# strongSwan - Bug #3589

## scepclient invalid encoding of signedAttrs

09.10.2020 15:39 - Marc Garvey

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Tobias Brunner | **Estimated time:** | 0.00 hour |
| **Category:** | scepclient | | |
| **Target version:** | 5.9.1 | | |
| **Affected version:** | 5.8.2 | **Resolution:** | Fixed |

**Description**

Hello,

I tried to use the scepclient command for a scep server project and I found a problem.

The scepclient does not encode the signedAttr of the pkcs#7 container in the correct way.
Because of this invalid encoding, some librarys will fail during the signature check of the message. (In my case bouncycastle)

The signed attributes are defined as a ASN.1 Set

SignedAttributes ::= SET SIZE (1..MAX) OF Attribute
[[https://tools.ietf.org/html/rfc5652#section-5.3]]

It also defines for the signature verification

When the field is present, however, the result is the message
digest of the complete DER encoding of the SignedAttrs value
contained in the signedAttrs field. Since the SignedAttrs value,
when present, must contain the content-type and the message-digest
attributes, those values are indirectly included in the result. The
content-type attribute MUST NOT be included in a countersignature
unsigned attribute as defined in Section 11.4. A separate encoding
of the signedAttrs field is performed for message digest calculation.
The IMPLICIT [0] tag in the signedAttrs is not used for the DER
encoding, rather an EXPLICIT SET OF tag is used. That is, the DER
encoding of the EXPLICIT SET OF tag, rather than of the IMPLICIT [0]
tag, MUST be included in the message digest calculation along with
the length and content octets of the SignedAttributes value.

[[https://tools.ietf.org/html/rfc5652#section-5.4]]

This means that the signed attributes must be encoded as DER structure

The ASN.1 specifikation for an DER Set ist like this

DER encoding. Constructed. Contents octets are the same as for the BER encoding, except that there is an order, namely ascending lexicographic order of BER encoding

[[http://luca.ntop.org/Teaching/Appunti/asn1.html]] 5.15

This is the Dump ASN.1 of the scepclient message (only the part of the signed Attr)

```
1386  197:           [0] {
1389   32:             SEQUENCE {
1391   10:               OBJECT IDENTIFIER senderNonce (2 16 840 1 113733 1 9 5)
1403   18:               SET {
1405   16:                 OCTET STRING 93 FE A2 E7 AC 57 2B C3 79 DB DE B0 D6 60 57 E7
         :                 }
         :               }
1423   48:             SEQUENCE {
1425   10:               OBJECT IDENTIFIER transID (2 16 840 1 113733 1 9 7)
```

```
1437   34:               SET {
1439   32:                 PrintableString 'C910E32E652D9BB47DEA2236CF16B89D'
         :                 }
         :               }
1473   18:             SEQUENCE {
1475   10:               OBJECT IDENTIFIER messageType (2 16 840 1 113733 1 9 2)
1487    4:               SET {
1489    2:                 PrintableString '19'
         :                 }
         :               }
1493   35:             SEQUENCE {
1495    9:               OBJECT IDENTIFIER messageDigest (1 2 840 113549 1 9 4)
1506   22:               SET {
1508   20:                 OCTET STRING
         :                   CA 8A 5D E1 E1 04 6A 44 5B B2 D5 10 34 EE 79 DD
         :                   19 3B 1E F8
         :                 }
         :               }
1530   28:             SEQUENCE {
1532    9:               OBJECT IDENTIFIER signingTime (1 2 840 113549 1 9 5)
1543   15:               SET {
1545   13:                 UTCTime 08/10/2020 10:53:49 GMT
         :                 }
         :               }
1560   24:             SEQUENCE {
1562    9:               OBJECT IDENTIFIER contentType (1 2 840 113549 1 9 3)
1573   11:               SET {
1575    9:                 OBJECT IDENTIFIER data (1 2 840 113549 1 7 1)
         :                 }
         :               }
         :             }
```

This is a dump of the Bouncycastle encoding of the same message which will be used by BC to verify the signature.

```
  0 197: SET {
  3  18:   SEQUENCE {
  5  10:     OBJECT IDENTIFIER messageType (2 16 840 1 113733 1 9 2)
 17   4:     SET {
 19   2:       PrintableString '19'
       :       }
       :     }
 23  24:   SEQUENCE {
 25   9:     OBJECT IDENTIFIER contentType (1 2 840 113549 1 9 3)
 36  11:     SET {
 38   9:       OBJECT IDENTIFIER data (1 2 840 113549 1 7 1)
       :       }
       :     }
 49  28:   SEQUENCE {
 51   9:     OBJECT IDENTIFIER signingTime (1 2 840 113549 1 9 5)
 62  15:     SET {
 64  13:       UTCTime 08/10/2020 10:53:49 GMT
       :       }
       :     }
 79  32:   SEQUENCE {
 81  10:     OBJECT IDENTIFIER senderNonce (2 16 840 1 113733 1 9 5)
 93  18:     SET {
 95  16:       OCTET STRING 93 FE A2 E7 AC 57 2B C3 79 DB DE B0 D6 60 57 E7
       :       }
       :     }
113  35:   SEQUENCE {
115   9:     OBJECT IDENTIFIER messageDigest (1 2 840 113549 1 9 4)
126  22:     SET {
128  20:       OCTET STRING CA 8A 5D E1 E1 04 6A 44 5B B2 D5 10 34 EE 79 DD 19 3B 1E F8
       :       }
       :     }
150  48:   SEQUENCE {
```

```
152  10:     OBJECT IDENTIFIER transID (2 16 840 1 113733 1 9 7)
164  34:     SET {
166  32:       PrintableString 'C910E32E652D9BB47DEA2236CF16B89D'
       :       }
       :     }
       :   }
```

You will see that the ordering is different thats why the digest inside the signature is different.
I know exactly that is never a good idea to reencode a ASN.1 message because something like this could happen during the signature verification, but nevertheless the scep client should encode the message correctly.

Best regards
Marc

### Associated revisions

**Revision c5baa4cb - 27.10.2020 11:21 - Tobias Brunner**

pkcs7: Order DER encoded attributes

The attributes are encoded as a SET OF, which means that in DER encoding
the encoded attributes have to be ordered lexicographically.

Fixes #3589.

### History

**#1 - 09.10.2020 18:09 - Tobias Brunner**

*- Tracker changed from Issue to Bug*

*- Category set to scepclient*

*- Status changed from New to Feedback*

*- Assignee set to Tobias Brunner*

*- Target version set to 5.9.1*

> I tried to use the scepclient command for a scep server project and I found a problem.
>
> The scepclient does not encode the signedAttr of the pkcs#7 container in the correct way.

Just because I feel I need to mention it, did you read the note on scepclient? But considering that, I wonder why nobody ever noticed this during the last 15 years. I guess some parsers/servers just accept the SET in any order and use it as it was received when verifying the signature (i.e. without re-encoding).

> DER encoding. Constructed. Contents octets are the same as for the BER encoding, except that there is an order, namely ascending lexicographic order of BER encoding

ASN.1 is really idiotic sometimes. Let's define SET OF as "an **unordered** collection of zero or more occurrences of a given type", but then, just for the fun of it, let's order the items when encoding for no apparent reason.

But yeah, that was clearly incorrect. Luckily it seems to be the only place where we encode a SET OF with more than one element. I pushed a fix to the *3589-pkcs7-attr* branch. Let me know if that works for you.

**#2 - 12.10.2020 10:34 - Marc Garvey**

Hello, yes I have read this notice and I would not open a ticket for a missing feature.

anyways thanks for this fast response. I will check this branch.

**#3 - 27.10.2020 11:28 - Tobias Brunner**

*- Status changed from Feedback to Closed*

*- Resolution set to Fixed*