           TRUE
    ID                     {ttc-attributeType 25}}
```

```
locationRegistrationAuthenticationInformation ATTRIBUTE::={
  WITH SYNTAX          OCTET STRING
    SINGLE VALUE               TRUE
    ID                         {ttc-attributeType  26}}

callSetupAuthenticationInformation ATTRIBUTE::={
  WITH SYNTAX          OCTET STRING
    SINGLE VALUE               TRUE
    ID                         {ttc-attributeType  27}}

--Object classes--

phsISPTServiceProvider OBJECT-CLASS::={
  SUBCLASS OF          top
  MUST CONTAIN         {phsISPTServiceProviderId}
  ID                   {ttc-objectClass  4}}

phsISPTSubscriberProfile OBJECT-CLASS::={
  SUBCLASS OF          top
  MUST CONTAIN         {phsNumber|
                        providedRoamingService|
                        phsRoamingNumber|
                        accessingNetworkId|
                        routingType|
                        locationRegistrationAuthenticationInformation|
                        callSetupAuthenticationInformation}
  ID                   {ttc-objectClass    5}}

phsRoamingNumberPool OBJECT-CLASS::={
 SUBCLASS OF           top
 MUST CONTAIN     {phsRoamingNumber}
 MAY CONTAIN      {phsNumber}
  ID              {X}}
```

(Note) The 'phsRoamingNumberPool' is applied only for roaming number assignment method No.2.Object identifier X is to be decided. New object identifiers to this PHS MoU Technical Specifications have not yet been assigned. At present PHS MoU Group itself has no right to assign object identifiers to PHS MoU Technical Specifications and so PHS MoU Group looking for organizations who are eligible and willing to assign object identifiers.

```
--Name forms--

phsISPTServiceProviderNameForm NAME-FORM::={
  NAMES                      phsISPTServiceProvider
  WITH ATTRIBUTES            {phsISPTServiceProviderId}
  ID                         {ttc-nameForm  3}}

phsISPTSubscriberProfileNameForm NAME-FORM::={
```

```
  NAMES                          phsISPTSubscriberProfile
  WITH ATTRIBUTES                {phsNumber}
  ID                             {ttc-nameForm  4}}

phsRoamingNumberPoolNameForm NAME-FORM::={
 NAMES                phsRoamingNumberPool
   WITH ATTRIBUTES            {phsRoamingNumber}
   ID                         {X}}
```

(Note) The 'phsRoamingNumberPoolNameForm' is applied only for roaming number assignment method No.2. Object identifier X is to be decided. New object identifiers to this PHS MoU Technical Specifications have not yet been assigned. At present PHS MoU Group itself has no right to assign object identifiers to PHS MoU Technical Specifications and so PHS MoU Group looking for organizations who are eligible and willing to assign object identifiers.

--Method--

```
phsRoamingNumberAssignment METHOD ::={
SPECIFIC-INPUT   OCTET STRING --- PHS number of terminating PS
OUTPUT-ATTRIBUTE phsRoamingNumber
BEHAVIOUR        "This method performs following actions:
                 (1) selects a value of phsRoamingNumber attribute in entities of
                   phsRoamingNumberPool object class, which has no context
                   associated with it or has the expired temporal context associated with
                   it.
                 (2) if necessary, adds phsNumber attribute to an entity, which stores the
                   selected value as a value of phsRoamingNumber attribute, of
                   phsRoamingNumberPool object class.
                 (3) stores a value of specific input as a value of the phsNumber attribute
                 (4) attaches temporalContext value which is current time to the selected
                   value.
                 (5) returns the selected value without context values. "
ID               {X}}
```

(Note) This 'phsRoamingNumberAssignment' method is used only in chained execute operation for roaming number assignment method No.2. Object identifier X is to be decided. New object identifiers to this PHS MoU Technical Specifications have not yet been assigned. At present PHS MoU Group itself has no right to assign object identifiers to PHS MoU Technical Specifications and so PHS MoU Group looking for organizations who are eligible and willing to assign object identifiers.

--Object identifiers--

```
ttc-objectClass OBJECT IDENTIFIER ::=
   {ccitt(0)administration(2)jp(440)ds(5)objectClass(1)}

ttc-attributeType OBJECT IDENTIFIER ::=
   {ccitt(0)administration(2)jp(440)ds(5)attributeType(2)}

ttc-nameForm OBJECT IDENTIFIER ::=
   {ccitt(0)administration(2)jp(440)ds(5)nameForm(4)}
```

```
--Upper bounds--
ub-phsProviderId            INTEGER ::= 16
ub-accessingNetworkId       INTEGER ::= 18
```

Annex B

Actions taken by SDF Data Manager

1. Introduction

The specific functions to basic PHS roaming capability set provided by SDF Data Manager are described in this annex. This section describes the functions related to interactions between networks only.

2. Functions of SDF Data Manager

The functions of SDF Data Manager are shown below.

2.1 Function of first location registration

This is a function to refer to the value of Substring, which shows the state of accessing in the accessingNetworkId attribute, and to deny to transfer in the case that one of the networks is accessing when SDF Data Manager received the inChainedModifyEntry operation, which is the procedure of service profile transfer at the first location registration. This function is provided by SDF Data Manager in the home network.

2.2 Function of subsequent service profile transfer

This is a function to initiate the shadow request sent from a shadow consumer in order to carry out the procedure of subsequent service profile transfer for acquiring new authentication information from the SDF in the home network when SDF Data Manager received the request to transfer the authentication information from the SCF in the network, and there is no rest of the information. This function is provided by SDF Data Manager in the visited network.

This is a function to create a set of authentication information for the interested PHS number which is needed for the procedure of subsequent service profile transfer and service profile transfer at the first location registration. This function is provided by SDF Data Manager in the home network.

3. Function to transit to the state “Idle”

Following cases cause transitions to the state “Idle”:

3.1 Function of internetwork location registration

When the phsRoamingNumber attribute is changed by the procedure of internetwork location registration, SDF Data Manager refers to Substring indicating a network in the accessingNetworkId attribute, and if the network is as same as the one shown by the updated phsRoamingNumber, it updates Substring in the accessingNetworkId attribute from “Location Registering” to “Idle”, which shows the state of accessing. This function is provided by SDF Data Manager in the home network.

3.2 Procedure for deleting PHS roaming service profile copied in the previously visited network

When Substring in the accessingNetworkId attribute is set to “Location Registration Failed” by the newly visited network during the PHS roaming service transfer, SDF Data Manager in the home network starts deletion of PHS roaming service profile in the newly visited networks (refers to annex). On completion of the procedure above, SDF Data Manager in the home network changes Substring in the accessingNetworkId from “Location Registration Failed” to “Idle”, which shows the state of accessing.

Annex C

Procedure for Failure of First Location Registration

1. Introduction

Basic PHS roaming capability set specifies following actions for the first location registration which is carried out when the public PS is moved to the visited network. First, the PHS roaming service profile is copied from the home network to the visited network. The visited network refers to the providedRoamingService attribute which is included in the PHS roaming service profile, and checks whether it is possible or not to provide roaming service to the roaming public PS. Also, it authenticates the public PS using the locationRegistrationAuthenticationInformation attribute. After these procedures, it initiates the internetwork location registration in the home network when the visited network determines to allow roaming.
It is needed to delete the PHS roaming service profile copied in the visited network in the case that the visited network does not allow roaming as the result of the check to provide roaming service to the roaming public PS and the authentication of the public PS. This annex describes the way to delete the PHS roaming service profile which has been explained above (which is called the procedure for deleting PHS roaming service profile copied in the previously visited network). The procedure for deleting PHS roaming service profile copied in the previously visited network is a kind of basic procedures, and it can be carried out depending upon the situation of the home network and the visited network at the first location registration.

2. Internetwork information flows

2.1 Outline flow

The procedure for deleting PHS roaming service profile copied in the previously visited network is initiated when roaming of the public PS becomes impossible as the result that the visited network checks whether it is possible or not to provide roaming service to the interested public PS, using the PHS roaming service profile which was copied to the visited network from the home network at the first location registration. Figure C-l/B-IF4.50 shows the outline flow of the first location registration in this case.

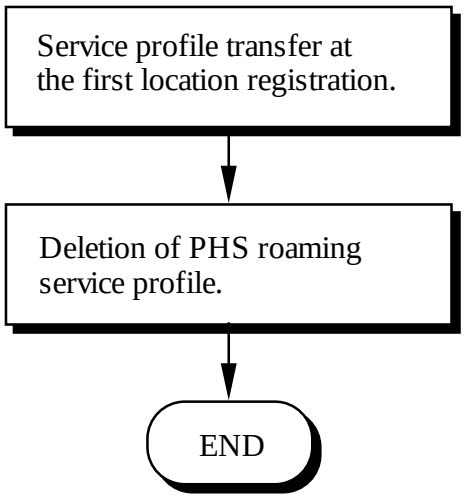


Figure C-1/B-IF4.50 Outline flow of first location registration

2.2 Procedure for deleting PHS roaming service profile in the newly visited network

2.2.1 Outline of procedure

The procedures for deleting PHS roaming service profile in the newly visited network between the SDF(Vnew) and the SDF(H) are as follows :

(1) The SDF(Vnew) requests that the information in the SDF(H), which is about the state of the interested PHS number entry is modified to the state “Location Registration Failed”.

(2) The SDF(H) requests the SDF(Vnew) to delete the information about the interested PHS number upon completion of modification requested at (1).

(3) Based on the request, the SDF(Vnew) deletes the information about the interested PHS number.

2.2.2 Information flow diagram

The information flow diagram is shown in Figure C-2/B-IF4.50.

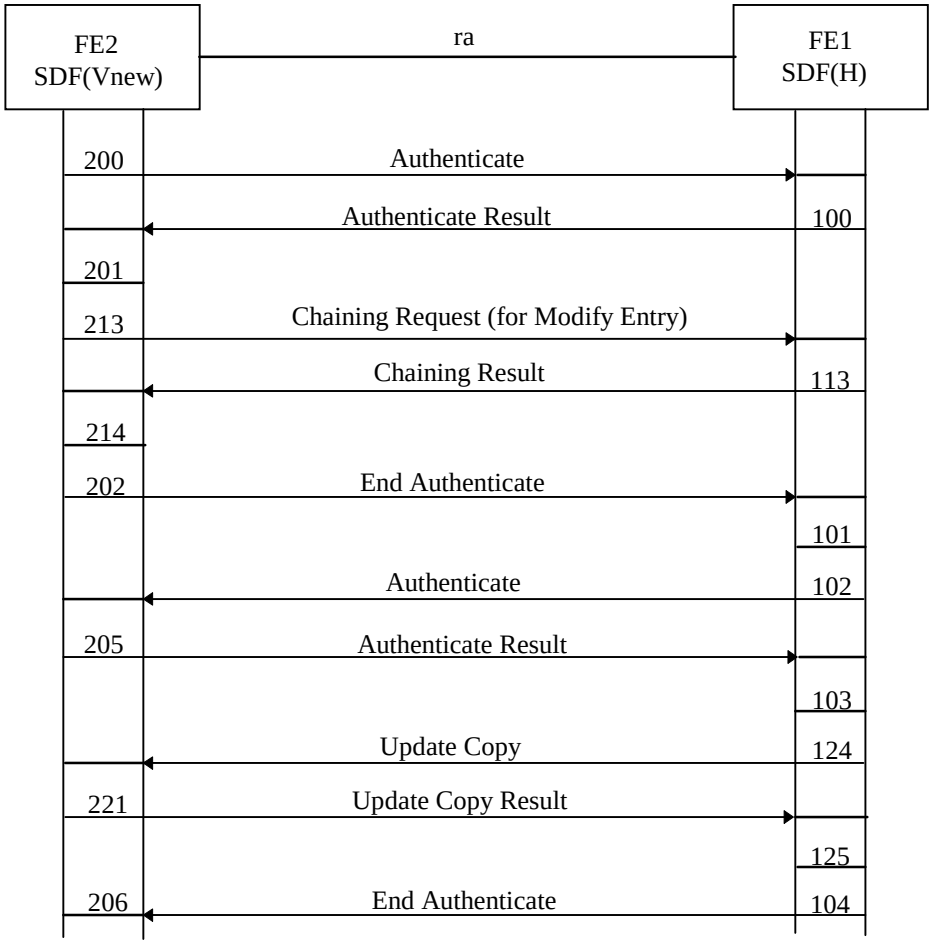


Figure C-2/B-IF4.50 Flow of the procedure for deleting PHS roaming service profile.

2.2.3 Definition of each information flow

The information flow used in this procedure is as same as the information flow defined in B-IF0.50 document.

2.3 Functional entity actions

Although the functional entity actions have been defined in B-IF0.50 document, there are new actions that are needed in this procedure, and they are shown below.

2.3.1 Functional Entity -FE1 (SDF(H))

FEA:113 [C-2]
- Receive and react to ChainingRequest from SDF(Vnew).
  - Modify the information about the state of the interested PHS number to the state “Location Registration Failed”.
  - Formulate and Send ChainingResult to SDF(Vnew).

FEA:124 [C-2]
- Receive and react to the request of SDF Data Manager.
  - Formulate and send UpdateCopy to SDF(Vnew) to delete the PHS roaming service profile for the interested PHS number from SDF(Vnew).

FEA:125 [C-2]
- Receive and react to UpdateCopyResult from SDF(Vnew).

2.3.2 Functional Entity - FE2 (SDF(Vnew))

FEA:213 [C-2]
  - Receive and react to the request of SDF Data Manager.
  - Formulate and send ChainingRequest to SDF(H) to modify the information about the state of the interested PHS number to “Location Registration Failed”.

FEA:214 [C-2]
- Receive and react to ChainingResult.

FEA:221 [C-2]
  - Receive and react to UpdateCopy from SDF(H).
  - Delete the PHS roaming service profile copy for the interested PHS number.
  - Formulate and send UpdateCopyResult to SDF(H).

3. Internetwork protocol

The procedure for deleting the PHS roaming service profile in the newly visited network is described in section.

3.1 Outline

The procedure for deleting PHS roaming service profile in the newly visited network is realized by the following three actions:

(1) Based on the request of SDF Data Manager, the SDF in the visited network modifies the part which shows the state of accessing in the accessingNetworkId attribute in the SDF in the home network to the state “Location Registration Failed”.
(2) When (1) is done, the shadow update by shadow suppliers is carried out in the SDF in the visited network by the SDF in the home network, and the service profile copied in the visited network is deleted.

3.2 Detailed Procedure

(1) Modification of accessingNetworkId attribute

The SDF in the visited network transits to the state “Waiting for Subsequent Request” from the state “Idle” when the SDF receives the request to modify entry from SDF Data Manager. Then the SDF in the visited network requests the bind by sending the dSABind operation to the SDF in the home network, and transits to the state “Waiting for Bind Result”. The SDF in the home network, which received the dSABind operation, transits to the state “Bind Pending” from the state “Idle”. When binding is succeeded, the SDF in the home network sends the dSABindResult in order to show the success of the bind, and transits to the state “SDF Bound”. The SDF in the visited network, which received the dSABindResult, transits to the state “SDF Bound”. If binding is failed for some reasons, the SDF in the home network sends the dSABindError to the SDF in the visited network. Then both SDFs go to the state “Idle”, and they are not bound. The subsequent procedures are not taken place in that case. When the dSABind is succeeded, the SDF in the visited network sends the inChainedModifyEntry operation to the SDF in the home network. When the SDF in the home network receives the inChainedModifyEntry operation, it modifies the part which shows the state of accessing in the accessingNetworkId attribute to the state “Location Registration Failed”. The SDF in the home network, which has completed the modification, sends the inChainedModifyEntryResult to the SDF.Also, when it is impossible to process the operation, such as the case that the data which modification requested is not allowed to be modified by the SDF or the data does not exit, the SDF in the home network sends one of the 6 error messages shown in the clause 4.2.1.2 to the SDF in the visited network. The SDF in the visited network, which received the inChainedModifyEntryResult, sends the dSAUnbind operation to the SDF in the home network. The SDF in the visited network unbinds the SDF in the home network, and transits to the state “Idle”. The SDF in the home network, which received the dSAUnbind operation, unbinds the SDF in the visited network and transits to the state “Idle”.

When a usable and authenticated association exist already, it is not necessary to send the dSABind operation in the procedure described above.

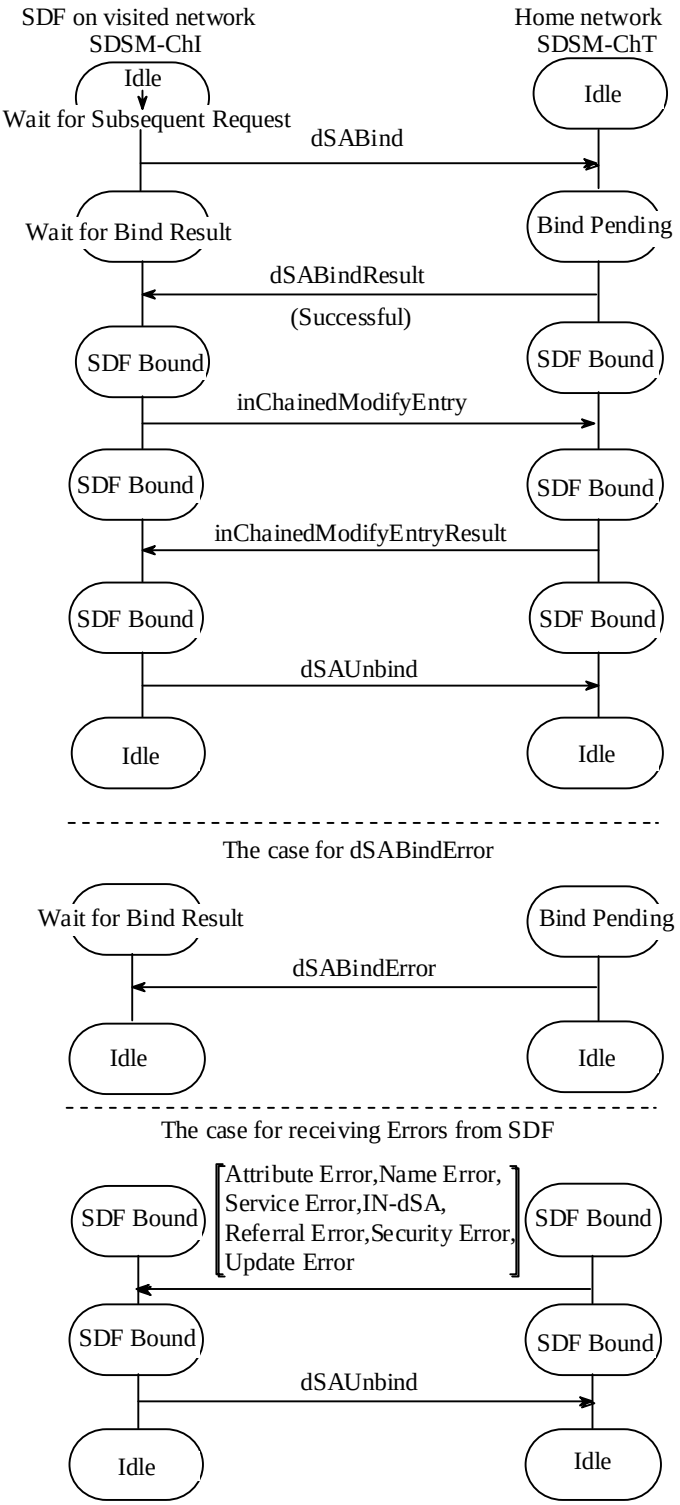
(2) Deletion of PHS roaming service profile copied in the newly visited network

When the modification of the accessingNetworkId is succeeded, SDF Data Manager in the home network initiates the shadow update from the SDF in the home network to the SDF in the visited network. The SDF in the home network transits to the state “Waiting for Subsequent Request” from the state “Idle”. Then the SDF in the home network sends the dSAShadowBind operation to the SDF in the visited network, and transits to the state “Waiting for the Result”. The SDF in the visited network, which received the dSAShadowBind, transits to the state “Waiting for Bind Result” from the state “Idle”. When binding is succeeded, the SDF in the visited network sends the dSAShadowBindResult in order to show the success of binding, and transits to the state “SDF Bound”. The SDF in the home network, which received the dSAShadowBindResult, transits to the state “SDF Bound”. If binding fails for some reasons, the SDF in the visited network sends the dSAShadowBindError to the SDF in the home network. Then both SDFs transit to the state “Idle”, and they are not bound. The subsequent procedures are not taken place in that case. When the dSAShadowBind is succeeded, the SDF in the home network sends the inCoordinateShadowUpdate operation to the SDF in the visited network, and transits to the state “Waiting for Coordination Result”. The CoordinateShadowUpdate is used to indicate the shadow agreement about sending the update which shadow suppliers intend to. The SDF in the visited network, which received the inCoordinateShadowUpdate operation, transits to the state “Waiting for Coordination Result”, then

returns the inCordinateShadowUpdateResult to the SDF in the home network, and transits to the state "Waiting for Update". The SDF in the home network, which received the inCordinateShadowUpdateResult, transits to the state "Waiting for Update", then if it can provide shadow, it sends the inUpdateShadow operation, and transits to the state "Waiting for Update Confirmation". The copy of the PHS roaming service profile in the visited network is deleted by the updatingshadow. The SDF in the visited network, which received the ShadowUpdate operation, transits to the state "Waiting for Update Confirmation," then if the shadowupdate operation is completed normally, it sends the inUpdateShadowResult to the SDF in the home network, and transits to the state "SDF Bound". The SDF in the home network, which received the inUpdateShadowResult, sends the dSAShadowUnbind operation to the SDF in the visited network. Then the SDF in the home network unbinds the SDF in the visited network, and transits to the state "Idle". The SDF in the visited network, which received the dSAShadowUnbind operation, unbinds the SDF in the home network, and moves to the state "Idle". Then the SDF Data Manager in the home network modifies the state of accessing in the accessingNetworkId attribute to the state "Idle".

3.3 Signaling Sequence

The signaling sequence in the procedure for deleting PHS roaming service profile in the newly visited network is shown below. The procedure can be separated into two action sequences so that it is shown one by one.



When a usable and authenticated association exists already, it is not necessary to send the dSABind operation in this procedure.

Figure C-3/B-IF4.50 (1) Modification of accessinngNetworkID

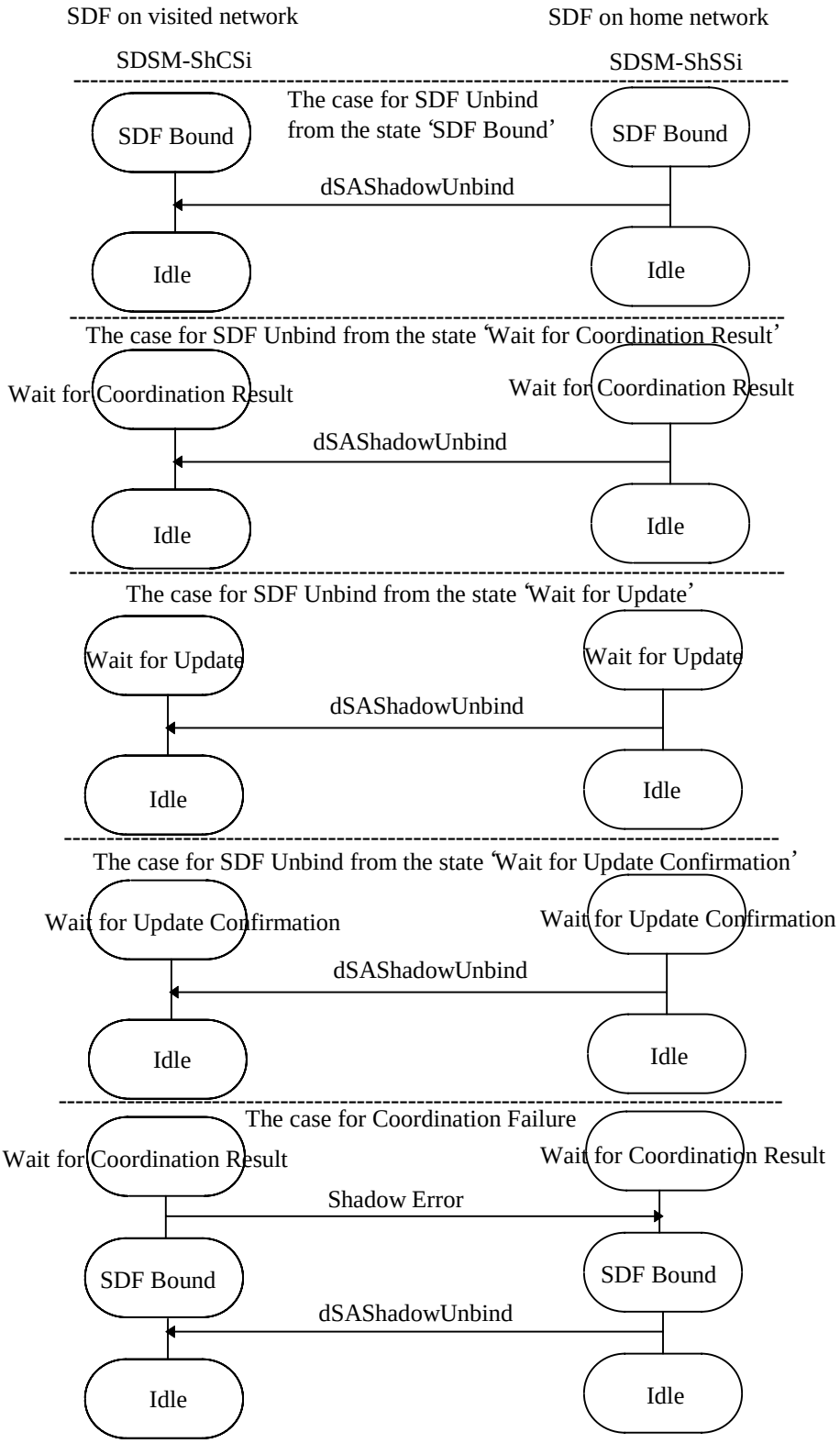


Figure C-4/B-IF4.50 (2) Deletion of PHS roaming service profile in the newly visited network

Appendix I
(Informative)

Authentication for Basic Roaming Capability Set

I.1 Introduction

Authentication for the basic roaming capability set is a security function (service user authentication) provided to verify authenticity of a public PS roaming at a visited network. This is not message authentication function that verifies the transferred messages. This appendix summarizes of the authentication scheme.

I.2 Authentication Scheme

The authentication scheme is specified by the authentication mechanism, the authentication procedure, and the authentication algorithm.

I.2.1 Authentication Mechanism

The following describes possible example of challenge and response type of authentication mechanism is described. In this mechanism a user (public PS) is treated as a challenger of the authentication and a network provider (SDF in the visited network) is acted as a verifier of the authentication. The visited SDF as the verifier stores the multiple pairs of a random number C and a process result R in advance. The result R is the information calculated with the random number C and the secret information concealed in the public PS.

For example, if an encryption function is specified by f( ), the process result R can be described as R = f (C). In this case the secret key for the encryption function f( ) corresponds to the above secret information, and only the home network (SDF) and the legitimate public PS could have it. It is assumed that the secret information for the public PS must not be disclosed in the visited network and must be managed in a secure manner by both the home network and the public PS.
Note: For f( ), it is required f^{-1}( ) may not be easily obtained.

The visited network that has C/R pairs of the random number C and the result R, could authenticate a roaming user (public PS) only by executing the comparing transaction without having the algorithm to generate R. Specifically, the following mechanism is executed. In the storage format for the C/R pairs in the visited SDF, the C/R pair is represented by one attribute, and the attribute value keeps a set of the multiple C/R pairs (in a single value) for each user.

1) The verifier (visited SDF) sends a challenger (public PS) a random number C out of the stored random number and results (C/R) pairs.

2) The challenger calculates the result R' from the received random number C using the calculation function. Then the challenger sends back the verifier the result R'.

3) The verifier compares the result R stored in above step 1 and the result R' received from the

challenger. If both results are the same, the visited network which is a verifier judges that it could verify the authority of the public PS.

4) If both results of R and R' are not the same, the verifier judges that the accessing public PS is illegal.

I.2.2 Authentication Procedure

The authentication function for the basic roaming capability set can be realized as the following steps.

Step1) Procedure of service profile retrieval at first location registration: Because the authentication information (C/R pair set) is a part of the service profile information for a public PHS subscriber, the C/R pair stored in the home network is transferred to the SDF in the visited network.

Step2) Authentication procedure in visited network using the above-mentioned authentication information (C/R pair)

Step 3) Additional retrieval procedure autonomously executed by visited SDF after all the authentication information has been processed

For the above steps 1 and 3, refer to the main part of this Specifications and Annex B. This clause describes the above step 2 as follows.

I.2.2.1 Stored Information for Authentication

The following two types of authentication information are stored for the basic roaming capability set by the visited SDF:

– Authentication information for location registration:
Available to authentication at location registration
– Authentication information for call setup:
Available to authentication at call setup and handover

These types of authentication information consist of the above-mentioned C/R pair sets, but the uses of them are different.

I.2.2.2 Authentication Procedure for Location Registration

The authentication information (C/R pair set) stored in the visited SDF has the following constitution:

C_1/R_1, C_2/R_2, C_3/R_3, C_4/R_4, ...

The C_1/R_1 pair is available at the first location registration. Then the C_2/R_2 pair is available at the second location registration. In this case it is desirable that there is no correlation between C_1/R_1 and C_2/R_2. Therefore, the pairs could be selected independently of the order stored in visited SDF.

For the authentication procedure, SCF (service logic for roaming) generates a search operation inquiring the attribute (attribute: authentication information for location registration) to the SDF in the visited network. Then the SDF manager (see Annex B) in the visited network retrieves all of the

C/R pairs, that is the search result of authentication information for location registration. The SDF manager selects one C/R pair among them and returns it to the SCF to authenticate the user at the actual location registration. For example the visited SDF manager executes an operation replacing the unused C/R pair sets with ones already stored in the visited SDF. It stores only unused sets. These SDF operations are the local process within the visited SDF, and the Specific possible method is dependent on the implementation.

I.2.2.3 Authentication Procedure for Call Setup

The C/R pair sets of authentication information stored in the visited SDF are constituted as follows:

C_1/R_{1-1}, R_{1-1}/R_{1-2}, R_{1-2}/R_{1-3}, R_{1-3}/R_{1-4}, ... (for first call setup)
C_2/R_{2-1}, R_{2-1}/R_{2-2}, R_{2-2}/R_{2-3}, R_{2-3}/R_{2-4}, ... (for second call setup)
C_3/R_{3-1}, R_{3-1}/R_{3-2}, R_{3-2}/R_{3-3}, R_{3-3}/R_{3-4}, ... (for third call setup)
...
C_n/R_{n-1}, R_{n-1}/R_{n-2}, R_{n-2}/R_{n-3}, R_{n-3}/R_{n-4}, ... (for n-th call setup)
...

Namely the C_1/R_{1-1} pair is used for the first call setup, and the C_2/R_{2-1} pair is for the second call setup. Therefore the n-th C_n/ R_{n-1} pair is consumed for the n-th call setup.

In the authentication procedure the SCF (service logic for roaming) issues a search operation inquiring the attributes (attribute: authentication information for call setup) to the visited SDF. Then the SDF manager (see Annex B) in the visited network receives all of the search results of the authentication information for call setup. The SDF manager selects the authentication information which has the lowest number of C_x/R_{x-1}, R_{x-2}/R_{x-3} ... among the authentication information for call setup. In the case of above example (for first call setup) it will select the set of C_1/R_{1-1}, R_{1-2}, R_{1-3} ... Then it returns this set to the SCF to authenticate the user for the actual call setup or handover. Then the SDF manager in the visited network executes an operation to exchange the unused authentication information sets for call setup except previously used ones with ones already stored in visited SDF. In the above examples C_2, R_{2-1}, R_{2-2} …, C_3, R_{3-1}, R_{3-2} … are unused sets. C_1/R_{1-1}, R_{1-2}, R_{1-3} … are previously used ones to authenticate at that time. These SDF operations are local within the SDF in the visited network and the realization depends on the implementation. Any handover does not cause the SCF to make new access to the SDF and the SCF authenticates the user with the sets of authentication information obtained at the call setup.

The following example gives the returned information to the SCF and the stored information in the visited SDF after the authentication process:

First call setup
– Returned information to SCF:
C_1, R_{1-1}, R_{1-2}, R_{1-3}, R_{1-4}, …
– Stored information in visited SDF after this process:
C_2, R_{2-1}, R_{2-2}, R_{2-3}, R_{2-4}, …
C_3, R_{3-1}, R_{3-2}, R_{3-3}, R_{3-4}, …
…

Second call setup

– Returned information to SCF:

C_2, $R_{2\text{-}1}$, $R_{2\text{-}2}$, $R_{2\text{-}3}$, $R_{2\text{-}4}$, …

– Stored information in visited SDF after this process:

C_3, $R_{3\text{-}1}$, $R_{3\text{-}2}$, $R_{3\text{-}3}$, $R_{3\text{-}4}$, …

C_4, $R_{4\text{-}1}$, $R_{4\text{-}2}$, $R_{4\text{-}3}$, $R_{4\text{-}4}$, …

…

Handover during second call setup

– Returned information to SCF:

no return because of no access from SCF

– Stored information in visited SDF after this process:

C_3, $R_{3\text{-}1}$, $R_{3\text{-}2}$, $R_{3\text{-}3}$, $R_{3\text{-}4}$, …

C_4, $R_{4\text{-}1}$, $R_{4\text{-}2}$, $R_{4\text{-}3}$, $R_{4\text{-}4}$, …

…

I.2.3 Authentication Algorithm

The authentication algorithm means the classification of algorithm of f ( ) in previously mentioned authentication mechanism. This authentication algorithm is classified into an encryption function of symmetric encryption (secret key type) as above, but this standard does not particularly prescribe the algorithm classification.

I.2.4 Timing of Additional Retrieval of Authentication Information

The visited SDF stores the authentication information previously mentioned (sets of C and R of authentication information for location registration or for call setup). When no sets of authentication information is remaining on the SDF in the visited network, the visited SDF autonomously performs the additional retrieval procedure of the authentication information from the home SDF. The lack of the authentication information activates this procedure. If a few sets remain in the visited SDF and it initiates this additional retrieval procedure, it cannot reuse the remains for it overwrites them with new authentication information copied from the home network.

I.2.5 Generation of Authentication Information in Home Network

The SDF in the home network maintains two kinds of authentication information (authentication information for location registration and for call setup). Receiving the request of above additional retrieval procedure, it may copy authentication information stored in the home SDF to the visited SDF in theory. In practice the home SDF may generate the authentication information after it receives the request from the visited network. The timing of the generation of the authentication information in the home network is a local matter.

Appendix II
(Informative)

Handling of PHS Roaming Number in Visited Network

II.1 Introduction

This appendix describes the handling of PHS roaming number in the visited network prescribed in the basic roaming capability set of this Specifications. Figure II-1/B-IF4.50 depicts a Directory Information Tree (DIT) structure rule and this gives examples of procedures concerned with creation and removal of alias entry in the DIT structure rule. The handling of PHS roaming number described in this appendix applies in the case that PHS roaming number identifies public PS in the visited network.

II.2 Alias Object Class and DIT Structure Rule

II.2.1 PHS Roaming Subscriber

This clause describes the **phsRoamingSubscriber** object class.

II.2.1.1 Definition of Alias Object Class

An alias entry of the **phsRoamingSubscriber** alias object class contains the information used to provide an alternative name for an entry of the **phsISPTSubscriberProfile** object class. The distinguished name (DN) of this alias entry is defined as the name of the **phsISPTSubscriberProfile** object entry. It provides a DN of a shadow copy of PHS roaming service profile for the public PS as the **aliasedEntryName** attribute value of the alias entry. It may be represented as the following definition of alias object class.

```
phsRoamingSubscriber OBJECT-CLASS        ::=        {
        SUBCLASS OF                      { alias }
            MUST CONTAIN { aliasedEntryName }
            ID                           { local-phsRoamingSubscriber }}
```

This is to be granted an object identifier.

II.2.1.2 Definition of PHS Roaming Subscriber Name Form

The **phsRoamingSubscriberNameForm** name form specifies the attribute that is used as a Relative Distinguished Name (RDN) for the entry of the **phsRoamingSubscriber** object class.
The definition of PHS roaming subscriber name form allows that the **phsNumber** attribute is a RDN of the **phsRoamingSubscriber** object class.

```
phsRoamingSubscriberNameForm NAME-FORM      ::=        {
    NAMES                        phsRoamingSubscriber
    WITH ATTRIBUTES              { phsNumber }
```

ID { local-phsRoamingSubscriberNameForm }}

This should be granted an object identifier.

II.2.2 DIT Structure Rule

The following definition of the DIT structure rule specifies the DIT shown in Figure II-1/B-IF4.50. The basic roaming capability set of this Specification describes the object classes of **country**, **phsISPTServiceProvider**, **phsISPTSubscriberProfile** and the DIT structure rules of sr1, sr2, and sr3.

```
sr4   STRUCTURE-RULE      ::=   {
      NAME-FORM           phsRoamingNumberPoolNameForm
      SUPERIOR RULES      { sr2 }
      ID                  4 }

sr5   STRUCTURE-RULE      ::=   {
      NAME-FORM           phsRoamingSubscriberNameForm
      SUPERIOR RULES      { sr2 }
      ID                  5 }
```

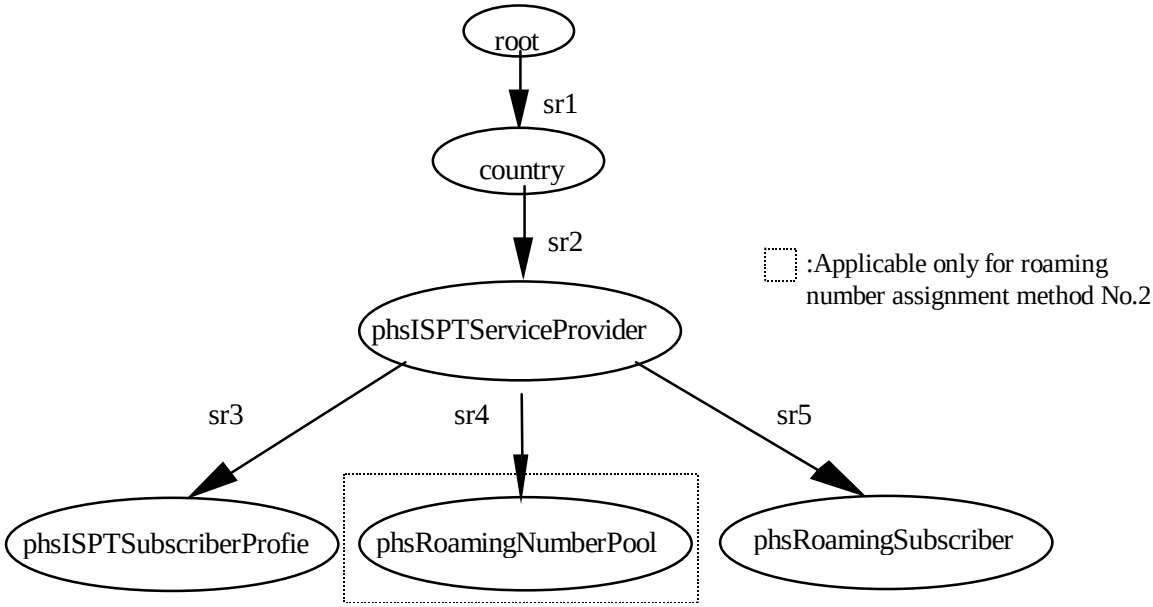


Figure II-1/B-IF4.50 Example of DIT Structure Rule

II.3 Example of Alias Entry in Visited Network

A DIT in the visited network is illustrated in Figure II-2/B-IF4.50. In this figure the service provider of home network for public PS (PHS number = PSN1, PSN2, or PSN3) is the service provider 1 (phsISPTServiceProvider = Provider1) and the service provider of visited network is the service provider 2 (phsISPTServiceProvider = Provider2). When the **phsISPTSubscriberProfile** is shadowed, an alias entry is created . The entries for PHS numbers of PSN1, PSN2, and PSN3 are

shadow copies of PHS roaming service profile stored in the home network. When each shadow copy is provided in visited SDF, the alias entry for PSN1, PSN2, or PSN3 is created.The following example outlines the alias entry PSN1. The name of the alias entry PSN1 is { country = JP, phsISPTServiceProvider = Provider2, phsRoamingSubscriber = PSN1 } and the attribute value of **aliasedEntryName** is { country = JP, phsISPTServiceProvider = Provider1, phsISPTSubscriberProfile = PSN1 }. The distinguished name of the alias entry PSN1 is { country = JP, phsISPTServiceProvider = Provider1, phsISPTSubscriberProfile = PSN1 } and the alias entry PSN1 points the shadow copy PSN1.

II.4 PHS Roaming Number and Procedure in Visited Network

The visited network identifies a public PS based on the PHS number in method No.1 or the PHS roaming number in the method No.2 for an incoming call. The following clauses describe the process for PHS roaming number in the procedures. The PHS service profile of roaming public PS is identified by the **phsRoamingNumber** attribute.

II.4.1 At First Location Registration

The procedure of service profile retrieval at first location registration retrieves PHS roaming service profile from home SDF and it provides shadow copy of PHS roaming service profile into the visited SDF.

II.4.2 At Incoming Call

In the method No.1, for incoming call to a public PS terminating call the visited network receives a PHS roaming number in the called party number parameter and PHS number of the public PS in IAM. Since this PHS roaming number cannot identify the public PS, the visited network uses the PHS number as a search key and retrieves a PHS roaming service profile corresponding to the public PS from the visited SDF.

In the method No.2, for incoming call to a public PS terminating call the visited network receives a PHS roaming number in the called party number parameter in IAM. This PHS roaming number was assigned temporally and sent to the PS's home network by the visited network using PHS roaming number assignment procedure described in subclause 4.4.1 before the call to the PS is routed to the visited network. When the call to the PS is routed to the PS's home network, the home network performs the PHS roaming number assignment procedure if the routing type attribute value in the PS's service profile indicates the method No.2.

The following argument of chained execute operation in the PHS roaming number assignment procedure is used. It is assumed that the home network of the PS is Provider 2, the visited network of the PS is provider 1 and the PHS number of the PS is PSN1.

```
{object        {country=JP, phsISPTServiceProvider=Provider1}
 method-id     {phsRoamingNumberAssignment}
 specific-input {PSN1}
}
```

Receiving the PHS roaming number from the visited network, the home network continues to route

the call with PHS roaming number according to the routing type attribute value. After the call routes to the visited network, the visited network uses the PHS roaming number as a search key and retrieves a PHS roaming service profile corresponding to the public PS from the visited SDF.
The method No.1 and No.2 are specified in PHS MoU Document B-NW0.00.

II.4.3 At Cancellation

The procedure of visited network information cancellation clears the copy of PHS roaming service profile corresponding to the public PS from the previously visited SDF. The operation of Directory Information Shadowing Protocol (DISP) removes only the copy of PHS roaming service profile corresponding to the public PS, but it does not remove its alias entry. So it must remove the alias entry using local process.

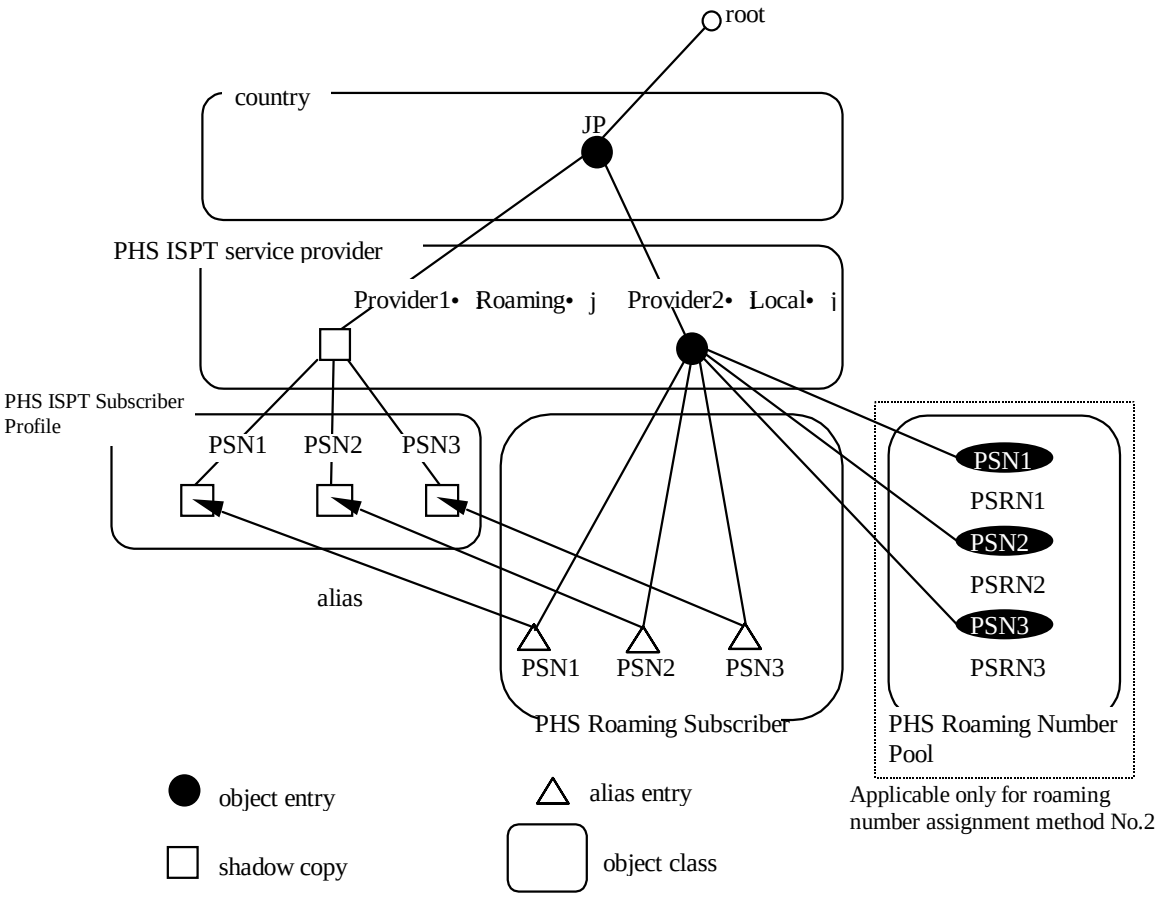


Figure II-2/B-IF4.50 Example of DIT in Visited Network

Appendix III
(Informative)

Example of Basic Access Control for Basic Roaming Capability Set

III.1 Introduction

The **ACIItem** specifies the access control about the information (attribute) in the entry of the **phsISPTSubscriberProfile** object class.

This appendix gives a configuration example of the access control for the DSP operations fulfilled in the procedures of service profile retrieval at first location registration and of inter-network location registration in the DIT shown in Figure III-1/B-IF4.50.

According to the following content rule, PHS ISPT service provider stores the access control information as the **entryACI** attribute value (**ACIItem**) in the entry specified by the **phsISPTSubscriberProfile** object class.

```
cr1 CONTENT-RULE ::= {
        STRUCTURAL OBJECT CLASS          phsISPTSubscriberProfile
         MAY CONTAIN                     { entryACI }}
```

Refer to ITU-T Recommendation X.501 ANNEX D for the entryACI attribute.

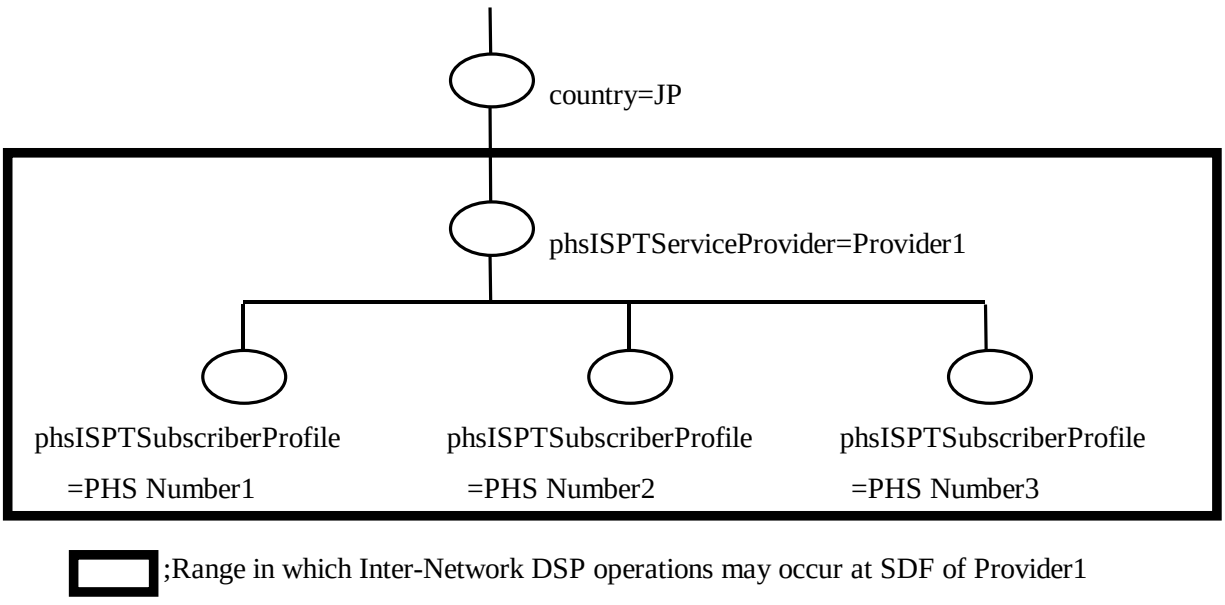


Figure III-1/B-IF4.50 Example of Directory Information Tree

III.2 Basic Access Control Information for Access from any FE (user)

The following condition is given to define the basic access control for any FE (user). Specifically, it is the definition of access control for the **ChainedModifyEntry** request sent from SDF in any network.

(1) Any user can update the **accessingNetworkId**, the **phsRoamingNumber**, and the **routingType** attribute values in the entry for users of Provider1.

Attributes listed in 1 above are updated in the procedures of service profile retrieval at first location registration and of inter-network location registration.

An example of the **entryACI** attribute value that meets the above condition 1 is given as follows:

identificationTag	"Public Access-Enable attribute access for Modify Operation"	
Precedence	10	
UserClasses	{ allUsers }	
authenticationLevel	none	
ProtectedItems	{ attributeType {	accessingNetworkId,
	phsRoamingNumber,	routingType },
	allAttributeValues {	accessingNetworkId,
		phsRoamingNumber,
		routingType }}
GrantsAndDenials	{ grantAdd, grantRemove }	

"Public Access-Enable attribute access for Modify Operation" specifies the attributes that can be removed or added in the procedures of service profile retrieval at first location registration and of inter-network location registration.

Appendix IV
(Informaive)

Agreement

IV.1 Introduction

As for ISPT model described in Specifications B-IF4.28, the agreement of DOP is implicitly established and the shadow operation is executed according to the contents. This appendix describes the details of agreement for shadow operations that are executed in the procedures of service profile retrieval at first location registration, of additional retrieval, and of visited network information cancellation.

IV.2 Agreement among all Roaming Users

In the procedures of service profile retrieval at first location registration and of visited network information cancellation, all PHS subscribers who have the roaming possibility shall establish an agreement. Figure IV-1/B-IF4.50 illustrates the agreement areas in the case that a terminal of Provider1 roams to Provider2.

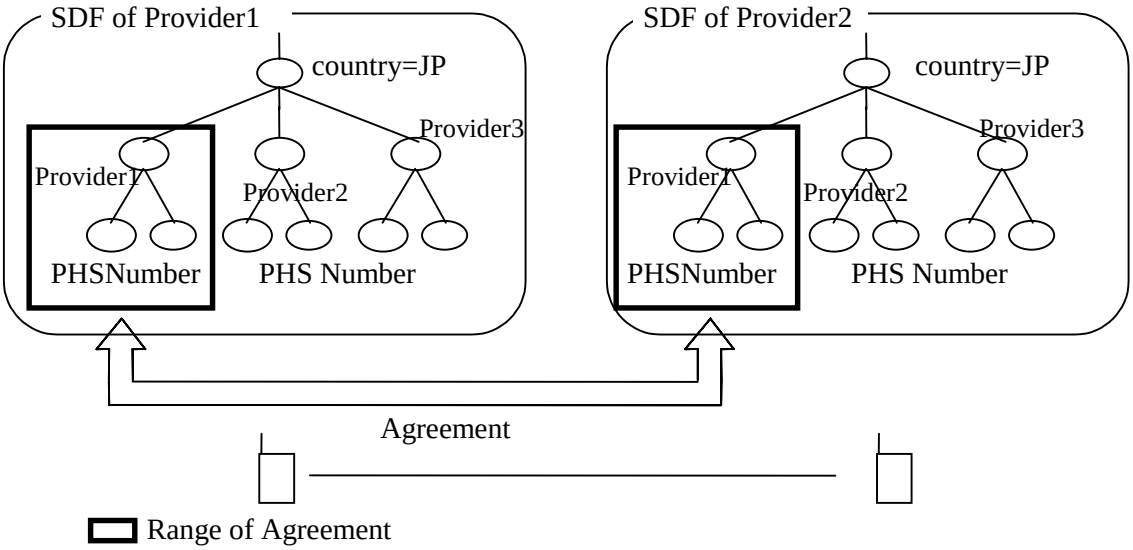


Figure IV-1/B-IF4.30 Agreement among all Roaming Users

IV.2.1 Agreement Information Used in Procedure of Service Profile Retrieval at First Location Registration

The operation and the agreement for the shadow used in the procedure of service profile retrieval at first location registration are described as follows:

When the accessing status of the **accessingNetworkId** attribute is updated to “during location

registration” and service provider identification is updated to the number of newly visited network, a shadow update operation is executed for the DIT existing in the network that is pointed by the updated service provider identification. As a result PHS service profile is copied to the newly visited network.

VI.2.2 Agreement Contents Used in Procedure of Visited Network Information Cancellation

The operation and agreement for the shadow used in the procedure of visited network information cancellation are described as follows:

When the **phsRoamingNumber** attribute is updated, a shadow update operation is executed for the DIT existing in the network where the attribute value has indicated before update. As a result the PHS service profile of the previously visited network is removed.

IV.2.3 Agreement Information Used in Procedure of PHS Roaming Service Profile Deletion

The operation and agreement for the shadow used in the procedure of PHS roaming service profile deletion are described as follows:

When the accessing status of the **accessingNetworkId** attribute is updated to the “location registration failure," shadow update is executed for the DIT existing in the network represented by the part that points a PHS ISPT service provider. As a result the PHS roaming service profile in the newly visited network is removed.

IV.3 Agreement for each PHS Number

An additional retrieval procedure uses an agreement established implicitly for each PHS number. There exist two types of agreement established for each PHS number. One type is to apply shadow update operations to the **locationRegistrationAuthenticationInformation**attribute for one PHSnumber and another type is to apply shadow update operations to the **callSetupAuthenticationInformation** attribute.

Appendix V
(Informative)

Example of realization for Inter-network operation

V.1 Introduction

INAP operations to realize basic roaming capability set are described in the B-IF-4.50-02-TS. Multiple operations described there can be sent by one TC message and there are also operations that can be omitted by sending them implicitly. This appendix provides a recommended example. Operations other than given by sequences represented in this appendix are not guaranteed.

V.2 Fundamental Method

Sequences shall be made in the following method.

(1) An Operation sent toward the same direction after one should be inserted into a single TC message.

(2) The binding and unbinding directory should be executed implicitly.

V.3 Sequences

The sequences described by obeying the above-mentioned fundamental method are given.

V.3.1 First Location Registration Sequence

The sequence at first location registration is shown in Figure V-1/B-IF4.50. This sequence contains the procedures of service profile retrieval at first location registration, of the inter-network location registration, and of the visited network information cancellation.

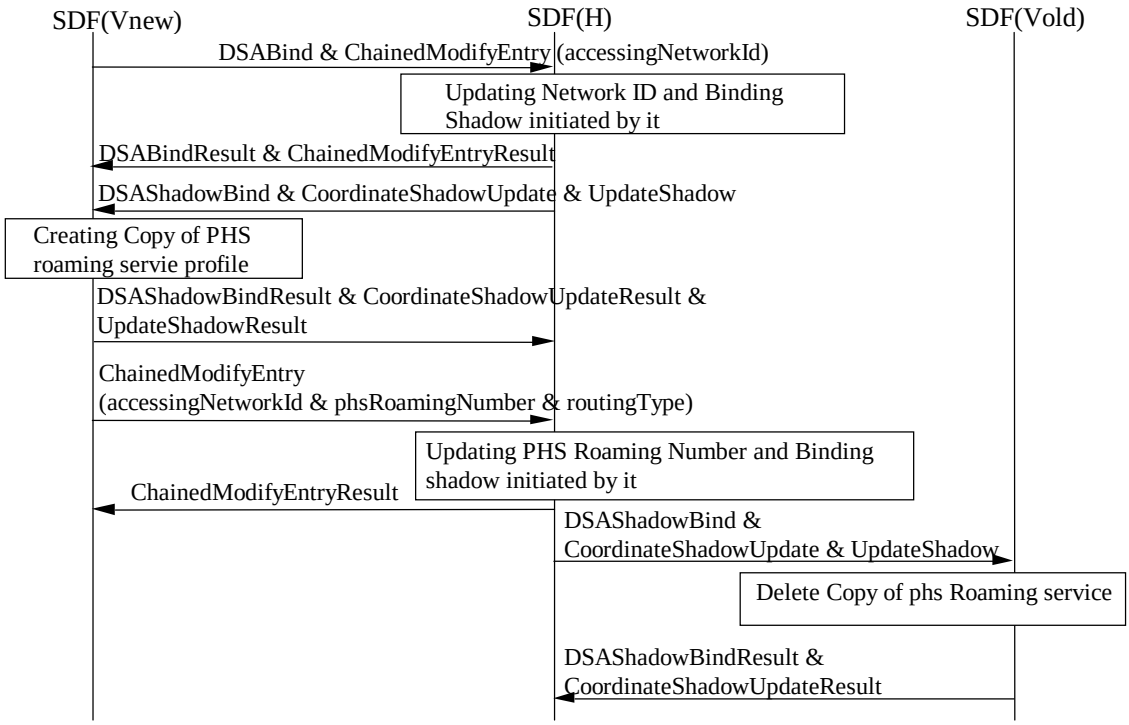


Figure V-1/B-IF4.50 Sequence at First Location Registration

V.3.2 Additional Retrieval Sequence

The sequence of the additional retrieval procedure is shown in Figure V-2/B-IF4.50.

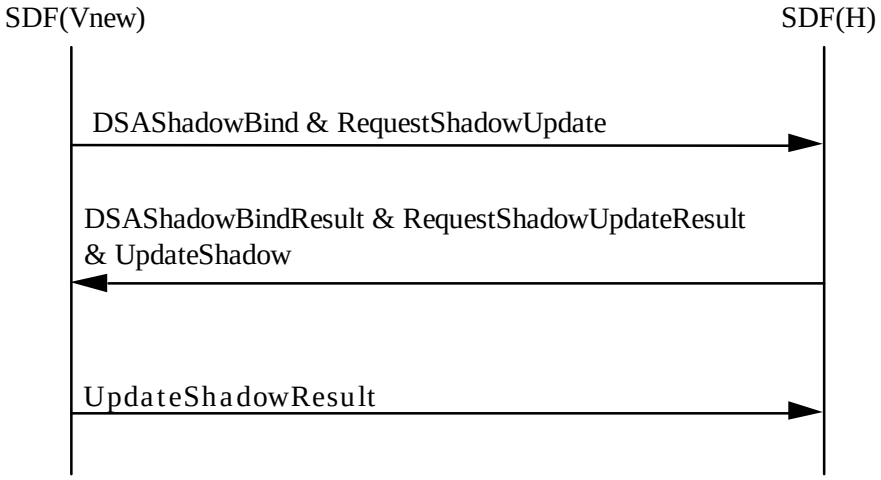


Figure V-2/B-IF4.50 Sequence of Additional Retrieval Procedure