|  |  |
| --- | --- |
| Agenda | |
| Meeting title: | SEC 23 F2F meeting (TP 23) |
| Chair: | Francois Ennesser |
| Secretary: | Karen Hughes, ETSI |
| Meeting Date: | 2016-05-16 to 2016-05-20 |
| Meeting Details: | Ordinary face-to-face meeting during TP23  in Seoul, South Korea |
| Intended purpose of  document: | Decision  Discussion  Information  Other <specify> |

Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by all provisions of IPR policy of the admitting Partner Type 1 and permission that all communications and statements, oral or written, or other information disclosed or presented, and any translation or derivative thereof, may without compensation, and to the extent such participant or attendee may legally and freely grant such copyright rights, be distributed, published, and posted on oneM2M’s web site, in whole or in part, on a non-exclusive basis by oneM2M or oneM2M Partners Type 1 or their licensees or assignees, or as oneM2M SC directs.

**oneM2M Procedure Notice**:   
oneM2M activities must adhere to the oneM2M Partnership Agreement and Working Procedures, which are based on principles such as fairness, due process, openness and transparency.

**IPR Notices:**Each oneM2M Partner Type 2 and oneM2M Member contributing to the technical work of oneM2M must grant a perpetual, worldwide, royalty-free, nonexclusive license: to incorporate material from contributions into oneM2M Technical Specifications and Technical Reports; and for the oneM2M Partners Type 1 to publish the contributed material in Technical Specifications and Technical Reports. Care should be taken when making contributions containing third party material to ensure that the contributor has the right to grant the appropriate license for this material.

Each oneM2M Member who engages in oneM2M activities through its membership in a Partner shall be required to comply with that Partner Type 1’s IPR policies, procedures and guidelines with respect to the availability of licenses for IPR(s) that are or may be essential to implement Technical Specifications and/or Technical Reports developed in oneM2M.

oneM2M cannot ensure the accuracy or completeness of any disclosure, investigate the validity or existence of a patent, or determine whether a patent is essential to the use of a oneM2M Technical Specification or Technical Report.

**Antitrust Risk Notice:**oneM2M participants should be sensitive to, and avoid discussions within oneM2M on, sensitive topics such as licensing terms, price, territories, specific contractual terms, etc.

1 Opening of meeting

1.1 Welcome

1.2 Schedule for WG4 SEC

|  |  |  |
| --- | --- | --- |
| MONDAY | | |
| **Kumkang 3** | | **11:00-12:30** | **SEC Opening Session S1**  Agenda Items 7.1, 7.2 |
| **Kumkang 1 & 2** | | **15:30-17:00** | **Joint Session with ARC & PRO Jap1**  Handling of Agenda Items 5.4 / 5.5 between ARC, PRO and SEC |
| **Kumkang 4** | | **17:00-18:30** | **Drafting Session D1**  Agenda Item 5.4 (Stage 2 Finalization), 7.1 |
| TUESDAY | | |
| **Kumkang 3** | | **8:30-10:00** | **SEC Session S2**  Agenda Item 5.1, 5.2 |
| **Kumkang 1 & 2** | | **15:30-17:00** | **Joint Session with REQ Jr1**  Agenda Item 5.3 / 7.1 |
| **Kumkang 4** | | **17:00- 18:30** | **Drafting Session D2**  Agenda Item 5.1, 5.2 |
| WEDNESDAY | | |
| **Kumkang 1** | | **8:30-10:00** | **Joint Session with ARC and PRO Jap2**  Agenda Item 5.4, 5.5 |
| **Kumkang 4** | | **13:30-17:00** | **Double Drafting Session D3**  Agenda Item 5.1, 5.2 (5.4, 5.5) |
| Thursday | | |
| **Kumkang 1** | | **10:30-12:00** | **SEC Session S3**  Agenda Item 5.x, 6.x |
| **Kumkang 4** | | **13:30-15:00** | **Drafting Session D4**  Any remaining issue |
| **Kumkang 1** | | **15:30-17:00** | **Joint Session with MAS Jm1**  Agenda Item 5.6  TS-0022 and TS-0003 synchronization |
| **Kumkang 3** | | **17:00-18:30** | **Joint Session with ARC and PRO Jap3** |
| FRIDAY | | |
| **Kumkang 3** | | **8:30-10:00** | **SEC Closing Session S4**  Conclusions on Agenda Items 6.x  Any pending contributions / topics  Review of Action Points  Future meetings |

1.3 Attendees

2 Review of Agenda

Present document

3 Approval of previous Minutes and draft deliverables

* SEC 22.4 Minutes: SEC-2016-0097 agreed by Correspondence
* Draft deliverables:
  + TS-0003 Rel-1 Baseline: v1.4.1 available on portal
  + TS-0003 Rel-2 Baseline: v2.1.0 (SEC-2016-0077)
  + TS-0016 draft Baseline: v0.5.0 (in SEC-2016-0075)
  + TR-0012 draft Baseline: v0.9.0 (in SEC-2016-0076)
  + TR-0016 draft baseline: v0.6.0 (in SEC-2016-0078)
  + TR-0019 draft baseline: v0.5.0 available on portal

3 Review of Objectives for the Meeting

* Any pending Release 2 Stage 2 clarification (as needed) on TS-0003 or TS-0001
  + TBD with ARC and PRO
* Review and implement Stage 3 action plan for each Release 2 security features (to be discussed with PRO)
  + Stage 3 impact on TS-0003
  + Impact on TS-0004 and Bindings
* Addressing and removing editor’s notes from TS-0003
* Update status of TR deliverables scheduled for Release 2: TR-0008 (Rel-2), TR-0012, TR-0019, TR-0016. Move status forward toward publication according to decisions.
  + Freeze and / or approval of intended deliverables
* Start discussing Use Cases / Requirements / features for future releases, if time permits

4 Review of Action Items

|  |  |  |  |
| --- | --- | --- | --- |
| REFERENCE | WHAT | WHO | STATUS |
| A-WG4-SEC22-1 | Clean-up TS-0001 for Distributed Authorization, following discussions on ARC-2016-0185R05 | All | OPEN |
| A-WG4-SEC22-2 | Clean-up TS-0003 for Role-Based Access Control, following discussions on SEC-2016-0059R01 | All | OPEN |
| A-WG4-ARC22.3 | Identify changes needed to TS-0003 to enable a single AE to register to multiple CSE, potentially using different identifiers and credentials for each CSEs (see ARC-2016-234R01)  Note: Is there anything that prevents breaking an “AE” with such requirements into several AEs, each one corresponding to only one ID/Credential? An AE is just an instantiation of a code into a process on a computing hardware. Constraining the instantiation of a code into multiple processes for such use cases could solve the issue, without introducing an additional layer of complexity in our specs. | All | OPEN |

5 Corrections and enhancements CRs (generic WIs)

5.1 Corrections / Clarifications to TS-0003 Rel-1

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

5.2 Enhancements to TS-0003 (Rel-2)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SEC-2016-0094R02 | TS-0003 CR Role Based Access Control | Datang | | R01:Remove AppID  R02: Merge PDP and PIP in Hosting CSE (steps 6, 7) as distributed Auth is Rel-3  R03: split issuance of roles vs tokens,indicate that role definition/assignation is out of scope |
| SEC-2016-0098R03 | TS-0003 CR Token Structure | Datang | | To Open first before ARC discussion  R01: Remove AppID |
| SEC-2016-0065R05 | CR TS-0003 R2 Updates to MAF text | Qualcomm | | R06 agreed with editorials |
| SEC-2016-0091 | CR TS-0003 R2 Certificate Enrolment procedure call flow | Qualcomm | | Ex part of 71 |
| SEC-2016-0092 | CR TS-0003 Usage-constrained key derivation from Ke | Qualcomm | | Ex part of 71 |
| SEC-2016-0095 | CR TS-0003 R2 Cl 8.4 ESPrim cleanup | Qualcomm | |  |
| SEC-2016-0096 | CR TS-0003 R2 Defining E2E parameters and attributes | Qualcomm | |  |
| SEC-2016-0099R01 | CR TS-0003 R2 ESPrim stage 3 | Qualcomm | |  |
| SEC-2016-0100 | CR TS-0003 R2 ESData stage 3 | Qualcomm | |  |
| SEC-2016-0106 | CR Dynamic Authorization Cleanup | Interdigital | |  |
| SEC-2016-0107 | CR TS-0003 E2EKey becomes ESCertKE | Qualcomm | |  |
| SEC-2016-0071R02 | CR TS-0003 Cert Enrolment core changes | | Qualcomm |  |
| SEC-2016-0108 | CR Token Evaluation | Datang | | *Extract from 94* |
| SEC-2016-0TBC | CRF Clause 11 Rel-2 update | KDDI | |  |

5.3 Security related contributions affecting REQ deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| REQ-2016-0040 | TR-0026 Vehicle location privacy protection | Huawei |  |
| REQ-2016-0042 | CR TS-0002 Requirements coverage for Release 2 | NEC (Vice-chair) |  |
| REQ-2016-0045 (SEC-2016-0103) | Work item on requirements for a new secure element | ETSI TC SCP |  |

5.4 Security related contributions affecting ARC deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| ARC-2016-0244 | CR TS-00001 R2 Local-Token-IDs | Qualcomm | **TBD: R2 Bug Fix OK? (not SEC)** |
| ARC-2016-0245R01 | CR TS-00001 R2 cl 11.4.2 ESPrim cleanup | Qualcomm | **R2 Bug Fix presented** |
| ARC-2016-0236R04 | CR Role and Token Resource types | Datang | **R4: Restrict permissions, clarify why roles vs Priivileges?** |
| ARC-2016-0231R03 | CR Role Parameter Name in Request | Datang | **R2 > Multiple or single AppID, and Roles? Structure to clarify**  **R03 AGREED** |
| ARC-2016-0232R04 | Distributed Authorization Resource types and procedures | Datang | **R3** |
| ARC-2016-0233R03 | CR Access Control Policy Resource type | Datang | **R3** |
| ARC-2016-0286 | CR TS-0001 E2EKey becomes ESCertKE | Qualcomm | **(editorial)** |
| ARC-2016-0285 | CR Dynamic Authorization Cleanup | Interdigital |  |
| ARC-2016-0155R03 | App-ID field for message | Fujitsu |  |

5.5 Security related contributions affecting PRO deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| PRO-2016-0132R01 | ACP interpretation on Registration procedure | Fujitsu | Action M2MSS /CSE |
| PRO-2016-0142R02 | Role Based Access Control Stage 3 | Datang | Update MemberType table for Ch. 3; Would allow multiple roles (cf Shingo Prez for creating new resce types PRO-0125); Add roleID/tokenID formats in NEW contrib., data type names to define and align for roleID/tokenID; roleID attrib + role content in CREATE request |
| PRO-2016-0143R03 | Token Based Access Control Stage 3 | Datang | Cf Notes on ARC/PRO discussion |
| PRO-2016-0179R02 | Notification for security R2 | InterDigital | Procedure in TS-3 or 4? Cleanup needed |
| PRO-2016-0180R01 | R2 security related type definitions | InterDigital | Align roles (list of roleID) > R02 |
| PRO-2016-0154R01 | CR TS-0004 R2 Dynamic Authorization primitive parameters | Qualcomm | Add discriminator for JWx; leave DAS supported protocols to discovery; move part to TS-0003  R02 AGREED |
| PRO-2016-0183R01 | CR TS-0004 R2 E2E Security data types | Qualcomm | R02 Integer value + corrections (ARC to align R0 not RW)  R02 agreed (PRO) |
| PRO-2016-0187 | CR TS-0004 R2 Notify and ESPrim RAND retrieval | Qualcomm |  |
| PRO-2016-0188 | CR TS-0004 R2 Notify and ESPrim Object | Qualcomm |  |
| PRO-2016-0189 | CR TS-0004 R2 Notify and ESCertKE | Qualcomm |  |
| PRO-2016-0206 | CR TS-0004 R2 Dynamic Authorization general procedures and common operations | Qualcomm | Introduce to PRO |
| PRO-2016-0207R01 | CR TS-0004 R2 ESPriml general procedures and common operations | Qualcomm | IR02 > add Notify Retargeting, encrypted error, |
| PRO-2016-0147 |  | Fujitsu | Action default ACP |
| PRO-2016-0209 | Presentation on PRO changes for E2E security and Dynamic Authorization | Qualcomm |  |

5.6 Security related contributions affecting MAS deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| MAS-2016-0128 | CR TR-0007 Access Control for semantic query on semantic repository | China Unicom |  |
| MAS-2016-0132 | DevConfig CR flexContainer | Fujitsu |  |
| MAS-2016-0133 | DevConfig CR data types | Fujitsu |  |
| MAS-2016-0134 | DevConfig NodeEnrolmentProc | Fujitsu |  |
|  |  |  |  |

5.7 Security related contributions affecting TST deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| TST-2016-0091 /  SEC-2016-0104 | Test Suite Structure and Test Purposes from TS-0003 v1.4.2 | Easy Global Market |  |

**6 Contributions to existing WIs**

6.1 TR-0012 / WI 0016 Group Authentication and End-to-End Security

|  |  |  |  |
| --- | --- | --- | --- |
| SEC-2016-0101 | CR TR-0012 Release 2 E2E Security and Rationale | Qualcomm |  |
| SEC-2016-0102 | CR TR-0012 reorganizing clauses etc. | China Mobile |  |
|  |  |  |  |

6.2 TR-0016 / WI 0023 Authorization Architecture and Policies

|  |  |  |  |
| --- | --- | --- | --- |
| SEC-2016-0086R01 | CR TR-0016 Conclusion | Datang |  |
|  |  |  |  |

6.3 TR-0019 / WI 0019 Dynamic Authorization for IoT

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

6.4 TS-0016 / WI 0021 Secure Environment Abstraction

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

6.5 TR-0008 Release 2 oneM2M Threat Analysis

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

6.6 Release 2 Privacy Profiles interoperability

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

**7 Other contributions**

7.1 Liaisons, New Work Items and revisions of Work Items

|  |  |  |  |
| --- | --- | --- | --- |
| SEC-2016-0103 (REQ-2016-0045, TP-2016-0110) | Work Item on Requirements for a new secure element | ETSI TC SCP | François to centralize reply |
| TP-2016-0101 | LS about GSMA IoT Security Guidelines | GSMA | Colin to centralize reply |

7.2 Other contributions for discussion

|  |  |  |  |
| --- | --- | --- | --- |
| SEC-2016-0088R02 | Stage 3 plan for Dynamic Authorization | Qualcomm | Joint > Local/global tokenID need new contrib; 142, 143, 154R01, 206 |
| SEC-2016-0O89R03 | Stage 3 plan for Security use of Notification | Qualcomm | Joint > SecInfo param 179, 180, 187, 188, 189 (IDCC/Qcom) |
| SEC-2016-0087R03 | Stage 3 plan for E2E security | Qualcomm | Joint > 183R1, 207 are big PRO part |
| SEC-2016-0081R02 | Overview of E2E Security TS-0003 CRs | Qualcomm |  |
| SEC-2016-0093 | Certificate Enrolment – Proposals for Stage 3 and Demo | BT Group |  |
|  |  |  |  |

8 Planning for next Meeting(s)

Organization of e-mail discussion threads

Next Conference Calls

Next Face-to-Face

9 Any other business

10 Closure of meeting