Why Red Hat switched to NSS

. . . and still uses it?

Kamil Dudka <kdudka@redhat.com>
Red Hat, Inc.

March 19th 2017

Fedora Crypto Consolidation

- plan to port approx. 200 Fedora packages to NSS
- approx. 10 of them succeeded
- at least 3 of them already reverted
- originally motivated by FIPS-140-2 certification
- badly underestimated:
  - insufficient manpower (mainly for NSS development)
  - insufficient communication with upstream developers

curl over NSS in Fedora and RHEL

- implemented in 2007 and (force-)pushed to Fedora
- initially unusable:
  - double free after 66 subsequent TLS handshakes
  - excessive memory consumption
  - fixed passphrase length, etc.
- started to work in 2009
- successfully used since RHEL-6.0 (introduced in 2010)

Running curl over NSS

- NSS is a crypto library originally used by Firefox
- rebased regularly with Firefox on Fedora/RHEL
- more stable API/ABI than OpenSSL
- supports loading certificates from Firefox database
- needs nss-pem (PKCS #11 module) to load certs from files:

  https://github.com/kdudka/nss-pem