



Workshop zur Einrichtung der Anbindung an die
Telematikinfrasturktur

Michael Gillessen & Gaetano Di Bernardo

Was passiert heute?

- Theorie: VSDM & Kommunikation
 - Versichertenstammdatenabgleich & folgende Anwendungen
 - Was steckt im Konnektor? Warum ist der so teuer?
 - Kommunikation zwischen DURIA und Konnektor
 - Aufrufkontexte
- Praxis: Konnektoren
 - Kennenlernen der Konnektoroberflächen
 - Darstellung der Aufrufkontexte
 - Konfiguration der Szenarien:
 - 1x Konnektor – 1x KT (1 Mandant)
 - 1x Konnektor – 2x KT (2 Mandanten)
- Erweiterte Netzwerkkonfiguration:
 - (Netzwerkgrundlagen: Subnetz, Gateway, Routing)
 - Installation parallel / seriell? DMZ?
 - Konfiguration: 1x Konnektor – 2x KT (2 Mandanten) an zwei Standorten (über VPN)
- Benutzerrollen auf dem Konnektor
- Debugging: Wireshark und SoapUI



Einleitung: Aktueller Stand der Dinge

- CompuGroup und Telekom sind zugelassen. Mit RISE rechnet man in den kommenden Wochen
- Arvato scheint neben secunet auch mit RISE zu verhandeln
- DURIA ist seit 2/2018 von der gematik zugelassen
- DURIA kann mit allen 4 Konnektoren kommunizieren
- Bisher noch keine „echte“ Installation
- Mit dem Update 4.73 / 4.3 werden die Installationsroutinen verteilt



Versichertenstammdatenabgleich & folgende Anwendungen

- Aktuell gibt es lediglich eine Anwendung: **VSDM** =
Versichertenstammdatenmanagement = Aktualisierung der Daten auf der eGK
- Einer der nächsten Dienste ist **KOM-LE**: Kommunikation Leistungserbringer =
elektronischer Arztbrief (aber nicht kompatibel zum jetzigen eAB)

Was steckt im Konnektor? Warum ist der so teuer?

- Besteht aus zwei Teilen:
 - **Netzkonnektor & Anwendungskonnektor**
 - Netzkonnektor ist für die grundlegenden Netzwerkaufgaben zuständig:
 - IP-Kommunikation (LAN und WAN, IPSec)
 - Routing
 - DNS, ggf. DHCP
 - etc.
 - Anwendungskonnektor stellt Schnittstellen für:
 - PVS (DURIA)
 - Kartenterminals (SICCT Protokoll = Secure Interoperable ChipCard Terminal)
- Konnektor Quellcode muss dem BSI vollständig offen gelegt werden.

Kommunikation zwischen DURIA und Konnektor

- Der Konnektor stellt Webservices bereit über die mittels SOAP-Abfragen kommuniziert wird
- Die connector.sds ist das Dienstverzeichnis und enthält alle verfügbaren „Services“ und die zugehörigen „Endpoints Locations“. DURIA und die anderen PVS fragen diese ab und richten dann künftige Anfragen direkt an die Endpunkte (z.B. CardTerminalService):

```
- <ns3:Service Name="CardTerminalService">
  - <ns3:Abstract>
    Die Aufgabe des Kartenterminaldienstes ist das Management aller vom Konnektor adressierbaren Kartenterminals. Dies umfasst den Kartenterminaldienst die Zugriffe auf Kartenterminals durch Basisdienste und Fachmodule.
  </ns3:Abstract>
  - <ns3:Versions>
    - <ns3:Version TargetNamespace="http://ws.gematik.de/conn/CardTerminalService/v1.1" Version="1.1.0">
      - <ns3:Abstract>
        Die Aufgabe des Kartenterminaldienstes ist das Management aller vom Konnektor adressierbaren Kartenterminals. Dies umfasst den Kartenterminaldienst die Zugriffe auf Kartenterminals durch Basisdienste und Fachmodule.
      </ns3:Abstract>
      <ns3:Endpoint Location="http://172.18.0.9:80/ws/CardTerminalService"/>
      <ns3:EndpointTLS Location="https://172.18.0.9:443/ws/CardTerminalService"/>
    </ns3:Version>
  </ns3:Versions>
</ns3:Service>
```



Kommunikation zwischen DURIA und Konnektor

- Die Anfragen und Antworten sind mittels Web Services Description Language-Dateien (WSDL) normiert.
- Eine typische Anfrage enthält immer die Aufforderung, was gewünscht wird, z.B. „GetCardTerminals“ und einen „Context“. Die Antwort kann entsprechend der Anforderung sehr unterschiedlich sein. In diesem Beispiel werden alle mit dem Konnektor verbunden Kartenterminals zurück geliefert.

```

<?xml version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:v1="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <v7:GetCardTerminals mandant-wide="true">
      <v2:Context>
        <v5:MandantId>PRAX1</v5:MandantId>
        <v5:ClientSystemId>DURIA</v5:ClientSystemId>
        <v5:WorkplaceId>Anmeldung</v5:WorkplaceId>
      </v2:Context>
    </v7:GetCardTerminals>
  </soapenv:Body>
</soapenv:Envelope>

```

```

<?xml version="1.0" encoding="UTF-8" ?>
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Body>
    <ns10:GetCardTerminalsResponse xmlns="http://ws.gematik.de/conn/ConnectorCommon/v5.0" xmlns:ns1="http://schemas.xmlsoap.org/soap/envelope/">
      <Status>
        <Result>OK</Result>
      </Status>
      <ns8:CardTerminals>
        <ns8:CardTerminal>
          <ns9:ProductInformation>
            <ns9:InformationDate>2018-08-02T12:46:45.213+02:00</ns9:InformationDate>
            <ns9:ProductTypeInformation>
              <ns9:ProductType>KT</ns9:ProductType>
              <ns9:ProductTypeVersion>1.2.1</ns9:ProductTypeVersion>
            </ns9:ProductTypeInformation>
            <ns9:ProductIdentification>
              <ns9:ProductVendorID>INGHC</ns9:ProductVendorID>
              <ns9:ProductCode>ORGA6100</ns9:ProductCode>
              <ns9:ProductVersion>
                <ns9:Local>
                  <ns9:HWVersion>1.2.0</ns9:HWVersion>
                  <ns9:FWVersion>3.7.2</ns9:FWVersion>
                </ns9:Local>
              </ns9:ProductVersion>
            </ns9:ProductIdentification>
            <ns9:ProductMiscellaneous>
              <ns9:ProductVendorName/>
              <ns9:ProductName/>
            </ns9:ProductMiscellaneous>
          </ns9:ProductInformation>
          <ns5:CtId>CT_ID_0002</ns5:CtId>
          <WorkplaceIds>
            <WorkplaceId>Konnektor</WorkplaceId>
            <WorkplaceId>Anmeldung</WorkplaceId>
          </WorkplaceIds>
          <ns8:Name>ORGA6100-01410000007A10</ns8:Name>
          <ns8:MacAddress>00-0D-F8-04-2C-3F</ns8:MacAddress>
          <ns8:IPAddress>
            <ns8:IPv4Address>192.168.5.117</ns8:IPv4Address>
          </ns8:IPAddress>
          <ns8:Slots>4</ns8:Slots>
          <ns8:IS_PHYSICAL>true</ns8:IS_PHYSICAL>
          <ns8:Connected>true</ns8:Connected>
        </ns8:CardTerminal>
      </ns8:CardTerminals>
    </ns10:GetCardTerminalsResponse>
  </S:Body>
</S:Envelope>

```


Aufrufkontexte

- Im vorangegangenen Screenshot hat man neben dem angesprochenen „Service“ auch den Kontext gesehen
- Der Kontext besteht immer aus 3 Parametern:
 - MandantID, kann z.B. die BSNR sein, oder der PRAX-Stand
 - Die ClientSystemID, hier „DURIA“ ist bei CGM z.B. „CS01“
 - und die WorkplaceID, z.B. Anmeldung, Sprechzimmer etc.
- Aus diesen Parametern können nun Kontexte für verschiedene Arbeitsplätze, Mandanten und ggf. auch gemischte PVS abgebildet werden

Darstellung der Aufrufkontexte

- KoCoBox MED+ (Infomodell)
 - <https://192.168.5.9:9443/administration/start.htm>
- Medical Access Port (Zugriffsberechtigungen)
 - <https://10.10.8.15:4433/>
- RISE Konnektor (Konnektor -> Arbeitsumgebung)
 - <https://192.168.42.1:8443/>
- Secunet konnektor (Praxis -> Aufrufkontexte)
 - <https://172.18.0.9:8500/management/home>



Workshop zur Einrichtung der Anbindung an die Telematikinfrastruktur

Konfiguration der Szenarien

- 1x Konnektor – 1x KT (1 Mandant)
- 1x Konnektor – 2x KT (2 Mandanten)

Netzwerkgrundlagen: Subnetz, Gateway, Routing

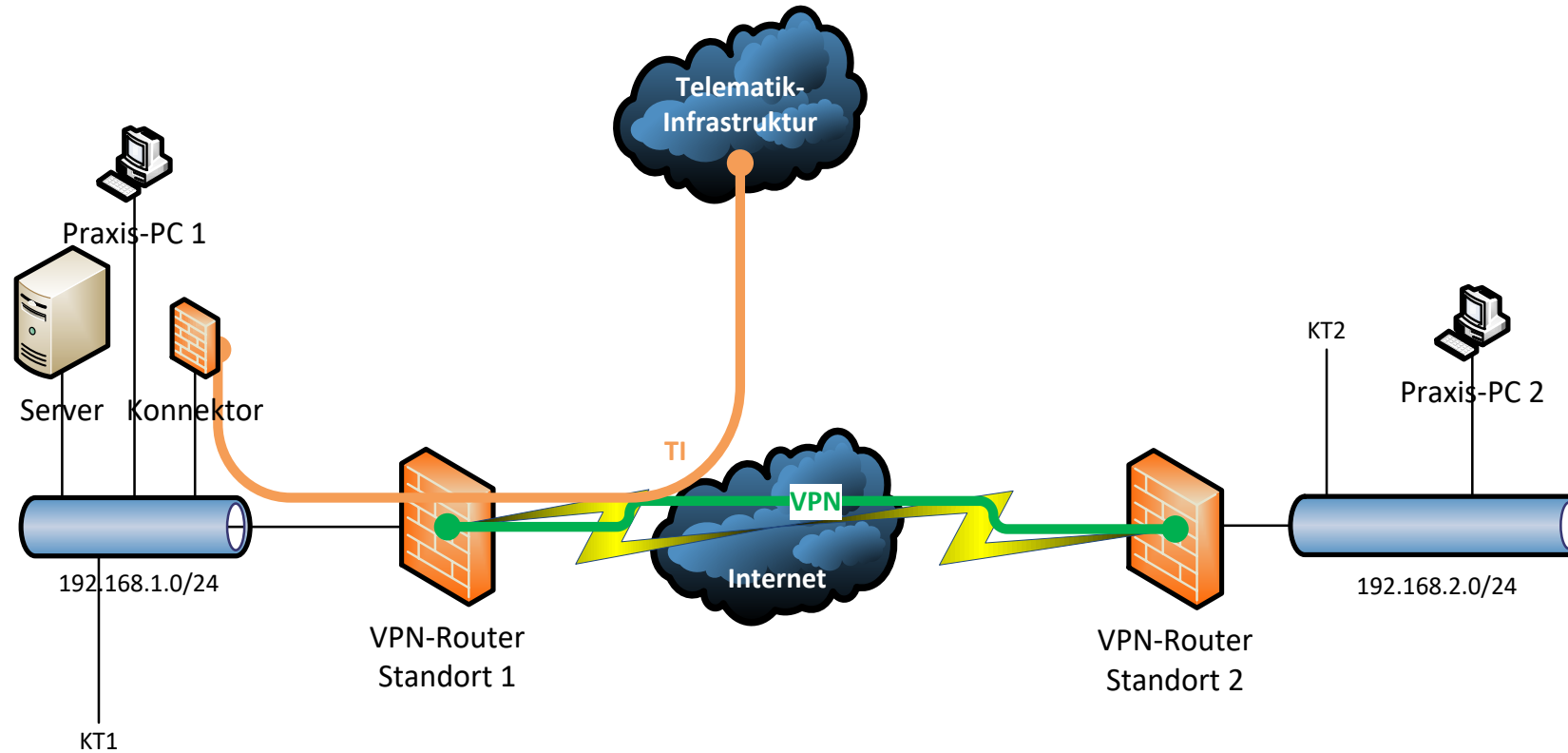
- Als Subnetz wird ein Teilnetz eines IP-Netzwerks bezeichnet. Subnetze dienen dazu, große Netzwerke zu unterteilen, oder um die Kommunikation zwischen diesen zu kontrollieren und ggf. zu reglementieren.
- Subnetze sind auch bei örtlich getrennten Praxen (üöGP, Zusammenschluss) anzutreffen. Diese sind in der Regel mittels VPN-Tunnel verbunden.
- Ein Gateway oder Router vermittelt IP Pakete zwischen den Netzwerken (Routing). Der VPN-Router kennt „die Wege“ (Routen) in das entfernte VPN-Netzwerk und das Internet.
- Ein Broadcast, welcher z.B. dazu genutzt wird Kartenterminals zu finden, wird nicht in andere Subnetze übertragen, weshalb die Konfiguration manuell erfolgen muss.

Installation parallel / seriell? DMZ?

- Parallele Installation: Der Konnektor wird wie ein Client (z.B. Drucker) in das bestehende Netzwerk integriert. Das WAN-Interface ist dann deaktiviert. Der Verkehr ins Internet wird **nicht gefiltert**.
- Serielle Installation: Der Konnektor wird mit dem WAN-Interface an den Internetrouter angeschlossen, das LAN-Interface an den Praxisswitch. Der Verkehr ins Internet **wird gefiltert (SIS)**.
- Die Installation in einer DMZ erfordert professionelle Geräte. Durch diese Installation kann mittels Firewallregeln der Konnektor logisch vom Praxisnetz getrennt und unerwünschte Zugriffe unterbunden werden.

Konfiguration der Szenarien

- 1x Konnektor – 2x KT (2 Mandanten) an zwei Standorten (über VPN)





Benutzerrollen auf dem Konnektor

- **Super-Admin**, darf alles außer remote administrieren
- **Lokaler-Admin**, darf grundlegende Dinge konfigurieren und Werksreset durchführen, aber z.B. keine Benutzer anlegen.
- **Remote-Admin**, wie der lokale Admin, jedoch lediglich per remote Administration



Debugging: Wireshark und SoapUI

- Folgende Tests waren positiv:
 - LAN ist anpingbar, MAC-Adresse passt zum Konnektor?
 - Die connector.sds lässt sich im Browser aufrufen?
- Filterregeln für Wireshark:
 - `ip.addr == <LAN-IP Konnektor> && tcp.port == 80`
 - Rechte Maustaste -> Folgen -> TCP/HTTP-Stream



Wireshark interface showing a network capture of an HTTP stream. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. A detailed view of the selected packet (No. 36) is shown in the left pane, displaying the raw data and its decoded content as an XML SOAP message. A context menu is open over the selected packet, listing various actions such as 'Paket markieren', 'Paket ignorieren', and 'Folgen'. The 'Folgen' option is selected, and a sub-menu is visible, showing options like 'TCP Stream', 'UDP Stream', 'SSL Stream', and 'HTTP Stream'. The status bar at the bottom indicates 311 packets captured, with 50 (16.1%) displayed.

No.	Time	Source	Destination	Protocol	Length	Info
31	4.045559	172.18.0.9	172.18.0.5	TCP	1414	80 → 12520 [ACK] Seq=5441 Ack=119 Win=27264 Len=1360 [TCP segment of a reassembled PDU]
32	4.045559	172.18.0.9	172.18.0.5	TCP	145	80 → 12520 [PSH, ACK] Seq=6801 Ack=119 Win=27264 Len=91 [TCP segment of a reassembled PDU]
33	4.045595	172.18.0.5	172.18.0.9	TCP	54	12520 → 80 [ACK] Seq=119 Ack=6892 Win=66560 Len=0
34	4.046283	172.18.0.9	172.18.0.5	HTTP/X...	60	HTTP/1.1 200 OK
35	4.050522	172.18.0.5	172.18.0.9	TCP	66	12521 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
36	4.051141	172.18.0.9	172.18.0.5	TCP	66	80 → 12521 [SYN, ACK] Seq=0 Ack=1 Win=27200 Len=0 MSS=1360 SACK_PERM=1 WS=128

```
POST /ws/EventService HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; Cache;)
Host: 172.18.0.9
Accept-Encoding: gzip
SOAPAction: http://ws.gematik.de/conn/EventService/v7.2#GetCardTerminals
Content-Length: 726
Content-Type: text/xml; charset=UTF-8

<?xml version="1.0" encoding="UTF-8" ?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:s="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body><GetCardTerminals xmlns="http://ws.gematik.de/conn/EventService/v7.2" mandant-wide="true"><Context xmlns="http://ws.gematik.de/conn/ConnectorContext/v2.0"><MandantId xmlns="http://ws.gematik.de/conn/ConnectorCommon/v5.0">PRAX1</MandantId><ClientSystemId xmlns="http://ws.gematik.de/conn/ConnectorCommon/v5.0">DURIA</ClientSystemId><WorkplaceId xmlns="http://ws.gematik.de/conn/ConnectorCommon/v5.0">Anmeldung</WorkplaceId></Context></GetCardTerminals></SOAP-ENV:Body>
</SOAP-ENV:Envelope>
HTTP/1.1 200 OK
Accept: text/xml, text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Expires: 0
SOAPAction: ""
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
X-XSS-Protection: 1; mode=block
Pragma: no-cache
X-Frame-Options: DENY
Date: Mon, 27 Aug 2018 12:57:21 GMT
Connection: keep-alive
X-Content-Type-Options: nosniff
Content-Type: text/xml; charset=utf-8
Content-Length: 2851

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header/><SOAP-ENV:Body><ns7:GetCardTerminalsResponse xmlns:ns7="http://ws.gematik.de/conn/EventService/v7.2" xmlns:ns2="http://ws.gematik.de/conn/ConnectorCommon/v5.0" xmlns:ns3="http://ws.gematik.de/conn/ConnectorCommon/v5.0" xmlns:ns4="http://ws.gematik.de/int/version/ProductInformation/v1.1" xmlns:ns5="http://ws.gematik.de/conn/CardServiceCommon/v2.0" xmlns:ns6="http://ws.gematik.de/conn/CardTerminalInfo/v8.0"><ns2:Status><ns2:Result>OK</ns2:Result></ns2:Status><ns6:CardTerminals><ns6:CardTerminal><ns4:ProductInformation><ns4:InformationDate>2018-08-22T13:18:03.540Z</ns4:InformationDate><ns4:ProductTypeInformation><ns4:ProductType>XT</ns4:ProductType><ns4:ProductTypeVersion>1.2.1</ns4:ProductTypeVersion></ns4:ProductTypeInformation><ns4:ProductIdentification><ns4:ProductVendorID>TMGH</ns4:ProductIdentification></ns6:CardTerminal></ns6:CardTerminals></ns7:GetCardTerminalsResponse></SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

- Paket markieren (Strg+M)
- Paket ignorieren bzw. zurücksetzen (Strg+D)
- Zeitreferenz setzen/zurücksetzen (Strg+T)
- Zeitverschieben... (Strg+Umschalt+T)
- Paketkommentar... (Strg+Alt+C)
- Auflösbare Namen editieren
- Als Filter anwenden
- Filter vorbereiten
- Verbindungsfilter
- Verbindung einfärben
- SCTP
- Folgen (Strg+Alt+Umschalt+T)
- Kopieren (Strg+Alt+Umschalt+U)
- Protokolleinstellungen (Strg+Alt+Umschalt+S)
- Dekodieren als... (Strg+Alt+Umschalt+H)
- Paket in einem neuen Fenster anzeigen

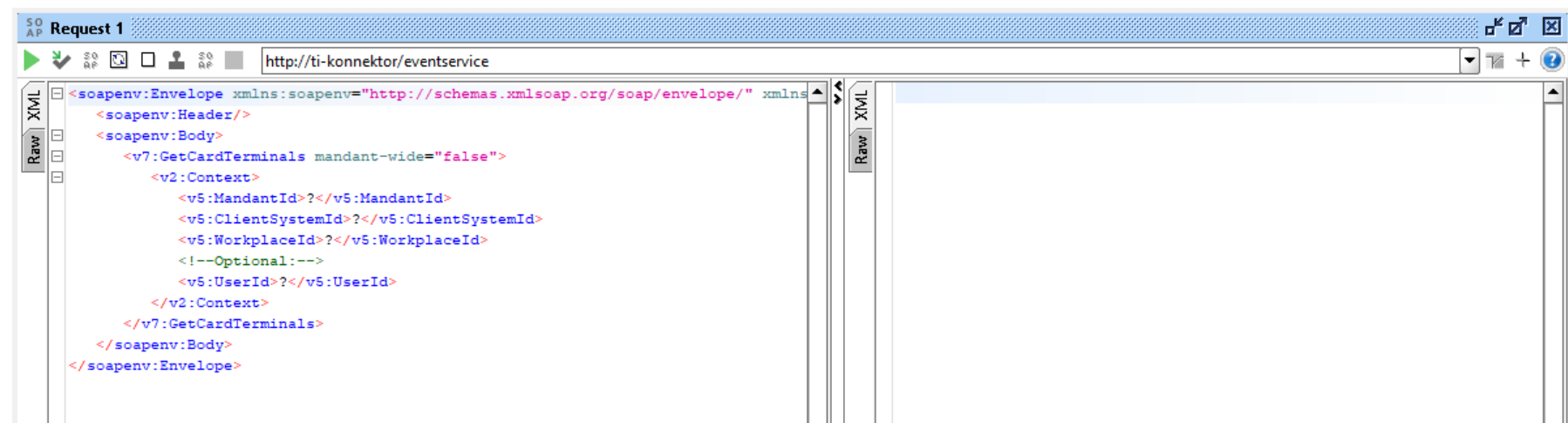
1032 bytes captured (8256 bits) on interface 0
9:a6:84:ec:a1, Dst: Congatec_2b:4c:59 (00:13:95:2b:4c:59)
0.5, Dst: 172.18.0.9
12522, Dst Port: 80, Seq: 1, Ack: 1, Len: 978

0000 00 13 95 2b 4c 59 98 29 a6 84 ec a1 08 00 45 00 ...+LY.)E.
0010 03 fa 1c cb 40 00 80 06 82 00 ac 12 00 05 ac 12 ...@.....
0020 00 09 30 ea 00 50 85 ae 07 84 ca ed 0c f9 50 18 ...P.....P.
0030 01 04 ea 1e 00 00 50 4f 53 54 20 2f 77 73 2f 45PO ST /ws/E
0040 76 65 6e 74 53 65 72 76 69 63 65 20 48 54 54 50 ventServ ice HTTP

wireshark_869FB42C-37EB-4EC4-8011-FC0D34B051EA_20180827145307_a15776.pcapng | Pakete: 311 · Angezeigt: 50 (16.1%) | Profil: Default

Debugging: Wireshark und SoapUI

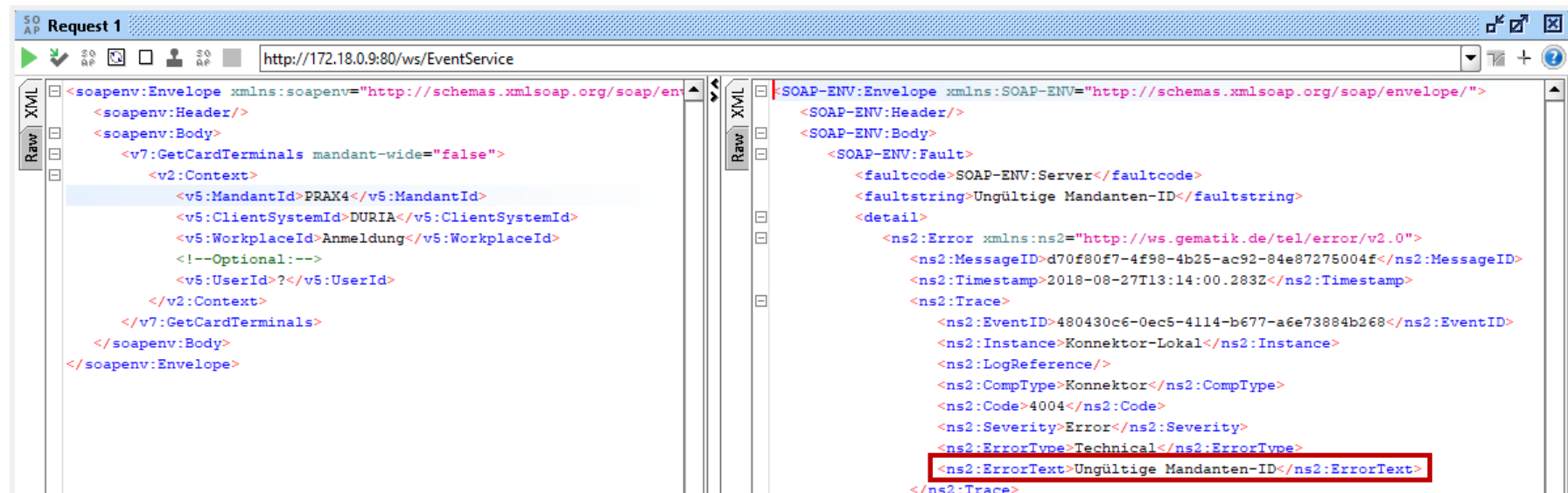
- SoapUI
- Download der Schemadateien auf der gematik-Webseite:
 - <https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/schemata-wsdl-und-andere-dateien/>
- Import der WSDL Dateien über: File -> New SOAP Project -> Name vergeben und bei „Initial WSDL“ aus dem Verzeichnis „conn“ die EventService.wsdl auswählen.
- Im Bereich GetCardTerminals gibt es nun den Request 1, mittels Doppelklick wird dieser geöffnet:



```
SOAP
Request 1
http://ti-konnektor/eventservice
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:
<soapenv:Header/>
<soapenv:Body>
  <v7:GetCardTerminals mandant-wide="false">
    <v2:Context>
      <v5:MandantId?</v5:MandantId>
      <v5:ClientSystemId?</v5:ClientSystemId>
      <v5:WorkplaceId?</v5:WorkplaceId>
      <!--Optional:-->
      <v5:UserId?</v5:UserId>
    </v2:Context>
  </v7:GetCardTerminals>
</soapenv:Body>
</soapenv:Envelope>
```

Debugging: Wireshark und SoapUI

- Nun übernehmen wir die URL (Endpoint Location des EventService) aus der connector.sds: <http://172.18.0.9:80/ws/EventService>
- Und tragen bei den ? die entsprechenden Parameter ein und klicken auf das grüne „Play“ Symbol:



```

Request 1
http://172.18.0.9:80/ws/EventService

Raw XML
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header/>
  <soapenv:Body>
    <v7:GetCardTerminals mandant-wide="false">
      <v2:Context>
        <v5:MandantId>PRAX4</v5:MandantId>
        <v5:ClientSystemId>DURIA</v5:ClientSystemId>
        <v5:WorkplaceId>Anmeldung</v5:WorkplaceId>
        <!--Optional:-->
        <v5:UserId?</v5:UserId>
      </v2:Context>
    </v7:GetCardTerminals>
  </soapenv:Body>
</soapenv:Envelope>

Raw XML
:SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
      <faultcode>SOAP-ENV:Server</faultcode>
      <faultstring>Ungültige Mandanten-ID</faultstring>
      <detail>
        <ns2:Error xmlns:ns2="http://ws.gematik.de/tel/error/v2.0">
          <ns2:MessageID>d70f80f7-4f98-4b25-ac92-84e87275004f</ns2:MessageID>
          <ns2:Timestamp>2018-08-27T13:14:00.283Z</ns2:Timestamp>
          <ns2:Trace>
            <ns2:EventID>480430c6-0ec5-4114-b677-a6e73884b268</ns2:EventID>
            <ns2:Instance>Konnektor-Lokal</ns2:Instance>
            <ns2:LogReference/>
            <ns2:CompType>Konnektor</ns2:CompType>
            <ns2:Code>4004</ns2:Code>
            <ns2:Severity>Error</ns2:Severity>
            <ns2:ErrorType>Technical</ns2:ErrorType>
            <ns2:ErrorText>Ungültige Mandanten-ID</ns2:ErrorText>
          </ns2:Trace>
        </ns2:Error>
      </detail>
    </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
  
```