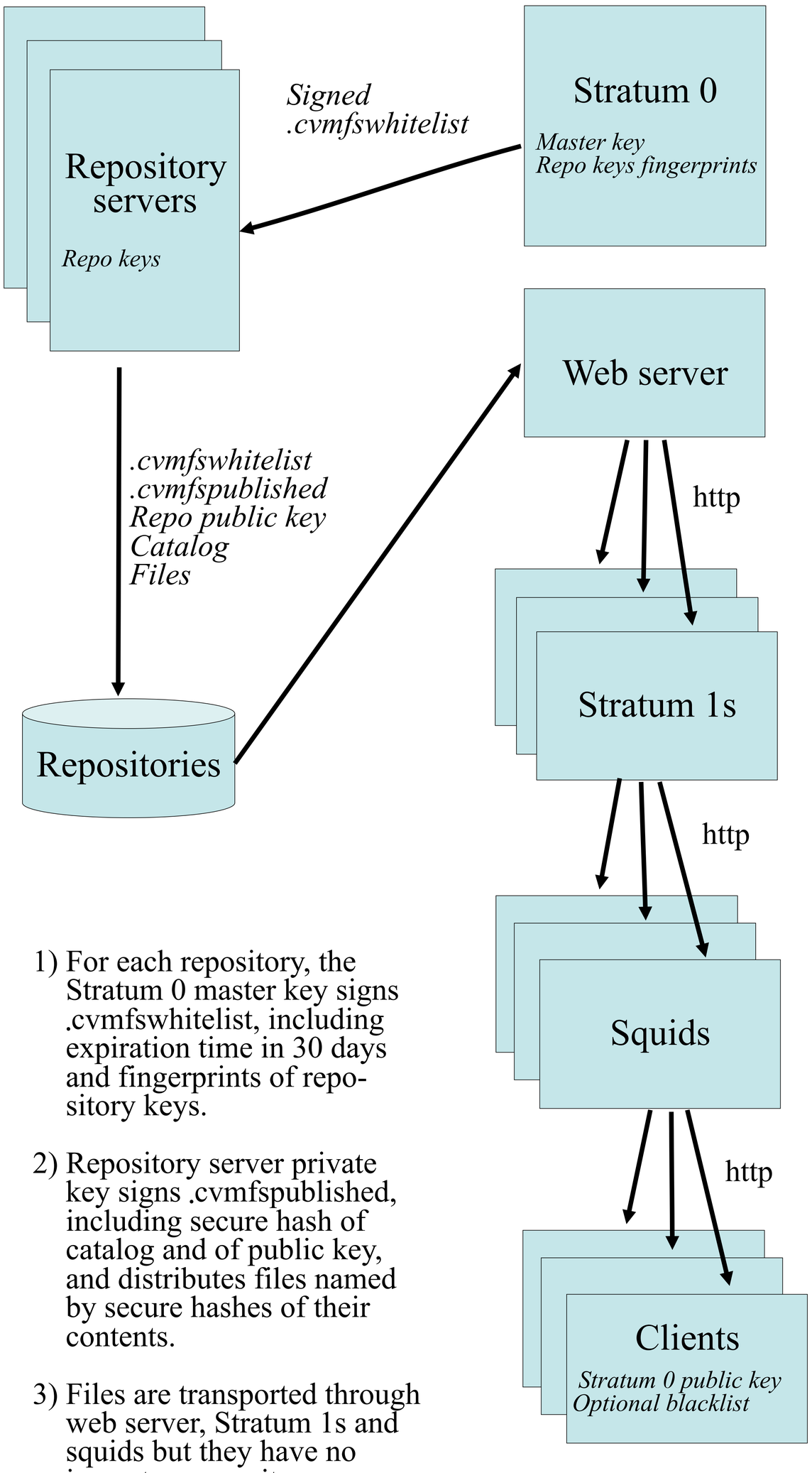
Security in the CernVM File System and the Frontier Distributed Database Caching System

Dave Dykstra
Scientific Computing Division, Fermilab, Batavia, IL

Jakob Blomer
PH-SFT Department, CERN, Geneva, Switzerland

CVMFS



1) For each repository, the Stratum 0 master key signs .cvmfswhitelist, including expiration time in 30 days and fingerprints of repository keys.

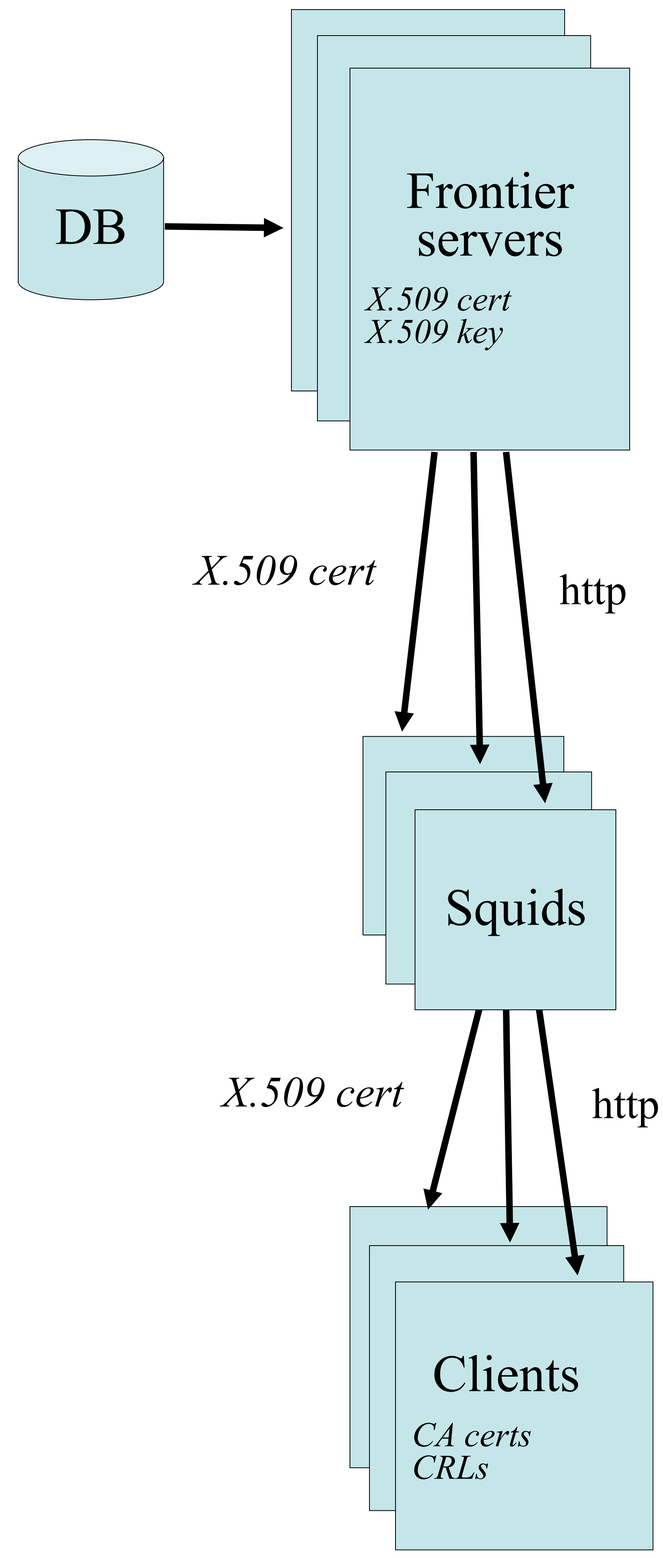
2) Repository server private key signs .cvmfspublished, including secure hash of catalog and of public key, and distributes files named by secure hashes of their contents.

3) Files are transported through web server, Stratum 1s and squids but they have no impact on security.

4) Clients verify signature on .cvmfswhitelist with Stratum 0 public key (which is installed by rpm), fingerprint of repository public key, signature on .cvmfspublished, and hashes on catalogs and files. They also verify that repository version number and timestamp (which are also in .cvmfspublished) only move forward, to prevent replay attacks.

5) Clients support blacklist file in case of repository key compromise, which lists fingerprints to reject.

Frontier



1) When a client connects to a new server, it requests the X.509 certificate for that server, confirms the certificate is valid based on its CA certs and CRLs, and confirms that the server name matches a name in the certificate.

2) Server appends signature to every response, covering the contents of URL plus the response data, using its X.509 key.

3) Responses are passed through squids which do not impact security.

4) Clients confirm that the signatures correspond to the server's certificate.

Frontier servers cannot predict requests so they cannot pre-calculate hashes and signatures like CVMFS can. Frontier's authenticity & integrity-checking mechanism is simpler than CVMFS's mechanism, but it is less efficient. Caching makes it efficient enough, however.

Work supported by the U.S. Department of Energy under contract No. DE-AC02-07CH11359