06 - 10 October 2003

Povoa de Varzim, Portugal

Title:	**Adding domain component support to NDS/AF certificate profiles**
Source:	**Nokia, Siemens, SSH, T-Mobile**
Agenda item:	**7.4**
Document for:	**Discussion and decision**

1 Introduction

This contribution discusses the addition of domain component (dc) support to the certificate subject and issuer names in NDS/AF certificate profiles. Currently only the country-organisation (o,c) structure is supported by the draft NDS/AF TS.

An industry leader in directory and PKI research, The Burton Group, has done a survey for companies deploying large scale directories [BURTON]. The study indicates that most people listed the use of dc's as a "best practice", so there is a quite wide support for dc’s already. However, it should be noted that the traditional o,c naming is still used widely.

There are benefits from using the same structure in certificates and directories. If you're mapping structure one way in certificates and another way in the directory, then the possibilities for automatic certificate publishing become very limited and inflexible. Also, it might cause some applications not to work. Thus, it is important that NDS/AF certificates have the possibility to support also domain components in certificate subject names.

Annex A shortly lists the RFCs that support domain components.

2 Discussion

2.1 subjectAltName used for IPsec authentication

PKIX (i.e. [RFC 3280]) requires that compliant implementations must accept dc-structure in subject names. In practise subject name itself is not used in IPsec case as subjectAltName is generally used and this applies also to the NDS/AF environment. From IPsec point of view the Distinguished Name in subject name is a publishing feature and does not affect authentication as such. Subject and Issuer names are mainly meant for directory, and organizing that is operators own decision.

PKIX specificly states that implementations do not have to care about subject name – dns name mapping. This is only to organize a directory tree according to the DNS hierarchy. [RFC3280] denies the usage of subject name instead of subjectAltName dnsname, so there is no problem of utilising possibly flawed information from subject name when correct name is available in the subjectAltName.

2.2 Subject and issuer name

The PKI certificate and CRL profile [RFC3280] states that ‘*implementations of this specification MUST be prepared to receive the domainComponent attribute, as defined in [RFC2247]*’.

Subject and issuer name format in certificate profile according to country-organisation structure:

> *Subject and issuer name format. Note that c is optional element. : cn=<some distinguishing name>, o=<organization name>, (c=<country>)*

Subject and issuer name format with domain components:

> *Subject and issuer name format: cn=<hostname>, ou=<servers>, dc=<domain>, dc=<domain>*

Example for a gateway host which is named ‘*gateway1.companyX.com’*

The ‘gateways’ container could be left out. That just makes it clean if publishing to LDAP [RFC 2252] is desired, so that entries are not scattered all over the top level.

2.3 Name constraint support

Name constraint is basically a clause that defines who to trust or who not to trust based on names on certificates. In case of bridge CA would be desirable in the future, then name constraints would be needed. The domain components have the necessary name constraint support built in. However, it should be noted that the current architecture does not rely on bridge CAs, but instead uses direct cross certifications between the security domains, and no name constraints are needed.

[X.509] requires that name constraints must be hierarchical. Hierarchy is needed in order to be able to define a subtree. It is possible with domain components or DNS names since they have a one-to-one mapping. Domain components and ordering is defined in [RFC2247].

2.4 X.500 naming components with dc’s

Domain components were born from X.500. It inherited the capability to use all of the X.500 naming components. LDAP naming plan is just an extension and loosening of the rules from X.500. It is fully backwards compatible. The standard components can be used in the same DN - they just have be in order like described in [RFC2377].

The only difference is that dc components do not exist in X.500 standards or implementations. The dc components can replace the traditional o,c as a base but they don't have to. The domain components are not restricted to just the base of a DN, however if dc’s are used in an LDAP DN, then there can be no other type between the dc’s.

Example:

Correct: `cn=test person,ou=people,dc=ny,dc=us,dc=company,dc=com`

Incorrect: `cn=test person,dc=ny,ou=people,dc=company,dc=com`

3 Conclusion and proposal

From NDS/AF IPsec authentication point of view the Distinguished Name in certificate subject field is a publishing feature and does not affect the authentication as such, but the domain component support should be possible also as required by the PKIX [RFC 3280].

The proposal is to have domain component support added to the certificate subject and issuer names in NDS/AF certificate profiles in addition to the country-organisation (o,c) structure. Thus the supporting companies propose that the respective pseudo-CR presented to the SA3#30 meeting is approved.

4 References

[RFC3280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC2247] Using Domains in LDAP/X.500 Distinguished Names

[RFC2252] Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions

[RFC2377] Naming Plan for Internet Directory-Enabled Applications

[BURTON] Network strategy methodologies & best practices, Developing a directory namespace and schema, v1, 29 Jan 2001, Dan Blum, Ian Clark, Christy Hudgins

[X.509] ITU-T Recommendation X.509, Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks

Annex: Related RFCs

Domain components are supported by these RFCs:

RFC 1279 - X.500 and domains
RFC 3039 - Internet X.509 PKI Qualified Certificates Profile
RFC 3280 - Internet X.509 PKI Certificate and CRL Profile
RFC 1274 - The COSINE and Internet X.500 Schema
RFC 2164 - Use of an X.500/LDAP directory to support MIXER address mapping
RFC 1838 - Use of the X.500 Directory to support mapping between X.400 and RFC 822 addresses
RFC 3088 - OpenLDAP Root Service - An experimental LDAP referral service
RFC 2459 - Internet X.509 PKI Certificate and CRL Profile
RFC 2377 - Naming Plan for Internet Directory-Enabled Applications
RFC 2253 - LDAPv3: UTF-8 String Representation of Distinguished Names
RFC 2247 - Using Domains in LDAP/X.500 Distinguished Names