draft-ietf-ipsecme-eddsa-00 & draft-mglt-ipsecme-implicit-iv-01

Yoav Nir

Agenda

- Status of the EdDSA draft
- Status of the implicit IV draft
- Next Steps

EdDSA

- Published the first version of the EdDSA as a WG draft on October 28.
- Changed the OID to match the example in draft-ietf-curdle-pkix
  - Now in WGLC
- Added hex representation of OID to avoid the need for a DER/ASN.1 module as part of IKE.
- Pre-hashed versions of Edwards curves prohibited. Need to see what text we need to address context in Ed448 (and lack of it in Ed25519).
- CFRG draft seems stuck. All three will probably end up as a cluster.
- The only really new thing in this draft is a null has needed for using EdDSA without pre-hash.

Implicit IV

- Published version -01
  - Removed other negotiation options. Only new transforms remain.
  - Re-wrote IANA considerations accordingly.
  - Fixed references
- Still not a WG draft…
  - …although accepted as a charter item.

EdDSA - contexts

- Ed448 adds a context parameter.
- If you use the same key in two applications (like, IKE, TLS, certificate signing) an attacker might be able to compromise the signer by having identical plaintexts feature in >1 protocol.
  - Similar TBSCertificate and IKE_SA_INIT request?
  - Creates a signing oracle.
- The traditional PKI counter-measure is not to use the same key for two applications.
- Using different contexts for each application makes key re-use safe
  - And key re-use is probably happening anyway.

EdDSA - contexts

- So we could have a context string to be used with signatures in IKE that is different from the context string of TLS or PKIX.
- There are really two algorithms that support context: Ed448 and Ed25519ctx.
- RSA, DSA, and ECDSA do not have context strings.
- The CFRG draft warns against using context strings opportunistically. No reason is given except that it is error-prone
    - I re-used my key because contexts protect me, but then it turned out that we were using RSA.
- Contexts are a neat idea. It’s up to us to decide if we want them despite the CFRG warning
    - We are not likely to turn all RSA, DSA and ECDSA into MUST NOTs.

Next Steps

- WG needs to decide about EdDSA contexts.
  - curdle needs to do the same.
- Then it can go to WGLC
- We will submit implicit-IV as WG document
  - The conversation about CCM tag lengths can happen in WGLC, I think.

Questions?