Karlsruher Institut für Technologie

DNS wildcards in certificates?

Ursula Epting

STEINBUCH CENTRE FOR COMPUTING - SCC

Motivateion and example

Role of FTS2 Service could be overtaken by FTS3 Service by only changing DNS entry pointers

FTS2 nodes with A-records [Domain always .gridka.de]:

fts-node1-kit, fts-node2-kit, fts-node3-kit

Alias fts2-kit

FTS3 nodes A-records

fts3-node1-kit, fts3-node2-kit,...

Alias fts3-kit

So SubjAltNames in certificate:
all of the above nodenames

As time goes by...

Additional new nodes might be installed in the future:
fts-node4-kit (and so forth) and put into production

→ Certificate has to be renewed and names added

→ Admin has to take care and shall not forget
(if he does forget errors occur and the reason has to be found...)

Request by host-admin

So the admin wished to have DNS wildcards in the host certificate

e.g. fts-node?-kit or fts-node*-kit
(Domain gridka.de)

At the moment there is no defintive statement in EuGridPMA rules

Testing

So we were issuing test certificates with DNS wildcards for:

fts-node?-kit and fts-node*-kit
(Domain gridka.de)

However it was not possible to access monitoring pages with firefox (bad cert domain).

Anyone else has experiences?

(Think seen in the wild: *.domain.org)

Discussion

What do people think about DNS-wildcards in certificates?

Should we allow (and test until it works ;) or not?