

## 7. Pseudonymous System Access through Authorisation Certificates

<u>Identity Certificates:</u>	<u>Authorisation Certificates:</u>
binds an identity to a public key	binds an authorisation to a public key
<u>Requesting party:</u> The person concerned	<u>Requesting party:</u> A customer wishing to access a resource
<u>Issuing Party:</u> The appropriate (government) agency	<u>Issuing Party:</u> The resource owner
<u>Verifying Party:</u> Anyone undertaking an identity check	<u>Verifying Party:</u> The resource owner

Example: SPKI (Simple Public Key Format and Infrastructure) Certificate:

digitally signed record which may be expressed as a 5-tuple (I, S, D, A, V) where

- I = public key or a hash of the public key of the certificate's issuer
- S = subject acquiring the authority (typically its public key, hash of a public key or a local name of the subject in the issuer's local name space)
- D = delegation bit indicating whether the subject has the right to further delegate the rights granted in this certificate
- A = authorisation field (also called tag) specifying the permissions granted by the issuer to the subject
- V = validity field of the certificate.

Purpose: to communicate permission from one keyholder to another

ACL-entry:

like a SPKI certificate, except that it is issued by "self" and need not to be signed: (self, S, D, A,V)

Example:

The bank wants to grant Alice on-line access to her account:

( $K_B$ ,  $K_A$ , yes, access to account X, always)

→ with this certificate, Alice can access her account if she proves to hold the private key corresponding to  $K_A$ .

Alice can give Carl the right to pay her bills while she is on vacation:

( $K_A$ ,  $K_C$ , no, access to account X for paying bills, the time of the vacation)

→ with the chain of the 2 certificates, Carl can pay the bills if he proves to hold the private key corresponding to  $K_C$ .

SPKI certificate with threshold subject:

Subject field is a threshold, i.e. group of N keys, from which k are needed simultaneously.

Example:

2 of 3 managers of a company are needed to approve purchases exceeding \$100000.

(K<sub>company</sub>, 2-of-3 K<sub>manager1</sub> K<sub>manager2</sub> K<sub>manager3</sub>, D, may\_approve\_purchase\_exceeding\_\$100000, V)

SPKI certificates can be chained together into sequences, where:

- the last certificate is a permission certificate
- last certificate is preceded by delegation certificate
- first certificate (or ACL entry) was issued by verifier of the sequence (self)

-> all useful SPKI certificate chains form loops.

### Certificate Chain Reduction:

Given  $(I1, S1, D, A1, V1)$  and  $(I2, S2, D, A2, V2)$   
where  $S1 = I2$

→ (5 tuple reduction rule):

$(I1, S2, D, A, V)$

with  $A = \text{Intersection}(A1, A2)$ ,  $V = \text{Intersection}(V1, V2)$ .

### Reduction with K-of-N threshold certificates:

- make k copies of threshold certificate and indicate which of those copies is handled by that copy
- reduce copies separately
- stop separate reductions when all K of the reduced values have the same subject

## Pseudonymous Accessthrough SPKI Certificate Chains



