|  |
| --- |
| Input Contribution |
| Meeting ID\* | SDS- TP 54 |
| Title:\* | Updated resolution table |
| Source:\* | Rana Kamill, BT, rana.kamill@bt.com |
| Date:\* | 2020-05-10 |
| Input related to\* | TS0003 Rel 2, Rel 3, Rel 4 |
| Intended purpose ofdocument:\* | [ ]  Decision[x]  Discussion[ ]  Information[ ]  Other <specify> |
| Impacted other TS/TR(s) | TS0003, 2.18 and Editorial issues, new diagram, new Annexes |
| Decision requested or recommendation:\* | Docu |
| Template Version: January 2020 (do not modify) |

**oneM2M Notice**

The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in Annex 1 of the Partnership Agreement.

# Updated resolution table.

**Table updated to reflect the changes applied/ to be applied to Rel 2. Based on ITU-T recommendations**.

# Resolution list to draft new Recommendation ITU-T Y oneM2M.SEC.SOL.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **C/Q** | **ITU-T- SG20 Question**  | **oneM2M Response**  | **ITU & oneM2M Discussions outcome** | **oneM2M proposed Changes to TS-0003** |  **Current Status** | **Final agreements** |
| 1 | Clarifications on listing certain encryption protocols (e.g. starting from article 10.1.1.1) without clarifying the possibility to use alternative IETF RFCs (for example - RFC This may limit the use of different RFCs rather than the ones listed in this oneM2M Security Solutions V2.4.1 document. | These RFC’s describe the Russian Federal standard GOST crypto algorithms. oneM2M’s intention in listing certain encryption protocols was to ensure the maximum support in deployed devices and applications by maintaining alignment with 3GPP TS33.210. This serves as a central repository for cryptographic profiles for security above the IP layer. ( see [S3-182166.zip](https://www.3gpp.org/ftp/tsg_sa/wg3_security/TSGS3_92_Dalian/Docs/S3-182166.zip) ) | Further clarification is needed for reflecting other crypto algorithms and how they can be reflected (e.g. disclaimer).\* Procedure related for modification. | Not changing anything for now.From an operability perspective, we didn’t want to leave it open. We chose an example that is used in the industry.The intention was to reduce cost and complexity by aligning with the algorithms of 3GPP. TS33.210. | Not changed. |  Agreed with the addition of the following text:Given RFCs in this Draft recomemndations are just examples for crypto algorithms and not intended to be an exclusive list of such algorithms. Note: It was agreed to add an additional sentence clarifying that these are just examples which are not exclusive. |
| 2 | TLS RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2", and RFC 6347: "Datagram Transport Layer Security Version 1.2" are obsoleted by the IETF who have replaced these RFCs with V1.3 of both protocols. TLS version 1.3 is documented in RFC8446 which was published in August 2018. Work on DTLS V1.3 has completed and new RFC is expected on within Q1 2020. | This will be reviewed when DTLS version 1.3 is published.oneM2M’s previous view was that TLS 1.3 contains major changes which may cause backward compatibility issues in context oneM2M specifications, and a simple reference change to TLS 1.3 will break the assumption that TLS and DTLS versions are aligned in TS-0003, especially for cipher suites. [LS in [TP-2018-0299R02](http://member.onem2m.org/Application/documentApp/documentinfo/?documentId=28592&fromList=Y)] | OneM2M needs more time to change the reference to DTLS v1.3 as more secured protocols and to align with 3GPP on using relevant versions of TLS protocol. It is to be considered as part of release 4 of oneM2 Specs.\* Procedure related for reference of latest versions of protocols that are being considered in oneM2M Rel 4 Specs. | Positive agreement, if we can link it to protocols which may have already been released. oneM2M preference would be to keep the existing one and to put a note in TS-0003 stating that v1.3 shall be considered in a future release of the document (t.b.c. by ITU-T SG20 Q6) | Agreed- Work in Progress in oneM2M. | AgreedNote: oneM2M will ensure the text in the Draft Recommendation and oneM2M TS will be aligned reflecting the agreement.  |
| 3 | Other concerns about IETF standards are: RFC2104 updated by RFC6151 | RFC6151 is a supplement to RFC2104 and does not replace it. Both RFCs to be referenced in TS-0003. | To be updated in oneM2M Rel. 4 Specs. Also, maintenance of Rel. 2 & Rel. 3 will be also discussed in OneM2M\* Procedure related for reference of latest references that are being considered in oneM2M Rel 4 Specs or maintenance of previous releases. | [Q3- In Progress]:// Keep (Original) + Add (Selected Supplement) |  Work In progress in oneM2M. | AgreedNote: oneM2M will ensure the text in the Draft Recommendation and oneM2M TS will be aligned reflecting the agreement. |
|  | RFC3548 obsoleted by RFC4648 | RFC3548 to be replaced by RFC4648. | RFC to be replaced. |  | Further comments:\* Procedure related for reference of latest references that are being considered in oneM2M Rel 4 Specs or maintenance of previous releases |
|  | RFC4492 updated by RFC5246, RFC7027, RFC7919 | RFC4492, RFC5246 and RF7027 are to be referenced in TS-0003. RFC7919 is a specialised RFC focused on Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS) and does not have to be referenced in TS-003. | Agreed: keep the reference to RFC4492, add reference to supplements RFC5246 and RFC7027: To be updated in oneM2M Rel. 4 Specs. Also, maintenance of Rel. 2 & Rel. 3 will be also discussed in OneM2M\* Procedure related for reference of latest references that are being considered in oneM2M Rel 4 Specs or maintenance of previous releases.Agreed: RFC7919 does not have to be referenced in new releases. | Keep original RFC/ Add supplement RFCs |  |  |
|   | RFC5246 updated by RFC5746, RFC5878, RFC6176, RFC7465, RFC7507, RFC7568, RFC7627, RFC7685, RFC7905, RFC7919 | To align with the TLS profiles within 3GPP [TS33.210], the specification shall be amended to support RFC7465, RFC7627 and RFC7919.The other RFCs do not need to be specifically referenced in TS-0003. | Agreed: Keep reference RFC5246, add supplements RFC7465, RFC7627 and RFC7919: To be updated in oneM2M Rel. 4 Specs. Also, maintenance of Rel. 2 & Rel. 3 will be also discussed in OneM2M\* Procedure related for reference of latest references that are being considered in oneM2M Rel 4 Specs or maintenance of previous releases.Agreed: the other RFCs do not need to be specifically referenced. | Keep original RFC l/ Add supplement RFCs |  |  |
|  | RFC5280 updated by RFC6818 | RCF6818 is only an 8 page supplement for a particular case. It could not replace RFC5280 which is 147 pages. Both RFCs to be referenced in TS-0003.  | Agreed: Keep existing reference and add new: To be updated in oneM2M Rel. 4 Specs. Also, maintenance of Rel. 2 & Rel. 3 will be also discussed in OneM2M\* Procedure related for reference of latest references that are being considered in oneM2M Rel 4 Specs or maintenance of previous releases. | Keep original RFC l/ Add supplement RFCs |  |  |
|  | RFC6347 updated by RFC7507, RFC7905 | RFC7507 and RFC7905 are each considered an 8 page supplement to RFC6347 which is 31 pages. All RFCs to be referenced in TS-0003. | Keep original RFC l/ Add supplement RFCs |  |  |
|  | Unused reference to RFC7252 | To be deleted. | AgreedTo be updated in oneM2M Rel. 4 Specs. Also, maintenance of Rel. 2 & Rel. 3 will be also discussed in OneM2M\* Procedure related for reference of latest references that are being considered in oneM2M Rel 4 Specs or maintenance of previous releases. | Mentioned 6 times, There was a space between RFC and 7252. Space deleted. |  |  |
|  | Unused reference to RFC6920 | To be deleted. | Mentioned 4 times, There was a space between RFC and 6920. Space removed. |  |  |
| 4 | It is recommended to avoid using the term “legal” within ITU documents due to its policy implications; for example in page 217 in the wording “country legal mandate” and in page 219 such as “Legal Region, Legal country, Legal city, Legal state”, and considering the obligatory requirement when using “shall be”. | This is intentional, as it is important to have a mechanism in the Privacy Policy Manager (PPM) that ensures that, for example, the ability for a Service Provider to collect specific items of data, according to their local policy, can be overridden by a national policy. Perhaps “Policy Precedence- City” etc. should be used instead.  | Agreed:-Change the word “Legal” across the document and to use instead “Policy Precedence”-Use “should” instead of “shall”To be updated in oneM2M Rel. 4 Specs. Also, maintenance of Rel. 2 & Rel. 3 will be also discussed in OneM2M\* Procedure related for reference of latest references that are being considered in oneM2M Rel 4 Specs or maintenance of previous releases. | Replace “legal” with “Policy Precedence Region/ City” | Changed | Agreed as requested by Q6/20 experts. Note 1: -Changed the word “Legal” across the document and to use instead “Policy Precedence”-Use “should” instead of “shall”Note 2: oneM2M will ensure the text in the Draft Recommendation and oneM2M TS will be aligned reflecting the agreement. |
| 5 | The use of Country Code is not aligned throughout the document in different cases. At page 37, 2‑character Country code is used, while at page 244 F.1.2, two-letters country codes is used to represent countries and special regions of geographical interest. [b-ISO 3166-1]. However, Parameter CC - The country where the device or service provider is located with CC Value “variable” (not 2 character/letter) is used in Annex J (page 249). It is highly recommended to align all relevant cases.  | Agree. This should be aligned ISO 3166-1:2013 and annex J will be updated  | Agreed: | Code to be changed to make sure that it is fully aligned with the spec.  | Changed. | Agreed as requested by Q6/20 experts. Note: oneM2M will ensure the text in the Draft Recommendation and oneM2M TS will be aligned reflecting the agreement. |
| 6 | The Reference to “ISO 3166” is recommended to be normative. | Agree. This will be made normative  | Agreed | Reference to be made normative. | Changed. | Agreed as requested by Q6/20 experts. Note: oneM2M will ensure the text in the Draft Recommendation and oneM2M TS will be aligned reflecting the agreement. |
| 7 | ISO CC may be user defined and there is already user defined CC for some organizations. Does it mean that user-defined CC is used for IoT security identification?  | ISO 3166 has “*User-assigned code elements are codes at the disposal of users who need to add further names of countries, territories, or other geographical entities to their in-house application of ISO 3166-1, and the ISO 3166/MA will never use these codes in the updating process of the standard. The following codes can be user-assigned:[[12]](https://en.wikipedia.org/wiki/ISO_3166-1%22%20%5Cl%20%22cite_note-13)* * *[Alpha-2](https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2%22%20%5Cl%20%22User-assigned_code_elements%22%20%5Co%20%22ISO%203166-1%20alpha-2): AA, QM to QZ, XA to XZ, and ZZ*
* *[Alpha-3](https://en.wikipedia.org/wiki/ISO_3166-1_alpha-3%22%20%5Cl%20%22User-assigned_code_elements%22%20%5Co%20%22ISO%203166-1%20alpha-3): AAA to AAZ, QMA to QZZ, XAA to XZZ, and ZZA to ZZZ*
* *[Numeric](https://en.wikipedia.org/wiki/ISO_3166-1_numeric%22%20%5Cl%20%22User-assigned_code_elements%22%20%5Co%20%22ISO%203166-1%20numeric): 900 to 999*

Decision for oneM2M plenary?  | OneM2M to check at next plenary the following: - Confirm that user-defined CC can, or can’t, be used for IoT security identification- adding the *following codes to Specifications which can be user-assigned:[[12]](https://en.wikipedia.org/wiki/ISO_3166-1%22%20%5Cl%20%22cite_note-13)* * *[Alpha-2](https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2%22%20%5Cl%20%22User-assigned_code_elements%22%20%5Co%20%22ISO%203166-1%20alpha-2): AA, QM to QZ, XA to XZ, and ZZ*
* *[Alpha-3](https://en.wikipedia.org/wiki/ISO_3166-1_alpha-3%22%20%5Cl%20%22User-assigned_code_elements%22%20%5Co%20%22ISO%203166-1%20alpha-3): AAA to AAZ, QMA to QZZ, XAA to XZZ, and ZZA to ZZZ*
* *[Numeric](https://en.wikipedia.org/wiki/ISO_3166-1_numeric%22%20%5Cl%20%22User-assigned_code_elements%22%20%5Co%20%22ISO%203166-1%20numeric): 900 to 999*

- Adding user-defined codes to oneM2M registry (May not be recommended by oneM2M experts) | We will allow this, oneM2M will not maintain a register to make sure that implementations do not select clashing codes. | Changed | Agreed as requested by Q6/20 experts. Note: oneM2M will ensure the text in the Draft Recommendation and oneM2M TS will be aligned reflecting the agreement. |
| 8 | In Annex J, the term “nation” is used many times. For example, “The nation **were** the data stored, or if part of a wider framework (such as the EU)”. Should it read as “The nation **where** the data stored…)? Is it different from Country and/or Country code? | Will change to country  | Agreed with changing “nation” to “country”.(e.g. change the given example from “The nation **were** the data stored…)?” to “The **country** **where** the data stored…)?” | The term ‘nation’ to be replaced by. ‘Country’.Spelling of ‘where’ to be corrected. | Changed | Agreed as reflected in the updated Draft Recommendation text |
| 9 | In Annex J, there is a reference to “Tag Company Registration number”. It is not clear who is the registrar, and how to get or use this number? | OK. This was UK specific and thinking of the UK company registration authority <https://beta.companieshouse.gov.uk/>This could be changed to be more generalIts use would be as an aid to checking the authenticity of the company asking to use the data and how much trust to place in it  | Agreed to change “Tag Company Registration number” to be more general regarding the registrar.Note: To be checked through correspondence how this to be reflected. | We will add the following to the text: ‘Other equivalent country registration authorities can be used as an aid to check the authenticity of the company asking to use the data and how much trust to place in it.’  | Changed | Agreed as reflected in the updated Draft Recommendation text |
| 10 | There are number of editorial modifications that will be done in order to comply with the ITU-T rules and procedures for drafting ITU Recommendations. a.       Numbering of Annexes and Appendices should comply with the Author’s Guide for drafting ITU-T Recommendation. Numbering of Appendices should use roman numbering instead of using letters in alphabetical order. b.      Definitions with references (e.g. TIA, ETSI) should be listed under section “3.1 Terms defined elsewhere” | Decision for oneM2M plenary on whose responsibility it is to make the changes if agreed | Agreed to write in annex and relevant paragraphs “that original text in this section is not available anymore“ for and section with blanked text.Secretariats between ETSI and ITU should make the alignment across the text considering possibility of not referring to “ deleted text in oneM2M” or to keep any text for reference.Note: oneM2M follows the ETSI template rules and procedures. oneM2M may check such alignment in next plenary including the reason for deletion if possible. | AGREEDSecretariats between ETSI and ITU should make the alignment across the text considering possibility of not referring to “ deleted text in oneM2M” or to keep any text for reference.Another discussion:Solved by Q28 comments. There will be empty sections and annexes which will be intentionally left blank. | No change for now.According to oneM2m drafting rules, we cannot draft the letters.However, it can be removed from ITU-T document. | Note: oneM2M will send a request to consider the use of numbering in the Annexes to TSB and TSB will provide an update at the next e-meeting.  |
| 11 | There are number of other issues that can be of editorial nature. For example: a.       “NA” values in Annex J with possible yes/no Parameters, b.      ITU-T X.509 deletion from references while it is used in the body of the Recommendation; c.       Any reference to oneM2M Technical Specification, which is transposed to ITU-T documents, should follow ITU-T referencing procedure within ITU-T Recommendation, (e.g. reference to TS-0022 vs [ITU-T Y.4500.22]) | 1. will review and correct if necessary

 1. included in section 2.2 informative references.
2. Decision for oneM2M plenary on whose responsibility it is to make the changes if agreed

  | For “a”:Agreed to use “Data not collected” instead of “NA”.For “b”: Agreed to add reference to “ITU-T X.509” to normative referencesFor “c”Agreed on changing the references from oneM2M Technical Specification, corresponding ITU-T references/ITU-T Recommendation, (e.g. reference to TS-0022 to change to [ITU-T Y.4500.22])Note: OneM2M plenary to discuss the proposed editorial modifications to ensure consistency and confirm back to ITU.Russia reserves position for point “a” considering consultation with programmer. | We will replace ‘NA’ with for example‘Data not collected’We will change Annex K to say ‘If the filter frame value is not equal to ‘no data collected’ or ‘No data shared’, etc.’For c: <No changes will be done in OneM2M documents>Editorial update on the side of ITU-TWe will include ‘X.509’ in Section 2.2.Check with OneM2M who would be responsible for making the changes. | a) Changed.b) Work in Progress.c) Editorial update on the ITU-T side. | a) Agreed as reflected in the updated Draft Recommendation text.b) Changedc) Changed.Note: oneM2M will send a request to consider the use of numbering in the Annexes to TSB and TSB will provide an update at the next e-meeting.  |
| 12 | Further clarification is required for the following text in the Summary “This Recommendation provides normative and informative specifications”. Which part of the document is considered as “informative specifications” and which is “normative specifications”? | Can’t find the quoted text in TS-0003-Security\_Solutions-V4\_1\_0(cl).doc or TS-0003-Security\_Solutions-V2\_15\_0(cl).docx | Agreed to modify “Summary section” of ITU-T Draft Recommendation by deleting “normative and informative” to be “This Recommendation provides specifications for M2M Security and Privacy protection. | Agreed | Changed.// The text does not currently exist in neither Rel 2or further releases. | Agreed as reflected in the updated Draft Recommendation text |
| 13 | Two bibliography sections are given; one is under Appendix I, and the second one is at the end of Recommendation. Hence, Appendix I may need to be deleted and only relevant references to be moved to the bibliography at the end. | Corrected in TS-0003-Security\_Solutions-V4\_1\_0(cl).docAnnex N (informative): Bibliography Page 269  | Correction is already reflected in new oneM2M TS version.Corresponding modifications to current version of Draft ITU-T Recommendation need to be shared by oneM2M. Proposed to take the text from Release 4 and update Release 2 accordingly.To be further checked during the correspondence. | Corrected in TS-0003-Security\_Solutions-V4\_1\_0(cl).docAnnex N (informative): Bibliography Page 269  | Changed.Annex I no longer exists. It has been removed from version 2. (To be removed from the ITU-T version) | Agreed as reflected in the updated Draft Recommendation text |
| 14 | Alignment may be needed between Figure 5.1.0-1 on high level overview of the Security architecture, and the description of the layers and functions in section 5.1, 5.2, 5.3 and the detailed explanation in section 6.2 as follows: a.       The figure did not capture the “Security service layer” in section 5.2.1 b.  “Trust Enabling security functions” in section 6.2.6 is not captured in Figure 5.1.0-1 and is not listed under section 5.2.1. c.   Section 6.2.2 (Authorization Architecture) should be listed as sub-section of 6.2.1 on “Access Management”, so numbering should change to section 6.2.1.2 instead of 6.2.2. d. “Access control” service is listed in section 5.2.1 under “Access Management” service group, but no corresponding details are found under section 6.2. e.   “security Association Establishment” function has no corresponding details under section 6.2 | This will be reviewed and corrected  | Agreed, to consider the following corrections:a.       The figure did not capture the “Security service layer” in section 5.2.1 b.  “Trust Enabling security functions” in section 6.2.6 is not captured in Figure 5.1.0-1 and is not listed under section 5.2.1. c.   Section 6.2.2 (Authorization Architecture) should be listed as sub-section of 6.2.1 on “Access Management”, so numbering should change to section 6.2.1.2 instead of 6.2.2. d. “Access control” service is listed in section 5.2.1 under “Access Management” service group, but no corresponding details are found under section 6.2. e.   “security Association Establishment” function has no corresponding details under section 6.2 | Check availability of an editable copy of the diagram.Figure 5.1.0-1: High level overview of the Security architectureAgreed that it will be reviewed and corrected. | Changed.New Diagram added. | Agreed as reflected in the updated Draft Recommendation textEd. note under section 5.2.1 has been resolved and deleted accordingly  |
| 15 | Further clarification on the direct security association between Application Entities (AE)/ Common Service Entity (CSE) and the encryption of the content of resources exchanged between them. | Will clarify that "direct security association" in 6.1.1 Interactions between layers is detailed in section 8.5 End-to-End Security of Data (ESData) | Agreed to add paragraphs in both sections:6.1.1 Interactions between layers is detailed in section 8.5 End-to-End Security of Data (ESData)For clarification of direct security association between Application Entities (AE)/ Common Service Entity (CSE) and the encryption of the content.Note: Text to be prepared and agreed through correspondence discussions.  | Add text: “Direct security association" in 6.1.1 Interactions between layers is detailed in section 8.5 End-to-End Security of Data (ESData) | Changed. | Agreed as reflected in the updated Draft Recommendation text |
| 16 | Further clarification is requested for the security pre-provisioning and security post-provisioning phases under section 6.1.2.1 on Enrolment phase, including how remote pre-provisioning of security keys can be used with a post-provisioning framework. | Will review this and provide further clarification  | OneM2M will review this and provide further clarification in next meeting | To be reviewed/ Further text to be added.We do not use ‘Pre-provisioning’ or ‘Post-provisioning’ terminology in One M2M | Details referred to in sections 8.2.3.1, 8.2.3.2, 8.2.3.3. These sections are referred to in section 6.1.2.1. | Sentence added. |
| 17 | The GBA based remote security provisioning framework provides details for only 3GPP related specifications. Questions are raised on how to extend such functionality to non-3GPP based devices? | The intention of the GBA framework was to allow 3rd parties to make use of the globally recognised symmetric credentials within the device and secure API’s into the HSS in a mobile operator’s network. For oneM2M, this third party was foreseen as a one M2M Service Provider who could make use of this pre-existing connectivity and credentials from the underlying mobile network to “bootstrap” derived credentials to be used in the oneM2M service layer. If the definition of a non-3GPP based device is one without 2G, 3G, 4G functionality and the associated credentials, then by definition, it is not possible to extend such functionality as suggested. This is the reason why certificate based solutions are also specified in TS-0003. Also, please remember that GBA was specified some 19 years ago and there are now many other globally recognised credentials in use. See [S3-010040.zip](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_17_Gothenberg/Docs/ZIP/S3-010040.zip)  | Agreed to add the following:“The definition of a non-3GPP device is one without 2G, 3G, 4G functionality and the associated credentials. So it is not possible to use this functionality for non-3GPP devices.However, it should be note that there are many other globally recognised credentials in use for non-3GPP devices.” | Applies definition to 3GPP devices.We will add the following statement:“The definition of a non-3GPP device is one without 2G, 3G, 4G functionality and the associated credentials. So it is not possible to use this functionality for non-3GPP devices.” | // Sentence added to 6.1.2.1 | Agreed as reflected in the updated Draft Recommendation text |
| 18 | In section 6.1.2.2 on operational phase and as stated in the document, the pre-provisioning key could impose security threats unless used in conjunction with secured environments. As mentioned in this specification document, the reference framework to interface M2M entities with the 3GPP UICCs specifications is provided in Annex D. Questions are raised on how to extend such functionality to non-3GPP based devices? | Since by definition, there will be a very wide range of non-3GPP based devices with many different implementations. As these are not likely to be standardised, this is not in the scope of oneM2M or 3GPP. However, security best practice guides are available from ETSI <https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf>IoTSF, https://www.iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2\_Digitalv3.pdfGSMA <https://www.gsma.com/iot/iot-security/iot-security-guidelines/>  | Agreed, (e.g. in section 6.1.2.2) to add:Long-term Provisioned Secure Connection Keys can pose a security risk if not adequately secured, and for this reason long term Provisioned Secure Connection Keys are recommended to be stored in Secure Environments.Long-term Pre-Provisioned Symmetric Enrolee Keys can pose a security risk if not adequately secured, and for this reason it is recommended that Long term Pre-Provisioned Symmetric Enrolee Keys are stored in Secure Environments.[See also “Annex – Secure storage of Long Terms keys”.]Also, text to be add:“ The focus of this oneM2M specification is the xxxxxxx related to 3GPP systems and devices. Other systems related aspects could be addressed by other specifications and fora.”Note: Additional information on future features and to consider extending these features to other non-3GPP systems is useful. | [Since by definition, there will be a very wide range of non-3GPP based devices with many different implementations. As these are not likely to be standardised, this is not in the scope of oneM2M or 3GPP. However, security best practice guides are available from ETSI <https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf>IoTSF, https://www.iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2\_Digitalv3.pdfGSMA <https://www.gsma.com/iot/iot-security/iot-security-guidelines/>Long term Provisioned Secure Connection Keys can pose a security risk if not adequately secured, and for this reason long term Provisioned Secure Connection Keys are recommended to be stored in Secure EnvironmentsLong term Pre-Provisioned Symmetric Enrolee Keys can pose a security risk if not adequately secured, and for this reason it is recommended that Long term Pre-Provisioned Symmetric Enrolee Keys are stored in Secure Environments.Added to an Annex K- Secure storage of Long Terms Keys.?? | Work in progress. |  |
| 19 | In the sequence of events highlighted in the certificate based security association establishment framework (as detailed in section 8.2.2.2), the certificate chain is listed as optional. This could have negative security implications. To avoid such implication, setting the certificate chain as a mandatory feature is to be recommended rather than being optional, while still clarifying to the end users that non-compliance would raise a considerable risk for them. | Will consider making mandatory  | Agreed to remove (Optionally) and make it mandatory as well as adjust it in section 8.2.2.2:A Certificate Chain from the entity's Certificate to a Root Certificate:The entities validate each other's Certificate before trusting the Public Verification Keys in the Certificate. Within the Security Handshake, entity A creates a digital signature of the session parameters using its private signing key and entity B verifies the digital signature using entity A's public verification key. Then the roles are reversed: entity B creates a digital signature and entity A verifies it. For more details see clause 8.2.2.2. | Will consider making mandatory.(Optionally) a Certificate Chain from the entity's Certificate to a Root Certificate.The entities validate each other's Certificate before trusting the Public Verification Keys in the Certificate. Within the Security Handshake, entity A creates a digital signature of the session parameters using its private signing key and entity B verifies the digital signature using entity A's public verification key. Then the roles are reversed: entity B creates a digital signature and entity A verifies it. For more details see clause 8.2.2.2.  | Work in Progress |  |
| 20 | Further clarification on the rational for not including the GBA based authentication in the operational phases similar to the enrolment phase. | The intention of the GBA framework was to allow 3rd parties to make use of the globally recognised symmetric credentials within the device and secure API’s into the HSS in a mobile operator’s networkThe use of GBA is intended only to then use that to derive a number of symmetric credentials that can be used for any purpose at the application layer, not necessarily for authentication. The oneM2M specifications then use these to derive a number of symmetric credentials as input to the Pre-Shared Key (PSK) authentication and confidentiality and integrity protection security protocols, specifically (D)TLS-PSK and PSK-Based SAEF, ESPrim and ESData as described in TS-0003.  | Agree as clarified with no further modifications |  In this case, the M2M Enrolment Function includes the functionality of a GBA Bootstrap Server Function. This framework uses 3GPP or 3GPP2 symmetric keys to authenticate the Enrolee and the M2M Enrolment Function (which is also a GBA BSF). The details are specified by 3GPP TS 33.220 [**Error! Reference source not found.**] and 3GPP2 S.S0109-A [**Error! Reference source not found.**]. The use of GBA is intended only to then use that to derive a number of symmetric credentials that can be used for any purpose at the application layer, not necessarily for authentication. The oneM2M specifications then use these to derive a number of symmetric credentials as input to the Pre-Shared Key (PSK) authentication and confidentiality and integrity protection security protocols, specifically (D)TLS-PSK and PSK-Based SAEF, ESPrim and ESData as described in TS-0003. For more details see clause 8.3.2.3. | No modifications needed. | Agreed – with no change  |
| 21 | The 3GPP generic authentication architecture identified two types of authentication mechanisms; GBA in TS 33.220 and Support for Subscriber Certificates (SSC) in TS 33.221. A question is raised on the possibility of including both mechanisms for the security provisioning framework and security association establishment framework in both enrolment and operational phases, respectively? | As mentioned in response to Question 17, GBA was specified GBA was specified some 19 years ago See [S3-010040.zip](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_17_Gothenberg/Docs/ZIP/S3-010040.zip) There are now many other globally recognised ways of deploying certificate in devices. In fact oneM2M specifies two on these in TS-0003. These are:- Simple Certificate Enrolment Protocol (SCEP) in section 8.3.6.3 Certificate Provisioning procedures using SCEP and Enrolment over Secure Transport (EST) in section 8.3.6.2 Certificate Provisioning procedures using EST.GBA was specified for 3G and 4G LTE networks and is not supported on 5G networks. However, 3GPP has a study on providing an equivalent feature called AKMA see  [http://www.3gpp.org/ftp//Specs/archive/33\_series/33.535/33535-040.zip](http://www.3gpp.org/ftp/Specs/archive/33_series/33.535/33535-040.zip) oneM2M’s priority would be to ensure that this new 5G feature was integrated in oneM2M specifications. Also IoT devices that have an eSIM with remote change of subscription as defined in the GSMA specifications <https://www.gsma.com/esim/esim-specification/> require device certificates and oneM2M priority would be to ensure that this eSIM feature is integrated in oneM2M specifications.  | Agree to add regarding Simple Certificate Enrolment Protocol (SCEP) in section 8.3.6.3 Certificate Provisioning procedures using SCEP the following:“TS33.221 supports for subscriber certificates (SSC) is not supported in this specification considering that there are many other globally recognized ways of deploying certificates in devices.“ | M2M Enrolment Function includes the functionality of a GBA Bootstrap Server Function. This framework uses 3GPP or 3GPP2 symmetric keys to authenticate the Enrolee and the M2M Enrolment Function (which is also a GBA BSF). The details are specified by 3GPP TS 33.220 [**Error! Reference source not found.**] and 3GPP2 S.S0109-A [**Error! Reference source not found.**]. TS33.220 supports the subscriber certificates (SSC) is not supported in the specification as there are now many other globally recognized ways of deploying certificate in devices. Simple Certificate Enrolment Protocol (SCEP) in section 8.3.6.3 Certificate Provisioning procedures using SCEP and Enrolment over Secure Transport (EST) in section 8.3.6.2 Certificate Provisioning procedures using EST.For more details see clause 8.3.2.3. |  Work in Progress. | Work in progress |
| 22 | It is suggested to change "data is" to "data are". | Both uses seem to be accepted in modern English  | Agreed to change "data is" to "data are" |  | Changed. | Agreed as reflected in the updated Draft Recommendation text |
| 23 | Section 5.2.1 on Access Management needs to be expanded for Identification (service) with corresponding amendments in the text. | Agree will add text | Agreed for Section 5.2.1 on Access Management needs to be expanded for Identification (service) with corresponding amendments in the text. | Agree will add text.Identification added (Before Authorization) | Changed. | Agreed as reflected in the updated Draft Recommendation text |
| 24 | Further clarification is needed for Identity protection in section 6.2.4 (e.g. there are not limited to Identity protection only, but some other tasks are provided as well.) | oneM2M has a new work item on oneM2M System Enhancement to Support Privacy Data Protection Regulations (eDPR). We will update this clause with the results of that work.  | Agree as clarified with no further modificationsNote: This issue will be addressed in future versions/releases of oneM2M  | AGREED - Awaiting the completion of (eDPR) work item by oneM2M delegate.. | No change for now. | No change for now. |
| 25 | Section 6.3.2 needs basic model description or requirements for SE Plug-in to ensure compatibility. | We will provide a summary for both section 6.3.2 and 6.3.3 oneM2M TS-0016: "Secure Environment Abstraction as this work is now complete  | Agree to add summaries related to (basic model description or requirements for SE Plug-in to ensure compatibility) to sections 6.3.2 and 6.3.3 oneM2M TS-0016 “Secure Environment Abstraction” | AGREED: Summarizing the sections in the documents is in progress. To be updated once finished. (Sections in 0016 will be summarized and added to TS-0003 and 0016 is explicitly referenced as this work had not been done in release 2) | No change for now//Not Rel. 2 related. | No change for now |
| 26 | Further clarification is needed for proposal to use RSA, which may not be reliable in many implementations. | Need more clarification on what the concerns are with the use of RSA Cryptography  | Agree as clarified with no further modificationsNote: Further discussions might be needed to the relevant aspects of RSA (e.g. efficiency) compared with other Cryptographies. ITU Q6 may also further clarify the meaning by reliability of RSA, if necessary, noting that other Cryptographies are already referenced in this oneM2M specification. | The action is currently on ITU-T side and we are awaiting their comment. | No change for now. | Added the following paragraph:Agreed with the addition of the following text:Given RFCs in this Draft recomemndations are just examples for crypto algorithms and not intended to be an exclusive list of such algorithms. |
| 27 | Further clarification is needed to describe PSO-Decipher for RSA implementation/usage | There is only one mention in TS-0003 of“Perform Security Operation (PSO)” but following links could be used as a basis for further clarification Asymmetric Secure Element (ASE)GlobalPlatform Card Specifications GlobalPlatform® Card Specification, Version 2.3<https://globalplatform.org/wp-content/uploads/2017/09/GPC_2.2_F_SCP11_v1.0.pdf><https://globalplatform.org/wp-content/uploads/2017/09/GPC_2_3_F_SCP11_v1.2_PublicRelease.pdf>However, it is not needed for the specification and the reference to the PSO command shall be deleted. | Agreed to Delete reference to the PSO command since it is not needed for the specification. | To be researched.If f we can’t find it, we will remove it.It is suggested to remove the reference completely. | Work in progress.//Comment deleted | No change required. |
| 28 | Further clarification is needed for the validity of keeping the “Void” text in draft ITU-T Recommendation (e.g. paragraphs (8.3.3, 9.2.2.2), Annexes B, E, G, H, I, K, L, Appendices C, D, F, J). ITU-T SG20 would seek oneM2M approval to delete sections with “Void” text in the relevant ITU-T Recommendation. | This would mean continually renumbering TS-003 and the clause references in other specifications that refer to it. This is not in accordance line with the ETSI Drafting Rules [https://portal.etsi.org/Portals/0/TBpages/edithelp/Docs/40\_directives\_apr\_2019\_part2%20(EDR).pdf](https://portal.etsi.org/Portals/0/TBpages/edithelp/Docs/40_directives_apr_2019_part2%20%28EDR%29.pdf)2.12.1 Clause numbering2.12.1.0 Clause numbering issuesEXAMPLE 1: It is necessary to update an ETSI deliverable. A new clause needs to be inserted between the existing clauses 8 and 9. A new clause 8a **shall** be inserted in preference to avoid re-numbering the existing clauses. EXAMPLE 2: A new figure needs to be inserted between existing figures 4 and 5. A new figure 4a **shall** be inserted to avoid re-numbering of all subsequent figures. Similarly, an existing element may be deleted and replaced with the term "Void" to minimize disruption to the numbering scheme. EXAMPLE 3: During the updating of an ETSI deliverable, it is decided that annex C is no longer required. The title of annex C becomes "Void". Later annexes, therefore, remain unchanged. EXAMPLE 4: It is decided to delete a note 3, so the text of note 3 becomes "Void" and there is no need to re-number note 4. | Agreed to keep blank text for alignment purpose but with clarification that the text is intentionally left blank:“*This annex/section/xxx is intentionally left blank”* |  ITU-T decided to accept the internal comment to introduce a text saying something along the lines of ‘This Annex will intentionally be left blanc’ | Corrected in the ITU-T document.The numbering system remains the same in oneM2M Specifications. | Added‘This annex is intentionally left blank. ‘The difference between an annex and an appendix in ITU-T is that annexes are used to include normative material, while appendices are used for non-normative material. (See [The Author’s guide](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itu.int%2Foth%2FT0A0F000004%2Fen&data=04%7C01%7Crana.kamill%40bt.com%7Cac724ddc73d64866adb708da1bba3d22%7Ca7f356889c004d5eba4129f146377ab0%7C0%7C0%7C637852783955053837%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=QvUTYRq13njz8GAQxFJ2ic38wsDWm6Z0Mn9YBy%2BacFc%3D&reserved=0))’ |

\_\_\_\_\_\_\_\_\_\_\_\_