An LDAPv3 Schema for X.509 Certificates

IETF 53, PKIX Meeting

March 20, 2002

Peter Gietz / Norbert Klasen

DAASI International

peter.gietz@daasi.de

Motivation

- Address problem of multiple certificates for one entity
  - How can the client find the right certificate?
- Find a simple and easy to implement solution
- Solution should be usable in the frame of a large scale distributed LDAP / Common Indexing Protocol (CIP) based certificate repository

Schema as a simple solution

- Find a set of certificate fields and extensions that one might want to search upon
  - Meta-data approach
- Parse the certificate and store this set as LDAP attributes
- Advantages:
  - no new server features needed
  - easy to implement in clients
  - usable in a CIP environment

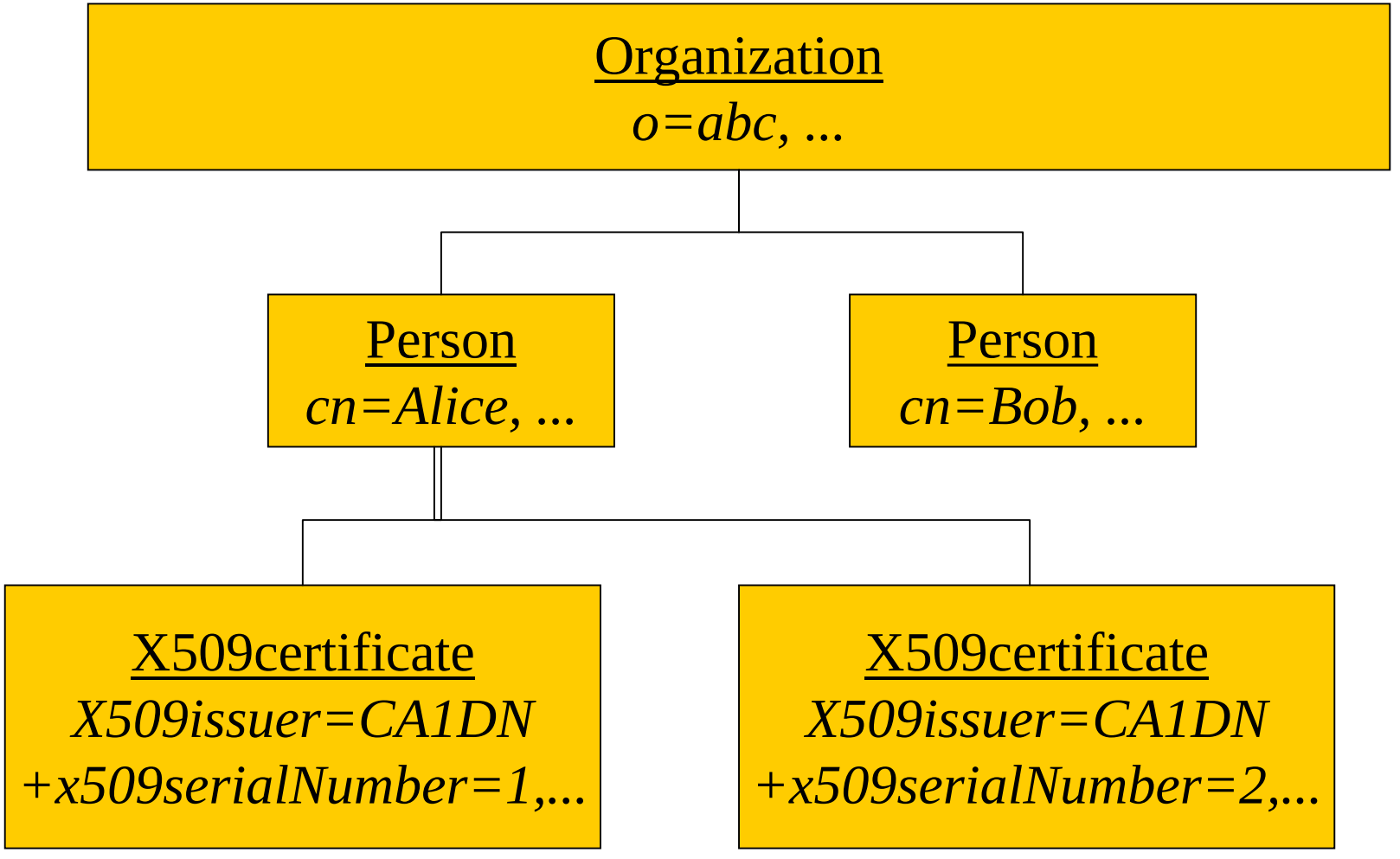
x509certificate object class

(1.3.6.1.4.1.10126.1.5.4.2.1
NAME 'x509certificate'
STRUCTURAL
MUST (x509serialNumber $ x509signatureAlgorithm $ x509issuer $
x509validityNotBefore $ x509validityNotAfter $ x509subject $
x509subjectPublicKeyInfoAlgorithm)
MAY (mail $ x509subjectKeyIdentifier $ x509keyUsage $
x509policyInformationIdentifier $
x509subjectAltNameRfc822Name $ x509subjectAltNameDnsName $
x509subjectAltNameDirectoryName $ x509subjectAltNameURI $
x509subjectAltNameIpAddress $ x509subjectAltNameRegisteredID $
x509isssuerAltNameRfc822Name $ x509isssuerAltNameDnsName $
x509isssuerAltNameDirectoryName $ x509isssuerAltNameURI $
x509isssuerAltNameIpAddress $ x509isssuerAltNameRegisteredID $
x509extKeyUsage $ x509cRLDistributionPoint))

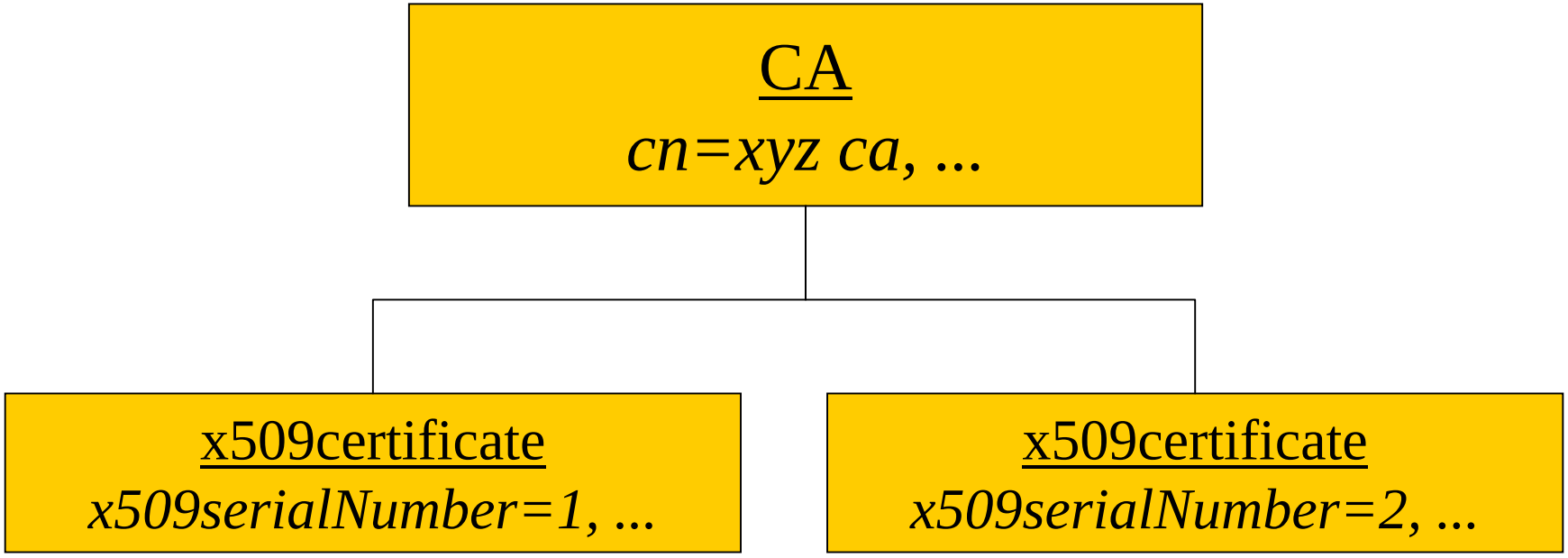
Additional rule

- Entries MUST also have one of the two auxiliary object classes:
  - "pkiUser"
  - "pkiCA".
- This way the entry will contain the binary certificate in on of the two attributes:
  - "userCertificate"
  - "caCertficate"

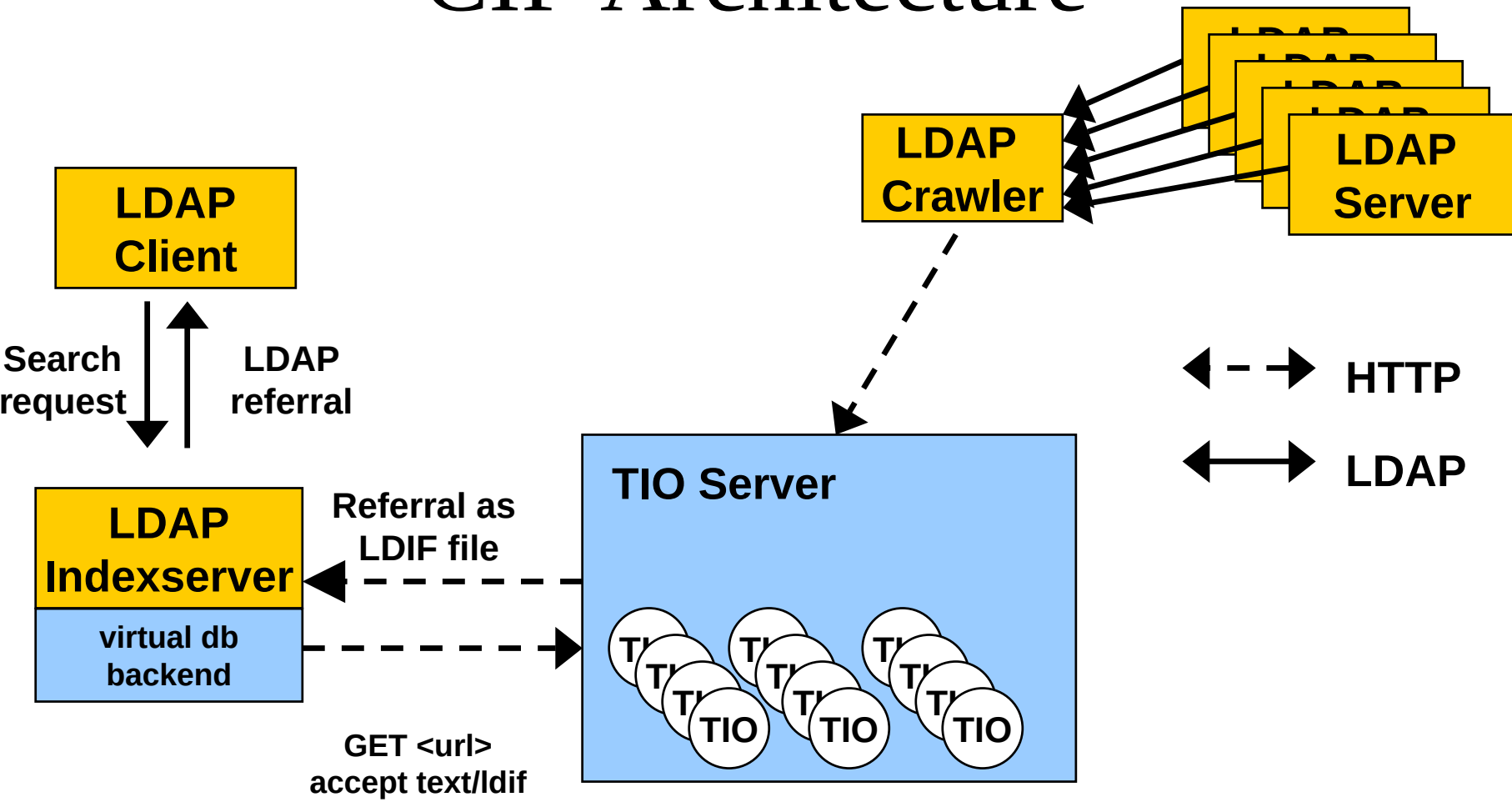
DIT Structure in white-pages services



DIT Structure
in certificate repositories



CIP Architecture



Related work

- This approach:
  - Greenblatt, B., "LDAP Object Class for Holding Certificate Information", Internet Draft (work in progress, expired), Februar 2000, draft-greenblatt-ldap-certinfo-schema-02.txt
- The smarter but more complex solutions:
  - Chadwick, D. and S. Mullan, "Returning Matched Values with LDAPv3", Internet Draft (work in progress, expired), December 2000, draft-ietf-ldapext-matchedval-05.txt
  - Legg, S., "LDAP & X.500 Component Matching Rules", Internet Draft (work in progress), March 2002, draft-legg-ldapext-component-matching-06.txt

Where do we want to go from here?

- Make this part of PKIX work
  - Get comments from this group and integrate them
  - Integrate references to other PKIX WG
- Discuss component matching approach
- Include a use case chapter
- Include IANA consideration
- Fix bugs and language
- Publish as proposed or experimental RFC
- Do similar work for revocation information