From: Peralta, Rene (Fed)
To: Kelsey, John M. (Fed)
Subject: Re: Beacon NISTIR to-dos
Date: Monday, January 28, 2019 10:35:15 AM

Let us try to meet before the 1pm meeting.

****

From: Kelsey, John M. (Fed)
Sent: Monday, January 28, 2019 9:45 AM
To: Peralta, Rene (Fed)
Subject: Re: Beacon NISTIR to-dos

Rene,

(b) (6) I'm going to the PQC meeting, but otherwise am free.

--John

From: "Peralta, Rene (Fed)" <rene.peralta@nist.gov>
Date: Monday, January 28, 2019 at 09:44
To: Luís Brandão (b) (6), "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>
Cc: Rene Peralta (b) (6), John Keysey (b) (6), "Brandao, Luis (IntlAssoc)" <luis.brandao@nist.gov>
Subject: Re: Beacon NISTIR to-dos

Hi John,

Are you coming in today? If you are, could we have a short meeting in the morning? If not, how about tomorrow?

Rene.

From: Luís Brandão (b) (6)
Sent: Thursday, December 27, 2018 10:15 PM

To: Peralta, Rene (Fed); Kelsey, John M. (Fed)
Cc: Rene Peralta; John Keysey; Brandao, Luis (IntlAssoc)
Subject: Re: Beacon NISTIR to-dos

Hi John, Rene,

Following the notes in the previous email, did a (quite longer than expected) pass through the Beacon NISTIR. Update attached. Now passing the token to John.

Revised the previously enumerated items R1--R24 (notes further below). This lead to several other edits, mostly in sections 4 and 6, some of which require sanity checking (e.g., bit flags, ext.SrcId description, TXT format, REST calls). Specially the following would benefit from a sanity check / revision iteration from you: 4.1 (data formatting and representation), 4.3.4 (status), 4.5 (external value fields), 6 (the beacon interface) and 7.4 (combining Beacons).

Edit at will. Feel also free to simply delete/address any red note I still left hanging, in case you think it can be discarded/integrated.

A selected question: do we want to allow a signing key to change within a chain? If yes, then we should define a corresponding bit flag in the status field. If no, then we should mention it explicitly. (I'd be inclined for a "no", namely since we are allowing keys to be self-signed, and also to avoid multiple forking in case a CA gets compromised and issues certificates for many keys for the same domain.)

============ A. Highlights of the review:

=== Section 4.1
- Generalized to be about data formatting and representations.
- Described notation for different formats (dec, hex, ...). For example: <pulseId:dec> means the pulse index as a decimal string, which is how it is used within the URI; <preCom:hex> is the precommitment value in hexadecimal, which is how it is used within the XML file. This notation is useful in several places in the remainder of the document and, I believe, hereafter.
- Tentatively added a complementary TXT pulse format, which allows a direct representation in simple textual formal, exemplified in the NISTIR (see Fig. 4). Will probably be useful for human-readable representations / storage.

=== Section 4.2.1: more rigorous explanation of URI

=== Section 4.2.2: description of version field explains the sub-version updates

=== Section "4.4.4": explains the "Status" field based on flags (also exemplifies several integer values);

=== Section 4.5 (external value fields):
  - ext.SrcId: recommendations for attributes of the description; an example for using output values from other beacons; procedure for "registration" of new srcId
  - ext.status: now explained based on flags; proposed several new flags; proposed letting 32 bits be (optionally) for the pulseId of the first pulse where the same ext.value appears.
  - ext.value: explained how&why it remains unchanged until a new one is used
  - Sketched an example of source description for using output values from other beacons.

=== Section "6 Interface Calls"
- New section 6.1 details query-format and reply-format
- Clarified the format of input parameters (using notation <variable:format>) of interface calls
- Added "Opt?" column to indicate which calls are optional
- New optional queries about certificates, external values and status flags
(- Latex counters for interface calls are now automatically numbered;)

=== Section 7.4
- Based on the timing promises, integrated time-windows [T,T+Pi/4] and [T+Pi,T+2Pi] in the description of how to derive a random seed from a combination of beacons. Revised the description.

============ B. Notes about previously enumerated items to review:
- R1: Changed public comment period to tentatively start on Jan 21
- R2: Removed color in index of list of tables
- R3: Clarified which fields are invariant within a chain (new paragraph in sec. 3.2, short statements in sections 4.3.2 (Version), 4.3.3 (Cipher), 4.3.4 (Period) and 4.4.1 (chainId)).
- R4: Description of version number: slight improvement in section 1.2; section 4.2.2 (Version) explains better the non-inclusion of the "sub-version" component (z); sections 4.2.1 (URI) and 4.2.2 (version) has guidance on using "beta".
- R5: Removed many red notes ... also included new ones, which still require review.
- R6. Section 4.3.1 (URI): improved the explanation of virtual sub-fields used to construct the full URI
- R7. Used abbreviated field names in many places
- R8. In section "4.2.1 (URI)", recommended the use of "-beta" in beta versions
- R9--R12: Description of status based on bit flags, improved designations, explain repetition of values
- R13--R14: Past output values: improved description
- R15: Sec. 4.4: Specify that randLocal is filled with all zeros when it is previously lost; also mentioned the same in Sec. 4.3 when explaining the example of status=3=0b11.
- R16: Change to regular text the note that a hash-chaining by different time intervals (e.g.,

minute or hour) can be considered in a future format version.
- R17: Sec 4.6.5 describes that a loss of past pulses is unacceptable within a chain
- R18: adjust title of encoding functions, using "serialize"
- R19. Mentioned RFC 5280, which describe PEM file, which supposedly allows several certificates (requires thorougher reading)
- R20. Sec 4.9: added sig as input to serialize_fields_for_hashing
- R21. Sect. 6: Removed several red notes; re-organized subsections of REST calls,using a new column "opt?" to identify which calls are optional
- R22: Section 8: removed several red noted
- R23. Several format adjustments
- R24. Sec 8.3 "verify results from external sources" --> "external repositories"

---------- Original message ---------
From: **Luís Brandão** (b) (6)
Date: Sun, Dec 16, 2018 at 8:16 AM
Subject: Beacon NISTIR to-dos
To: John Kelsey <john.kelsey@nist.gov>, Peralta, Rene (Fed) <rene.peralta@nist.gov>
Cc: Rene Peralta <rene@peralta.one>, Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>

Hi John, Rene,

Below, notes from the 2018-Dec-14's meeting (John and I) about components to finalize/review in the Beacon NISTIR.

Based on the expected availability we talked, organized the items as follows:
- attributed most items to section "LB" below, since I hope to be able to do those edits early this coming week (will send email when having done it);
- then John would review those edits and also consider the items in the section "JK" further below.

Regards,
Luís

===== LB =====
- R1. Change public comment period
- R2. Remove color in index entries of list of tables
- R3. Add note on which terms MUST remain constant within a chain
- R4. Improve description of version numbering, to make a better case of why not including the "z" component
- R5. Remove all red "temporary notes": different way of calculating randLocal
- R6. Sec. 4.2.1 (URI), p.14, change <server> to <webDomain>

- R7. Accept proposed succinct formulas/descriptions with succinct notation (promote red text to regular text)
- R8. Sec. 4.2.2 (version): incorporate into regular text the recommendation of "2.0-beta"
- R9. Sec. 4.3.4 (status): Adopt flag description that is fully compatible with current integers (0,1,2,3): flag1: (1st) localRand without corresponding preCom; (2nd) gap in chain; (3rd) certId changed; (4th) end of chain. This is consistent with 0 normal; 1 start of chain; 2 gap without loss of randLocal; 3 gap with loss of randLocal.
- R10. Sec. 4.3.4 (Status): In the description of values 2 and 3, change the "valid/invalid" property of the preCom to a "no corresponding" property, since the actual preCom will be valid in the pulse in question (it's the randLocal that became invalid wrt to the information in the previous pulse).
- R11. (page 21) Revise description of external source: external.value remains fixed until it is changed [doubt: but what about ext.scrId?]
- R12. p.21: sec. 4.5.3: "When no external source is being used" --> "In the beginning of a chain, the field "external source" starts filled with all zeros. When the external source is used, "
- R13. Page 22: use "Past output values"
- R14. p.23: when describing logic of past pulses, improve the text that makes a description based on pulse indices (i-1)
- R15. Sec 4.4: Specify that randLocal is filled with all zeros when it is previously lost ... make the case that freshness is in anycase always guaranteed by the new preCom. (Review)
- R16. p.24: convert red note about different timings of "past output values" (e.g., minute, if a beacon outputs every 5 sec; or remove the "hour", if the pulse only outputs once an hour) into a note about this being to be considered in a future revision of the beacon
- R17. p.26: Convert red note about "what to do if past values are lost from beacon app [cache]" into regular text description of what to do: either (i) manual insertion from the outside, or (ii) start a new chain ... but never put out a new pulse in the same chain without showing the past pulse values.
- R18. p.27 (sec. 4.9), p.28 (sec. 4.11): In some places, change "encode_pulse" to "encode_pulse_for_signing"
- R19. p.27/28: search whether there is already a standard to pack more than one certificate in a single file; If the is, use it. If not, descibe the case of several certificates as being left for next revision.
- R20. p.28: review notation used in equation that shows signatureValue and outputValue ... use "serialize" notation (overline when using the serialized version)
- R21. Section 6 (The beacon interface): remove all red notes; [identify better the parts that require verification with HB;] add new recommended REST calls: all previously used extSrcIds; for a given extSrcId, all pulse indices where a new ext.value was used; all used certIds and when they started/finished; description of localStatusCodes; News / history / policy.
- R22. Section 8 -- remove several red notes
- R23. p.59: format minipage to fit within page width

- R24. p.60: last paragraph of section 8.3: "external sources" --> third parties that store values output by the Beacon

===== JK =====
- R25. Confirm length of statusCode: NISTIR says int32 (e.g., in Table 1 in page 6)... but might it be int64 that is being used?
- R26. Revise all section 7
- R27. Explain how to handle unknown status codes (locally defined)? Explain how each Beacon may define their own local codes within a particular range of flags.
- R28. Describe possible external value based on "transparency log" chain
- R29. Revise all changes by LB, with special attention to:
  - description of "external status" field based on flags ... and the same for "ext.status"
  - explanation of ext.srcId and ext.value between allzeros vs. remaining fixed
  - new recommended REST calls
  - explanation of field localRandomValue when there was loss of info in a gap