Gwenhywfar - Bug #22

"Signer not found " on Windows

01/18/2019 09:42 AM - rhabacker

Status:	Closed	**Start date:**	01/18/2019
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Running

```
aqhbci-tools4 getcert -u xxx
```

with gwenhywfar 4.20.1 on a configured Ing-Diba user shows an issue that the Signer of a certificate is not found:

Windows

```
===== Abruf des Zertifikats =====
Verbindung vorbereiten
7:2019/01/18 00-00-33:gwen(5600):urlfns.c:  122: Server: [fints.ing-diba.de]
7:2019/01/18 00-00-33:gwen(5600):urlfns.c:  175: Path: [/fints/]
Mit Server verbinden...
6:2019/01/18 00-00-33:gwen(5600):syncio_tls.c: 1177: Connecting base layer
Hostname "fints.ing-diba.de" wird aufgelöst...
IP-Adresse ist "194.127.138.150"
Verbindung zu "fints.ing-diba.de" wird aufgebaut
6:2019/01/18 00-00-33:gwen(5600):syncio_socket.c:  244: Connected to "fints.ing-diba.de"
Verbunden mit "fints.ing-diba.de"
6:2019/01/18 00-00-33:gwen(5600):syncio_tls.c: 1183: Base layer connected
6:2019/01/18 00-00-33:gwen(5600):syncio_tls.c:  340: Preparing SSL (00000014)
6:2019/01/18 00-00-33:gwen(5600):syncio_tls.c:  348: Init as client
Using GnuTLS default ciphers.
5:2019/01/18 00-00-33:gwen(5600):syncio_tls.c: 1130: Protocol: TLS1.2 Key exchange algorithm: ECDH
E-RSA cipher algorithm: AES-256-GCM MAC algorithm: AEAD
TLS: SSL-Ciphers negotiated: TLS1.2:ECDHE-RSA-AES-256-GCM:AEAD
6:2019/01/18 00-00-33:gwen(5600):syncio_tls.c:  656: Signer not found
Unterzeichner des Zertifikats wurde nicht gefunden
6:2019/01/18 00-00-33:gwen(5600):syncio_tls.c:  663: Certificate is not trusted
Dem Zertifikat wird nicht vertraut
6:2019/01/18 00-00-33:gwen(5600):syncio_tls.c:  712: Key stored within certificate, extracting (mo
dlen=513, explen=3)
6:2019/01/18 00-00-33:gwen(5600):syncio_tls.c:  811: Checking hostname [fints.ing-diba.de]
6:2019/01/18 00-00-34:gwen(5600):syncio_tls.c:  820: Cert is for this server
6:2019/01/18 00-00-34:gwen(5600):fslock.c:  219: FS-Lock applied to C:\Users\Ralf\aqbanking\settin
gs\shared\certs.conf
5:2019/01/18 00-00-34:aqbanking(5600):abgui.c:  165: Automatically accepting certificate [9A:16:82
:DB:4D:D3:0D:0C:C5:41:21:40:62:0E:E7:35]
6:2019/01/18 00-00-34:gwen(5600):fslock.c:  239: FS-Lock released from C:\Users\Ralf\aqbanking\set
tings\shared\certs.conf
6:2019/01/18 00-00-34:gwen(5600):syncio_tls.c: 1254: SSL connected (secure)
Verbunden.
6:2019/01/18 00-00-34:gwen(5600):syncio_socket.c:  266: Disconnected socket
Verbindung beendet.
6:2019/01/18 00-00-34:gwen(5600):syncio_http.c:  138: Not connected
Zertifikat erhalten
Abruf des Zertifikats: Finished.
```

Performing the same request on linux works as expected:

Linux

```
Abruf des Zertifikats: Started.
Verbindung vorbereiten
Mit Server verbinden...
6:2019/01/17 23-59-33:gwen(14958):syncio_tls.c:  940: Connecting base layer
Hostname "hbci-pintan.gad.de" wird aufgelöst...
IP-Adresse ist "194.149.255.76"
Verbindung zu "hbci-pintan.gad.de" wird aufgebaut
6:2019/01/17 23-59-33:gwen(14958):syncio_socket.c:  244: Connected to "hbci-pintan.gad.de"
Verbunden mit "hbci-pintan.gad.de"
6:2019/01/17 23-59-33:gwen(14958):syncio_tls.c:  946: Base layer connected
6:2019/01/17 23-59-33:gwen(14958):syncio_tls.c:  269: Preparing SSL (00000014)
6:2019/01/17 23-59-33:gwen(14958):syncio_tls.c:  277: Init as client
6:2019/01/17 23-59-33:gwen(14958):syncio_tls.c:  384: Using default ca-bundle from [/usr/share/gwe
nhywfar/ca-bundle.crt]
6:2019/01/17 23-59-33:gwen(14958):syncio_tls.c:  413: Added 168 trusted certs
6:2019/01/17 23-59-33:gwen(14958):syncio_tls.c:  612: Key stored within certificate, extracting (m
odlen=257, explen=3)
6:2019/01/17 23-59-33:gwen(14958):syncio_tls.c:  662: Checking hostname [hbci-pintan.gad.de]
6:2019/01/17 23-59-33:gwen(14958):syncio_tls.c:  671: Cert is for this server
5:2019/01/17 23-59-33:aqbanking(14958):abgui.c:  165: Automatically accepting certificate [32:16:E
A:C7:1D:8E:55:B7:A5:AD:3A:7D:46:23:9F:E8]
6:2019/01/17 23-59-33:gwen(14958):syncio_tls.c: 1013: SSL connected (secure)
Verbunden.
6:2019/01/17 23-59-33:gwen(14958):inetsocket.c:  281: Closing socket 4
6:2019/01/17 23-59-33:gwen(14958):syncio_socket.c:  266: Disconnected socket
Verbindung beendet.
6:2019/01/17 23-59-33:gwen(14958):syncio_http.c:  138: Not connected
Zertifikat erhalten
Abruf des Zertifikats: Finished.
```

The difference are to the following lines

```
6:2019/01/17 23-59-33:gwen(14958):syncio_tls.c:  384: Using default ca-bundle from [/usr/share/gwe
nhywfar/ca-bundle.crt]
6:2019/01/17 23-59-33:gwen(14958):syncio_tls.c:  413: Added 168 trusted certs
```

The source (https://github.com/aqbanking/gwenhywfar/blob/07716cbff92b53bb1c81418e85abaaca11c78e88/src/sio/syncio_tls.c#L475) shows that on Windows there is currently no support for using the default ca bundle. Because the ca bundle is installed also on Windows it should be possible to add related support.

In contrast to Unix/Linux, where an installation is based on absolute paths, an installation of gwenhywfar on Windows must be portable, i.e. the file path of ca-bundle.crt must be determined relative to the directory in which the binaries of gwenhywfar are contained, which is <executable-path>/../share/gwenhywfar for default installations.

History

#1 - 01/18/2019 11:47 AM - rhabacker

- File gwenhywfar-default-bundle-support-on-windows.patch added

Related patch appended

#2 - 01/31/2019 08:03 AM - rhabacker

Priorität: Normal

I did not find a way to increase the priority, but I think this is a major issue on Windows because it concerns connection security

#3 - 08/31/2019 09:55 AM - rhabacker

Since this patch is not yet included https://github.com/aqbanking/gwenhywfar/blob/branch-4/src/sio/syncio_tls.c#L424, I ask again that this patch be applied to git branch-4 and master,so that it will be included in future versions.

#4 - 09/01/2019 08:39 PM - martin

- Status changed from New to Closed

Patch applied to both branches.
Thanks!

Files

gwenhywfar-default-bundle-support-on-windows.patch	1.55 KB	01/18/2019	rhabacker