**3GPP TSG-CT WG1 Meeting #125-eC1-20xxxx**

**Electronic meeting, 20-28 August 2020**

**Source: FirstNet**

**Title: Plugtest Issues for Standards**

**Agenda item: 16.3.12**

**Document for: Discussion**

**1. Introduction**

This contribution gathers the issues for standards reported by the ETSI Plugtest events for Plugtest 2 and Plugtest 3. It provides a tracking method for those issues and resolutions by 3GPP. It is intended to revise this contribution at this meeting with the inputs from the delegates and have the final revision noted. That final revision will then serve as the basis for a discussion paper at the next CT1 meeting, thus creating a tracking tool that will assist 3GPP in addressing all of the issues raised.

**2. Changes since the last version of this contribution**

Revision marks are used to show changes since this list of issues was last discussed in CT1.

Green highlighting has been added to indicate the lead working group when CT1 does not have that role.

Yellow highlighting has been added to the issue number for issues that are open.

A large number of issues have proposed resolutions.

**3. Plugtest reported issues for 3GPP standards**

The following table provides a summary of the issues reported from Plugtest 2 and Plugtest 3 and some status on what 3GPP has done to address them. It was noted during compilation of this table that the majority of Plugtest 3 issues are already included in the Plugtest 2 report. In the table, the prefix (PT2) / (PT3) / (PT2, PT3) is used. The text of all but those beginning with (PT3) is taken from the Plugtest 2 report. Where the issue statement was a bit long, only the beginning and end of the issue is included. The full text can be found in the report.

| **ISSUE**  **#** | **REPORTED ISSUE** | **COMMENTS / RESULTS** |
| --- | --- | --- |
| 1 | (PT2)10.1.1 MCPTT Administrator designation and checks  Not only on TS 24.484, but on other MCPTT related standards, the "MCPTT Administrator" is mentioned several times. In no single document is specified how this special MCPTT User is identified or distinguished from other regular MCPTT users. For CMS in particular, it is important to clarify this point, as this is the only user that can provision/manage configuration documents in this server. The checking mechanism should be specified. It is suggested to check the MCPTT ID of the access token against a configured value in the CMS.  (Also reported for Plugtest 3) | CT1 believes that SA6 should take the lead on this issue. SA6, please confirm. A statement from SA6 about the role of the administrator would be of value. |
| 2 | (PT2) 10.1.2 MO and XML Document relationship  It is mentioned in TS 24.484, Figure 4.2.2-1, that following the bootstrap procedure, UE must download the "MCS UE initial configuration MO" and the "identified default MCS user profile configuration MO". This point is somewhat confusing, because it differs greatly with the wording regarding other CMS documents, where it clearly states that the UE must subscribe to the XML document.  …  So, it needs to be clarified whether these two documents must be handled as normal XML CMS documents or have a different handling procedure. Based on what is specified in section 7, these documents should be handled the same way as the rest of the CMS documents. And thus, that figure and accompanying text should be changed to avoid confusion.  (Also reported for Plugtest 3) | Note that the "MCS UE initial configuration MO" and the "identified default MCS user profile configuration MO" files are downloaded because the MCS client does not yet have authorization to use the MCS system, and so the MCS client cannot subscribe via the procedures available to an authorized and logged in MCS client. Therefore, the text is correct as written. Once the MCS client is logged in, it can use the subscribe mechanism to obtain updates to these documents if they occur. |
| 3 | (PT2) 10.1.3 CMS Direct Subscription procedure  This procedure wording is causing very different interpretations and may have several technical limitations that can cause serious problems in the implementation phase. First, the direct subscription as defined in 6.3.13.2.2 has several confusing points:  …  It is proposed to use a procedure very similar to the Subscription Proxy for the Direct Subscription use cases: a SIP SUBSCRIBE request with the subscription proxy R-URI, with a application/resource-lists+xml body and a unique <entry> element. It is suggested that this modified Direct Subscription method will be used in case of unauthenticated requests only, that is, MCS Server originated subscriptions and UE (pre-auth) originated subscriptions. For the rest of the UE (post-auth) originated subscriptions we advocate to use Subscription Proxy procedures. | CT1 believes that SA6 should take the lead on this issue. SA6, please confirm. A statement from SA6 about the bootstrap procedure, specifically regarding whether a subscription is needed to the UE-init-config. |
| 4 | (PT2)) 10.1.4 UE-init-conf and UE-conf storage paths and access URIs  It is mentioned on 3GPP TS 24.484 sections 7.2 and 8.2 that "The master MCS UE (initial) configuration document name is assigned by an MCS administrator when the document is created and is stored in the user directory of that MCS administrator." So it is clearly defined where MASTER UE (initial) documents belongs to. These must serve as a template for generating specially targeted configuration documents that eventually are fetched from the correspondent UEs. But the standard does not indicate what URI must the UEs use to access those documents. It is highly improbable for the UEs to be capable of getting the documents from the MCPTT Administrator User's Tree, as this is the only defined path for UE initial document.  …  We think this should be more thoroughly specified in the standard, and provide a base set of parameters for each configuration document, such as (UE accessible URI, Admin provisionable URI, detailed MASTER -> concrete document transformation procedures). In the current state of the standard, interoperability capacity is very low due to missing details and open interpretation possibilities.  (Also reported for Plugtest 3) | CT1 believes that SA6 should take the lead on this issue. SA6, please confirm. A statement from SA6 about the role of the administrator would be of value. |
| 5 | (PT2) 10.1.5 File Extension inclusion in XML values  In several places in the standard it is necessary to reflect documents filenames in different XML elements of the documents. In these cases, the full document file name has to be reflected, such as "mcvideo-userprofile-3shift.xml" or only the filename without the extension "mcvideo-userprofile-3shift".  …  We advocate for the full filename option in this case, although we hold a little uncertainty about whether this refers to the filename (or document selector in XCAP jargon) or to another kind of "document name.  (Also reported for Plugtest 3) | **OPEN**: Need to obtain specific information from Plugtest folks. Have searched several standards and cannot find what is being referenced. |
| 6 | (PT2) 10.1.6 User profile static name  In 3GPP TS 24.484, all of the user-profile MCS documents have a "Naming Conventions" sections defining static filenames for them like "mcXXX-user-profile".  As we understand user-profile documents, it is possible to have several of them per user, so this unique name definition is somewhat insufficient.  We advocate a change to the specification. The default name for the document shall be the unique name definition with the addition of the profile index value. For instance user-profile-<index-value>.xml or user-profile-1.xml, mcvideo-user-profile-1.xml, etc. | From Release 15 onward, the MCPTT, MCVideo, and MCData user profiles have a profile index specified. |
| 7 | (PT2) 10.1.7 MCX Service Authorization  3GPP TS 33.180 defines two ways of performing MCX Service authorization with the MCX Server, but if we consider the full procedure a UE has to perform to bootstrap from cold start to a full working state within the network, there is a conflict with the REGISTER based workflow.  The REGISTER authorization workflow is based on the idea of including the MCPTT Access Token right in the IMS REGISTER SIP message the UE sends towards the IMS network when contacting it for the first time. But if according to 3GPP TS 24.484, the UE must subscribe to the UE-initial-conf document and the default-user-profile, it has to be already registered in the IMS network, thus rendering the REGISTER workflow unusable.  For the moment PUBLISH Authorization workflow seems to be the only alternative.  (Also reported for Plugtest 3) | CT1 believes that SA3 should take the lead on this issue. SA3, please confirm. SA6 is invited to provide comments as they determine are appropriate. |
| 8 | (PT2) 10.1.8 MCS Server PSI missing  The MCS Server PSI does not seem to be configured anywhere in the CMS documents. Being a very necessary address to have in order to bootstrap MCPTT functionality in the UE, it seems logical to find it in the UE-initial-conf document, but it is completely missing.  If no other mechanism or impediment is found, we think UE-init-conf document is ideal to add the MCS Server address in order to have all of the network servers addresses specified together. | Release 16 includes a server-URI value in the UE initial configuration file for MCPTT, MCData, and MCVideo. |
| 9 | (PT2)) 10.1.9 Misleading typos  There are some types in configuration documents which can be specially misleading or modify significantly the meaning of the sentence. Following are some of them:  • "initial" word misplaced in sentences like "If there is no <mcvideo-UE-id> element in the MCVideo UE configuration document, then by default the MCVideo UE configuration document applies to all MCVideo UEs of the mission critical organization that are not specifically identified in the <mcvideo-UE-id> element of another MCVideo UE initial configuration document of the mission critical organization." This happens in 3GPPP TS 24.484 subclauses 8.2.1, 9.2.1, 9.2.2.7, 10.2.1 and 10.2.2.7 sections.  • The extra point at MCPTT User Profile Document at section 8.3.2.5 of 3GPP TS 24.484. It now says "application/vnd.3gpp.mcptt.-user-profile+xml". That point after the "mcptt" is misleading and probably incorrect, as the other MCX User profile counterparts do not have it.  (Also reported for Plugtest 3) | Regarding the point:  • "initial" word misplaced in sentences like "If there is no <mcvideo-UE-id> element in the MCVideo UE configuration document, then by default the MCVideo UE configuration document applies to all MCVideo UEs of the mission critical organization that are not specifically identified in the <mcvideo-UE-id> element of another MCVideo UE initial configuration document of the mission critical organization."  -- The word "initial" does not appear in the quoted text. Clarification is needed.  Regarding the point:  "application/vnd.3gpp.mcptt.-user-profile+xml" contains an extra period after "mcptt"  -- this has been corrected. |
| 10 | (PT2) 10.1.10 Duration Data Type in Service Configurations  In 3GPP TS24.484 Section 8.4.2.6 (Page 84) it is stated that:  *The elements of "xs: duration" type specified above shall be represented in seconds using the element value: "PT<h>H<m>M<n>S" where <n> represents a valid value in seconds.*  *NOTE 3: "xs:duration" allows the use of decimal notion for seconds, e.g. 300ms is represented as <PT0.3S>.*  *If any of the elements of "xs: duration" type specified above contain values that do not conform to the "PT <n>S" structure then the configuration management server shall return an HTTP 409 (Conflict) response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute should be set to "invalid format for duration"*  1. The first sentence is confusing, stating to use the XML Schema's *duration* data type, and also redefining it with a format string of "PT<h>H<m>M<n>S" to prevent the use of "<y>Y<m>M<d>D" between "P" and "T".  2. Also a few lines below, the format string changes to "PT <n>S".  We think that the actual intent behind this text is to define how an amount of time may be specified in the service configuration document. Our proposed way to do that would be to use the XML Schema's duration datatype without modifications as in the other configuration documents.  (Also reported for Plugtest 3) | The raised issue was discussed by 3GPP in Feb 2019, and the agreed upon fix is reflected in C1-191425 (CR0112R1) for Rel-14, C1-191426 (CR0113R1) for Rel-15 and C1-191427 (CR0114R1) for Rel-16. 3GPP thinks that no other changes are needed and that the issue is closed. |
| 11 | (PT2) 10.1.11 Nested PrivateCallKMSURI Element in User Profile Configuration  In 3GPP TS 24.484 Section 8.3.2.1 item 8)-i-C-I a *PrivateCallKMSURI* element that contains one or more entry elements is defined. However, in the XSD, the *PrivateCallKMSURI* contains another nested *PrivateCallKMSURI* element, so that for example the following XML snippet is the only way to define a KMS URI with the value "sip:kms1@example.com":  <PrivateCallKMSURI>  <PrivateCallKMSURI>  <uri-entry>sip:kms1@example.com</uri-entry>  </PrivateCallKMSURI>  </PrivateCallKMSURI>  …  So it could be considered a definition like:  <xs:element name="PrivateCallKMSURI" type="xs:anyURI"/>  Since the *PrivateCallKMSURI* is integrated in the enclosing *PrivateCallList* element using an *anyExt* element there can be an unbounded number of *PrivateCallKMSURI* anyway, which would satisfy the semantics of the textual definition in the standard.  (Also reported for Plugtest 3) | The use of the same element name “PrivateCallKMSURI” for two different elements, one of which is contained in the other, can be seen as unfortunate and maybe a bit confusing. However, the set of text in TS 24.484 dealing with “PrivateCallKMSURI” is considered correct. No changes are being made by CT1 in this regard. If Plugtest participants feel that we misunderstand the concern, we ask that they resubmit the issue with explanation of how their thoughts differ from CT1’s view. |
| 12 | (PT2) 10.1.12 Resource Namespace/Priority in Service Configuration  In 3GPP TS 24.484 Section 8.4.2 it is stated that the *emergency-resource-priority*, *imminent-peril-resource-priority*, and *normal-resource-priority* elements have to contain two elements defined as follows:  a) one <resource-priority-namespace> string element containing a namespace defined in IETF RFC 8101 [20]; and  b) one <resource-priority-priority> string element element containing a priority level in the range specified in IETF RFC 8101 [20];  …  We think that this definition could be improved to not only eliminate (potential errors due to) the redundancy (e.g. a namespace of mcpttp with a priority of mcpttq.0 could be defined) but also restrict the priority value.  …  (Also reported for Plugtest 3) | 3GPP has chosen the method in RFC 8101 to define the priorities for MCPTT. While any number of solutions could have been chosen, this is what now exists. For reasons of maintaining backward compatibility, no changes will be made to the use of RFC 8101. |
| 13 | (PT2) 10.1.13 On-network and Off-network: May, Shall and how often?  In TS 24.484 Section 7.2.2.1 the contents of the *mcptt-UE-initial-configuration* root element are defined as follows:  *The <mcptt-UE- initial-configuration> document:*  *…*  We would need some clarification on whether presence of an on-network/off-network element is mandatory or not, and in any case, whether a restriction to a single maximum occurrence should be considered.  (Also reported for Plugtest 3) | The text of TS 24.484 is:  The <mcptt-UE- initial-configuration> document:  1) shall include a "domain" attribute;  2) may include a <mcptt-UE-id> element;  3) may include a <name> element;  4) may include a <Default-user-profile> element;  5) may include an <on-network> element;  6) may include an <off-network> element; and  7) may include any other attribute for the purposes of extensibility.  The use of "may" for both on-network and off-network indicates that inclusion of each of these is optional. The use of "an" indicates a single occurrence and does not allow for multiple occurrences. |
| 14 | (PT2) 10.1.14 User Profile Document Name  In TS 24.484 Section 8.3.2.8 it is stated, that *The name of user profile configuration document shall be "user-profile"*, while in Section 8.3.1 the following definition is given: *The name of the MCPTT user profile document matches the value of the <ProfileName> element in the MCPTT user profile document.*  We think the latter naming convention for user profile documents is more practical, since there are certainly more than one in most cases. However, the ProfileName element is not mandatory, so clarification would be needed.  (Also reported for Plugtest 3) | As noted for Issu 6: from Release 15 onward, the MCPTT, MCVideo, and MCData user profiles have a profile index specified. |
| 15 | (PT2) 10.1.15 User Profile: PrivateCallURI and PrivateCallProSeUser  The standard states in Section 8.3.2.1 that the *PrivateCallList* element contains a "*<PrivateCallURI> element that contains one or more <entry> elements*" and a "*<PrivateCallProSeUser> element that contains one or more <ProSeUserID-entry> elements*".  In the XSD the *PrivateCallURI* element actually is of type *EntryType* itself and therefore a single entry (named *PrivateCallURI*) and not a list of elements named *entry* of type *EntryType*. Basically the same applies to the *PrivateCallProSeUser* element.  However, because both are nested within a *choice* element with maxOccurs="unbounded" they themselves may occur more than once.  (Also reported for Plugtest 3) | This issue was resolved by changes in release 16. Please see TS 24.484 v16.6.0 or later. |
| 16 | (PT2) 10.1.16 Minor but recurring inconsistencies between Structure & Validation chapters and the XSD  In this section a few common types of inconsistencies between the standard text in natural language (mostly the *Structure* and *Validation* sections for **every configuration document** (in 24.484 and 24.481) and the *XML Schema Definition*, are listed with examples. Only one example per type is given.  1. Undefined *any*, *anyExt* and *anyAttribute* elements that are, nevertheless, in the XSD. For example: In the *mcptt-UE-initial-configuration* complex type an *any* and an *anyExt* element are defined without being mentioned in the text. In the textual definintion of the *mcptt-UE-id* neither an *any*, *anyExt*, or *anyAttribute* element are mentioned, but present in the XSD.  2. The *attributeGroup IndexType* is also never mentioned in the text.  (Also reported for Plugtest 3) | GPP CT1 have no plans to define the "any", "anyExt", or "anyAtribute" components of the schemas. These components constitute a technique for being able to add extensions to the schema without creating a backward compatibility. They are defined by W3C. See, for example, https://www.w3schools.com/xml/schema\_complex\_any.asp .  IndexType is defined as type "token". |
| 17 | (PT2) 10.1.17 Minor inconsistencies between the textual definition and the XSD  In this section a few minor inconsistencies between the standard text in natural language and the *XML Schema Definition*, are listed.  • 7.2.2.3: *mcptt-UE-initial-configuration*: <xs:element name="HPLM"> maybe should be <xs:element name="HPLMN">  • 7.2.2.3: *mcptt-UE-initial-configuration*: <xs:element name="VPLM"> maybe should be <xs:element name="VPLMN">  • The *Instance-ID-URN* attribute in the *mcptt-UE-initial-configuration* complex type is never mentioned to be there in the text.  • 8.3.2.1: *mcptt-user-profile*: The *EmergencyCall* element in the *PrivateCall* element is defined mandatory, but optionally in the XSD.  (Also reported for Plugtest 3) | Partial Response:  The misspellings of "HPLM", "VPLM" and "VPLMType" are corrected.  OPEN: The lack of description of the attribute "Instance-ID-URN" is under investigation.  The incorrect XML specification of the EmergencyCall subelement of the PrivateCall element is fixed from Rel-14 onward. |
| 18 | (PT2) 10.1.18 The *any*, *anyExt*, and *anyAttribute* Discussion  There has been quite some discussion on the pros and cons of using the XML Schema's *any* element, *anyAttribute*, and in this case also the locally defined *anyExtType* (For the sake of readability in the following it will be referred to these elements/attributes casually as "*anys*".). Especially when it comes to the validation of XML documents, there are many different views. We want to point out some examples of noteworthy effects we encountered.  …  Although the root element is a complex type with a choice element with minOccurs="1" and some mandatory elements in that choice this is possible. The reason is, that there is an any element with minOccurs="0", so one can choose "minimally 1 times 0 any" which results in an empty root element.  (Also reported for Plugtest 3) | 3GPP CT1 have chosen to use the "any", "anyExt", and "anyAttribute" techniques from W3C. There are no plans to change that decision. |
| 19 | (PT2) 10.1.19 MCData notifications  MCData notifications work in the following way:  When a MCData client sends a SDS or FD message, a request to receive notifications can be included. The MCData client who receives the message generates the notifications. The request to receive notifications is included in an additional field in message signalling. The notification messages use their own type and they are also included in the signalling part.  When the server receives a message including a notification request, it must save the Conv ID and Msg ID included in the message. This is necessary because when the server receives a notification it must check that the Conv ID and MSG ID included in it can be correlated to a previous message requesting the notification.  …  The solution to this issue could be for the server to include its PSI in <mdata-controller-psi> in the initial MESSAGE.  (Also reported for Plugtest 3) | The steps in 12.2.1.1 and 12.2.2.1 that were of concern have been deleted. This removes the problem of the notifiying client sending an invalid message. |
| 20 | (PT2) 10.1.20 MCVideo Media ID field  A definition for the Media ID field is still missing in TS 24.581. This field is used when the media is multiplexed and is included in some of the message definitions in Section 9.2.4.  (Also reported for Plugtest 3) | The Media ID field has been removed. |
| 21 | (PT3) 10.1.18 Usage of <mcptt-request-uri> element of mcptt-info+xml  As per 3GPP TS 24.379 [9], <mcptt-request-uri> should be used as follows:  3) the <mcptt-request-uri> can be included with:  a) a value set to an MCPTT group ID or temporary MCPTT   group ID when the <session-type> is set to a value of   "prearranged" or "chat"; and  b) a value set to the MCPTT ID of the called MCPTT user   when the <session-type> is set to a value of "private";  But, in subclause 11.1.1.2.1.1 of 3GPP TS 24.379 [9], MCPTT ID of invited user is placed in MIME resource-lists body. To make prearranged group call and private call procedure consistent, the suggestion would be to remove usage of MIME resource-lists body in subclause 11.1.1.2.1.1 and instead use <mcptt-request-uri> element of application/vnd.3gpp.mcptt-info+xml MIME body. | While the approach suggested in issue statement may be a possible solution, the existing standard accomplishes the goal. For backward compatibility reasons, 3GPP CT1 has no plans to change the existing usage. |
| 22 | (PT3)10.1.19 Usage of <mcptt-called-party-id> element in mcptt-info+xml  The element <mcptt-called-party-id> of mcptt-info+xml MIME body contains redundant information which is already present in <mcptt-request-uri> element of mcptt-info+xml.  The usage of element <mcptt-called-party-id> of mcptt-info+xml MIME body can be removed. Information is already passed to relevant entity using <mcptt-request-uri> element of mcptt-info+xml. | The TS 24.379 rapporteur indicates:  While I agree that when the CF resolves a group-id and targets individual users, then the <mcptt-request-uri> essentially contains the same content as the <mcptt-called-party-id>, I believe that this XML element is also used in the procedures for remotely initiated private calls in TS 24.379.  Additionally please check the tables at the back of TS 24.379 in H.2 and H.3. We also set the <mcptt-called-party-id> in the 200 OK to the SIP INVITE.  Thus, I do not agree to remove the use of <mcptt-called-party-id>. That may have an impact on procedures.  Investigation of clauses H.2 and H.3 finds specific indications of the use of <mcptt-called-party-id> that have been in the TS since Rel-13. Therefore, no changes are planned as a result of this comment. |
| 23 | **ETSI Plugtest Technical Constraint 10.2.4:**  **CLARIFICATION: Need for Client Authentication in IDMS**  Many of the vendors’ implementations of IdMS and MCPTT Auth included/required Client Authentication using HTTP Basic Auth.  Regarding 3GPP TS 33.180 [24] this type of mechanisms is only mentioned a couple of times, for example: "Note that client authentication is REQUIRED for native applications (using PKCE) in order to exchange the authorization code for an access token. Assuming that client secrets are used, the client secret is sent in the HTTP Authorization Header."  But nowhere else in the standard is mentioned the use of client authentication or Basic HTTP Auth mechanisms. It is missing completely from the example just below the aforementioned sentence, in section B.4.2.4. Moreover, most of the implementations require the presence of this Basic HTTP Auth (Authorization header) with a content consisting of user:password coded in Base64. This basic method is not specified in the standard (other than inter-domain auth), although it's specified in IETF [RFC 6749](https://tools.ietf.org/html/rfc6749) [38].  Adding an additional layer of client/UE authentication to the mix (apart from UE-id registering in the IdMS), would probably not represent any benefit. It really adds up to the UE registration phase, because instead of only provisioning the IdMS with the UE-id, the client secret must be also provisioned back to the UE.  If a discussion finally validates this HTTP Basic mechanism, it would be reasonable to modify the standard to include more details about this, and clarify client authentication procedures. | **SA3 Response:**  Please note that the use of HTTP Basic authentication is optional but “recommended” per OAuth 2.0 RFC 6749 section 2.3.1 (copied here for convenience):  “2.3.1. Client Password  Clients in possession of a client password MAY use the HTTP Basic authentication scheme as defined in [RFC2617] to authenticate with the authorization server. The client identifier is encoded using the "application/x-www-form-urlencoded" encoding algorithm per Appendix B, and the encoded value is used as the username; the client password is encoded using the same algorithm and used as the password. The authorization server MUST support the HTTP Basic authentication scheme for authenticating clients that were issued a client password.  For example (with extra line breaks for display purposes only):  Authorization: Basic czZCaGRSa3F0Mzo3RmpmcDBaQnIxS3REUmJuZlZkbUl3  Alternatively, the authorization server MAY support including the client credentials in the request-body using the following parameters:  client\_id  REQUIRED. The client identifier issued to the client during the registration process described by Section 2.2.  client\_secret  REQUIRED. The client secret. The client MAY omit the parameter if the client secret is an empty string.  Including the client credentials in the request-body using the two parameters is NOT RECOMMENDED and SHOULD be limited to clients unable to directly utilize the HTTP Basic authentication scheme (or other password-based HTTP authentication schemes). The parameters can only be transmitted in the request-body and MUST NOT be included in the request URI.  For example, a request to refresh an access token (Section 6) using the body parameters (with extra line breaks for display purposes only):  POST /token HTTP/1.1  Host: server.example.com  Content-Type: application/x-www-form-urlencoded  grant\_type=refresh\_token&refresh\_token=tGzv3JOkF0XG5Qx2TlKWIA  &client\_id=s6BhdRkqt3&client\_secret=7Fjfp0ZBr1KtDRbnfVdmIw  The authorization server MUST require the use of TLS as described in Section 1.6 when sending requests using password authentication. Since this client authentication method involves a password, the authorization server MUST protect any endpoint utilizing it against brute force attacks.”  In TS 33.180 (annex B.4.2.4), it states; “Note that client authentication is REQUIRED for native applications (using PKCE) in order to exchange the authorization code for an access token. Assuming that client secrets are used, the client secret is sent in the HTTP Authorization Header.” This sentence applies specifically to the OAuth redirection step when the client is redirected from the authoriz authorization endpoint to the token endpoint and must use Proof Key for Code Exchange (PKCE). While PKCE is required, HTTP Basic authentication SHOULD be used if client secrets are used. The use of client secrets is not mandatory.  When not otherwise specified in 33.180, the use of HTTP Basic authentication is per OAuth 2.0 specifications RFC 6749 & RFC 6750.  To clarify this, SA3 has agreed on the following CR: S3-194000. |

**3. Proposal**

It is proposed that CT1 improve this table with whatever information can be added. Those issues that are to be addressed by SA6, SA3 or another 3GPP WG will be addressed upon notification by the WG with primary responsibilty for the issue.

It is proposed that CT1 continue to gather issue resolutions and forward them to ETSI Plugtest at an appropriate time. It is understood that a report to ETSI Plugtest could be made prior to completion of all resolutions to assist them in their work and any upcoming Plugtest events.