AqBanking - Feature #43

Schlüsseländerung / Medienwechsel

09/11/2019 06:59 PM - thbe

Status:	New	**Start date:**	09/11/2019
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	AqBanking	**Estimated time:**	0.00 hour
Target version:			
Betriebssystem:		**Anwendung:**	
AqBanking-Version:		**Version der Anwendung:**	

Description

Da ja sehr bald einige Verfahren nicht mehr angeboten werden von den Banken,
braucht man evtl. bei der Umstellung neue Schlüssel und / oder Medien.
Das ist für einige Wechselmöglichkeiten, z.B. RDH1 nach RAH10, auch so vorgesehen, dass einfach neue Schlüssel
und ein anderes Sicherheitsprofil an die Bank gesendet wird, ohne weiteres Freischalten, INI-Brief o.ä.
(Aussage HVB-Hotline: "Einfach Medienwechsel durchführen")

Ok, damit das machbar ist, hab ich dafür etwas gebaut.
Das ist bisher noch an keiner echten Bank getestet worden.
(Wird/sollte/müsste hier aber bald passieren ^^)

Was funktionieren sollte:
Schlüsseldatei RDH nach Schlüsseldatei RAH
Das gleiche mit Karte **könnte** auch funktionieren.
Nicht unterstützt zur Zeit ein Profilwechsel ohne Schlüsselwechsel.

Der interne Ablauf ist folgender:
- Auswahl/Erzeugen Medium
- Dialoginitialisierung mit HKISA und darin keyname-num/vers. 999, und secprofile das neue Verfahren
- die damit geholten Serverkeys auf das neue Medium schreiben, da AH_Provider_CreateKeys() die Key-Längen von da nimmt
- zuvor gesicherte Serverkeys auf aktuellem Token zurückschreiben
- ggf. Schlüssel erzeugen
- Schlüssel in nächster Msg an Server
- bei Erfolg, user mit neuen token und serverkeys abschliessen

Wer das nicht gut findet, Fehler findet oder so, sollte das schnell mitteilen,
bevor ich oder jemand das mit seiner Bank probiert.
(Schlüsseldatei vorher sichern)

Noch ein patch ist dabei (aqbanking-create-keys.patch) für provider_keys.c,
damit wird auch bei RAH nach der serverschlüssellänge gegangen.

Gruss,
Thomas

History

#1 - 09/11/2019 08:25 PM - martin

Moin Thomas,

vielen Dank fuer Deine Patches.

Den ersten habe ich gerade eingecheck, naeheres dazu per Mail.

Gruss
Martin

#2 - 09/13/2019 07:21 PM - thbe

Hallo,

ein Status-Update:

(HVB, Wechsel RDH1 -> RAH10)
Set gestern morgen weiss ich, der Patch funktioniert so wie er ist definitiv nicht.
Einmal gibt es ein Problem weil ein neuer, anderer Schlüssel von der Bank geholt wird,
dann kann es in user.c beim verify crashen (und das tat es), da hier der aktuelle cryptmode des users
für keysizes etc. genommen wird.
Das hab ich umgangen, indem ich dem user vorrübergehend den neuen mode setze.
Es kann aber immernoch vorkommen, wenn vorher kein S-Schlüssel der Bank vorhanden war und
die Bank **jetzt** einen mitschickt, da findet die Prüfung eher statt, da ist das nicht so einfach.
Wird zwar eher nicht vorkommen, aber dennoch, mal schauen.
U.a. vergass ich noch einige Werte für Segmente zu setzen.

Mit Änderungen dann ein weiterer Versuch, und die Bank meinte allen Ernstes:
"HIRMS:3:2:3+0020::Schlüssel wurde geändert".
Yeah.
Ok nicht soo sehr, da crash bevor die user-config geschrieben wurde (noch k.A. warum).
Dann eben von Hand geändert auf neue Schlüsseldatei usw., und ein getkeys gemacht.
Die nächste Nachricht der Bank fand ich dann nicht so erfreulich:
"9010::Nachricht konnte nicht entschlüsselt werden.+9040::Authentifizierung des Einreichers fehlt"
Hmm. Mist.
Ein wenig mit der Hotline geplaudert - jo, Schlüssel sind wohl da ... RAH neu, andere auch Probleme...
(und alte RDH-Schlüssel werden gleich gelöscht beim Wechsel)
Nochmal alles durchgegangen - Parameter, Verschlüsselung...
Heute aus Verzweiflung einen Win-Rechner eingerichtet und Starmoney-Testversion installiert (nix anderes gefunden
was RAH kann und sich so installieren lässt), die hvb-hbci-Adresse per
hosts auf einen testserver geleitet. Einrichten, Schlüsseldatei usw... und das geht ohne Probleme.
Arrgh, warum nicht mit der HVB?
Und nu? Ok, nochmal logs durchgehen... halt, da steht "HVB-2048-RAH10" als Kennung (peer-id). Das war vorher "HVB".
Also conf geändert, Test, und jaaa, **das war die verdammte Lösung**.
Nix furchtbar kompliziertes bei der Verschlüsselung, keine geheimnisvollen Parameter.

Nun gut, die id sollte also besser auch mit geschrieben werden beim Schlüssel holen.
Die "Kundensystem-ID" hat sich übrigens auch geändert, die muss auch geholt werden.

Patch-Anpassung kommt dann demnächst.

Die HVB hat die Umstellungsfrist wg. RDH übrigens bis Jahresende verlängert.

Gruss,
Thomas

#3 - 09/14/2019 06:39 PM - thbe

Hi,

hmm, also:
- Peer-id wird geschrieben wenn getkeys ausgeführt wird **und** der user vorher keine
gesetzt hatte.
- Eigentlich müsste bei jedem Dialog HKISA mit rein, siehe
FinTS_3.0_Formals_2017-10-06_final_version.pdf C.3.1.1
(wenn asym. Keys)

Mein Vorschlag, Peer-id in AH_Job__CommitSystemData(), und da **immer** setzen.

'getkeys' macht ja eigenlich nur zusätzlich, den/die Serverschlüssel auf das Medium zu schreiben,
gibts da einen Grund, das nicht im job-commit zu machen?
Oder anders, wenn HKISA im Dialog ist, und die Bank Schlüssel geändert hat, sollten die dann
nicht auch auf das Medium?

Ach ja Martin,

> naeheres dazu per Mail.

hab ich da was übersehen oder kam noch nichts?

Gruss,
Thomas

#4 - 10/03/2019 02:17 PM - martin

- Category set to AqBanking

Files

aqbanking-change-keys.patch	53.7 KB	09/11/2019	thbe
aqbanking-create-keys.patch	1.58 KB	09/11/2019	thbe