Lurk – BoF
“This is the Problem”

Rich Salz

Problem Statement

- How can “I” authorize others to use my key?
  - Without risking full long-term exposure

- Why do “you” want to do this?
- One major use case agreed-on: CDN’s
- Others proposed: code signing (e.g., Debian, etc., packages)
- Others?

Use-case 1: CDN

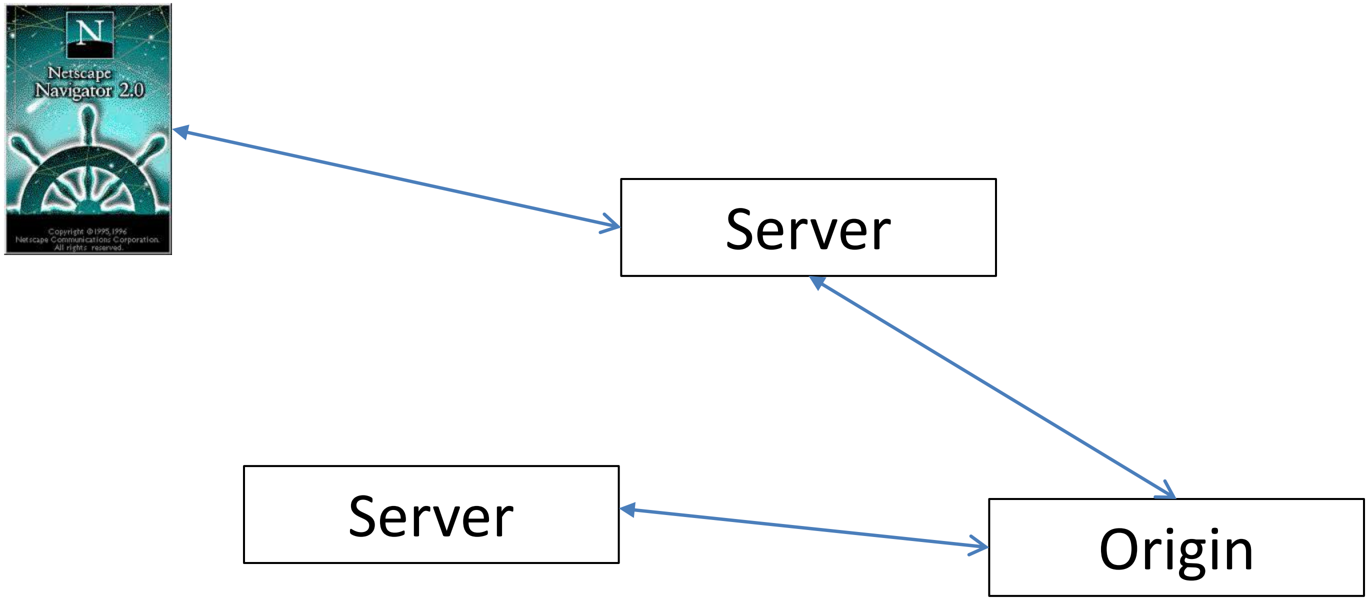
- Origin’s contract with (one or more) CDN’s to provide better user experience
- CDN’s work by replicating and caching over the Internet.
- They terminate the TLS
  - *They replicate the private key!*
- Sometimes in “hostile” areas

Use-cases 2..*n*

- TBD on mailing list

Approach 1

- Many approaches use this architecture:



N
Netscape Navigator 2.0
Copyright © 1995, 1996 Netscape Communications Corporation. All rights reserved.

Server

Server

Origin

Approach 2

- Time-limit the certificate/keypair