

AqBanking - Bug #35

RAH, Umsatzabfrage

07.08.2019 07:47 - thbe

Status:	Closed	Beginn:	07.08.2019
Priorität:	Normal	Abgabedatum:	
Kategorie:	AqBanking	Anwendung:	AqFinance, GnuCash, KMyMoney, aqbanking-cli
Betriebssystem:	Linux	Version der Anwendung:	
AqBanking-Version:	6.x		

Beschreibung

Hallo,

hier im Haus existiert ein Konto bei der Hypovereinsbank mit einem RDH1-Keyfile. Da das ab September ja nicht mehr geht, wollte ich RAH mal mit aqbanking gegen meinen (Eigenbau-)hcbi-testserver testen, allerdings wurde da bei der Schlüsselabfrage (HKISA) immer RDH gesendet. In dlg_newkeyfile.c wird der crypt-mode nicht abgefragt, dazu hab ich mal einen patch gemacht. Mein testserver sagt mir damit nun immerhin, dass er (noch) kein RAH kann, weiter kann ich jetzt also erstmal nicht testen. Wenn ein Schlüssel geholt werden kann, wird der Hash nicht im Dialog angezeigt (user.c, auch im patch).

Wenn ich Umsätze abrufe (HKKAZ/HIKAZ MT940) und das Buchungsdatum '0' ist (erster Auszug) gibts einen segfault.

Für gwen sind noch einige memleak-fixes dabei.

Gruss

Historie

#1 - 07.08.2019 09:31 - thbe

Hmm ok, die Unterstützung der neuen RDH- und RAH-Verfahren ab 5.99.18beta ist wohl generell nur für Karten?

provider_keys.c: 66: Key generation not supported with this token

provider_keys.c:64

```
if (AH_User_GetCryptMode(u) != AH_CryptMode_Rdh) {
    DBG_ERROR(AQHBCI_LOGDOMAIN,
              "Key generation not supported with this token");
    return GWEN_ERROR_INVALID;
}
```

und dann

provider_keys.c:184

```
switch (rdhType)
```

nur 1-5 und 10

#2 - 07.08.2019 09:34 - thbe

- Datei aqbanking-memleaks.txt wurde hinzugefügt

Vergessen: aqbanking-memleaks

#3 - 07.08.2019 12:50 - martin

- Status wurde von New zu In Progress geändert

Moin,

koenntest Du die Patches bitte in einer Version erzeugen, die ich direkt mit "patch" verwenden kann? Idealerweise sogar mit git erstellt? "patch" sagt mir mit allen moeglichen Optionen

patch: **** Only garbage was found in the patch input.

BTW: Ist Dein Test-Server oeffentlich bzw. der Code Open-Source? Ich arbeite zwar gerade selber an einem Test-Server, aber wenn es schon einen gaebe, mit dem man testen koennte...

Gruss
Martin

#4 - 07.08.2019 15:47 - thbe

- Datei *aqbanking-rah-mode.patch* wurde hinzugefügt
- Datei *aqbanking-memleaks.patch* wurde hinzugefügt
- Datei *gwen-memleaks.patch* wurde hinzugefügt

So, das betrifft ja nur das anlegen mit dem Dialog-Setup, mit aqhbc-tool4 hab ich jetzt zumindest einen user mit RAH erstellen können, damit sollte das auch über 'AB_Banking_ProviderControl' gehen. Dann mal weiterschauen...

Der testserver ist nicht öffentlich erreichbar, source-code bisher auch nur bei mir. An sich könnte es auch open-source werden. Würde dir das mal direkt zuschicken, wie am besten? Muss aber erst noch bisschen was anpassen.

"patch" sagt mir mit allen moeglichen Optionen

Ja, sorry, neue angehängt.
Gruss

#5 - 07.08.2019 15:52 - thbe

Weisst Du/jemand, was die hvb/unicredit aktuell an Chipkarten ausgibt?
Das soll zumindest mal SECCOS gewesen sein, das würde dann nicht gehen?

#6 - 07.08.2019 16:52 - martin

Moin,

vielen Dank, habe die Patches fuer AqBanking gerade eingebaut.

Was die Karten angeht: Frage am besten mal auf unserer Liste nach, denn en aktuellen Chipkarten-Code haben zwei andere Programmierer beigesteuert, die auch auf der Liste mitlesen (aqbanking-user).

Gruss
Martin

#7 - 08.08.2019 09:55 - bayerstefan

Servus,

als einer der RDH/RAH-Implementierer, was wir bis jetzt tatsächlich erfolgreich testen konnten sind RDH-7 und RDH-9, also bloß die Chipkartenvarianten von RDH. RAH ist zwar implentiert, ich hab aber bis jetzt kein Feedback dazu bekommen und konnte es auch nicht selber testen. Das kann natürlich auch heißen das es mit Chipkarten tatsächlich funktioniert. Ich hab mal in die Spezifikationen gelinst, das einzige RAH Profil mit Schlüsseldatei ist RAH-10, der schnelle Blick auf die angezeigten Codestellen läßt da tatsächlich den passenden Code noch vermissen.

Zum Thema Chipkarten selber, relevante RDH/RAH Karten sind zwingend SECCOS-Karten, wenn eine Bank also eine RAH-fähige Karte rausgibt ist das SECCOS mit der DF_SIG Signaturanwendung auf der Karte.

Grüße,
Stefan

#8 - 08.08.2019 10:39 - Berny

Hallo Stefan,

RAH-7 hatte ich mit Martins Hilfe zum Laufen gebracht und meine Erkenntnisse im Wiki https://www.aquamaniac.de/rdm/projects/aqbanking/wiki/RAH7_einrichten veröffentlicht.

Danke & viele Grüße
Bernhard

#9 - 08.08.2019 13:45 - thbe

- Datei *aqbanking-gen-rah-keys.patch* wurde hinzugefügt

Hallo,

also, ja, ich konnte einen user mit aqhbci-tool4 erstellen, aber auch da keinen Schlüssel erzeugen.

Mit aqbanking-gen-rah-keys.patch funktioniert das jetzt auch, und ich kann auch (RAH-10) mit meinem testserver entschlüsseln (verschlüsseln und signing hab ich noch nicht eingebaut).

Einen User über die Dialoge anlegen geht auch.

Zu dem Patch: da ist die Anmerkung

```
/* the specs say that for RDH-10 we must not create keys longer than the server's  
 * sign key (or, if absent, the server's encipher key) */
```

gilt das auch für RAH?

Bzw ist ja noch die Frage, ob ein richtiger Bankserver die Ver-/Entschlüsselung auch so sieht wie meiner.

Stefan, danke.

Nach ca 1h Warteschleife sagte man mir vorhin, dass man bei der Hypo Karten SECCOS 6 verwendet.

Gruss,
Thomas

#10 - 08.08.2019 19:51 - martin

Danke Dir, habe Deinen Patch ins GIT repo uebernommen.

Gruss
Martin

#11 - 08.08.2019 19:51 - thbe

Wie ist das eigentlich - ist eine Schlüsseländerung oder "Medienwechsel" überhaupt vorgesehen?

Also, laut 'FinTS Security - Sicherheitsverfahren HBCI'

Schlüssel ändern:

"Der Nachricht muss eine Dialoginitialisierung vorausgehen. Der Auftrag muss mit dem alten Signierschlüssel signiert werden."

anstelle von Schlüssel neu:

"Diese Nachricht wird an Stelle einer Dialoginitialisierung gesendet."

usw.

Wäre, wenn ein "richtiger" Wechsel nicht geht, erst sperren und dann neu einreichen der Weg?

Oder seh ich grad alles komplett falsch...

#12 - 08.08.2019 22:28 - thbe

martin schrieb:

Danke Dir, habe Deinen Patch ins GIT repo uebernommen.

Aber gerne doch, und freut mich.

#13 - 09.08.2019 10:57 - bayerstefan

Berny schrieb:

Hallo Stefan,

RAH-7 hatte ich mit Martins Hilfe zum Laufen gebracht und meine Erkenntnisse im Wiki https://www.aquamaniac.de/rdm/projects/aqbanking/wiki/RAH7_einrichten veröffentlicht.

Danke & viele Grüße
Bernhard

Servus Bernhard,

wird jetzt schön langsam OT, aber ich seh in der Kommandozeile bei Deinem Wiki-Eintrag -t ddvcard, was ja eigentlich theoretisch laut Standard gar net funktionieren darf, da RAH-7 zwingend nach einer Seccos-Karte (bei aqbanking wäre das -t zakcard) verlangt. Bist Du sicher das das stimmt?

LG,

Stefan

#14 - 09.08.2019 18:03 - Berny

Hallo Stefan,

gerade noch mal getestet: Mit '-t zkacard' klappt's nicht, auch `gct-tool showuser -t zkacard` resultiert in einem Fehler. Mit '-t ddvcard' läuft alles durch.

Viele Grüße
Bernhard

#15 - 28.08.2019 10:26 - bayerstefan

Hallo Bernhard, (weiterhin sehr OT)

tschuldige die lange Stille, da RAH und DDV-Karte prinzipiell gar net funktionieren kann, glaub ich eher, daß beim Aufruf mit `ddvcard` alle RxH-spezifischen Parameter ignoriert werden und ein DDV-Zugang eingerichtet wird, da müßtest mal in die Userkonfigurationsdatei reinschauen ob das so ist. War zu faul selber im Quellcode rumzusuchen ;-)

Grüße,
Stefan

#16 - 09.09.2019 22:32 - Berny

Hallo Stefan (immer noch OT),

oh Schande, da hast Du Recht! Ich kann --rdhtype weglassen, und es läuft immer noch. Da habe ich <https://bs-ag.com/images/Download/DDBAC/Bankenliste.pdf> heftig fehlinterpretiert (BYLADEM1AIC).

Sorry for the noise
Bernhard

#17 - 03.10.2019 14:15 - martin

- Kategorie wurde auf AqBanking gesetzt

#18 - 12.05.2020 14:02 - martin

- Status wurde von In Progress zu Closed geändert
- AqBanking-Version wurde auf 6.x gesetzt
- Betriebssystem Linux wurde hinzugefügt
- Anwendung AqFinance, GnuCash, KMyMoney, aqbanking-cli wurde hinzugefügt

Dateien

aqbanking-rah-mode.txt	3,75 KB	07.08.2019	thbe
gwen-memleaks.txt	1,65 KB	07.08.2019	thbe
aqbanking-memleaks.txt	1,82 KB	07.08.2019	thbe
aqbanking-rah-mode.patch	4,26 KB	07.08.2019	thbe
aqbanking-memleaks.patch	2,28 KB	07.08.2019	thbe
gwen-memleaks.patch	1,8 KB	07.08.2019	thbe
aqbanking-gen-rah-keys.patch	4,47 KB	08.08.2019	thbe