3GPP TSG SA WG3 Security — S3#29 **S3-030379**

15 – 18 July 2003

San Francisco, USA

Source: **Nokia, Siemens, SSH, T-Mobile**

Title: **NDS/AF – Fetching Cross-Certificates**

Document for: **Discussion**

Agenda Item: **7.4**

1. INTRODUCTION

SEGs need to resolve and validate the certification path upto their trusted roaming CA. A cross-certificate that allows to trust the partner PLMN is not sent within the IKE payload and needs to be fetched from some local storage.

This discussion paper compares methods to fetch cross-certificates to the SEG.

There are two different methods for fetching cross-certificates during the IKE phase 1 negotiation:

- directly from the local SEG where they have been stored upon the cross-certification procedure
- using LDAP from the Certificate Repository (CR) where they have been stored upon the cross-certification procedure

Here we assume that operator's Certificate Repository (CR) may contain both CRLs and actual (cross-)certificates.

2. CROSS-CERTIFICATION

Both operators use the following procedure to create cross-certificates:

1. The roaming CA creates a PKCS#10 certificate request, and sends it to the other operator.
2. The roaming CA receives a similar request from the other operator.
3. The roaming CA accepts the request and creates a new cross-certificate.
4. If LDAP is not used to fetch cross-certificates the new cross-certificate is stored into all SEGs. If LDAP is used to fetch cross-certificates the cross-certificate is stored once into the CR.

3. REVOKING A CROSS-CERTIFICATE

The following procedure is used to revoke a cross-certificate:

1. The cross-certificate is added into the CRL.
2. If LDAP is not used to fetch cross-certificates the cross-certificate is removed from all SEGs. If LDAP is used to fetch cross-certificates the cross-certificate is removed once from the CR.

4. AUTHENTICATION DURING THE IKE PHASE 1

Authentication during the IKE Phase 1 is shown in the figure 1 below. The SEGa uses the following procedure to authenticate the SEGb:

1. SEGa requests SEGb's certificate using the IKE certificate request payload
2. SEGa receives SEGb's certificate inside the IKE certificate payload
3. SEGa fetches a CRL from the (public) CRb if the locally cached CRL has not yet expired.
4. SEGa uses this CRL to verify the status of SEGb's certificate
5. SEGa uses either the locally cached cross-certificate or fetches the cross-certificate from the (local) CRa
6. SEGa fetches a CRL from the (local) CRa if the locally cached CRL has not yet expired.
7. SEGa uses this CRL to verify the status of the cross-certificate
8. SEGa verifies the status of roaming CAa certificate if roaming CAa is not a top-level CA otherwise roaming CAa is implicitly trusted.
9. SEGa authenticates the SEGb (verifies signatures)

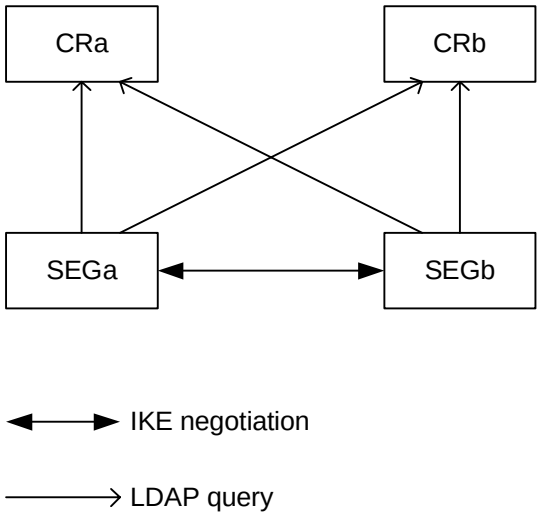

Figure 1. Fetching Cross-Certificates and CRLs.

5. SUMMARY AND CONCLUSIONS

The following table summarizes differences between alternatives:

Issue	**A) Cross-certificates are stored into SEGs:**	**B) Cross-certificates are stored into CRs:**	**C) Cross-certificates are stored into CRs and cached in SEGs upon usage:**
1) Initialization issues: storing the cross-certificate during the cross-certification	The cross-certificate is *initially* stored in several places, that is, into *all* SEGs (estimated number is between 2 and 10). Pros: - Cons: Certificate must be initially copied in several places. SEGs from different manufacturers may have other O&M interfaces to handle the certificates.	The cross-certificate is *initially* stored in CR. Pros: The handling is fully standardized. Certificate is initially copied in one place only. The operator should have the repository anyway (due to CRL handling). Cons: -	The cross-certificate is *initially* stored in CR. Pros and cons as in B).
2) Usage issues: latency during the IKE Phase 1	Pros: No extra latency Cons: -	Pros: - Cons: More latency caused by extra LDAP query (the cross-certificate is queried)	Pros & cons: as in B) at the first time, and as in A) at subsequent times
3) Cleanup issues: removing the cross-certificate NOTE: this functionality is needed only to be able to revoke cross-certificates before the next CRL gets published.	Pros: - Cons: The cross-certificate has to be removed from several places, that is, from *all* SEGs	Pros: The cross-certificate has to be removed from one single place only Cons: -	Pros: - Cons: The cross-certificate has to be removed from *both* CR *and* each SEG.
4) Security issues	Pros: No single point of failure exists. Cons: -	Pros: - Cons: CR represents a single point of failure suitable for an attacker, e.g. to submit a denial of service attack by breaking the communication at the CR.	Pros: Single point of failure partly mitigated Cons: -

Analysis:

- Alternative B) requires one additional LDAP query in every IKE Phase 1 negotiation and will introduce new error cases

- Latency of LDAP: information from LDAP to local disk is cached and populating it takes some time, but in practice this time is not significant.

- The benefit of alternative B) and C) compared to alternative A) is easier management, that is, storing and removing the certificate in/from one single place only.

Conclusion: alternative C) is the most feasible choice, because it combines good points of alternatives A) and B). It is proposed that the C) alternative (i.e. cross-certificates are stored into CRs, fetched with LDAP and cached in SEGs) is chosen as a working assumption in the NDS/AF work.