

Validity Management in SPKI

24 April 2002

Yki.Kortesniemi@hut.fi (author)

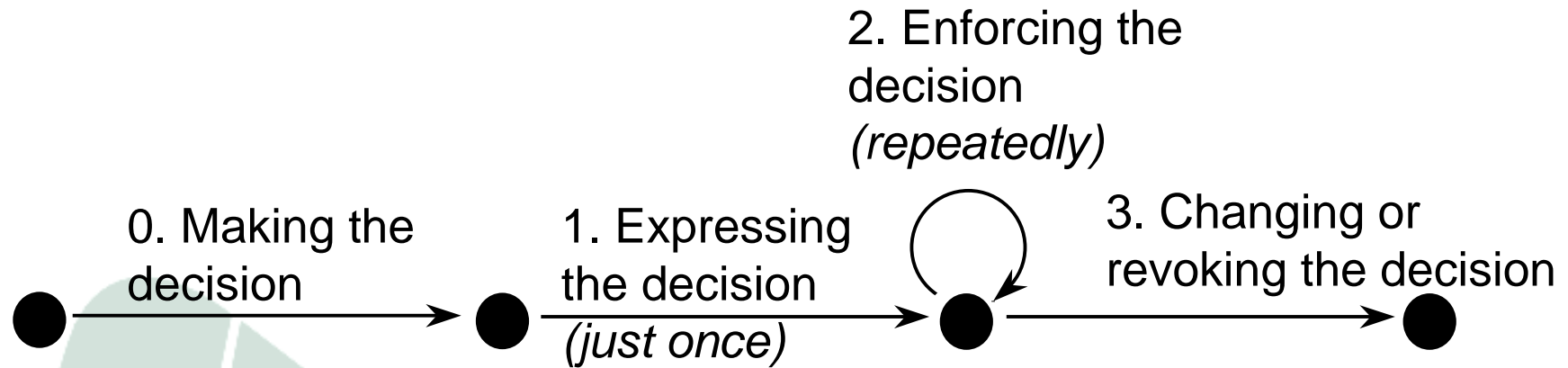
Tero.Hasu@hut.fi (presentation)

INSTITUTE FOR
INFORMATION
TECHNOLOGY

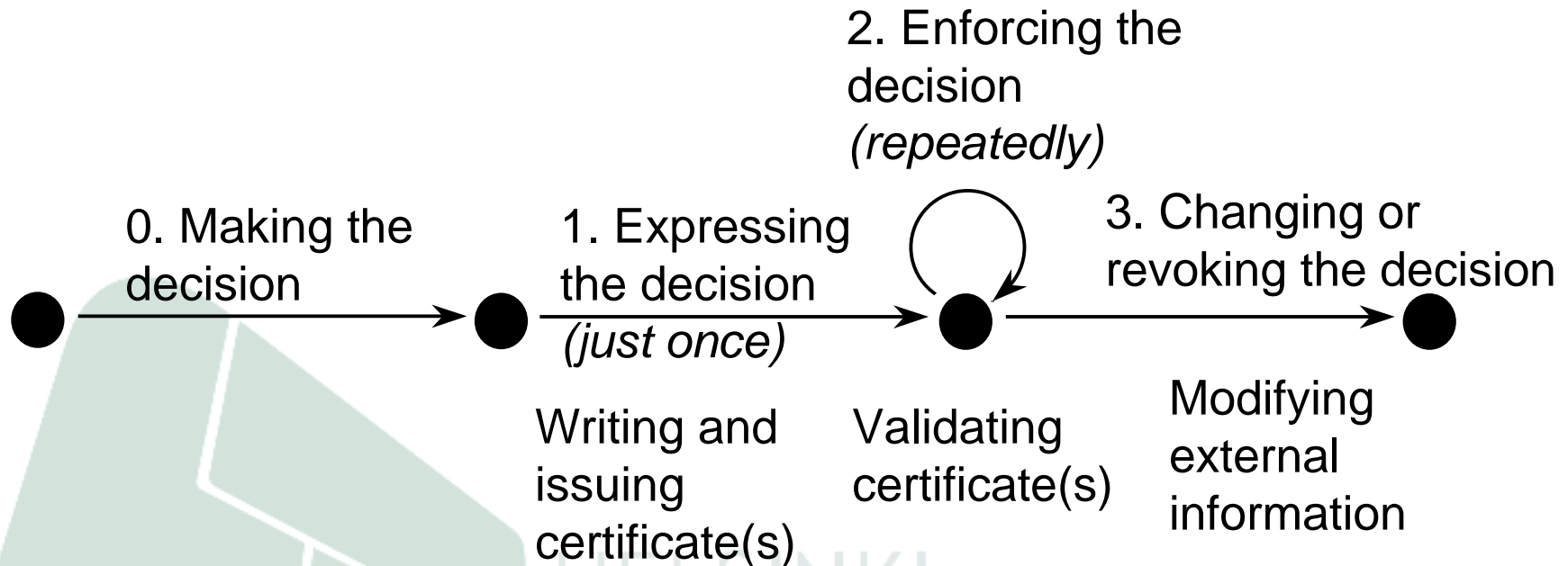
Overview

- Access control
- Types of certificates (and how the type affects validation and revocation)
- Validation and revocation methods in SPKI
- SPKI validity management protocol

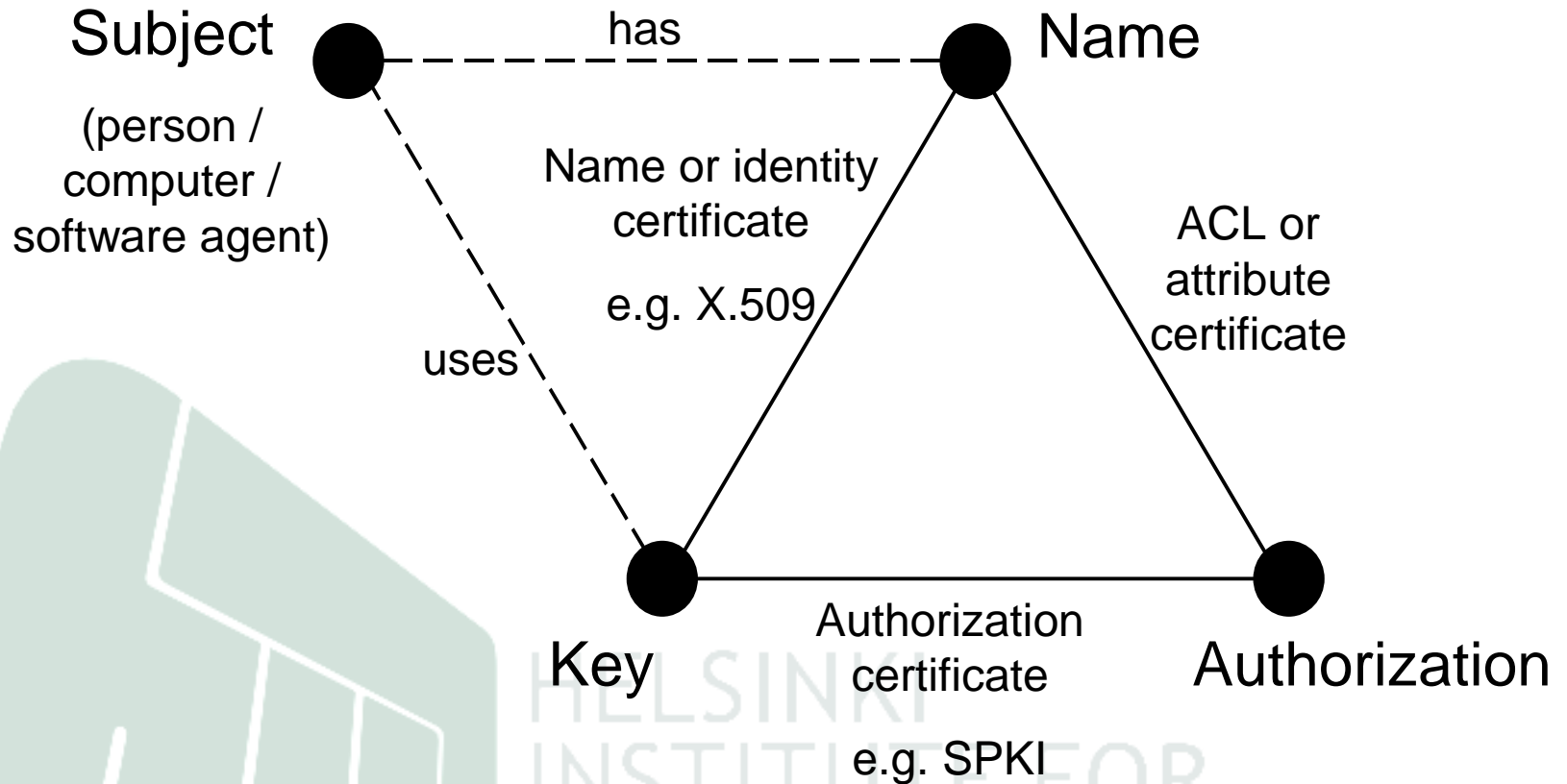
Phases of access control



Access control w/certificates



Types of certificates



HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY

Identity certificates

- Key - Name - Authorization binding proved during validation
 - no anonymity
- Unique name required for each identity across the system
 - otherwise namesakes share rights
 - management burden
- Grouping of rights
 - revoke just one certificate

Authorization certificates

- Key - Authorization binding proved during validation
 - more straightforward
 - performance
- Anonymity is possible
 - benefits privacy of users
 - identity established if required (when acquiring the public key)

Identity certificate issuers

- Capable of establishing identity
- Considered trustworthy
- Typically have plenty of resources
- Small number of issuers (in a system)
- Small number of CRLs
 - may be practical to distribute to access control points

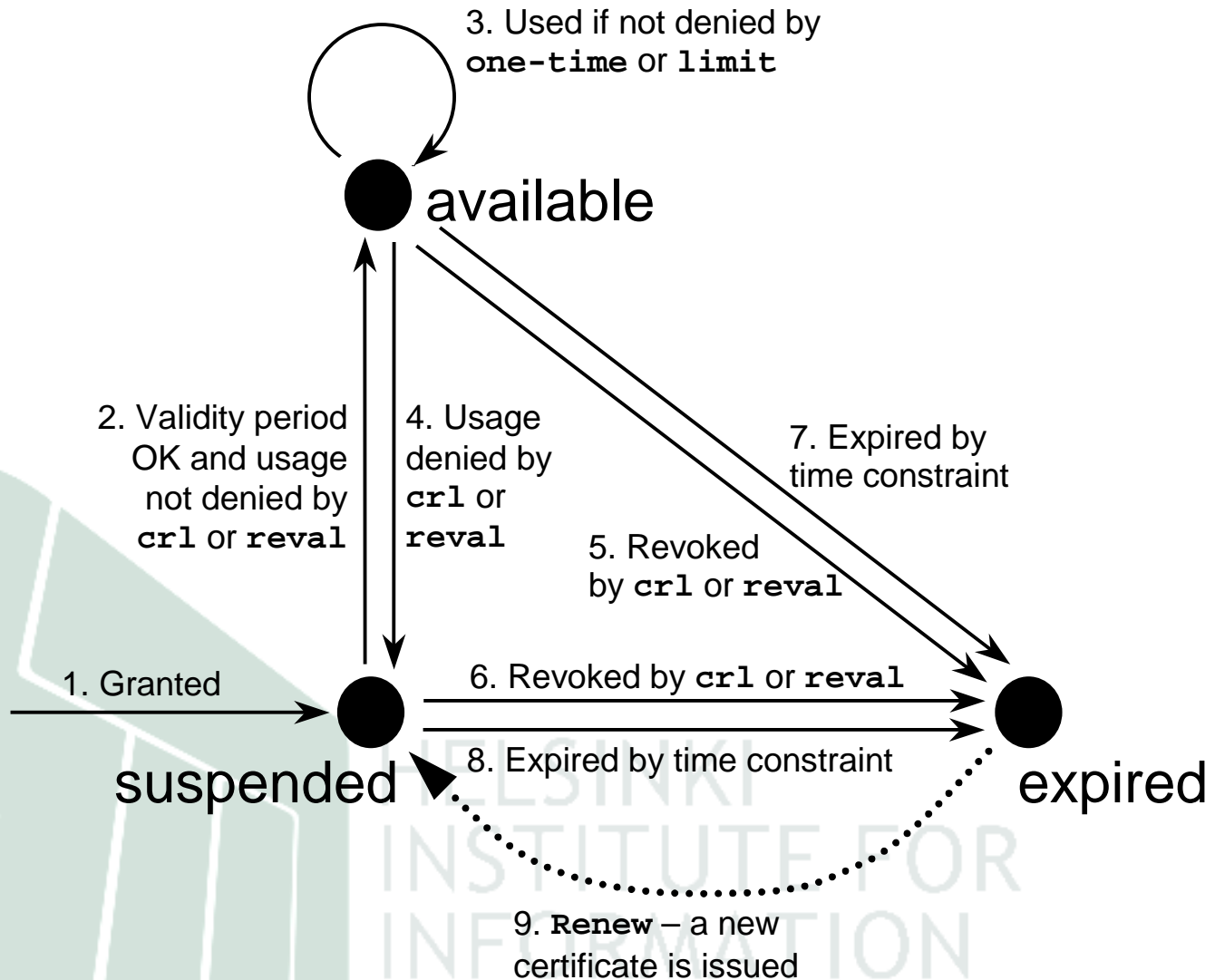
Authorization certificate issuers

- Anyone can be an issuer
- Large number of issuers
- Large number of CRLs
 - impractical to distribute in advance
 - obtain relevant CRLs online when required
- Verifier can also be the issuer
 - issuer arranges revocation mechanisms
 - verifier normally owns protected resource
 - control revocation to balance risk

Validity control in SPKI

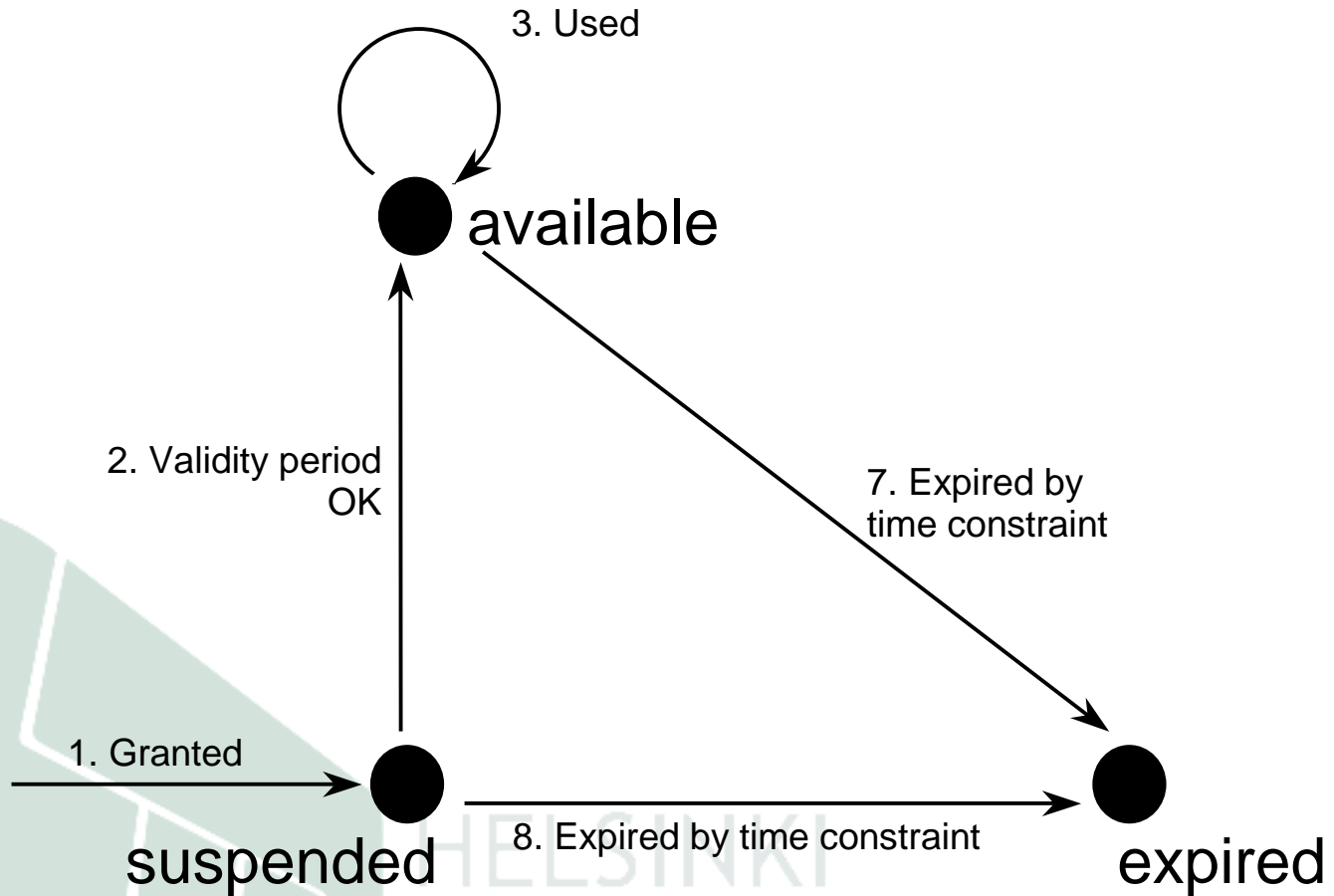
- Has to be considered when issuing a certificate
- Validity period
- Online checks
 - CRL
 - reval
 - one-time
 - limit
 - renew

Lifecycle model

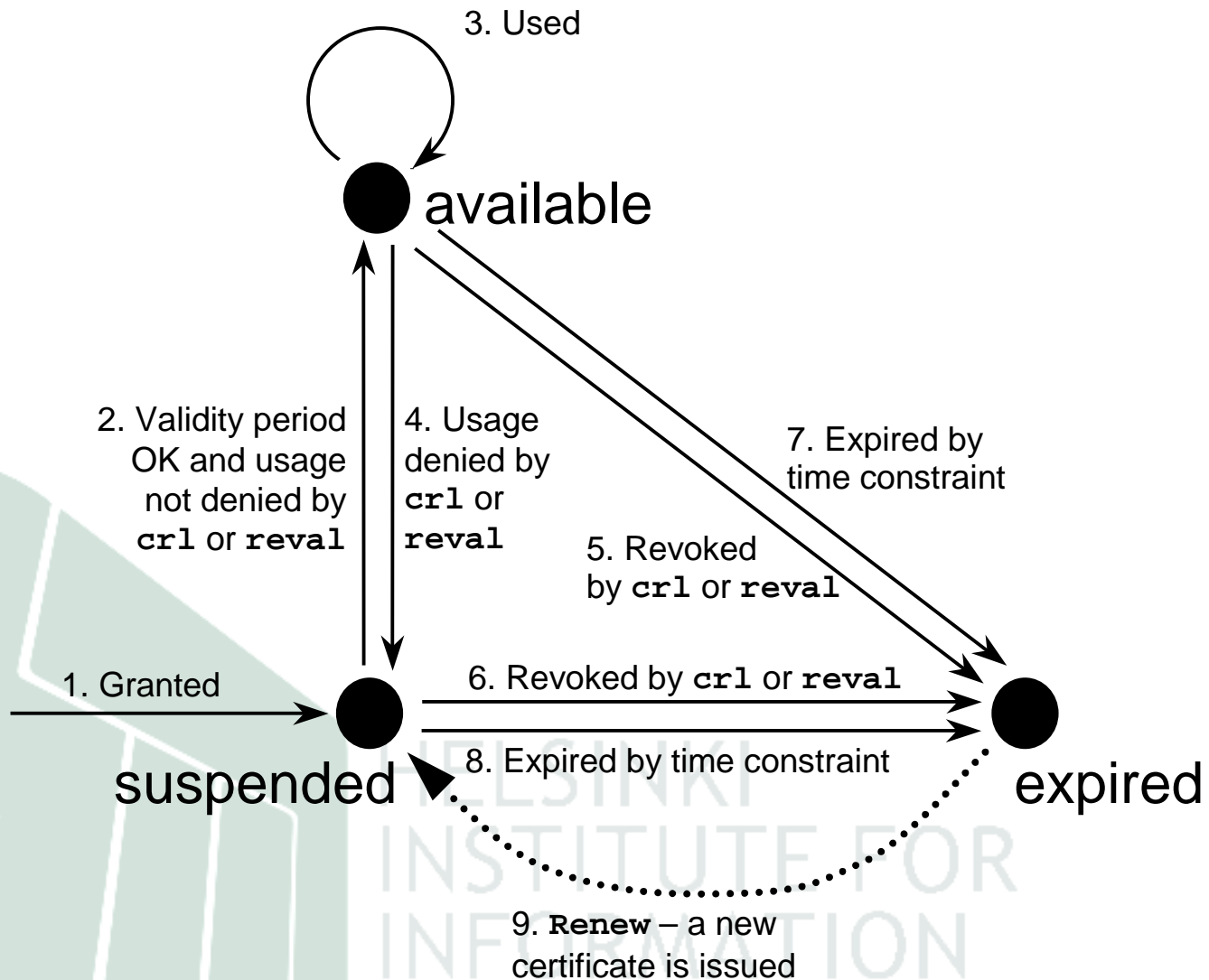


HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY

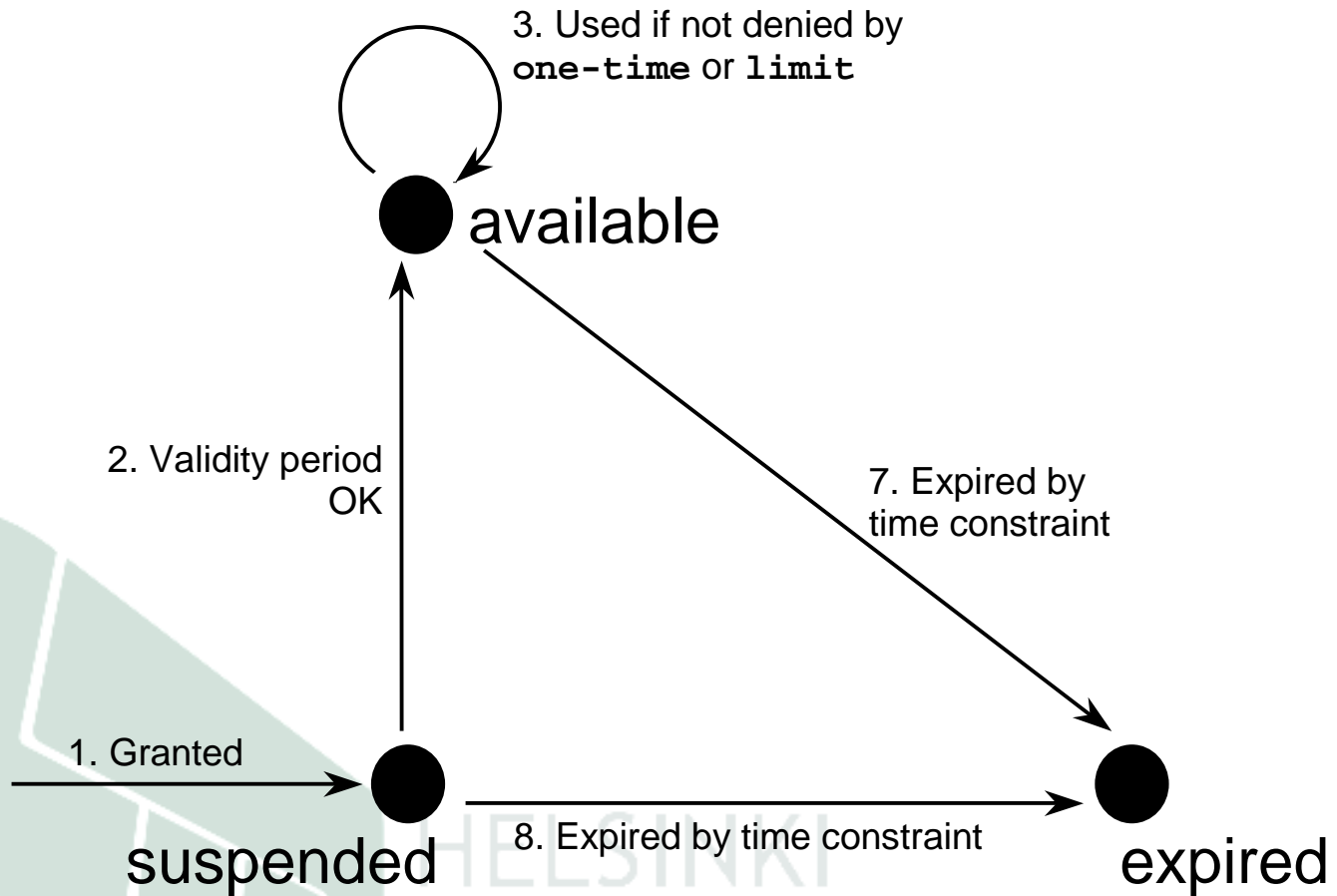
Validity period



CRL, Reval, Renew



One-time, Limit



Summary of methods

Method	Typical use	Processing overhead	Revocation speed
Limit	Quota	High	Immediate
One-time	Limit usage on non-user specific factors	Moderate	Immediate
Reval	Revocation	Low	After current reval validity period
CRL	Revocation	Low	After current crl validity period
Renew	Revocation	Low	After current certificate expires

Management protocol requirements

- Configuration of SPKI validation server
 - can be done remotely
- All SPKI online checks supported
- Certificate issuer can issue commands
 - others need to prove permission
- Status information available
 - use of limited resource can be followed
 - there may be multiple entities with revocation ability

Management protocol design

- Two messages:
 - command
 - reply
- Command message
 - e.g. revoke, re-enable, change quota
 - static and dynamic rules
- Defined in XML
 - signed messages
 - requires secure transport protocol

Command and reply

- server_update cert, chain?,
online_test_hash, delete_request*,
test_definition*, status_query*, signature
- server_reply cert_hash, online_test_hash,
delete_reply*, test_definition_reply*,
status_reply*, service_status, signature

The end

- Questions?
 - (hope not)



HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY