3GPP TSG SA WG3 Security — S3#13 **S3-000347**

23-26 May, 2000

Yokohama, Japan

Source: **TSG-S WG3**

Title: **Liaison statement to CN4 on Protection Mode 0 for MAP Security**

Document for: **Information**

At the last TSG-N WG4 meeting in Charleston (27th-31st March), it was agreed to follow the principles in Tdoc N2B-000394 for the incorporation of MAP Security Layer III at TSG-N WG4 specifications (mainly 29.002).

These principles define “noProtection” as a valid value for “Protection Mode” parameter specified at the “Security Header” field of the protected MAP message.

```
SecurityHeader ::= SEQUENCE {
     sendingEntityAddress                ISDN-AddressString,
     protectionMode                      ProtectionMode,
     originalComponentIdentifier         OriginalComponentIdentifier,
     ...}
```

```
ProtectionMode ::= ENUMERATED {
     noProtection                        (0),
     integrityAuthenticity               (1),
     confidentialityIntegrityAuthenticity (2)}
```

TSG-S WG3 would like to inform TSG-N WG4 that there is no security reason why ‘noProtection’ (ProtectionMode 0) shall be defined as a valid Protection Mode value for the Layer III protected MAP messages.

Furthermore, the use of ProtectionMode 0 does not introduce additional security to the MAP message while introducing additional overheads.

Following this reasoning, TSG-S WG3 recommends TSG-N WG4 to discard ‘noProtection’ (ProtectionMode 0) as a valid Protection Mode value for the Layer III protected MAP messages.

Only ProtectionMode 1 and ProtectionMode 2 shall be then defined as valid values. The original unprotected MAP message shall be considered as offering ProtectionMode 0 for MAP Security Layer III messages.

On the other hand, it shall be also defined a policy mechanism to determine whether the receiving entity allows the reception of specific unprotected MAP messages.

3GPP TSG-N WG2 SWGB #5 **Tdoc N2B000394**
Stockholm, 2-3 March 2000

Source:	**Siemens**
Subject:	**Network Domain Security Mechanism**
Title:	**MAP Security Proposal**
For:	**Discussion**

This contribution is based on the proposal from Nortel Networks Tdoc N2B000378 discussed in Milan. It outlines some general principles and proposes details on ASN.1 and the MAP Dialogue State Machine. The intention is to provide ideas for a complete and future proof solution although for R99 it is not required to make use of all parts of this proposal.

Principles:

- The TCAP operation class of the protected operation shall be the same as the TCAP operation class of the unprotected operation. This means that instead of introducing one new operation "SecurityTransport", it is proposed to introduce four new operations: SecurityTransportClass1, Security TransportClass2, SecurityTransportClass3 and SecurityTransportClass4. All four operations shall run under the same new AC "SecureTransportHandlingContext". Note that for R99 only SecurityTransportClass1 is required.
- Information transported in the Dialogue Portion of the unprotected message shall not be moved to the Component Portion when protecting the message. This means that the original AC shall be kept in the Dialogue Portion. Since the Dialogue Portion of the protected message contains the new AC secureTransportHandlingContext, the original AC shall be coded within the User Info of the Dialogue Portion.
- The concept shall allow to protect error parameters in ReturnError Components and UserInfo in the Dialogue Portion. Note that for R99 protection of User Info is not required.
- For AC version negotiation primarily the new AC (secureTransportHandlingContext) and secondarily the original AC (both within the Dialogue Portion) shall be taken into account. If the receiving entity supports the secureTransportHandlingContext but does not support the original AC, it shall mirror back the secureTransportHandlingContext in an Abort message and add information in the User Info of the Abort to indicate that the original AC is not supported, and, if appropriate, to indicate which alternative for the original AC is supported.
- For overload control the original AC shall be taken into account.

ASN.1:
new AC secureTransportHandlingContext:

```
secureTransportHandlingContext-v3  OBJECT IDENTIFIER ::=
     {map-ac secureTransportHandlingContext(x) version3(3)}
```

new operation Package:

```
SecureTransportHandlingPackage-v3 ::= OPERATION-PACKAGE
     CONSUMER INVOKES {
          SecureTransportClass1
          SecureTransportClass2
          SecureTransportClass3
          SecureTransportClass4}
```

new operations:

```
SecureTransportClass1 ::= OPERATION           --Timer shall be the same as for the
                                              --original operation
    ARGUMENT
         securityEnvelopeArg             SecurityEnvelopeArg
    RESULT
         securityEnvelopeRes             SecurityEnvelopeRes
    ERRORS {
         SecureTransportError}
```

```
SecureTransportClass2 ::= OPERATION           --Timer shall be the same as for the
                                              --original operation
    ARGUMENT
         securityEnvelopeArg             SecurityEnvelopeArg
    ERRORS {
         SecureTransportError}
```

```
SecureTransportClass3 ::= OPERATION           --Timer shall be the same as for the
                                              --original operation
    ARGUMENT
         securityEnvelopeArg             SecurityEnvelopeArg
    RESULT
         securityEnvelopeRes             SecurityEnvelopeRes
```

```
SecureTransportClass4 ::= OPERATION           --Timer shall be the same as for the
                                              --original operation
    ARGUMENT
         securityEnvelopeArg             SecurityEnvelopeArg
```

new data types:

```
SecurityEnvelopeArg ::= SEQUENCE {
    securityHeader                  SecurityHeader,
    protectedPayload                ProtectedPayload                OPTIONAL
    }
    -- The protectedPayload carries the result of applying the
    -- encryption function specified in TS 33.102 to the encoding of the
    -- original operation's argument.
```

```
SecurityEnvelopeRes ::= SEQUENCE {
    securityHeader                  SecurityHeader,
    protectedPayload                ProtectedPayload                OPTIONAL
    }
    -- The protectedPayload carries the result of applying the
    -- encryption function specified in TS 33.102 to the encoding of the
    -- original operation's result.
```

```
SecurityHeader ::= SEQUENCE {
    sendingEntityAddress            ISDN-AddressString,
    protectionMode                  ProtectionMode,
    originalComponentIdentifier     OriginalComponentIdentifier,
    ...}
```

```
ProtectedPayload ::= OCTET STRING (SIZE (1..1000))
    -- Length of protectedPayload is adjusted according to the
    -- capabilities of lower protocol layers
```

```
ProtectionMode ::= ENUMERATED {
    noProtection                    (0),
    integrityAuthenticity           (1),
    confidentialityIntegrityAuthenticity (2)}
```

```
OriginalComponentIdentifier ::= CHOICE {
    operationCode                   [0] OperationCode,
    errorCode                       [1] ErrorCode,
    userInfo                        [2] NULL}
```

```
OperationCode ::= CHOICE {
     localValue                          INTEGER,
     globalValue                         OBJECT IDENTIFIER}
```

```
ErrorCode ::= CHOICE {
     localValue                          INTEGER,
     globalValue                         OBJECT IDENTIFIER}
```

new Error:

```
SecureTransportError ::= ERROR
     PARAMETER
          secureTransportErrorParam       SecureTransportErrorParam
```

new error data type:

```
SecureTransportErrorParam ::= SEQUENCE {
     securityHeader                      SecurityHeader,
     protectedPayload                    ProtectedPayload                  OPTIONAL
     }
     -- The protectedPayload carries the result of applying the
     -- encryption function specified in TS 33.102 to the encoding of the
     -- original error parameter.
```

new Dialogue Information to protect TCAP User Info:

```
map-ProtectedDialogueAS OBJECT IDENTIFIER ::=
     {gsm-NetworkID as-Id map-ProtectedDialoguePDU (2) version1 (1)}
```

```
MAP-ProtectedDialoguePDU ::= SEQUENCE {
     securityHeader                      SecurityHeader,
     protectedPayload                    ProtectedPayload
     }
     -- The protectedPayload carries the result of applying the
     -- encryption function specified in TS 33.102 to the encoding of the
     -- original MAP-DialoguePDU.
```

new Dialogue Information to transport the original AC:

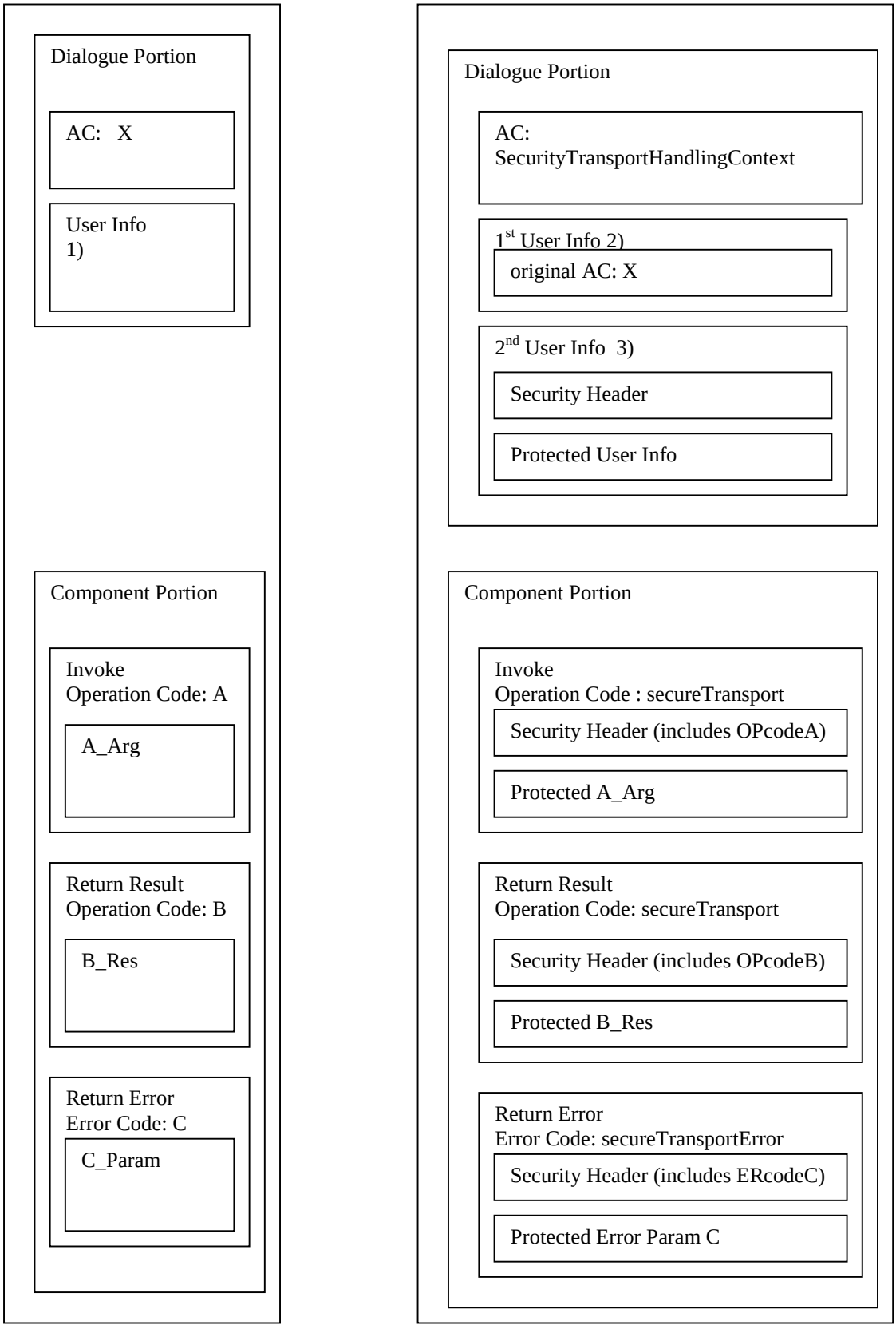
```
map-OriginalAC-AS OBJECT IDENTIFIER ::=
     {gsm-NetworkID as-Id map-OriginalAC-PDU (3) version1 (1)}
```

```
MAP-OriginalAC-PDU ::= OBJECT IDENTIFIER
```

original message (unprotected)

protected message

BEGIN/CONTINUE/END

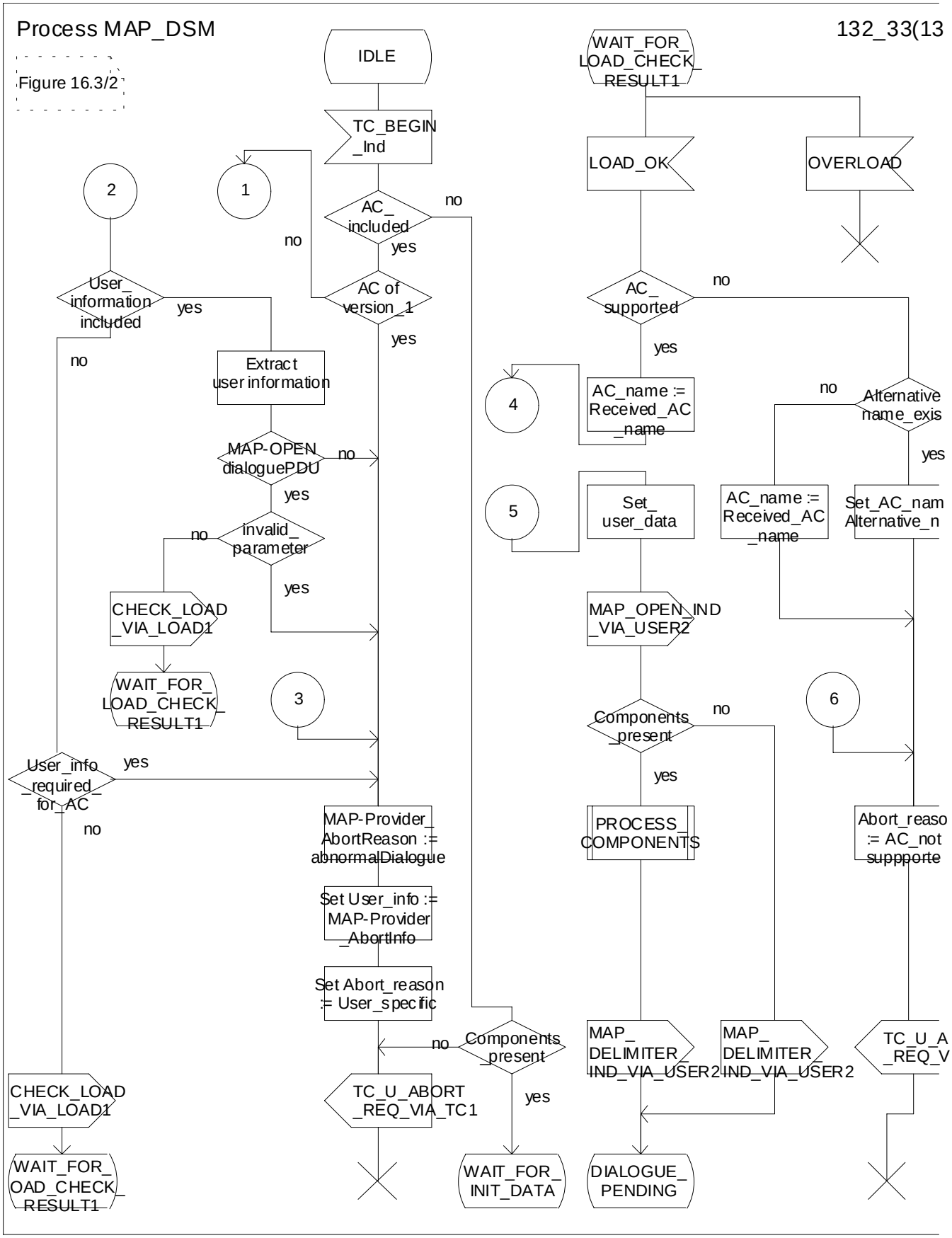


1) identified by map-DialogueAS
2) identified by map-OriginalAC-AS
3) identified by map-ProtectedDialogueAS

MAP Dialogue State Machine:

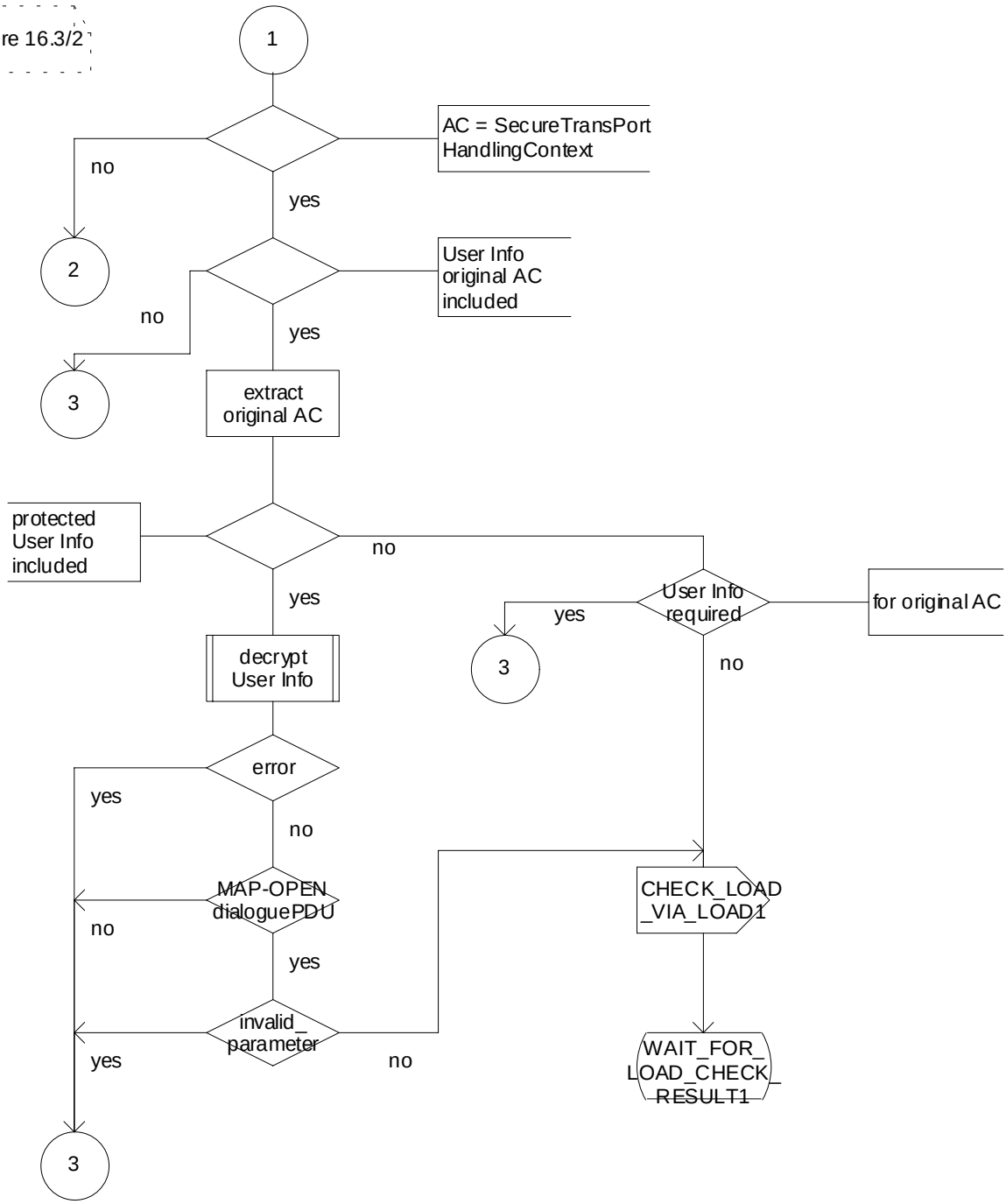
The following modifications in the SDLs of the MAP_Provider (29.002 section 16) are far from complete. If the general concept is acceptable by N2B, delegates are invited to contribute to the completion of this work.

Figure 16.3/2


IDLE
TC_BEGIN _Ind
AC_ included
no
yes
AC of version_1
yes
no
1
2
User_ information included
yes
no
Extract user information
MAP-OPEN dialoguePDU
no
yes
invalid_ parameter
no
yes
CHECK_LOAD _VIA_LOAD1
WAIT_FOR_ LOAD_CHECK_ RESULT1
3
User_info _required_ for_AC
yes
no
CHECK_LOAD _VIA_LOAD1
WAIT_FOR_ OAD_CHECK_ RESULT1
MAP-Provider_ AbortReason := abnormalDialogue
Set User_info := MAP-Provider _AbortInfo
Set Abort_reason := User_specific
TC_U_ABORT _REQ_VIA_TC1
no
Components _present
yes
WAIT_FOR_ INIT_DATA
WAIT_FOR_ LOAD_CHECK_ RESULT1
LOAD_OK
OVERLOAD
AC_ supported
no
yes
4
AC_name := Received_AC _name
5
Set_ user_data
MAP_OPEN_IND _VIA_USER2
Components _present
no
yes
PROCESS_ COMPONENTS
MAP_ DELIMITER_ IND_VIA_USER2
DIALOGUE_ PENDING
no
Alternative name_exis
yes
AC_name := Received_AC _name
Set_AC_nam Alternative_n
6
Abort_reaso := AC_not suppporte
MAP_ DELIMITER_ IND_VIA_USER2
TC_U_A _REQ_V

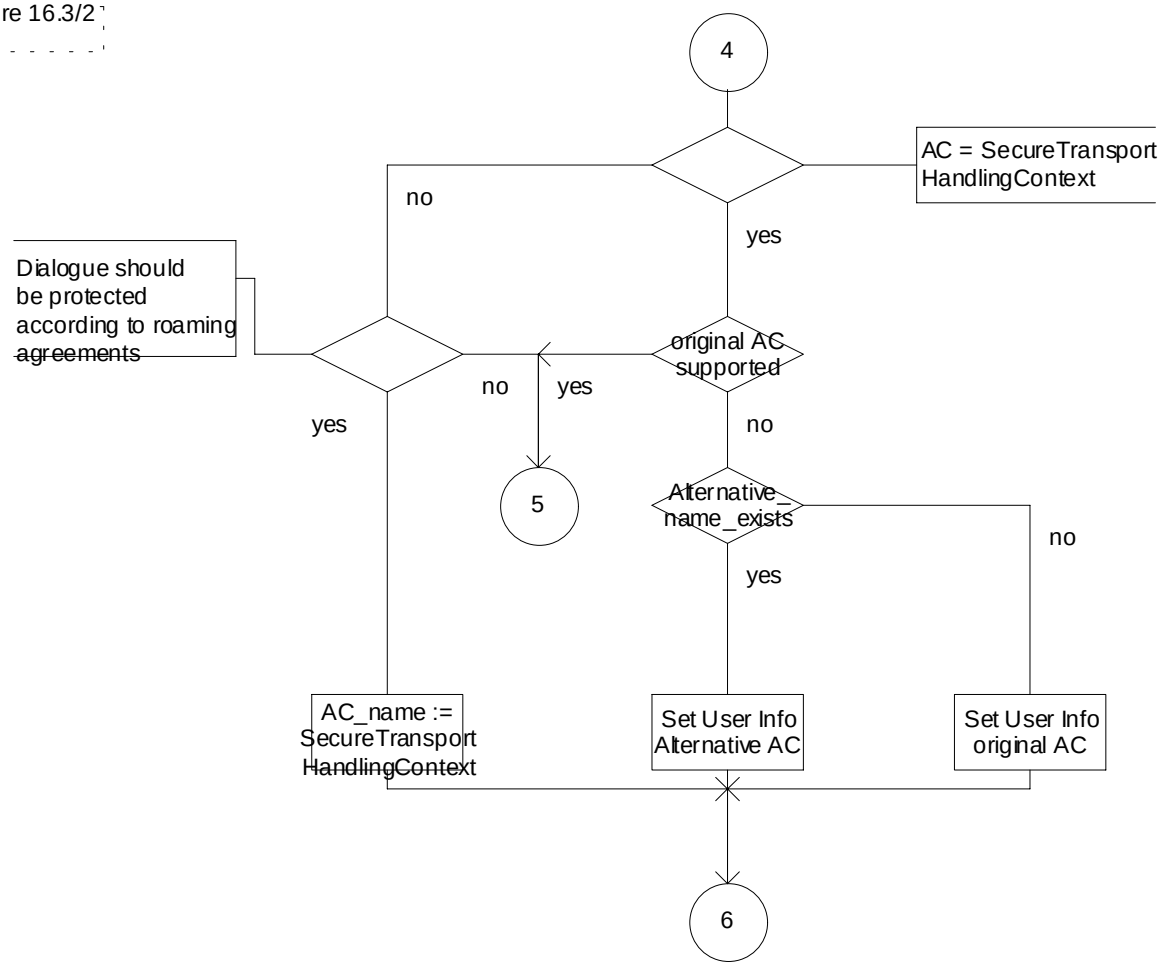
Process MAP_DSM

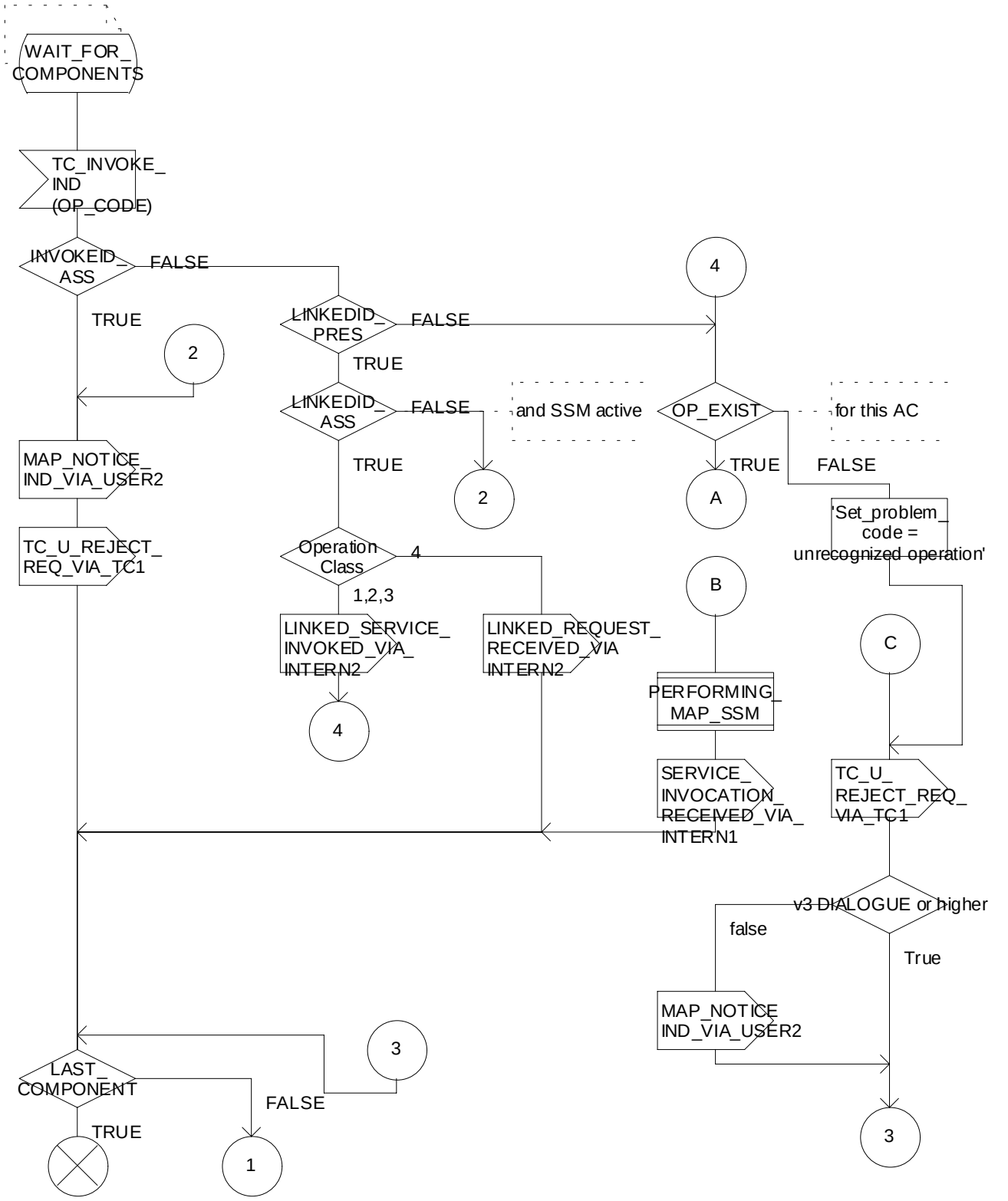
Figure 16.3/2



Process MAP_DSM

Figure 16.3/2




WAIT_FOR_
COMPONENTS
TC_INVOKE_
IND
(OP_CODE)
INVOKEID_
ASS
FALSE
TRUE
2
LINKEDID_
PRES
FALSE
TRUE
LINKEDID_
ASS
FALSE
TRUE
2
4
OP_EXIST
and SSM active
for this AC
TRUE
FALSE
A
'Set_problem_
code =
unrecognized operation'
MAP_NOTICE_
IND_VIA_USER2
TC_U_REJECT_
REQ_VIA_TC1
Operation
Class
4
1,2,3
LINKED_SERVICE_
INVOKED_VIA_
INTERN2
LINKED_REQUEST_
RECEIVED_VIA
INTERN2
4
B
PERFORMING_
MAP_SSM
SERVICE_
INVOCATION_
RECEIVED_VIA_
INTERN1
C
TC_U_
REJECT_REQ_
VIA_TC1
v3 DIALOGUE or higher
false
True
MAP_NOTICE
IND_VIA_USER2
3
LAST_
COMPONENT
FALSE
TRUE
1
3

Procedure PROCESS_COMPONENTS