
# Distinguished problems with distinguished names

***Openssl legacy and RFC 2253 formats***

Krzysztof Benedyczak

# What is a DN?

- DN is an ordered list of unordered sets of attribute type and value pairs.
  - unordered set is called RDN (RelativeDN)
  - attribute type and value is called AVA
  - multivalued RDNs are rare.
- Each attribute value has its type.
  - PrintableString, UTF8String and IA5String are by far the most common, there are few others rarely occurring.
- AVAs are defined as OIDs with name, description and other metadata. E.g. 1.3.18.0.2.4.110 = billingCountry
  - Some has short labels, some multiple labels, some no label.
- DNs are defined as a binary structure (ASN.1) and are used to identify X.509 certificate principals.

# RFC 2253 format

- Defines reliable parsing and encoding algorithms.
- Does not store an information about AVA value type.
  - Influences case sensitiveness only, sensible default can be usually used using AVA name.
- Syntax:
  - RDNs are written in reversed order separated by ','.
  - AVAs of one RDN are glued with '+'.
  - There are escaping rules defined, rules for names presentation and for encoding not printable values.
- Example:

  CN=Krzysztof Benedyczak,OU=ICM+O=UWAR,C=PL

# Why should I care?

- DNs are often:
  - presented to users (end-, admins)
  - checked for equality (policies, lookups)
    - Often in security area!
- In all the cases a text representation must be used.
- Presenting can be tricky. Which one is better:

  2.5.4.3=#04024869

  CN=Lučić
- Comparison is super-difficult:

  OU=Sales+CN=Lučić,O=Widget Inc.,countryName=us

  2.5.4.3=#04024869+OU=Sales,O=Widget Inc.,C=US

  those are the same guys!
  Note: PrintableString is not case sensitive. UTF8String is.

# Openssl legacy format

- Globus and its heirs used an old Openssl-inspired format for DNs.
- The format is not defined anywhere.
- Implementations are not coherent.

  RFC `CN=gateway/hyx.plgrid.icm.edu.pl,O=ICM+C=PL`

  ossl `/C=PL/O=ICM/CN=gateway/hyx.plgrid.icm.edu.pl`

  ossl `/C=PL+O=ICM/CN=gateway/hyx.plgrid.icm.edu.pl`
- The most important problems:
  - escaping (e.g. '/')
  - encoding of not printable letters
  - encoding of multi RDNs ('+' or '/' which is ambiguous?)

# How RFC 2253 is handled?

- A big map of attribute names, labels and OIDs is implemented.
  - all mandatory and commonly used.
  - more then 100 entries in total!
- Equality test:
  - the input DNs are parsed to produce semantic representations (may have invalid types!) using the map.
  - the semantic representations are normalized using the 10 step algorithm: http://docs.oracle.com/javase/6/docs/api/javax/security/auth/x500/X500Principal.html#getName(java.lang.String)

    ... with additional fixes(!) applied in CANL before it.
  - string equality on normalized values is performed.