

Multiple Signature

Certificate

- A data packet binds key name to key bits
 - signed by certificate issuer
- Naming convention
 - /<key-name>/[version]
 - version
 - certificate issuer may replace its own key periodically
 - every time a new signing key is created, re-sign the binding between key name and key bits, leading to a certificate with new **version**
- Previously, we assume that there is only one issuer who can certify the binding between key name and key bits
 - version number is consistent from the issuer's perspective

Name: /<key_name>/[version]
MetaInfo
Content: key bits
SignatureInfo: KeyLocator: /<signing_key_name>
SignatureValue

Multiple Signature

- Signature on the same (key name, key bits) binding?
 - how to maintain the version? or as long as version is consistent for each signer
 - $v_{m1} < v_{m2} < v_{m3} < \dots$
 - $v_{n1} < v_{n2} < v_{n3} < \dots$
- Signature on the same data packet?
 - encapsulation
 - who determine the inner version, sigInfo, and sigVal?
 - how to name the outer packet?
 - how to interpret such an encapsulation?

Name: /<key_name>/v_m1
MetaInfo
Content: key bits
SignatureInfo: KeyLocator: /signer_m
SignatureValue

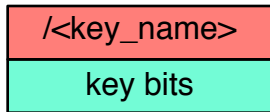
Name: /<key_name>/v_n1
MetaInfo
Content: key bits
SignatureInfo: KeyLocator: /signer_n
SignatureValue

Name
MetaInfo
Content
Name: /<key_name>/v_p
MetaInfo
Content: key bits
SignatureInfo: KeyLocator: /signer_p
SignatureValue
SignatureInfo: /signer_m
SignatureValue

Name
MetaInfo
Content
Name: /<key_name>/v_p
MetaInfo
Content: key bits
SignatureInfo: KeyLocator: /signer_p
SignatureValue
SignatureInfo: /signer_n
SignatureValue

Design Options

- Option 3: signature bundles
 - group signatures into a separate data packet **signature bundle**
 - rely on naming convention to retrieve signature bundle
 - /<key_name>/SIG/[seqNo]



Name: /<key_name>/v_nk
MetalInfo
Content: key bits
SignatureInfo: /signer_n
SignatureValue

Name: /<key_name>/v_ml
MetalInfo
Content: key bits
SignatureInfo: /signer_m
SignatureValue

Name: /<key_name>/v_n1
MetalInfo
Content: key bits
SignatureInfo: /signer_n
SignatureValue

Name: /<key_name>/v_m1
MetalInfo
Content: key bits
SignatureInfo: /signer_m
SignatureValue

Name: /<key_name>/SIG/Sn
MetalInfo:
Content:
Name: /<key_name>/v_ml
SigInfo: /signer_m
SigValue
Name: /<key_name>/v_nk
SigInfo: /signer_n
SigValue
SigInfo: self-sign
SigValue

...

Name: /<key_name>/SIG/S0
MetalInfo:
Content:
Name: /<key_name>/v_m1
SigInfo: /signer_m
SigValue
Name: /<key_name>/v_n1
SigInfo: /signer_n
SigValue
SigInfo: self-sign
SigValue

Signature Bundle

- Name:
 - /<key_name>/SIG/[SeqNo]
- Content:
 - a list of (Name, SignatureInfo, SignatureVal)
 - Name = key_name + signer specific version
 - (optional) full name of next signature bundle
- Signed by the key owner
- Retrieval
 - follow KeyLocator to retrieve key
 - KeyLocator does not include version number
 - (optionally) retrieve additional signatures