COMPOSITE CRYPTO FOR PKIX AND CMS

IETF LAMPS 114

Mike Ounsworth, John Gray, Serge Mister (Entrust), Max Pala (CableLabs), Jan Klaussner, Klaus-Dieter Wirth (D-Trust).
Composite crypto for PKIX and CMS

Outline

Main points

- Composite-keys and Composite-sigs are ready for WG adoption.

Outline

- Status of composite Keys and Sigs drafts
  - Ready for WG adoption!
    - Rough consensus …
    - … and running code

- Composite KEM -00
- IETF 115 hackathon: PQ X.509?
Composite drafts

CompositePublicKey ::= SEQUENCE SIZE (2..MAX)
   OF SubjectPublicKeyInfo

CompositeSignatureValue ::= SEQUENCE SIZE (2..MAX)
   OF BIT STRING

**draft-ounsworth-pq-composite-keys-02**
- Defines composite public and private keys
- Usable anywhere in PKIX that uses pub / priv keys.

**draft-ounsworth-pq-composite-sigs-07**
- Defines composite signatures
- Usable anywhere in PKIX that uses signatures.

**draft-ounsworth-pq-composite-kem-00**
- Defines composite as a KEM (Key Encapsulation Mechanism)
- Useable anywhere that accepts KEMs.
- Takes any combination of KeyTrans, KeyAgree, KEM components

NEW!!
Rough consensus …

Authors group

- Entrust
- CableLabs
- D-Trust
- DigiCert
- Cisco

Other Positive reviews

- Panos K. (AWS)
- François Rousseau
- ISARA
- Carl Wallace
- Michael Richardson
... and running code

<table>
<thead>
<tr>
<th>Implementation</th>
<th>Interop Tested</th>
<th>Licensing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Proprietary</td>
</tr>
<tr>
<td>Entrust PKIaaS/Toolkits</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Bouncy Castle</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Open Quantum Safe / Open SSL</td>
<td>In Progress</td>
<td>YES</td>
</tr>
<tr>
<td>OpenCA libPKI (in progress)</td>
<td>TBD</td>
<td>YES</td>
</tr>
<tr>
<td>CableLabs / DOCSIS PKI</td>
<td>TBD</td>
<td>YES</td>
</tr>
<tr>
<td>Botan crypto library (ICA D-TRUST)</td>
<td>TBD</td>
<td>YES</td>
</tr>
<tr>
<td>ISARA?</td>
<td></td>
<td>YES</td>
</tr>
</tbody>
</table>
IETF 115 hackathon: PQ X.509?

What?
- Cert / CRL validation
- CMS SignedData

Why?
- Sync up pre-standards OIDs and wire encodings.

Algs?
- Dilithium
- Falcon
- SPHINCS+
- Composite

Implementations to test against?
- Entrust toolkit
- Bouncy Castle
- Open Quantum Safe / OpenSSL
- Others ? !
Interaction with non-composite approaches

Ex.: draft-becker-guthrie-noncomposite-hybrid-auth-00

Complementary

◦ Non-composite (often) makes more sense for negotiated protocols.
◦ Composite (often) makes more sense for non-negotiated protocols.
◦ May even be combined: ex.: the PQ part of non-composite could itself be composite for greater algorithm certainty.
LAMPS Milestones

These LAMPS milestones would be accomplished by adopting pq-composite-keys and pq-composite-sigs:

- Dec 2021  Adopt draft for dual signature in CMS
- Dec 2021  Adopt draft for dual signatures in PKIX certificates
- Dec 2021  Adopt draft for public keys for hybrid key establishment in PKIX certificates

(and this one when we get pq-composite-kem published)

- Dec 2021  Adopt draft for hybrid key establishment in CMS
We propose that the following are ready for WG Adoption:

- draft-ounsworth-pq-composite-keys-02
- draft-ounsworth-pq-composite-sigs-07

Which would meet the LAMPS Milestones (Dec 2021) mentioned above.
Composite KEMs

Encrypt for a recipient with either a composite pub key, or multiple encryption certs.
BRAND NEW!!

Contains two things that need crypto review:

1. Transformations so everything can be treated as a KEM:
   - KeyTrans -> KEM
   - KeyAgree -> KEM

2. "Combiners" to combine multiple component shared secrets
   - SS = C( SS1, SS2, ..., SSn, CT1, CT2, ..., CTn )
   - This seems to be a hot area of research, so probably needs to be modular / agile.