KV TELEMATIK
eHealth für die Praxis

Tipps und Tricks zu KV-Connect

Dr. Volker Paul

Fahrplan für heute

- LDAP versus REST-Adressbuch (GET /vzd/accounts)
- Dienstkennungen in LDAP und Adressbuch
- Aktualisieren von KVC-Clients – worauf ist zu achten ?
- KVC-Clients auf virtuellen Maschinen: das Problem mit der Entropie

LDAP UND REST-ADRESSBUCH

Wann LDAP und wann REST ?

Vorausgeschickt:

- LDAP wird weiter laufen !
- LDAP wird – vorauss. ab 1. 10. 2017 – auf „Pagination“ umgestellt (Abrufbarkeit von „Folge-Sätzen“).
- LDAP wird –vorauss. auch ab 1. 10. 2017 – nur noch als LDAP/S angeboten.

- Ergänzend wird über eine neue REST-Funktion „GET /vzd/accounts.xml.zip“ ein XML-basiertes „Adressbuch“ angeboten

Wann LDAP ?

- LDAP ist hauptsächlich dafür ausgelegt, zu einer eingeschränkten Zahl bzw. einzelnen Einträgen Detail-Informationen abzufragen.
- z.B. Abfrage des Zertifikats eines bestimmten Nutzers
- z.B. Abfrage der Postadresse einer bestimmten Praxis

- LDAP ist typischerweise nicht ausgelegt zum Synchronisieren ganzer Adressbücher

Trotzdem geplant: LDAP mit Pagination

- Durch Verwendung einer Steuerinformation „pagedresultcontrol“ kann das Ergebnis einer Abfrage in mehreren aufeinanderfolgenden Requests abgefragt werden („cookie“)
- Funktion ab sofort auf Ref-2 aktiviert
- Ref-1 und Produktion werden zum 1. Oktober 2017 umgestellt

Wann GET /vzd/accounts.xml.zip

- Abgleich eigener Adressbücher mit dem zentralen KV-Connect-Adressbuch

- Weniger geeignet zum Suchen nach Angaben zu einzelnen Usern (jedenfalls nicht direkt; wenn, dann lokale Suche in der heruntergeladenen xml-Adressbuch)

Struktur des Adressbuchs

- Verfügbar als XML- und als JSON-Struktur
- Beispiel als XML:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<accounts date="2016-10-02 11:13:00">
    <account>
        <id>009d28a0-82f5-4bd8-a0fc-a8db1c1eac5f@72</id>
        <mandant>KVBW</mandant>
        <titel>Dr.</titel>
        <vorname>Karl</vorname>
        <nachname>Meier</nachname>
        <lanr>2222222</lanr>
        <bsnr>123456789</bsnr>
        <arzt>true</arzt>
        <fachgruppe>012 HNO</fachgruppe>
        <dienstkennungen>
            <dienstkennung>Arztbrief;VHitG-Versand;V1.0</dienstkennung>
            <dienstkennung>DALE-UV;Einsendung;V1.0</dienstkennung>
        </dienstkennungen>
        <iknr>1234567</iknr>
        <ou>Praxis am Rathaus</ou>
        <strasse>Rathausplatz</strasse>
        <hausnummer>1</hausnummer>
        <plz>53442</plz>
        <stadt>Stuttgart</stadt>
        <mail>b-1234567.kvbw@kv-safenet.de</mail>
        <certificate>https://kvlink1.kv-safenet.de:8443/kvcserver/rest/account/b-1234567/certificate
        </certificate>
    </account>
    <account>
        <id>111d28a0-82f5-4bd8-a0fc-a8db1c1eac5f@72</id>
        <mandant>KVBW</mandant>
        <titel>Dr.</titel>
```

Abruf-Möglichkeiten

- Basis-Abrufe:
  - GET /vzd/accounts.xml.zip HTTP/1.1
  - HEAD /vzd/accounts.xml.zip HTTP/1.1 (liefert Änderungsdatum)
  - GET /vzd/accounts.xml.zip HTTP/1.1 If-Modified-Since: Thu, 22 Sep 2016 12:45:26 GMT
- Mit Search-Funktionen:
  - ../search?stadt=Hamburg
  - ../search?stadt=Hamburg&nachname=~Meier
    (Alle Accounts in Hamburg für Meier, Meyer, Mair etc., „Kölner Phonetik“)
  - ../search?stadt=Hamburg&dienstkennung=eArztbrief;*;V1.0

KV TELEMATIK

DIENSTKENNUNGEN IN LDAP UND ADRESSBUCH

Wozu das Ganze ?

- Dienstkennungen sollen möglichst belastbare Aussagen liefern, welcher KV-Connect-Anwender als Kommunikationspartner für welche Art von Datenaustausch in Frage kommt:
- Wem kann ich Artbriefe per KV-Connect schicken ?
- Wer kann mir Arztbriefe per KV-Connect senden ?
- Außerdem können die Dienstkennungen zur Strukturierung eines lokal gehaltenen Adressbuches dienen.

Woher kommen die Einträge ?

- Aktuell:
  - aus allen Transaktionen
  - Ablage in der zentralen Benutzerverwaltung
  - Von dort Export in den LDAP
  - Basis für die „Anwendersuche“ mit oder ohne „Arztbrief-Filter“
  - „einmal Arztbrief, immer Arztbrief“

Geplante Änderungen

- Zeitnah:
  - Filterung mittels „Whitelist“
- Mittelfristig:
  - Aufnahme der Dienstkennungen in die erweiterte Benutzersuche
  - Rücksetzen / Sperren von Einträgen mittels Nachricht an speziellen Sperr-Account
  - Bewusstes Setzen von Einträgen mittels Nachricht an speziellen Freischalt-Account

Beispiel 1:

- Ein bei der Installation testweise versendeter Arztbrief setzt in LDAP und Adressbuch das Attribut *„<dienstkennung>Arztbrief;VHitG-Versand<dienstkennung>“*
- Durch Senden einer Nachricht mit der Dienstkennung „Arztbrief;VHitG-Versand“ an den Account *„KVC.Diensteintrag.sperren@kv-safenet.de“* wird dieser Eintrag gelöscht und ein Wieder-Eintragen verhindert („ich kann zwar senden, aber das soll keiner wissen“)
- Der Inhalt der Nachricht wird weder ausgewertet noch weitergeleitet.

Beispiel 2:

- Nach gutem Zureden durch seine Kollegen entscheidet sich ein solcher Anwender, doch Arztbriefe zu versenden und dies auch kundzutun
- Durch Senden einer Nachricht mit der Dienstkennung „Arztbrief;VHitG-Versand“ an den Account *„KVC.Diensteintrag.setzen@kv-safenet.de“* wird ein entsprechender Eintrag aktiv gesetzt sowie eine eventuell vorher gesetzte Eintrags-Sperre aufgehoben.
- Der Inhalt der Nachricht wird weder ausgewertet noch weitergeleitet.

Auch Empfänger können interessant sein

- Auch das Vorkommen der Dienstkennung „Arztbrief;Eingangsbestaetigung“ in einer Sendung führt zum Setzen des entsprechenden Eintrags (Sperren und Wieder-Freischalten analog)
- Für Anwender mit einem „receive-only“ System: „unmotiviertes“ Senden einer Arztbriefquittung an sich selbst oder an *„KVC.Diensteintrag.setzen@kv-safenet.de“* führt zum Setzen der Dienstkennung „Arztbrief;Eingangsbestaetigung“ und signalisiert: ***„Auch wenn ich nicht senden kann: mir könnt Ihr Arztbriefe schicken“***
  (Als Tipp an Systeme, bei denen der Arztbrief-Empfang kostenlos oder in ein Basis-Paket eingeschlossen ist)

PROBLEME MIT DER ENTROPIE

KVC-Clients brauchen Entropie

- Entropie steht hier als Quelle für Zufallszahlen, die in der Kryptographie gebraucht werden.
- „Gute“ Entropie entsteht „zufällig“ aus Hardware-Ereignissen des Computers und wird in einem Entropie-Buffer gesammelt.
- Anforderungen von Zufallszahlen „entnehmen“ Entropie aus diesem Buffer, die entstehende Lücke muss durch die Hardware wieder aufgefüllt werden.
- Funktionen, die Wert auf hochwertige Zufallszahlen legen, warten lieber auf das Nachfüllen des Buffers, statt „schlechtere“ (Pseudo-) Zufallszahlen zu verwenden.

Bedarf für Zufallszahlen („Seed“)

- Aufbau eines Tunnels zwischen lokaler Anwendung („MUC“) und dem KVC-Client:
  jeder Neuaufbau eines Tunnels benötigt 256 bit Entropie
- Aufbau eines Tunnels zwischen KVC-Client und KVC-Server:
  jeder Neuaufbau eines Tunnels benötigt 256 bit Entropie
- Verschlüsselung der KV-Connect-Nachrichten:
  jede Nachricht benötigt einen „Session-Key“ von 256 bit

Begrenzte Entropie-Ressourcen

- Insbesondere virtuelle Maschinen, die keine eigene Hardware besitzen, können den Entropie-Buffer ggf. nur sehr langsam „auffüllen“.
- Der KV-Connect-Client benötigt aktuell relativ viel Entropie (bis zu 1,5 kbit pro Nachricht), eine Optimierung ist mittelfristig geplant.
- Fehlende Entropie führt aktuell zu Exceptions und Abbruch der Transaktion.

KV TELEMATIK

Beobachtete Effekte

	Ohne VM	VM mit Windows	VM mit Linux
Windows-Host	Keine Entropie-Probleme	Keine Entropie-Probleme	**Akuter Entropie-Mangel**
Linux-Host	(Noch nicht getestet)	(Noch nicht getestet)	**Akuter Entropie-Mangel**

Randbedingungen:

- Host: Windows 7 bzw. OS-X
- Hypervisor: VirtualBox
- Linux: Kali Linux mit embedded Java JDK

Aktuelle Empfehlungen

- Eine de facto unbegrenzte Erhöhung der verfügbaren Entropie kann durch Anpassungen in der JRE (Umstellung auf /dev/urandom als Entropie-Buffer) erfolgen, allerdings wird dabei die Qualität der Zufallszahlen vermindert
- Eine Reduzierung des Entropie-Bedarfs kann durch Heruntersetzen der Abfrage-Häufigkeit von Nachrichten erfolgen (z.B. Abfrageintervall 10 Minuten statt 1 Minute).
- Die Einstellungen sollten sich an der tatsächlich verfügbaren Entropie orientieren.

KV TELEMATIK

WICHTIG!

- „Echte“ (Hardware-) Entropie ist immer nur begrenzt verfügbar
- Verschiedene Betriebssysteme, verschiedene Frameworks nutzen unterschiedliche Mechanismen, auf Entropie zuzugreifen.
- Deshalb schwankt die in einer konkreten Anwendung nutzbare Entropie zum Teil extrem in Abhängigkeit von OS, Hardware/VM und Frameworks.
- Eine allgemeingültige Messung der verfügbaren Entropie ist deshalb kaum direkt möglich.

Verfügbarkeit von Entropie messen

- Bei Linux-Systemen ist die Messung „mit Bordmitteln“ möglich, bei Windows-Systemen gibt es dafür keine geeigneten Werkzeuge.
- Aktuell wird an einem einfachen (JAVA-) Tool gearbeitet, dass es gestatten soll, die Verfügbarkeit von Entropie in einer konkreten Umgebung abzuschätzen.
- Das Tool wird dieselben Entropie-Quellen nutzen wie der KV-Connect-Client.
- Nach erfolgreichen Tests soll das Tool für Interessenten zur Verfügung gestellt werden.

KV TELEMATIK

Verfügbarkeit von Entropie verbessern

- Entropie-Buffer werden aus Hardware-Events gefüllt.
- Je weniger Hardware für eine VM zugreifbar ist, desto langsamer entsteht neue Entropie.
- Freigabe von Host-Hardware kann Verfügbarkeit von Entropie deutlich erhöhen.
- z.B.: Freigabe eines auf dem Host vorhandenen Audio-Eingangs (auch ohne Mikro, wird wie Rausch-Quelle genutzt).
- z.B.: Freigabe „echter“ Festplatten (Auswertung von Steuer-Events, ungenutzte Partition nützt also nichts).

KV TELEMATIK

Hardware-Entropie-Generatoren

- Für extrem hohe Anforderungen an Verfügbarkeit von Entropie gibt es Hardware-Appliances, die Entropie zur Verfügung stellen.
- Ein einfaches Beispiel hierfür ist der so genannte „Entropykey“ von Simtec Electronics, Kosten ca. 30£.
- Solche Generatoren nutzen das Hardware-Rauschen elektronischer Bauelemente zur Erzeugung von Zufallszahlen.
- Hardware muss für VM freigegeben werden.

UPDATE DES KV-CONNECT-CLIENTS

„Update“ des KV-Connect-Clients

- Mit den aktuellen Installations-Skripten von KV-Connect entstehen vollständige neue Installationen, in der Regel in neuen Verzeichnissen
- Es werden „jungfräuliche“ Properties-Einstellungen hinterlegt.
- User-Einstellungen werden nicht übernommen.
- Der zu startende Client befindet sich (i.d.R.) in einem neuen Verzeichnis (wichtig für Autostart, Start aus Primärsystem heraus usw.)

Kvconnect-global.core.properties

- Server-Einstellung wird bei neuen Skripten per Dialog abgefragt und automatisch korrekt eingetragen.
- Timeout-Einstellungen müssen ggf. aus der vorherigen Installation übertragen werden, sofern sie vom Standard abweichen.
- Ein Kopieren der kompletten global.core.properties ist in der Regel unkritisch.

felix-config.properties

- Hier sind die Parameter für das lokale WEB-Interface des Clients hinterlegt, also zum interaktiven Anmelden am Server, Ändern des Passworts und Erzeugen von Zertifikaten.
- Die WEB-Schnittstelle wird im Zusammenhang mit dem Update eigentlich nicht benötigt, erst dann, wenn neue Zertifikate gebraucht werden.
- Kritisch:
  Das Zertifikat für die lokale SSL-Verbindung wird bei der Installation neu erzeugt. Es sollte ggf. aus der vorherigen Installation übernommen werden, falls es vom Primärsystem geprüft wird (Zertifikat, PIN und Passwort übernehmen !).

Kvconnect-global.mailadapter.properties

- Hier sind die Parameter definiert, die für die lokale Mail-Schnittstelle (SMTP und POP) gelten
- Das (neue) lokale SSL-Zertifikat wird automatisch eingetragen und muss ersetzt werden, falls das alte (oder ein eigenes) weiter verwendet werden soll.
- Wichtig:
  - eventuell vom Standard abweichende Port-Einstellungen müssen an die bisherige Installation angepasst werden.
  - Die mailadapter.host- und mailadapter.allowed-Einstellungen müssen – sofern nicht Standard – ebenfalls übertragen werden.
  - mailadapter.message.maxsize=200000 (=200MB) wird aktuell automatisch gesetzt

Launcher-properties

- Console.enabled=
  und
- console.title=
- ggf. aus Alt-Einstellungen übernehmen

logback.xml

- <logger name="de.kvconnect" level="**INFO**" />

  → bei Bedarf auf “**DEBUG**” setzen

Benutzer übernehmen

- In jedem KV-Connect-Installationsordner befindet sich ein Ordner \users
- Dieser Ordner enthält je angelegtem User einen Unterordner mit dem Namen des jeweiligen Accounts
- Kopieren dieser Unterordner in das \users-Verzeichnis der neuen Installation übernimmt die Nutzer in die neue Konfiguration

Im Primärsystem:

Anpassungen je nach genutzten Funktionen:

- Korrektur des Pfades zum Start des Clients (oder Umbenennen des Pfades mit der neuen Installation)
- Bei Autostart: Erneuern des entsprechenden Eintrags in der Aufgabenplanung
- Einpflegen des neuen lokalen SSL-Zertifikats, sofern erforderlich

KV TELEMATIK
eHealth für die Praxis

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT !