CR-Form-v7

# PSEUDO CHANGE REQUEST

⌘ 33.310 CR - ⌘rev - ⌘ Current version: 1.0.0 ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

***Proposed change affects:*** UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network X

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Sending a CERTREQ |
| ***Source:*** | ⌘ | Nokia, Siemens, T-Mobile |
| ***Work item code:*** | ⌘ | NDS/AF |
| ***Date:*** | ⌘ | 12/01/2004 |
| ***Category:*** | ⌘ | F |
| ***Release:*** | ⌘ | Rel-6 |

*Use one of the following categories:*
***F*** *(correction)*
***A*** *(corresponds to a correction in an earlier release)*
***B*** *(addition of feature),*
***C*** *(functional modification of feature)*
***D*** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*

| | |
|---|---|
| *2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | There are at least four alternatives concerning sending the CERTREQ<br><br>1) do not send CERTREQ at all<br><br>2) send an empty CERTREQ<br><br>3) configure n CA names to SEG and send n CERTREQ's<br>- CA names can be generated according to cross-certs<br><br>4) configure CA names to SEG specific to each ISAKMP policy and send only one CERTREQ<br>- This might not even be possible in IKE main mode, since CERTREQ needs to be sent before peer ID payload is received. So ISAKMP policy should be obtained according to IP header source address.<br><br>Analysis:<br>1) Some peers would not send CERT at all.<br>2) Denied by pki-profile draft, but still the current practise.<br>3) Would reveal which CA's operator trusts.<br>4) Might imply implementation changes. |
| ***Summary of change:*** | ⌘ | Added a recommendation about at least sending an empty CERTREQ for interoperability reasons. |
| ***Consequences if not approved:*** | ⌘ | Ambiguous specification on sending the CERTREQ |

| | | | | | |
|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 6.2.1 IKE Phase-1 profiling | | | |
| ***Other specs affected:*** | ⌘ | Y | N | | |
| | | | N | Other core specifications | ⌘ |
| | | | N | Test specifications | |
| | | | N | O&M Specifications | |
| ***Other comments:*** | ⌘ | - | | | |

---

---------- CHANGED SECTION ----------

---

## 6.2.1 IKE Phase-1 profiling

The Internet Key Exchange protocol shall be used for negotiation of IPsec SAs. The following requirements on IKE in addition to those specified in NDS/IP [1] are made mandatory for inter-security domain SA negotiations over the Za-interface.

For IKE Phase 1 (ISAKMP SA):

- The use of RSA signatures for authentication shall be supported;
- The identity of the CERT payload (including the SEG certificate) shall be used for policy checks;

  *Motivation: ISAKMP contains two different payloads that allow the specification of the endpoint identity, the ID payload and the CERT payload. Within the NDS/AF framework only the SEG certificate is sent within IKE Phase 1 so there will be no ambiguity is selecting the peer ID from the received certificates. See also section 3.1.2 of draft-ietf-ipsec-pki-profile-02.txt on Endpoint identification.*

- Initiating/responding SEG are required to send certificate requests in the IKE messages;

  *Motivation: suggested by draft-ietf-ipsec-pki-profile-02.txt to avoid interoperability problems*

NOTE: At least an empty CERTREQ should be sent to avoid interoperability problems.

- Cross-certificates shall not be sent by the peer SEG as they are pre-configured in the SEG;

  *Motivation: avoiding known problems (see clause 5.3.5.2)*

- The SEG shall always send its own certificate in the certificate payload of the last (third) IKE Main Mode message;

  *Motivation: avoids the need to cache Peer SEG certificates.*

- The certificates in the certificate payload shall be encoded as type 4 (X.509 Certificate – Signature);
- The lifetime of the Phase 1 IKE SA shall be limited to at most the remaining validity time of the peer SEG certificate.

NOTE: Depending on the availability of DNS between peer SEGs, the following rule is applied:

- subjectAltName and ISAKMP policy should both contain IP address (in case DNS is not available);
- subjectAltName and ISAKMP policy should both contain FQDN (in case DNS is available).