Comments on SMP CID v0.6

1. 2.2 – Fix formatting
2. 2.5 – ServiceMetadataReference repeated 2 times in left column
3. 3.1.3
    a. "*The location information of the SMP itself for allowing the senders to discover the SML*" – should be "discover the SMP"
    b. *"These interfaces will not be detailed here but the document will refer to these when they are invoked from the SML REST services*." – should be "from the SMP REST services"
4. 3.2.1.4 – "endpointReference" – where does this come from? Shouldn't it be endpointURI?

5. 3.3.4 - "N/A: As User, I ask the SML to resolve the address of the SMP I need to invoke." -- shouldn't it be "ask DNS"?

3.4.1 – Alternative flows & Flow b – fix formatting

6. 3.4.2
    a. Brief description & Basic flow event – fix formatting
    b. Basic flow #3 - response should not be 200 OK but 201 Created, according to codes table. Sample response should reflect this. If not, then discuss.
    c. Exception flows: "*b Request is not well formed (or any other technical error)*
    2b1 The SMP replies with HTTP error "500 Server Internal Error" with details on the error allowing to identify the error in the request" -- HTTP error code varies according to the kind of error. Maybe just describe as error and point for detailed errors in Error Codes table.

    d. REST Service: PutServiceGroup: *"The complete collection of ServiceMetadataReference"* -- Isn't this responsibility of the Admin ServiceGroup (to provide the service metadata? References are derived from the existent metadata...). According to UC04: "As Admin ServiceGroup, I define ALL the ServiceMetadata for the participant that I administer." If this parameter is optional, there's no problem: it can be used, e.g., for the migration process (?). If mandatory, we've a problem. Discussion required

   e. Error codes table: XSD_INVALID - *"The SML included* " -- not "SML" but "XML"

7. 3.4.3
   a. Basic flow event: *"into table ServiceGroup"* -- "from"
   b. Exception flow b -- 500 is not listed in Error Codes table (3.4.5 is also an "Erase" and has it). Plus, if different problems raise HTTP 500 (like in 3.4.2) they should be listed in Error Codes table and this flow should just describe it generically as an error, pointing to the table for details.
   c. REST Service: DeleteServiceGroup: *"Output: HTTP 200 if done, 404 if the specified service group does not exist and 500 if any error occurred"* – Same as before. Plus, list of codes is not exhaustive (should it be or just point to error codes table?)
8. 3.4.4
   a. Same problem as in 3.4.2 regarding 201 code
   b. Same problem as in 3.4.3 with Exception flow b
   c. Error codes table does not have error 404 (exception flow c)
   d. Execution NB: may be relevant to discuss among SMP TF at a technical level
   e. *"don't retry later the SML because it might occur after a successful completion 2nd call and corrupt the configuration after restoration"* – I don't understand, maybe clarify the writing?
   f. About CertificateUID, from SMP spec: *"Holds the Subject Unique Identifier of the certificate of the destination SMP. A client SHOULD validate that the Subject Unique Identifier of the certificate used to sign the resource at the destination SMP matches the Subject Unique Identifier published in the redirecting SMP"*
   g. *"Output: HTTP response code 200 if ok, 403 if not allowed and 500 if any other error occurred. Details are available in the response text."* – It should be 401, not 403. Same problem as in 8c)
   h. Error codes table
      i. XSD_INVALID - "*The SML included* " -- not "SML" but "XML"
      ii. 404 is missing
9. 3.4.5
   a. Error codes table has extra column that no other table has
   b. Exception flow b: same as 3.4.3 (except that it's listed in the table)
   c. "*Output: HTTP 200 if done, 404 if the service metadata or the service group does not exist and 500 if any error occurred."* – Same problem as 8c)
10. 3.4.6

   a. Basic flow event - step 2: if this is public info, then SMP doesn't need to authenticate the user
   b. Exception flows
      i. A) If SMP is not reachable, the sender will not fallback to cached info, it'll simply fail, because asking SMP is only done after testing cache values
      ii. D) error 400 not in error codes table
   c. Post conditions
      i. Successful -- Redirect is only received if asking for ServiceMetadata, not for ServiceGroup
      ii. *"The sender is ready to use outdated ServiceGroup information*" – I don't understand
      iii. Failure – I don't understand. *"any information*"??

11. 3.4.7
   a. Exception flows
      i. A) Same as in 3.4.6
      ii. C) error 400 not in error codes table
   b. Post conditions
      i. Sender receives the metadata itself, not URIs
      ii. "The sender receives outdated the reference" – I don't understand
      iii. Failure is not correct
   c. *"he has the target URI of the other SMP in the extension column*" -- extension column or redirect column?
12. 3.5.1.3.1
   a. *"Password column contains then the password*" -- password or its hash?
   b. *"since the certificate is not by the application layer itself"* -- I think there's a missing word here

13. 3.5.1.4 - *"The "Admin SMP" user is created by the system administrator (cf.)."* -- missing reference in "cf."
14. 3.5.2.2 - *"In that case, the central authority (possibly DIGIT) owns only "System Admin" user who creates one "Admin SMP" for each country who are responsible for managing the "Admin ServiceGroup" users of the country."* – Is DIGIT responsible to for the System Admin of all SMPs? To be clarified with DIGIT
15. 6.1.2 - "processContents" in sample xml
16. 6.2 - From SMP spec: *"The service SHOULD NOT use redirection in the manner indicated by the HTTP 3xx codes. Clients are not required to support active redirection."* - SMP should return the same status code for a GET operation

17. Regarding Redirects, maybe this info can be included (from SMP spec): *In the case where a client encounters such a redirection element, the client MUST follow the first redirect reference to the alternative SMP. If the SignedServiceMetadata resource at the alternative SMP also contains a redirection element, the client SHOULD NOT follow that redirect. It is the responsibility of the client to enforce this constraint.*

Task force discussion points

A. Cf. point 4 above (§3.2.1.4) : it seems like the existing implementation deviates from the specification : implementation uses “endpointReference” tag in XML instead of “EndpointURI“ specified in http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/cs01/bdx-smp-v1.0-cs01.html (§2.3.4.2)

   → is this right ? (or a misunderstanding on my side)
   → if not, where does this deviation come from (eSense or CEF specifications ?)

B. Cf. point 6.d above, §3.4.2: Joao: explanations in comments ok? To discuss within TF?

C. Cf. point 8.d above, §3.4.4: to discuss at technical level:

   Service “*PutSignedServiceMetadata*” is unfortunately not completely safe since it involves distributed updates outside ad hoc transactional context that might end up in some inconsistent sate. The risk of failure is low though, and the service can be called multiple times with the same information (until it works) to obtain a final consistent state.

D. Cf. point 14 above, §3.5.2.2: Is DIGIT responsible to for the System Admin of all SMPs? To be clarified with DIGIT.

E. §3.4.2 : PutServiceGroup service specifies ALL *ServiceMetadataReference* **at once** (not possible to add one or several to the existing set).

F. §3.4.2 : (PutServiceGroup service) confirm that the client must **hash the password** in the XML and if confirmed, how the hash is calculated – alternative: password is sent in clear (over ssl) and hash code is calculated by the SMP).

   → which option to choose ?

G. §3.4.2 : (PutServiceGroup service) confirm that XSD is to be extended to hold the username Alternative is to use the extension.

→ which option to choose ?

H. §3.4.2 : (PutServiceGroup service) Should there be a redirect column in the configuration database.

I. §3.3.4 -

Comment of Joao to validate:

"N/A: As User, I ask the SML to resolve the address of the SMP I need to invoke." -- shouldn't it be "ask DNS"?

→ which option to choose SML or DNS ?