|  |
| --- |
| Agenda |
| Meeting title: | SEC 28 F2F meeting (TP 28) |
| Chair: | François Ennesser (Gemalto / ETSI) |
| Secretary: | Emily Hoefer, ATIS |
| Meeting Date: | 2017-03-27 to 2017-03-31 |
| Meeting Details: | Ordinary face-to-face meeting during TP28in Sophia Antipolis, France |
| Intended purpose ofdocument: | [x]  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 |
| **Amphi IRIS** | **11:00-12:30** | **SEC Opening Session S1**Agenda Items 2, 3, 4, 8, 5 (MEF) |
| **IRIS B3** | **13:30-15:00** | **Drafting Session D1**Agenda Item 7.2, 7.4 |
| **Amphi IRIS** | **17:00- 18:30** | **Joint Session with MAS Jm1**Agenda Item 6.4 |
| TUESDAY |
| **Amphi IRIS** | **10:30-12:00** | **Joint Session with TST Jt1**Agenda Items 6.5 |
| **Amphi Athena** | **13:30-15:00** | **Joint Session with ARC Ja1**Agenda Item 6.2 |
| **IRIS B3** | **15:30- 17:00** | **Drafting Session D2**Agenda Item 7.2 |
| WEDNESDAY |
| **Amphi IRIS** | **10:30-12:00** | **SEC Session S2**Agenda Items 7.2, 7.3, 7.4 |
| **Amphi Athena** | **13:30-15:00** | **Joint Session with ARC Ja2**Agenda Item 6.2 |
| **IRIS B3** | **15:30-17:00** | **Drafting Session D3**Agenda Item 5 |
| Thursday |
| **Amphi IRIS** | **8:30-10:00** | **SEC Session S3**Agenda Items 7, 5 |
| **IRIS B3** | **10:30-12:00** | **Drafting Session D4**Agenda Item 5, 7 |
| **Amphi IRIS** | **13:30-15:00** | **SEC Session S4**Agenda Items 5, 7 |
| **Amphi Athena** | **17:00-18:30** | **Joint Session with PRO Jp1**Agenda Item 6.3 |
| Friday |
| **Amphi IRIS** | **8:30-10:00** | **SEC Closing Session S5**Agenda Items 7.x, 8Any remaining topicReview of Action ItemsFuture meetings planning |

1.3 Attendees

 WG4 SEC Leadership nomination results

2 Review of Agenda

Present document

* SEC 27.1 Minutes: agreed by correspondence
* Latest Baseline:
	+ TS-0003 Rel-1 Baseline: v1.7.0 available on portal (SEC-2017-0025)
	+ TS-0003 Rel-2 Baseline: v2.7.0 (SEC-2017-0026)
	+ TS-0003 Rel-3 Baseline: v3.1.0 (SEC-2017-0027)
	+ TS-0016 draft Baseline: v0.6.0 (in SEC-2017-0023)
	+ TS-0032 draft Baseline v0.0.3 (in SEC-2017-0028)
	+ TR-0038 draft Baseline v0.1.0 (in SEC-2017-0024)
	+ TR-0041 Decentralized Authentication draft baseline v0.0.1 (in SEC-2017-0032)

3 Review of Objectives for the Meeting

* Corrections to TS-0003 Rel-2 and lower
* Small Technical Enhancements proposals for TS-0003 Rel-3
* Coordination with TST on resolving TS-0003 v2.5.0 Testing annotations (see SEC-2017-0030)
* Progress on Security Developers Guide TR-0038 (coordination with TST)
* Amendments of MEF/MAF Interface TS-0032 to support TS-0022 Device Configuration (coordination with MAS WG)
* Completion of Stage 2 impact, if any, for all open Rel-3 Work Items
	+ Secure Environment Abstraction TS-0016
	+ Asymmetric cryptography framework for secure elements
	+ Distributed Authorization
	+ Decentralized Authentication

 4 Review of Action Items

|  |  |  |  |
| --- | --- | --- | --- |
| REFERENCE | WHAT | WHO | STATUS |
| A-25-2 | SEC WG members to assess validity of Test Purposes proposed in contribution TST-2016-0190R01 by SEC/TST 25.1 teleconference | All | Cf. SEC 27.1 minutes |
| A-26-3 | Review Ciphersuites and negotiation schemes suitable for transmission of certificates in the context of TS-0022. Also check MAF and MEF context. | All (Lead Phil) |  |
| A-26-5 | Contribute testable Security Features Catalog to TST WG for inclusion in Product Profiles | All |  |
| A-26-6 | Resolve inconsistencies on Access Control Originator ID between TS-0003, TS-0001 and TS-0004 (e.g. interpretation of “\*”) – cf. PRO-2016-0485 | All | TS-0004 aligned with PRO-2017-0044R01; Need to align TS-0003 with TS-0001 and TS-0004: (R2) add GroupID, RoleID, and M2M-SP-ID sub-domain |
| A-26-7 | Contribute further to Security Developers Guide TS | All |  |
| A-27-2 | Define how private keys are provisioned for certificates in the context of TS-0022. | All |  |
| A-27-3 | Figure out how ES Data and ES PRIM should be figured in the context of TS-0022 | All |  |
| A-27-4 | Review the resources of TS-0016 related to mechanism such as access control. | All |  |
| A-27.1-1 | Create CR to address Testing remarks on TS-0003 v2.5.0 in SEC-2017-0030 | All |  |

5 CRs to TS-0003

5.1 Corrections / Clarifications to older releases of TS-0003 (R1, R2, R3)

|  |  |  |  |
| --- | --- | --- | --- |
| SEC-2017-0046 | R2 Normativity changes | Qualcomm | R01 agreed |
| SEC-2017-0047 | R2 Corrections to Access Control | Gemalto | R02 agreed |
|  |  |  |  |

5.2 Simple Technical Enhancements to TS-0003 Rel-3

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

5.3 Contributions to TS-0003 Rel-3 under other open Work Items

|  |  |  |  |
| --- | --- | --- | --- |
| SEC-2017-0038 | AE Authorization Relationship update | Huawei | R01 agreed |
| SEC-2017-0041 | CR TS-0003 MEF High Level changes | Qualcomm |  |
| SEC-2017-0042 | CR TS-0003 PKI SE framework – Stage 2 | Gemalto | TBR |
| SEC-2017-0044 | CR TS-0003 MEF Certificate Provisioning procedure | Qualcomm |  |
| SEC-2017-0045 | Add Distributed Authorization Parameter Values | Datang | R02 kept open (issue of Retrieve request) |
|  |  |  |  |

**6 SEC related contributions affecting other WGs**

6.1 Security related contributions affecting REQ deliverables

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

6.2 Security related contributions affecting ARC deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| ARC-2017-0142 | Distributed Authorization Align with existing names | Datang | R01 |
| ARC-2017-0140 | AE Authorization Relationship update Parameters | Huawei | **R02 agreed** |
| ARC-2017-0129 | Object Identifier Solution | CNIC | **Noted** |
|  |  |  |  |
|  |  |  |  |

6.3 Security related contributions affecting PRO deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| PRO-2017-0070 | AE Authorization relationship update parameter | Huawei |  |
| PRO-2017-0071R01 | Distributed Authorization R3 | Datang, CATR |  |
|  |  |  |  |

6.4 Security related contributions affecting MAS deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| MAS-2017-0070 | DevCfg TS-0022 editHelp Corrections | Rapporteur (FUJITSU) | R01 agreedXSD TBD Thursday |
|  |  |  |  |

6.5 Security related contributions affecting TST deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| SEC-2017-0030 | TS-0003 v2.5.0 Testing requirements annotations | Easy Global Market |  |
| TST-2017-0023R01 |  | EGM | Withdrawn (see 99) |
| TST-2017-0098 |  | EGM | Withdrawn (see 99) |
| TST-2017-0097 | TR-0038 Security Developer’s guide PSK SAEF | Qualcomm | R01 agreed |
| TST-2017-0099 | TS-0028 Security Test Purpose ESPrim (Rel-2) | Easy Global Market | 99R01 agreed |

**7 Contributions to other deliverables**

7.1 TS-0016 / WI 0021 Secure Environment Abstraction

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

7.2 WI-066 TR-0XYZ Decentralized Authentication

|  |  |  |  |
| --- | --- | --- | --- |
| SEC-2017-0032 | TR-0041 Decentralized Authentication baseline v0.0.1 | Rapporteur (Huawei) | (agreed baseline) |
| SEC-2017-0033 | TR-0041 remote provisioning issue for decentralized authentication | Huawei | R01 notedR03 agreed |
| SEC-2017-0034 | TR-0041 overview of authentication framework | Huawei | R01 agreed |
| SEC-2017-0035 | TR-0041 Pre-provisioned Symmetric Key RSPF | Huawei | R02 agreed |
| SEC-2017-0036 | TR-0041 Certificate-based RSPF for Decentralized Authentication | Huawei | R02 agreed |
| SEC-2017-0037 | Scope of TR-0041 Decentralized Authentication | Huawei | R01 agreed |
|  |  |  |  |

7.3 TS-0032 / WI-0057 MEF & MAF Interface

|  |  |  |  |
| --- | --- | --- | --- |
| SEC-2017-0039 | TS-0032 MEF Interface | Qualcomm | R01 agreed |
| SEC-2017-0040 | CR TS-0003 MEF High Level changes | Qualcomm |  |
| SEC-2017-0044 | CR TS-0003 MEF Certificate Provisioning procedure | Qualcomm |  |
|  |  |  |  |

7.4 WI-0061 Distributed Authorization

|  |  |  |  |
| --- | --- | --- | --- |
| ARC-2017-0142 | Distributed Authorization Alignment | Datang |  |
| SEC-2017-0045 | Distributed Authorization parameter values | Datang |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

7.5 TR-0038 Developers Guide implementing Security

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

7.6 TR-00xx Trust Management in oneM2M

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

**8 Other contributions**

8.1 Liaisons, New Work Items and revisions of Work Items

|  |  |  |  |
| --- | --- | --- | --- |
| TP-2017-0073 | WI-0067 revised schedule | Rapporteur (Gemalto) | Agreed in WGApproved in TP |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

8.2 Other contributions for discussion

|  |  |  |  |
| --- | --- | --- | --- |
| SEC-2017-0048 | Discusssion about new security requirements | KDDI |  |

9 Planning for next Meeting(s)

Organization of e-mail discussion threads

Next Conference Calls

Next Face-to-Face

10 Any other business

11 Closure of meeting