KEYPROV minutes (Charles Clancy)
2 December 2007
IETF 70

Dynamic Symmetric Key Provisioning Protocol (DSKPP), Andrea Doherty
(see presentation slides)

- Current status
  - Description of changes in v01
  - Still a number of open issues in v01 (6 in total)
- Discussion of open issues
  - #34: client authentication, too many options, look at use cases to reduce set
  - #36: apps review of http binding, conform better to BCP 56
    - Pasi: [comment]
    - Phil: date on BCP is 2002 and pre-SOAP, address IETF vs. W3C tools for building web services, WSDL could be useful
    - Hannes: shouldn't make this decision in this working group
    - Andrea: issue to be addressed beyond keyprov
  - #37: one-pass protocol variant, necessary for SMS-based push (not use case supported by core document), suggest removing, no disagreement
  - #32: conformance matrix, what does an implementer need to implement?, include a matrix of MAY/SHOULD/MUST for each feature
    - Hannes: potential to further simplify things, 2-pass not very secure so run over TLS, becomes almost as many RT as 4-pass, what's the point?
    - Andrea: run 2-pass or 4-pass over TLS, next slide provides TLS
    - Sean: matrix is a great idea
  - #33: why do we allow non-TLS? What's the value of allowing non-secure transport?
    - Pasi: any mobile phone that can't do TLS can't do TCP/IP, so requiring TLS is reasonable
    - Hannes: phones that can't support TLS aren't the targets of this protocol anyway
    - Andrea: intent of use cases for non-protected transport layer was to support legacy devices
    - Hannes: compare 2-pass w/ TLS and 4-pass w/o TLS, if you have devices with weak performance such that 2-pass w/o TLS is the only option…
    - Andrea: recommended that you run over TLS
    - Hannes: Pasi saying no such device exists
    - Andrea: if we want to remove use cases requiring non-secure transport, we can remove much complexity
    - Hannes: suggests simpler document, WG progress
    - Questions:
      - Who believes use case of 2-pass w/o TLS is important: silence
      - Who believes assuming TLS is reasonable: audible hum
    - Tim: needs to go to the list, get rid of the use cases
    - Hannes: what does this mean for simplification?
    - Andrea: remove allowances for unsecure transport
    - Phil: before requiring TLS, realize TLS may not be end-to-end
    - Andrea: require end-to-end, application layer manages, could assume sure WS rather than just TLS

        - Hannes: assume secure layer available, do we require 2-pass and 4-pass?
        - Andrea: 4-pass is not about transport layer security, it's about mutual key generation, different use case
        - Phil: 2-pass mutual key generation is easy
        - Andrea: based off CTKIP which was 4-pass, no mention of an alternative
        - Ming: 4-pass/2-pass can be over http/https, impact mostly related to authenticated data; 25% of handsets do not support TLS, in 2 years this will be lower, compare use case and market share vs introduced complexity
        - Hannes: support at client, ship it software all must have TLS; would like to better understand 2-pass w/ TLS and 4-pass w/o TLS
        - Andrea: 4-pass works without secure transport, but can run with TLS
        - Hannes: 2-pass w/o TLS off the table
        - Andrea: don't agree that 4-pass w/ TLS doesn't make sense, simplifies server and client authentication
        - Hannes: do you agree that there are too many options?
        - Andrea: disagree, 2 different problems (key gen vs key transport)
        - Lakshminath: tourist, would like to see call flow and payloads and a list of properties that each support and underlying assumptions
        - Andrea: in the draft
        - Russ: "in other words, read the draft!"
        - Hannes: some think things are too complicated, encourage everyone to look at document
        - Andrea: original goals substantially altered if we remove some of these options
        - Tim: look at how much things get simpler
    - #35: schema refinement, suggestions indicate people are trying to implement it
- Next steps:
    - resolve open issues
    - revise and resubmit draft for WGLC
    - decide whether to add SOAP binding document as a WG item

Presentation: Portable Symmetric Key Container, Ming Pei
(see presentation slides)

- Status update: list of changes in -01 and -02
- Topic 1: use of xmlenc / xmldsig, XML description of encryption key
    - Andrea: question on Magnus's proposal, comparing apples and oranges? Different encryption method per key?
    - Ming: both support that
    - Andrea: on the mailing list, based on the discussion, decision was that it was too complicated to talk about different encryption methods for each key, and the decision was to use single encryption key for all devices in the same container
    - Ming: bad example
- Topic 1: pros/cons
    - Tim: it seems that an awful lot of the decision has to do with the likelihood that your target devices will already have those tools on them anyway; if they're already there then it could be a good idea to take advantage of them; difficult judgment on penetration of tools
    - Andrea: on behalf of Magnus, his push is to enable XML encryption in DSIG, be as standard as possible, complicated if you rely on home-grown mechanisms

  - Phil: concern is that XML encryption is not a specification as a toolkit for exposing crypto API objects in an XML-friendly way; has lots of knobs; if we could find a way of specifying a very thin profile of XML encryption that would allow us to do what we're trying to do without going to the reference key module approach, could imagine a point where those folk with a keyprov implementation could turn it into an XML enc imp by moving pointers; real problem on message acceptance side, point where options come back to bite you, having to support anything you receive; if we did do this it would be with a very thin profile and not the whole thing
  - Ming: agree
  - Andrea: agree
  - Hannes: want to see more concrete proposals
  - Question: who has read the latest version of the document? 3 people
  - Question: who has read DSKPP? 4 people
  - Pasi: hopes someone from keyprov was in XML tutorial, make DSKPP readable
- Topic2: PIN policy, how to transmit initial PIN during provision
  - Ming: single PIN, multiple keys or one PIN per key?
  - Pasi: what does "device-level PIN policy" mean? What is the device?
  - Ming: phone is device, key container
  - Pasi: what parts of the device can I use without entering the PIN?
  - Phil: implementation decision within particular context
  - Pasi: existing protocols for managing device-level policy that try to address what "device" means, and different PINs unlock different functionalities
  - Ming: PIN unlocks software, use unlocking PIN to unlock key container
  - Hannes: slippery slope, can ignore or look at other documents
  - Tim: has to be required to meet your goals to investigate this; instinct is that it's not necessary and leave this out of it
  - Hannes: good advice, keep things simple
- Topic3: profiling of PSKC, many algorithms, what is MUST/SHOULD/MAY? Where do we find URIs?
  - Phil: personal draft trying to map things out, crypto ids defined per protocol, conflict in namespace; survey mapping out where all identifiers are defined; wants a more structured way to identify crypto ids at IETF level than a per-WG level
  - Pasi: works fine as long as algorithms are used exactly the same way in all protocols, which hasn't always been the case
  - Phil: if you have 2 identifiers it's okay to introduce new one for something different; don't create new identifier because you didn't know the old one exists
  - Pasi: example – AES-CBC used in IPsec is different because of key lengths and padding and IVs; HMAC-SHA1 should be pretty simple
  - Phil: not trying to argue that everything will be plug and play; standing up server to enter documents defining identifiers
- Topic4: logo type, logo schema
  - Phil: where does the logo data come from?
  - Ming: embedded in XML or could be URI to external source
  - Phil: include hash/authenticate?
  - Ming: if you trust server/key you will already trust logo
  - Phil: this usage is somewhat different, here logo is not for 3rd party but for key itself
  - Sean: seems silly, does it have to be in base spec?

    - Tim: if the logo is something for use by the device owner to help them sort out which key is which, is it something that has to be delivered securely? Can it be associated later? Not clear that it's integral to the key container and doesn't need to be transmitted together.
    - Russ: seconding Sean's suggestion, slippery slope
    - Ming: what do you recommend to move forward?
    - Hannes: thought it was clear
    - Tim: "not in the base spec"
    - Phil: do it later to allow more options in the future
    - Tim: suggest putting it on the back burner and push the rest of the document forward
    - Phil: feeling that information is useful
- Open issues
    - OTP algorithm URI definition
        - Phil: put in a 1-page draft to define code point for URI specified in PSKC
    - ValueDigest with keyed digest vs unkeyed (HMAC vs SHA1)
        - Hannes: is this created by the fact you don't use XML?
        - Ming: AES keywrap defines MAC, but not all, how do you know key is correct after decryption
    - URI for PKCS KeyContainer
        - Phil: just URI of the schema? Must be defined in the draft, in DSKPP that draft should take notice of these identifiers being developed elsewhere; when you define a data structure it's incumbent on you to define the OIDs
    - Alignment between DSKPP and PSKC, KeyType vs KeyAlgorithmType
        - Andrea: goal of not having home-grown types, KeyAlgorithmType is PKSC, KeyType is P11 and more commonly used; do we want to have a home-grown type here?
        - Ming: database key vs security key in google search
- Discussion
    - Charles: why require many REQUIRED crypto algorithms in Topic3? Only need one mandatory to implement to get interoperability.
    - [general agreement throughout]

Draft-turner-symmetrickeyformat-01.txt, Sean Turner
(see presentation slides)

- Status: adopt PKCS#12 or #15, v01 published, authors consider complete, WGLC?
    - Hannes: XML key container has a number of attributes, additional data long with the key, wonder if there is proposal on aligning; dump into PCKS doc same as XML doc?
    - Sean: XML and ASN.1 in a single doc
    - Hannes: suggest one document to describe both, does group have an idea? One document for both, or define attributes and elements in each of the two documents?
    - Sean: nice to say XML one is required, all attributes in one, easier for implementers
    - Hannes: nobody has opinion?
    - Tim: doesn't have a sense for the level of effort
    - Russ: for whom?
    - Pasi: another working group solved related problem that had a document defining data model and what it means, and then an appendix with an XML schema
    - Hannes: obviously further work needed to clearly describe semantics in DSKPP

    - Phil: less worried about number of documents, but more synchronization between them; use tools to generate specification since documents written in XML
    - Andrea: interest in both PKSC and ASN.1, this issue is very important for IEEE adoption of documents; OID tree; likes one place to go
    - Pasi: tool to encode ASN.1 inside XML [ugly]
    - Hannes: leaning toward separate documents

Open Discussion / Conversation / Announcements

- Hannes: Interim meeting necessary?
- Hannes: open-source code for DSKPP from PhD student, useful feedback
- Hannes: who willing to join an interim meeting, face-to-face?
    - Ming, Sean (depending on location)
- Tim: look at guidelines for interim, not opposed to seeing more work getting done