The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX

(draft-ietf-pki4ipsec-ikecert-profile-00.txt)

Brian Korver
briank@xythos.com

From -04 to -00

- draft-ietf-ipsec-pki-profile-04.txt (Feb ’04) to
- draft-ietf-pki4ipsec-ikecert-profile-00.txt (May ’04)

From -04 to -00

- Made it clearer that the format of the ID_IPV4_ADDR payload comes from RFC791 and is nothing new. (Tero Kivinen Feb 29)
- Permit implementations to skip verifying that the peer source address matches the contents of ID_IPV{4,6}_ADDR. (Tero Kivinen Feb 29, Gregory Lebovitz Feb 29)
- Removed paragraph suggesting that implementations favor unauthenticated peer source addresses over an unauthenticated ID for initial policy lookup. (Tero Kivinen Feb 29, Gregory Lebovitz Feb 29)

… -04 to -00

- Removed some text implying RSA encryption mode was in scope. (Tero Kivinen Feb 29)
- Relaxed deprecation of PKCS#7 CERT payloads. (Tero Kivinen Feb 29)
- Made it clearer that out-of-scope local heuristics should be used for picking an EE cert to use when generating CERTREQ, not when receiving CERTREQ. (Tero Kivinen Feb 29)
- Made it clearer that CERT processing can be skipped when the contents of a CERT are already known. (Tero Kivinen Feb 29)

From -04 to -00

- Implementations SHOULD generate BASE64 lines less than 76 characters. (Tero Kivinen Feb 29)
- Added "Except where specifically stated in this document, implementations MUST conform to the requirements of PKIX" (Steve Hanna Oct 7, 2003)
- RECOMMENDS against populating the ID payload with IP addresses due to interoperability issues such as problem with NAT traversal. (Gregory Lebovitz May 14)

… -04 to -00

- Changed "as revoked by one source" to "as revoked by one trusted source". (Michael Myers, May 15)
- Specifying Certificate Authorities section needed to be +regularized with Gregory Lebovitz's CERT proposal from -04. (Tylor Allison, May 15)
- Added text specifying how receipients SHOULD NOT be expected to iterate over multiple end-entity certs. (Tylor Allison, May 15)
- Modified text to refer to IKEv2 as well as IKEv1/ISAKMP where relevant.

From -04 to -00

- IKEv2: Explained that IDr sent by responder doesn't have to match the [IDr] sent initiator in second exchange.
- IKEv2: Noted that "The identity ... does not necessarily have to match anything in the CERT payload" (S3.5) is not contradicted by SHOULD in this document.
- IKEv2: Noted that ID_USER_FQDN renamed to ID_RFC822_ADDR, and ID_USER_FQDN would be used exclusively in this document.

…. -04 to -00

- IKEv2: Declared that 3 new CERTREQ and CERT types are not profiled in this document (well, at least not yet, pending WG discussion of what to do -- note that they are only SHOULDs in IKEv2).
- IKEv2: Noted that CERTREQ payload changed from DN to SHA-1 of SubjectPublicKeyInfo.
- IKEv2: Noted new requirement that specifies that the first certificate sent MUST be the EE cert (section 3.6).