

ETSI TS 102 921 V2.1.1 (2013-12)



**Machine-to-Machine communications (M2M);
mla, dla and mld interfaces**

(<https://standards.iteh.ai>)

Document Preview

[ETSI TS 102 921 V2.1.1 \(2013-12\)](https://standards.iteh.ai/catalog/standards/etsi/d8bd3934-c0ba-4281-9f89-cc3880385021/etsi-ts-102-921-v2-1-1-2013-12)

<https://standards.iteh.ai/catalog/standards/etsi/d8bd3934-c0ba-4281-9f89-cc3880385021/etsi-ts-102-921-v2-1-1-2013-12>



Reference

RTS/M2M-00010ed211

Keywords

interface, M2M, protocol, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

(<https://standards.iteh.ai>)
Document Preview

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2013.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	25
Foreword.....	25
1 Scope	26
2 References	26
2.1 Normative references	26
2.2 Informative references.....	30
3 Definitions, symbols, abbreviations and conventions	30
3.1 Definitions.....	30
3.2 Symbols.....	30
3.3 Abbreviations	30
3.4 Conventions.....	31
4 Overview	31
5 General security aspects	31
5.1 Key provisioning and hierarchy derivation	31
5.1.1 Kmr provisioning.....	32
5.1.1.1 Kmr provisioning independent of access network credentials	32
5.1.1.2 Kmr provisioning based on access network credentials.....	32
5.1.1.3 Kmr refresh and invalidation.....	32
5.1.2 Kmc derivation	32
5.1.2.1 Kmc derivation in the case of EAP based mutual authentication and key agreement.....	32
5.1.2.2 Kmc derivation in the case of GBA based mutual authentication and key agreement.....	32
5.1.2.3 Kmc derivation in the case of TLS based mutual authentication and key agreement	33
5.1.2.4 Kmc refresh and invalidation	33
5.2 Security Assumptions.....	33
5.2.1 UICC hosting a Secured Environment Domain	33
6 M2M Service Bootstrapping	33
6.1 General Principles	33
6.2 Access Network Assisted M2M Service Bootstrap Procedure.....	34
6.2.1 GBA-based M2M Service Bootstrap Procedure	34
6.2.1.1 Optional use of GBA_U with Ks_int_NAF	34
6.2.1.2 HTTP Digest Authentication and bootstrap parameter delivery	34
6.2.1.3 M2M Root Key (Kmr) derivation	35
6.2.2 EAP-based bootstrapping procedure using SIM/AKA Access Network Credentials	36
6.2.3 Bootstrapping from EAP-based access network layer	36
6.3 Bootstrapping using other methods	38
6.3.1 Bootstrapping methods using EAP over PANA	38
6.3.1.1 Generic procedure	38
6.3.1.1.1 Bootstrapping	38
6.3.1.1.2 Bootstrap-Erase	41
6.3.1.2 EAP/PANA - IBAKE bootstrapping operations	46
6.3.1.2.1 Provisioning of IBE specific parameters	46
6.3.1.2.2 Secure IBAKE protocol.....	47
6.3.1.3 EAP-TLS over PANA.....	48
6.3.2 M2M Service Bootstrap Procedure using TLS over TCP.....	49
6.3.2.1 Recap of M2M Service Bootstrap Procedure using TLS over TCP	49
6.3.2.2 Pre-Provisioning for M2M Service Bootstrap Procedure using TLS over TCP.....	49
6.3.2.3 Mutual Authentication for M2M Service Bootstrap Procedure using TLS over TCP	49
6.3.2.4 Parameter Delivery to D/G M2M Node for M2M Service Bootstrap Procedure using TLS over TCP	50
6.3.3 Specifications for TLS/Certificate-Based M2M Service Bootstrap Procedures	50
6.3.3.1 Introduction.....	50
6.3.3.2 TLS Details for TLS/Certificate-Based M2M Service Bootstrap Procedures.....	50
6.3.3.3 Certificate Considerations	51

6.3.3.3.1	M2M Device/Gateway Certificate Considerations	51
6.3.3.3.2	MSBF Certificate Considerations	52
6.4	M2M Service Bootstrap Parameter Delivery Procedure For Procedures using HTTP	53
6.4.1	Overview	53
6.4.2	bootstrapParamSet Resource	53
6.4.2.1	bootstrapParamSet Resource URI	53
6.4.2.2	bootstrapParamSet Resource Attributes	54
6.4.3	M2M Service Bootstrap Parameter Delivery Procedure Primitives	54
6.4.3.1	bootstrapParamSetExecuteRequestIndication	54
6.4.3.2	bootstrapParamSetExecuteResponseConfirm (successful case)	54
6.4.3.3	bootstrapParamSetExecuteResponseConfirm (unsuccessful case)	55
6.4.4	MSBF Filtering of Received bootstrapParamSetExecuteRequestIndication Primitives	55
6.4.5	M2M Service Bootstrap Parameter Delivery Procedure Sequence of Events	55
7	M2M Service Connection Procedures	58
7.1	General principles	58
7.2	M2M Service Connection Procedures leveraging access network credentials	58
7.2.1	M2M Service Connection Procedure based on GBA	58
7.2.1.1	TLS-PSK with GBA bootstrapped security association	59
7.2.1.1.1	M2M Connection Key (Kmc) derivation	60
7.2.2	M2M Service Connection Procedure Based On EAP/PANA with Access Network Credentials	61
7.3	M2M Service Connection Procedures using EAP/PANA	61
7.3.1	M2M Service Connection Setup Procedure using EAP/PANA	61
7.3.2	M2M Service Connection Tear-down Procedure using EAP/PANA	64
7.4	M2M Service Connection Procedure based on TLS-PSK	64
7.4.1	Introduction	64
7.4.2	TLS Details for M2M Service Connection Procedure Based On TLS-PSK	64
7.4.3	Sequence of events for M2M Service Connection Procedure based on TLS-PSK	65
7.4.4	Parameter Delivery to D/G M2M Node for M2M Service Connection Procedure based on TLS-PSK	65
7.4.5	M2M Service Connection Parameter Delivery Procedure For TLS-PSK-Based Procedures	66
7.4.5.1	Overview	66
7.4.5.2	connectionParamSet Resource	66
7.4.5.2.1	connectionParamSet Resource URI	66
7.4.5.2.2	connectionParamSet Resource Attributes	66
7.4.5.3	M2M Service Connection Parameter Delivery Procedure Primitives	67
7.4.5.3.1	connectionParamSetExecuteRequestIndication	67
7.4.5.3.2	connectionParamSetExecuteResponseConfirm (successful case)	67
7.4.5.3.3	connectionParamSetExecuteResponseConfirm (unsuccessful case)	68
7.4.5.4	M2M Service Connection Parameter Delivery Procedure Pre-Conditions	68
7.4.5.5	MAS Filtering of Received connectionParamSetExecuteRequestIndication Primitives	68
7.4.5.6	M2M Service Connection Parameter Delivery Sequence of Events	68
7.5	IVaI security attributes in connection establishment	72
7.6	Secure Channel with UICC	72
8	M2M Secure Communication over mId	73
8.1	Access Network Based Security	73
8.2	Channel Security	73
8.2.1	Supported Channel Security Methods	73
8.2.1.1	Negotiation to use a Channel Security Method	73
8.2.1.2	Supported TLS/DTLS Versions and TLS Cipher Suites for Channel Security Methods	74
8.2.1.3	Details of the DTLS/TLS Handshake	74
8.2.1.3.1	Applicability to DTLS and TLS	74
8.2.1.3.2	TLS ClientHello.server_name Field Details For Channel Security Methods	74
8.2.1.3.3	TLS ServerKeyExchange.psk_identity_hint Field Details For Channel Security Methods	74
8.2.1.3.4	TLS ClientKeyExchange.psk_identity and PSK Derivation for Channel Security Methods	75
8.3	Object Security	75
8.3.1	Securing CoAP-based mId	75
8.3.2	Securing XML-based mId	75
9	Resources	76
10	SCL Primitives	77
10.1	Introduction	77

10.2	General aspects.....	77
10.2.1	SCL primitives.....	77
10.2.2	Asynchronous and semi-asynchronous processing.....	77
10.3	Common operations	78
10.3.1	Issuer actions	78
10.3.1.1	Compose RequestIndication primitive	78
10.3.1.2	Send a RequestIndication to the Receiver SCL.....	78
10.3.1.2.1	Determination of the Receiver SCL	78
10.3.1.2.2	Selection of communication channel.....	79
10.3.1.3	Wait for ResponseConfirm primitive	85
10.3.1.4	NSCL information Recording.....	85
10.3.2	Hosting SCL actions	86
10.3.2.1	Check existence of the addressed resource	86
10.3.2.2	Check the syntax of received message	86
10.3.2.3	Check validity of resource representation for CREATE.....	86
10.3.2.4	Check validity of resource representation for UPDATE.....	87
10.3.2.5	Check authorization of the requestingEntity based on accessRightID.....	87
10.3.2.6	Check authorization of the requestingEntity based on selfPermission.....	88
10.3.2.7	Check authorization of the requestingEntity based on default access rights.....	89
10.3.2.8	Announce resource.....	90
10.3.2.8.1	Update of announce on request of application.....	90
10.3.2.8.2	Update of announce on request of local SCL	92
10.3.2.8.3	Create announced Resource.....	92
10.3.2.8.4	Retrieve announced Resource	93
10.3.2.8.5	Update announced Resource	93
10.3.2.8.6	Delete announced Resource.....	94
10.3.2.9	DeAnnounce resource	94
10.3.2.10	Create the resource.....	94
10.3.2.11	Create a collection resource representation.....	95
10.3.2.12	Create a successful ResponseConfirm	95
10.3.2.13	Create an unsuccessful ResponseConfirm	96
10.3.2.14	Read the addressed resource	96
10.3.2.15	Update the addressed resource	96
10.3.2.16	Delete the addressed resource	97
10.3.2.17	Send ResponseConfirm primitive	97
10.3.2.18	Identify the managed remote entity and the management protocol.....	97
10.3.2.19	Locate the MO information to be managed on the remote entity.....	98
10.3.2.20	Establish a management session with the remote entity.....	98
10.3.2.21	Send the management request(s) to the remote entity corresponding to the received RequestIndication primitive	98
10.3.2.22	Identify the managed remote entity and the management protocol.....	99
10.3.2.23	SCL retargeting to an application.....	101
10.3.2.24	Detect duplicated requests.....	103
10.3.2.25	NSCL information Recording.....	103
10.3.3	Receiver SCL actions.....	104
10.3.3.1	Re-targeting.....	104
10.3.3.2	NSCL information Recording	104
10.4	<sclBase> resource and management procedures	105
10.4.1	<sclBase> resource	105
10.4.2	sclBaseCreate.....	105
10.4.3	sclBaseRetrieve.....	106
10.4.3.1	sclBaseRetrieveRequestIndication	106
10.4.3.2	sclBaseRetrieveResponseConfirm (successful case)	107
10.4.3.3	sclBaseRetrieveResponseConfirm (unsuccessful case).....	107
10.4.4	sclBaseUpdate.....	107
10.4.4.1	sclBaseUpdateRequestIndication	107
10.4.4.2	sclBaseUpdateResponseConfirm (successful case)	108
10.4.4.3	sclBaseUpdateResponseConfirm (unsuccessful case)	108
10.4.5	sclBaseDelete.....	108
10.5	scls resource and management procedures	109
10.5.1	scls resource.....	109
10.5.2	sclsCreate.....	109

10.5.3	sclsRetrieve	109
10.5.3.1	sclsRetrieveRequestIndication	109
10.5.3.2	sclsRetrieveResponseConfirm (successful case)	110
10.5.3.3	sclsRetrieveResponseConfirm (unsuccessful case)	110
10.5.4	sclsUpdate	111
10.5.4.1	sclsUpdateRequestIndication	111
10.5.4.2	sclsUpdateResponseConfirm (successful case)	111
10.5.4.3	sclsUpdateResponseConfirm (unsuccessful case)	112
10.5.5	sclsDelete	112
10.5a	sclAnnCs resource and management procedures	112
10.5a.1	sclAnnCs resource	112
10.5a.2	sclAnnCsCreate	112
10.5a.3	sclAnnCsRetrieve	113
10.5a.3.1	sclAnnCsRetrieveRequestIndication	113
10.5a.3.2	sclAnnCsRetrieveResponseConfirm (successful case)	114
10.5a.3.3	sclAnnCsRetrieveResponseConfirm (unsuccessful case)	114
10.5a.4	sclAnnCsUpdate	114
10.5a.4.1	sclAnnCsUpdateRequestIndication	114
10.5a.4.2	sclAnnCsUpdateResponseConfirm (successful case)	115
10.5a.4.3	sclAnnCsUpdateResponseConfirm (unsuccessful case)	115
10.5a.5	sclAnnCsDelete	115
10.6	<scl> resource and management procedures	116
10.6.1	<scl> resource	116
10.6.2	sclCreate	118
10.6.2.1	sclCreateRequestIndication	118
10.6.2.2	sclCreateResponseConfirm (successful case)	121
10.6.2.3	sclCreateResponseConfirm (unsuccessful case)	122
10.6.3	sclRetrieve	122
10.6.3.1	sclRetrieveRequestIndication	122
10.6.3.2	sclRetrieveResponseConfirm (successful case)	123
10.6.3.3	sclRetrieveResponseConfirm (unsuccessful case)	123
10.6.4	sclUpdate	123
10.6.4.1	sclUpdateRequestIndication	123
10.6.4.2	sclUpdateResponseConfirm (successful case)	125
10.6.4.3	sclUpdateResponseConfirm (unsuccessful case)	125
10.6.5	sclDelete	125
10.6.5.1	sclDeleteRequestIndication	125
10.6.5.2	sclDeleteResponseConfirm (successful case)	126
10.6.5.3	sclDeleteResponseConfirm (unsuccessful case)	127
10.6a	<sclAnnC> resource and management procedures	127
10.6a.1	<sclAnnC> resource	127
10.6a.2	sclAnnCCreate	127
10.6a.2.1	sclAnnCCreateRequestIndication	127
10.6a.2.2	sclAnnCCreateResponseConfirm (successful case)	128
10.6a.2.3	sclAnnCCreateResponseConfirm (unsuccessful case)	128
10.6a.3	sclAnnCRetrieve	128
10.6a.3.1	sclAnnCRetrieveRequestIndication	128
10.6a.3.2	sclAnnCRetrieveResponseConfirm (successful case)	129
10.6a.3.3	sclAnnCRetrieveResponseConfirm (unsuccessful case)	129
10.6a.4	sclAnnCUpdate	130
10.6a.4.1	sclAnnCUpdateRequestIndication	130
10.6a.4.2	sclAnnCUpdateResponseConfirm (successful case)	130
10.6a.4.3	sclAnnCUpdateResponseConfirm (unsuccessful case)	130
10.6a.5	sclAnnCDelete	131
10.6a.5.1	sclAnnCDeleteRequestIndication	131
10.6a.5.2	sclAnnCDeleteResponseConfirm (successful case)	131
10.6a.5.3	sclAnnCDeleteResponseConfirm (unsuccessful case)	131
10.7	applications resource and management procedures	132
10.7.1	applications resource	132
10.7.2	applicationsCreate	132
10.7.3	applicationsRetrieve	132
10.7.3.1	applicationsRetrieveRequestIndication	132

10.7.3.2	applicationsRetrieveResponseConfirm (successful case)	133
10.7.3.3	applicationsRetrieveResponseConfirm (unsuccessful case)	133
10.7.4	applicationsUpdate	134
10.7.4.1	applicationsUpdateRequestIndication	134
10.7.4.2	applicationsUpdateResponseConfirm (successful case)	134
10.7.4.3	applicationsUpdateResponseConfirm (unsuccessful case)	135
10.7.5	applicationsDelete	135
10.8	<application> resource and management procedures	135
10.8.1	<application> resource	135
10.8.2	applicationCreate	136
10.8.2.1	applicationCreateRequestIndication	136
10.8.2.2	applicationCreateResponseConfirm (successful case)	137
10.8.2.3	applicationCreateResponseConfirm (unsuccessful case)	137
10.8.3	applicationRetrieve	138
10.8.3.1	applicationRetrieveRequestIndication	138
10.8.3.2	applicationRetrieveResponseConfirm (successful case)	139
10.8.3.3	applicationRetrieveResponseConfirm (unsuccessful case)	139
10.8.4	applicationUpdate	139
10.8.4.1	applicationUpdateRequestIndication	139
10.8.4.2	applicationUpdateResponseConfirm (successful case)	141
10.8.4.3	applicationUpdateResponseConfirm (unsuccessful case)	141
10.8.5	applicationDelete	141
10.8.5.1	applicationDeleteRequestIndication	141
10.8.5.2	applicationDeleteResponseConfirm (successful case)	142
10.8.5.3	applicationDeleteResponseConfirm (unsuccessful case)	142
10.9	<applicationAnnc> resource and management procedures	143
10.9.1	<applicationAnnc> resource	143
10.9.2	applicationAnncCreate	143
10.9.2.1	applicationAnncCreateRequestIndication	143
10.9.2.2	applicationAnncCreateResponseConfirm (successful case)	144
10.9.2.3	applicationAnncCreateResponseConfirm (unsuccessful case)	144
10.9.3	applicationAnncRetrieve	144
10.9.3.1	applicationAnncRetrieveRequestIndication	144
10.9.3.2	applicationAnncRetrieveResponseConfirm (successful case)	145
10.9.3.3	applicationAnncRetrieveResponseConfirm (unsuccessful case)	145
10.9.4	applicationAnncUpdate	145
10.9.4.1	applicationAnncUpdateRequestIndication	145
10.9.4.2	applicationAnncUpdateResponseConfirm (successful case)	146
10.9.4.3	applicationAnncUpdateResponseConfirm (unsuccessful case)	146
10.9.5	applicationAnncDelete	146
10.9.5.1	applicationAnncDeleteRequestIndication	146
10.9.5.2	applicationAnncDeleteResponseConfirm (successful case)	147
10.9.5.3	applicationAnncDeleteResponseConfirm (unsuccessful case)	147
10.10	accessRights resource and management procedures	147
10.10.1	accessRights resource	147
10.10.2	accessRightsCreate	148
10.10.3	accessRightsRetrieve	148
10.10.3.1	accessRightsRetrieveRequestIndication	148
10.10.3.2	accessRightsRetrieveResponseConfirm (successful case)	149
10.10.3.3	accessRightsRetrieveResponseConfirm (unsuccessful case)	149
10.10.4	accessRightsUpdate	149
10.10.4.1	accessRightsUpdateRequestIndication	149
10.10.4.2	accessRightsUpdateResponseConfirm (successful case)	150
10.10.4.3	accessRightsUpdateResponseConfirm (unsuccessful case)	150
10.10.5	accessRightsDelete	151
10.11	accessRight Resource and Management Procedures	151
10.11.1	accessRight resource	151
10.11.2	accessRightCreate	151
10.11.2.1	accessRightCreateRequestIndication	151
10.11.2.2	accessRightCreateResponseConfirm (successful case)	152
10.11.2.3	accessRightCreateResponseConfirm (unsuccessful case)	153
10.11.3	accessRightRetrieve	153