Named Data Networking

Trust Management Support Tool

Functional Specification

UCLA / REMAP

Third Draft

8.7.2013

Description

There is a need to make trust management on the NDN testbed as simple as possible. The current plan has not found deployment in the 5 months since publication of NDN-0009. The reasons for this are not unrelated to the overall cultural difficulties in testbed management. However, by making trust management as simple as possible, reduction of barriers will service future research in trust management without interfering with other NDN research.

Actors

Operator

An operator is someone trusted by NDN research team to delegate trust for their given namespace/s

User

A user (typically institutional) with an email address.

NDNVPS

The NDN Virtual host where the database and HTTP REST application resides

Needs statements

- NDN user wants to publish content on test bed (ie be authenticated)
- user needs to get a new certificate for a new public key
- user needs to be notified when new cert is ready to be installed
- operator needs to be notified when a user is requesting certification to publish a namespace the operator manages
- operator needs support for key signing / cert generation

Assumptions

- Initial focus is on institutional users, with non-institutional email support in future.
- operator rejection of key or cert will not generate NACK (i.e. don't reply to spammers)
- public keys remain distributed, on a host controlled by operator
- revocation will be possible in the future, leveraging this model / tool
- NDN testbed content can be freely accessed by anyone without authorization – only publishing on official NDN research test bed requires key signing.
- Eventually all is all handled in NDN, but meanwhile, this will be a TCP/IP app – all transactions with NDNVPS are performed over HTTPS REST

- Only the NDNVPS need be securely authenticated; operator identified merely by API key or user/pass
- Institutional emails are easily automatically decomposed into valid trust namespace.
- Eventually we will have to add login for operator to handle approval and custom mapping of users w/o institutional email address
- User receives certificate as email attachment
- A login for cert download / pub key list is nice to have eventually, but not necessary
- Thus there is no UI/login for either operator or user in the first version of this system’s implementation -

Naming

1/ we should follow DNS naming as closely as possible, for entities that have DNS presence.

so: lixia@cs.ucla.edu => /ndn/ucla.edu/cs/lixia (rather than /ndn/ucla.edu/lixia)

(more specific domain is better that more flat, and it is a good thing to have systematic mapping from NDN credential to Internet identity credential)

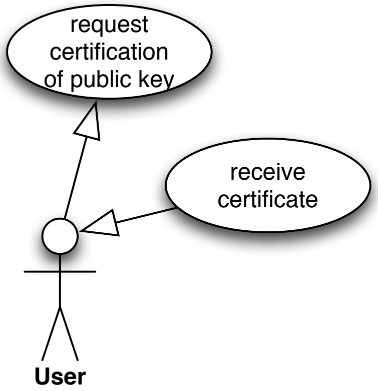
2/ at this time lets first focus on naming NDN team members so we get the cert signing work.

New name spaces like /ndn/ucla.edu/apps/ could be used in some new ways that we need to think about first.

Use cases

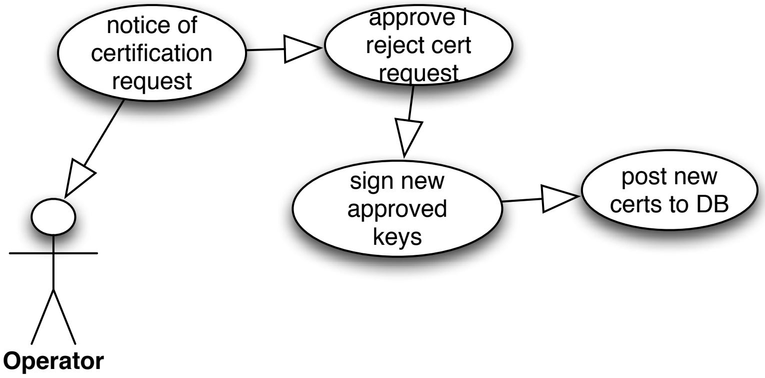
User Experience

This is the path user follows to gain authorization to submit certification requests.



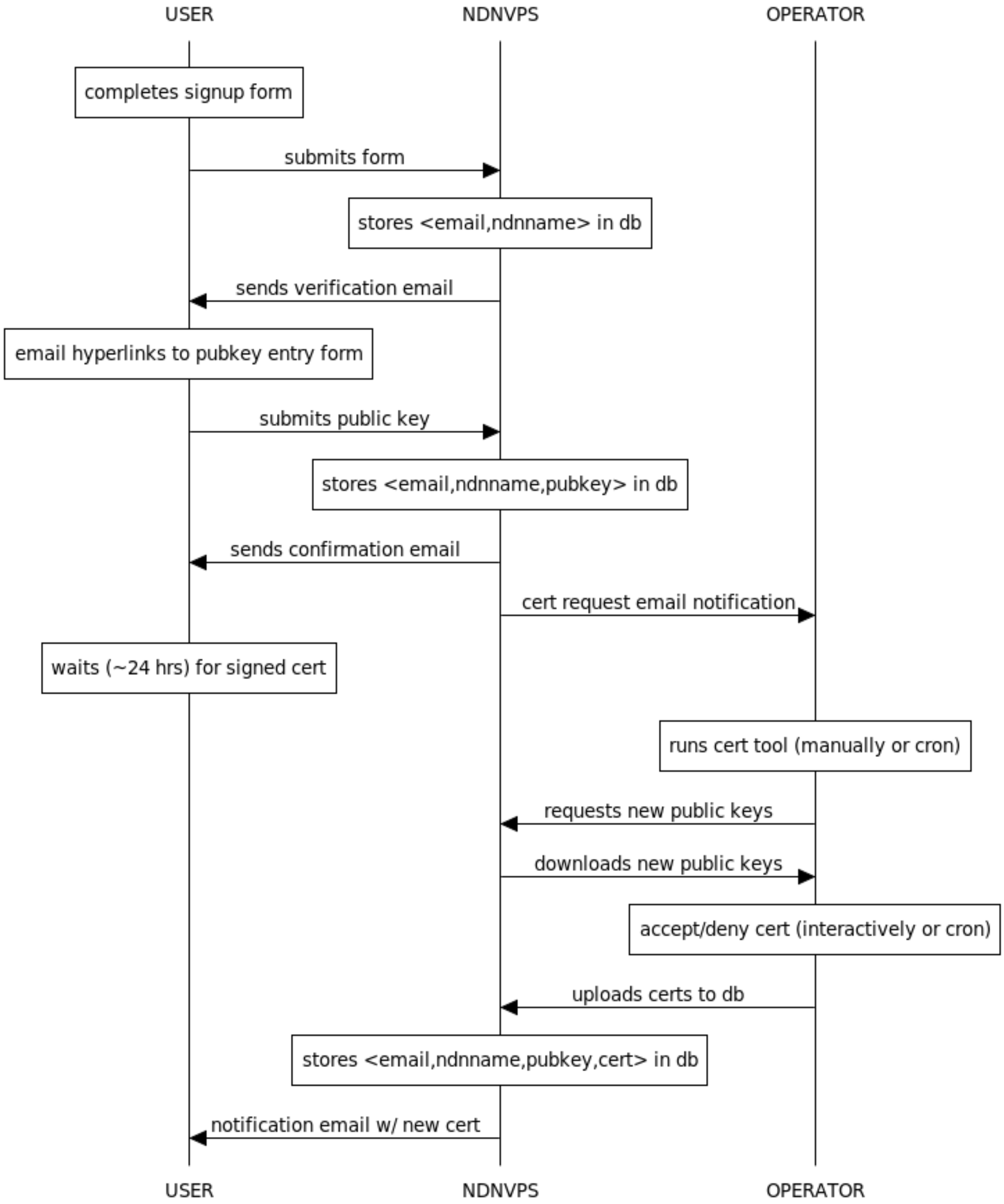
Operator User Experience

This is the path an operator follows to allow or deny user authorizations & certifications


notice of certification request
approve / reject cert request
sign new approved keys
post new certs to DB
Operator

Sequence Diagrams

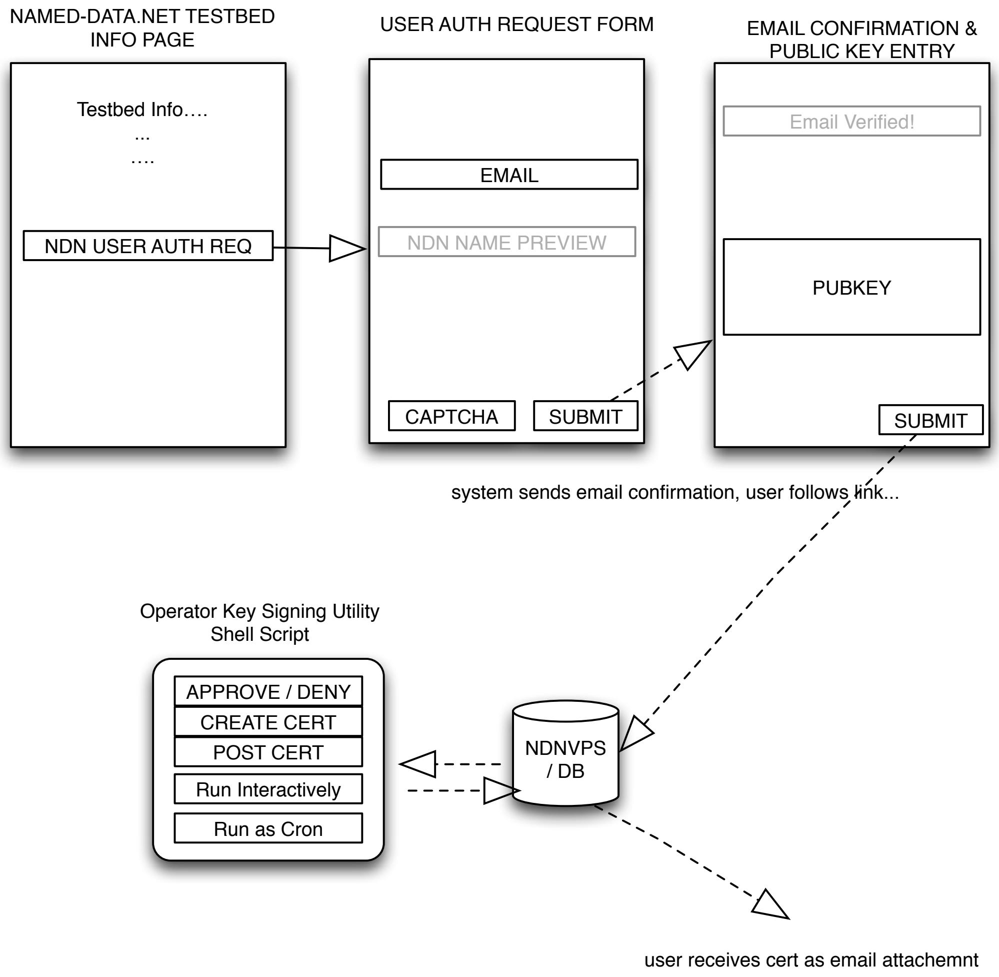
Certification Overview


USER
NDNVPS
OPERATOR
completes signup form
submits form
stores <email,ndnname> in db
sends verification email
email hyperlinks to pubkey entry form
submits public key
stores <email,ndnname,pubkey> in db
sends confirmation email
cert request email notification
waits (~24 hrs) for signed cert
runs cert tool (manually or cron)
requests new public keys
downloads new public keys
accept/deny cert (interactively or cron)
uploads certs to db
stores <email,ndnname,pubkey,cert> in db
notification email w/ new cert
USER
NDNVPS
OPERATOR

All transactions with NDNVPS are performed over HTTPS REST

UI/UX

These are the main points of interaction (pages or scripts) that enable the use cases


NAMED-DATA.NET TESTBED
INFO PAGE

USER AUTH REQUEST FORM

EMAIL CONFIRMATION &
PUBLIC KEY ENTRY

system sends email confirmation, user follows link...

Operator Key Signing Utility
Shell Script

user receives cert as email attachemnt

Problems / discussion / open questions

None, see ‘assumptions’