|  |
| --- |
| CHANGE REQUEST |
| Meeting ID:\* |  SDS 53 |
| Source:\* | Rana Kamill |
| Date:\* | 2022-02-01 |
| Reason for Change/s:\* | CR TS-0003 Country Codes update R2 |
| CR against: Release\* | Release 2 |
| CR against: WI\* | [ ]  Active <Work Item number> [x]  MNT maintenance / < Work Item number(optional)>Is this a mirror CR? Yes [ ]  No [ ] mirror CR number: (Note to Rapporteur - use latest agreed revision)[ ]  STE Small Technical Enhancements / < Work Item number (optional)>Only ONE of the above shall be ticked |
| CR against: TS/TR\* | TS-0003 v4.6 |
| Clauses \* | 2.1, 2.2, 11.4.1.3, Annex F.1.2 |
| Type of change: \* | [x]  Editorial change[ ]  Bug Fix or Correction[ ]  Change to existing feature or functionality[ ]  New feature or functionalityOnly ONE of the above shall be ticked |
| Other TS/TR(s) impacted | <TS/TR number>, <Version Number>, and <Description on which aspect should be reflected in this TS/TR> |
| Post Freeze checking:\* | This CR contains only essential changes and corrections? YES [ ]  NO [ ] This CR may break backwards compatibility with the last approved version of the TS? YES [ ]  NO [ ]  |
| 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.

GUIDELINES for Change Requests:

Provide an informative introduction containing the problem(s) being solved, and a summary list of proposals.

Each CR should contain changes related to only one particular issue/problem.

If this is a correction, and the change applies to previous releases, a separate “mirror CR” should be posted at the same time as this CR

Mirror CR: applies only when the text, including clause numbering are exactly the same.

Companion CR: applies when the change means the same but the baselines differ in some way (e.g. clause number).

Follow the principle of completeness, where all changes related to the issue or problem within a deliverable are simultaneously proposed to be made e.g. a change impacting 5 tables should not only include a proposal to change only 3 tables. Include any changes to references, definitions, and abbreviations in the same deliverable.

Follow the drafting rules.

All pictures must be editable.

Check spelling and grammar.

Use change bars for modifications.

The change should include the current and surrounding clauses to clearly show where a change is located and to provide technical context of the proposed change. Additions of complete clauses need not show surrounding clauses as long as the proposed clause number clearly shows where the proposed new clause is located.

Multiple changes in a single CR shall be clearly separated by horizontal lines with embedded text such as, start of change 1, end of change 1, start of new clause, end of new clause.

When subsequent changes are made to the content of a CR, then the accepted version should not show changes over changes. The accepted version of the CR should only show changes relative to the baseline approved text.

## Introduction

This CR proposes some updates to the TS-0003 Release 2 according to the conclusions of ITU-T SG20 and oneM2M joint meeting.

This contribution also proposes some changes for the TS-0003 Release 3.

### -----------------------------------Start of change 1------------------------------------------

# 2 References

## 2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non‑specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

The following referenced documents are necessary for the application of the present document.

[1] oneM2M TS-0001: "Functional Architecture".

[2] oneM2M TS-0011: "Common Terminology".

[3] Void.

[4] oneM2M TS-0004: "Service Layer Core Protocol Specification".

[5] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[6] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[7] ETSI TS 102 225 (V11.0.0): "Smart Cards; Secured packet structure for UICC based applications (Release 11)".

[8] ETSI TS 102 226 (V11.0.0): "Smart Cards; Remote APDU structure for UICC based applications (Release 11)".

[9] 3GPP TS 31.115 (V10.1.0): "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications (Release 10)".

[10] 3GPP TS 31.116 (V10.2.0): "Remote APDU Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications (Release 10)".

[11] 3GPP2 C.S0078-0 (V1.0): "Secured packet structure for CDMA Card Application Toolkit (CCAT) Applications".

[12] 3GPP2 C.S0079-0 (V1.0): "Remote APDU Structure for CDMA Card Application Toolkit (CCAT) Applications".

[13] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[14] 3GPP2 S.S0109-0: "Generic Bootstrapping Architecture (GBA) Framework".

[15] IETF RFC 4279: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[16] Void.

[17] Void.

[18] IETF RFC 5705: "Keying Material Exporters for Transport Layer Security (TLS)".

[19] IETF RFC 3629: "UTF-8, a transformation format of ISO 10646".

[20] "Unicode Standard Annex #15; Unicode Normalization Forms", Unicode 5.1.0, January 2008.

NOTE: Available at <http://www.unicode.org>.

[21] GlobalPlatform® Device Technology TEE Management Framework (TMF) Version 1.

[22] GlobalPlatform® Device Technology TEE System Architecture, Version 1.1.

[23] ETSI TS 102 671: "Smart Cards; Machine to Machine UICC; Physical and logical characteristics".

[24] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[25] ETSI TS 102 484: "Smart Cards; Secure channel between a UICC and an end-point terminal".

[26] ISO/IEC 7816-4: "Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange".

[27] ETSI TS 101 220: "Smart Cards; ETSI numbering system for telecommunication application providers".

[28] This reference is intentionally left blank

[29] This reference is intentionally left blank

[30] This reference is intentionally left blank

[31] IETF RFC 6655: "AES-CCM Cipher Suites for Transport Layer Security (TLS)".

[32] IETF RFC 5289: "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)".

[33] IETF RFC 2104: "HMAC: Keyed-Hashing for Message Authentication".

[34] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[35] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[36] IETF RFC 6961: "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension".

[37] IETF RFC 7250: "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)".

[38] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

[39] Federal Information Processing Standard (FIPS) 186-4: "Digital Signature Standard (DSS)".

NOTE: Available at <https://csrc.nist.gov/publications/detail/fips/186/4/final>.

[40] IETF RFC 6920: "Naming Things with Hashes".

[41] IETF RFC 4648: "The Base16, Base32, and Base64 Data Encodings".

[42] IETF RFC 5487: "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode".

[43] IETF RFC 4492: "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)".

[44] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[45] IETF RFC 7251: "AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS".

[46] IETF RFC 5480: "Elliptic Curve Cryptography Subject Public Key Information".

[47] GlobalPlatform® Device Technology Secure Element Remote Application Management v1.0 GPD‑SPE-008.

[48] IETF RFC 5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF).

[49] IETF RFC 7518 (2015): "JSON Web Algorithms (JWA)".

[50] IETF RFC 7516 (2015): "JSON Web Encryption (JWE)".

[51] IETF RFC 7515 (2015): "JSON Web Signature (JWS)".

[52] W3C® Recommendation: "XML Signature Syntax and Processing v1.1", 2013.

NOTE: Available at <http://www.w3.org/TR/xmldsig-core1/>.

[53] IETF RFC 7519 (2015): "JSON Web Token (JWT)".

[54] OpenID Foundation: "OpenID Connect Core 1.0", 2014.

[55] W3C® Recommendation: "XML Encryption Syntax and Processing v1.1", 2013.

NOTE: Available at <http://www.w3.org/TR/xmlenc-core1/>.

[56] Void.

[57] oneM2M TS-0022: "Field Device Configuration".

[58] oneM2M TS-0032: "MAF and MEF Interface Specification".

[59] IETF RFC 7030: "Enrollment over Secure Transport".

[60] IETF Historic draft: "Simple Certificate Enrollment Protocol", draft-nourse-scep-23.

NOTE: Available at <https://tools.ietf.org/html/draft-nourse-scep-23>.

[61] IETF Historic draft: "Simple Certificate Enrollment Protocol", draft-gutmann-scep-10.

NOTE: Available at <https://www.ietf.org/id/draft-gutmann-scep-10.txt>.

[62] SOG-IS: "SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms", Version 1.0, May 2016.

[63] IETF RFC 5639: "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation".

[64] ISO 3166-1:2013: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".

### -----------------------------------End of change 1------------------------------------------

### -----------------------------------Start of change 2------------------------------------------

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non‑specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] oneM2M Drafting Rules.

NOTE: Available at <http://www.onem2m.org/images/files/oneM2M-Drafting-Rules.pdf>.

[i.2] This reference is intentionally left blank

[i.3] This reference is intentionally left blank

[i.4] oneM2M TR-0008: "Analysis of Security Solutions".

[i.5] eXtensible Access Control Markup Language (XACML) Version 3.0. 22 January 2013. OASIS Standard.

[i.6] Handbook of Applied Cryptography, A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, CRC Press, 1996.

[i.7] Recommendation ITU-T X.509 (10/2012): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.8] This reference is intentionally left blank

[i.9] OMA-TS-REST-NetAPI-TerminalLocation-V1-0-20130924-A: "RESTful Network API for Terminal Location", Version 1.0.

[i.10] This reference is intentionally left blank

[i.11] ISO/IEC 7816-5: "Identification cards - Integrated circuit cards - Part 5: Registration of Application Providers".

[i.12] Guide to Attribute Based Access Control (ABAC) Definition and Considerations, NIST Special Publication 800-162.

NOTE: Available at <http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf>.

[i.13] National Institute of Standards and Technology: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)".

[i.14] This reference is intentionally left blank

[i.15] oneM2M TR-0019: "Dynamic Authorization for IoT".

[i.16] oneM2M TR-0012: "oneM2M End-to-End Security and Group Authentication".

[i.17] oneM2M TR-0001: "Use Cases collection".

[i.18] IANA JSON Web Token (JWT) registry.

NOTE: Available at <http://www.iana.org/assignments/jwt/jwt.xhtml>.

[i.19] IETF RFC 6455: "The Web Socket Protocol", December 2011.

[i.20] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[i.21] This reference is intentionally left blank

[i.22] <https://github.com/certnanny/sscep>.

[i.23] <https://github.com/jscep/jscep>.

[i.24] <https://github.com/certnanny/sscep/issues/42>.

[i.25] oneM2M TS-0005: "[Management Enablement (OMA)](http://member.onem2m.org/Application/documentApp/documentinfo/?documentId=25523&fromList=Y)".

[i.26] oneM2M TS-0006: "[Management Enablement (BBF)](http://member.onem2m.org/Application/documentApp/documentinfo/?documentId=25523&fromList=Y)".

### -----------------------------------End of change 2------------------------------------------

### -----------------------------------Start of change 3------------------------------------------

## 11.4 Privacy Policy Manager Implementation Models

### 11.4.1 Using Terms and Conditions Mark-up Language

#### 11.4.1.0 Introduction



Figure 11.4.1.0-1: Privacy Policy Manager Implementation Model Using Terms and Conditions
Mark-up Language, for one end user (#1) and one Application Service Provider (Provider 1)

The above model views the components of the Privacy Policy Manager (PPM) for one end user (#1) and one ASP (Provider 1), arranged as a number of selected/not selected filters in a series of stackable Filter Frames.

Four mandatory Filter Frames are defined:

1. Descriptor Filter Frame.
2. At least one "Provider Terms and Conditions" Filter Frame.
3. User Preferences Filter Frame.
4. At least one "Presented to user" Filter Frame.

Within each Filter Frame, there are grids representing the Privacy Tags in the Mark-up Language, vertically and the applications and/or devices, horizontally.

For the Provider Terms and Condition Filter Frame and User Preferences Filter Frame, each attribute represented by the privacy tag configured as being "selected" or "not selected" for a particular application/device is modelled by "dropping in" an appropriate coloured filter disc.

Discs at the same positions within one or more similarly structured "Presented to user Filter Frames" detect clear paths through the Filter Frame stack:

* Where provider terms and conditions and user preferences are in agreement, these discs turn green.
* Where the paths are blocked by one or more conflicts, similar detectors turn the discs red.

EXAMPLE: If the Application Service Provider expects the user to agree to location information to be collected and shared with a 3rd party, then the ASP selects those two attributes (clear discs) If the end user has set a preference that they do not want location information to be collected and shared, then there will be black discs in the User Preferences Filter Frame and path through the stack will be blocked.

Optional additional Filter Frames may be placed in the stack to "select" or "not select" those same features again by "dropping in" an appropriate coloured filter disc. For example, a country legal mandate may overrule an application Service Provider or end user selection. The position of these optional Filter Frames determines the precedence, with those at the front overruling those at the back.

The assumption with this model is that the vast majority of the provider attributes selected by the application Service Provider will not conflict with user preferences and will show green. However, there will be a very large numbers of devices, applications and frequency of software updates, and additions replacements of devices. While most will not result in a conflict, those that do will be instantly identified by one or more red discs which are only displayed to the end user, thus avoiding the need to constantly read and reread hundreds of pages of detailed T&Cs.

There shall be an instance of this stack for each end user who is registered with the PPM and an instance for each Application Service Provider for which they have subscribed. However, the Descriptor Filter Frame and optional city/state/country/region Filter Frames may be shared resources for these instances.

While the description software implementation of this model is outside the scope of the present document, sample code for implementation of the logic is shown in annex K (informative).

#### 11.4.1.1 Registration of Application Service Provider Privacy Policy

1. Optional registration of an applications Privacy Policy shall be part of the process of obtaining a Registered App‑ID for each application and version and presenting a security certificate to the oneM2M Registration Authority that is used to authenticate the application and version.
2. The ASP shall download an application Terms and Conditions (T&C) import template from the oneM2M App-ID Registry server, if they do not already have the correct application T&C import template.
3. The application T&C import template shall list in numeric order the tags in normative annex J.

NOTE: The format of the T&C import template is left to implementation, as long as it is able to convey the information specified in annex J.

1. For each tag in the list, the ASP shall provide a value for all devices and applications in the scope of the application that the ASP is registering in the format defined in normative annex J.
2. The ASP shall process the application T&C import template using their local systems and procedures with input from devices vendors and third parties who provide components of their application to create one or more provider T&Cs.
3. The oneM2M App-ID Registry shall, at a minimum, also provide the ASP with the "descriptors list" in the language of the oneM2M partner to support the ASP in completing the T&C import templates to form the set of Provider T&C for that ASP.
4. The security certificate that was used during the App-ID registration process shall also be used to ensure integrity and protect the completed application T&C import template in subsequent storage and transmission.
5. The oneM2M App-ID Registry shall check the authenticity and integrity of the ASP T&Cs by verifying the signature with the ASP public key certificate during App-ID Registration.
6. Each ASP or software vendor T&C completed shall be associated to the App-ID in the oneM2M App‑ID Registry.

#### 11.4.1.2 Registration of End User Privacy Preferences

1. When an end user subscribes to a service provided by an application service provider, the end user becomes a data subject, and the data subject downloads or views the end user privacy preferences template from the PPM Portal.
2. The template used by the end user to state their privacy preferences shall align with the template used by the Application Service Provider i.e. the tags as listed in normative Annex J shall be displayed in the same order.
3. The end user selects and deselects attributes to state their privacy preferences which are then registered on the PPM using the same portal.

#### 11.4.1.3 Creating a customized Privacy Policy for each end user

1. To make it easy for the data subject to confirm differences between the privacy preference and the privacy policy:

a) If the ASP's selection of the feature represented by the tag value matches the privacy preference selected by the user for that Application/Device, then the corresponding "presented to user" indicator shall be set to green.

b) If the ASP's non selection of the feature represented by the tag value matches the privacy preference set by the user for that Application/Device, then the corresponding "presented to user" indicator shall be set to green.

c) If the ASP's value selected for the feature represented by the tag value matches the privacy preference selected by the user for that Application/Device, then the corresponding "presented to user" indicator shall be set to green.

d) If the ASP's selection of the feature represented by the tag value does not match the privacy preference selected by the user for that Application/Device, then the corresponding "presented to user" indicator shall be set to red.

e) If the ASP's non selection of the feature represented by the tag value does not match the privacy preference selected by the user for that Application/Device, then the corresponding "presented to user" indicator shall be set to red.

f) If the ASP's value set for the feature represented by the tag value does not match the privacy preference set by the user for that Application/Device, then the corresponding "presented to user" indicator shall be set to red.

1. The above rules shall be overridden if one or more optional preference profiles are present.
2. The order of precedence shall be:

1) Policy PrecedenceRegion.

2) Policy PrecedenceCountry.

3) Policy PrecedenceCity.

4) Policy PrecedenceState.

5) Parental Control.

### -----------------------------------End of change 3------------------------------------------

### -----------------------------------Start of change 4------------------------------------------

Annex F (normative):
Acquisition of Location Information for Location based Access Control

# F.0 Introduction

When a request (resource access) is evaluated by a Hosting CSE and an accessControlLocationRegions parameter is defined in the privileges attribute of the <accessControlPolicy> resources, the Hosting CSE shall check whether the location of the Originator of a request is in the specified regions or not. Therefore, the Hosting CSE shall retain the location of the Originator, or acquire the location or deny the access. This annex indicates how to describe the location regions and obtain the location of the Originator.

# F.1 Description of Region

## F.1.1 Circular Description

The practical way of describing the region or area is the circular presentation and generally the circle is characterized by the co-ordinates of a center point of the circle and a radius. Geographically, the center point and radius is described as longitude and latitude, and meter respectively. For this description, the accessControlLocationRegions parameter shall be represented as a circle.



Figure F.1

## F.1.2 Country Description

Another simple way of describing the region or area is the country presentation. ISO-3166-1 alpha 2 codes [i.10] are two-letter 2 character/letter codes to represent countries and special regions of geographical interest. For example, KR is a code for Korea, Republic of.

Note: ISO 3166 states “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:[[](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

 OneM2M will not prevent users from making use of this feature but will not maintain a register of these user assigned codes so there is a risk of duplication in implementations leading to inconsistent operation .

### -----------------------------------End of change 4------------------------------------------