Wildcards in DNS Names

Stefan Santesson
Microsoft
stefans@microsoft.com
Background

• First introduced by Netscape
• Only used for Web Server “SSL” certificates
• Microsoft followed and now fully support wildcard certificates
• Issued by a wide range of CAs
How does it work

• Wildcard examples
  – *.example.com
  – a*.example.com

• Illegal
  – www.*.example.com (only in leftmost label)

• Where
  – SubjAltName (dNSName)
  – commonName (only first if several and only when EKU=ServerAuth)
Name constraints

• Wildcards are fully supported by name constraints processing
• No wildcards are allowed in the name constraints extension itself
Exceptions

• If a label contains punycode, no wildcards are allowed. I.e. A wildcard can only be combined with ascii characters in the same label
• No wild cards in the middle of a string
Current situation

• Wildcard certs are widely deployed
• They will not go away
• They are not compatible with current standards
Ways forward

• Pretend it does not exist and do nothing
• Document this in an informational RFC to allow vendors and service providers to interoperate
• Update 3280bis to make this legal