strongSwan - Bug #1370

Attribute Certificate's Authority Key Identifier extension's encoding is invalid

29.03.2016 10:50 - Joni Eskelinen

Status:	Closed	**Start date:**	29.03.2016
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	pki		
Target version:	5.5.0		
Affected version:	5.4.0	**Resolution:**	Fixed

Description

Authority Key Identifier extension in Attribute Certificate is broken when generated using ipsec pki --acert.

Steps to reproduce

Generate certificates:

```
ipsec pki --gen > ca.key &&
ipsec pki --self --in ca.key --dn "C=CH, O=strongSwan, CN=strongSwan CA" --ca > ca.crt &&
ipsec pki --gen > peer.key &&
ipsec pki --pub --in peer.key | ipsec pki --issue --cacert ca.crt --cakey ca.key --dn "C=CH, O=str
ongSwan, CN=peer" > peer.crt &&
ipsec pki --acert --in peer.crt --issuercert ca.crt --issuerkey ca.key > ac.crt
```

Extract extension DER (look for hex dump of X509v3 Authority Key Identifier):

```
openssl asn1parse -inform der -in ac.crt
```

Decode DER:

```
echo '305E75...' | xxd -r -p | openssl asn1parse -inform der
```

Decoding fails and results in varying error code, eg:

```
Error in encoding
139903245252240:error:0D07209B:asn1 encoding routines:ASN1_get_object:too long:asn1_lib.c:147
```

Associated revisions

Revision 9aaea4db - 06.06.2016 13:46 - Tobias Brunner

x509: Properly wrap keyid in authorityKeyIdentifier in attribute certificates

The correct encoding got lost in bdec2e4f5291 ("refactored openac and
its attribute certificate factory").

Fixes #1370.

History

#1 - 31.03.2016 12:37 - Tobias Brunner

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

- Target version set to 5.5.0

Yes, looks like the key identifier is not wrapped properly (it was at some point, but that got lost during a refactoring eight years ago). Please try the fix in the *1370-acert-authkeyid* branch.

#2 - 06.06.2016 13:47 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed