Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: November 27, 2016

M. Barnes

A. Allen
Blackberry

May 26, 2016

Mission Critical Push-to-Talk (MCPTT) Group Key Transport using MIKEY-SAKKE
draft-barnes-mikey-sakke-mcptt-00.txt

Abstract

3GPP TS 33.179 defines the group services and system aspects for the Security of Mission Critical Push-To-Talk (MCPTT) service. To create a group's security association, a Group Master Key (GMK) and associated identifier (GMK-ID) is distributed to MCPTT User Equipment (UE) by a Group Management Server (GMS). The GMK is distributed encrypted specifically to a user and signed using an identity representing the Group Management Server. The GMK is distributed within a Group Key Transport payload, which is a MIKEY-SAKKE I_MESSAGE, as defined in RFC 6509, which ensures the confidentiality, integrity and authenticity of the payload. In order to convey the MCPTT specific service in the MIKEY-SAKKE I_MESSAGE, this document defines new values for the Type field of the General Extensions Payload Field defined for MIKEY in RFC 3830 the ID Role field in RFC 6043 and the ID Scheme field in RFC 6509.

Table of Contents

1. Overview 2
2. Group Key Transport Payload 3
2.1. Type field of the General Extensions Payload Field . . . 3
2.2. ID Role Field 3
2.3. ID Scheme Field 4
3. IANA Considerations 4
3.1. Registration of Type field values for MCPTT 4
3.2. Registration of ID Role values for MCPTT 4
3.3. Registration of ID Scheme values for MCPTT 5
4. Security Considerations 5
5. Acknowledgements 5
6. References 5
6.1. Normative References 5
6.2. Informative References 6
Authors' Addresses 6

1. Overview

Multimedia Internet KEYing-Sakai-Kasahara Key Encryption (MIKEY-SAKKE) defines a method of key exchange that uses Identity-based Public Key Cryptography (IDPKC) to establish a shared secret value and certificateless signatures to provide source authentication. This scheme makes use of a Key Management Service (KMS) as a root of trust and distributor of key material.

3GPP TS 33.179 [TS33179] defines the Group Services and System Aspects for the Security of Mission Critical Push-To-Talk (MCPTT). To create a group's security association, a Group Master Key (GMK) and associated identifier (GMK-ID) is distributed to MCPTT User Equipment (UE) by a Group Management Server (GMS). The GMK is distributed encrypted specifically to a user and signed using an

identity representing the Group Management Server. The GMK is distributed within a Group Key Transport payload. This payload is a MIKEY-SAKKE I_MESSAGE, as defined in RFC 6509 [RFC6509], which ensures the confidentiality, integrity and authenticity of the payload.

2. Group Key Transport Payload

3GPP TS 24.381 [TS24381] details the procedures for composing the MIKEY-SAKKE I_MESSAGE for the Group Key Transport payload. These procedures require the definition of new values for the Type field of the General Extensions Payload Field in RFC 3830 [RFC3830], the ID Role field in RFC 6043 [RFC6043] and the ID Scheme field in RFC 6509 [RFC6509].

2.1. Type field of the General Extensions Payload Field

RFC 3830 [RFC3830] defines the Type field as a General Extensions Payload Field Name. Two new values are defined to indicate the general payload types specific to MCPTT. The following describes the two new values, to be assigned by IANA:

- "SAKKE-to-self (value TBD1):" Indicates that the Data field of a General Extension Payload contains a SAKKE Payload as specified in RFC 6509 [RFC6509]

- "GMK associated parameters (value TBD2):" Indicates that the Data field of a General Extension Payload contains the associated parameters of GMK as specified in 3GPP TS 33.179 [TS33179] figure E.6.1-1.

2.2. ID Role Field

The MIKEY-SAKKE I_MESSAGE contains an IDR Payload as defined in [RFC6043]. The IDR payload uses all the fields from the standard Identity (ID) payload but expands it with a field describing the role of the ID payload. The ID Role describes the meaning of the identity itself. The following describes the two new values, to be assigned by IANA, of the ID Role field specific to MCPTT:

- "IDRuidr (value TBD3):" Indicates that the ID Data field of an ID Payload contains a User Identity (UID) generated from the MCPTT ID of an MCPTT user or a UID generated from the MCPTT Group ID of an MCPTT group, as specified in 3GPP TS 33.179 [TS33179].

- "IDRuidi (value TBD4):" Indicates that the ID Data field of an ID Payload contains a UID generated from the GMS's URI as specified in 3GPP TS 33.179 [TS33179].

2.3. ID Scheme Field

RFC 6509 [RFC6509] defines the ID Scheme field of the SAKKE Payload. The following describes the two new values, to be assigned by IANA, for the ID Scheme field for usage in MCPTT:

- "MCPTT ID scheme (value TBD5):" Indicates that the The SAKKE Data field of a SAKKE Payload contains the GMK encapsulated to the UID generated from the IDRr payload or extracted from the IDRuidr payload according to 3GPP TS 33.179 [TS33179] subclause F.2.1.

- "MCPTT SAKKE-to-self (value TBD6):" Indicates that the SAKKE Data field of a SAKKE Payload contains the GMK encapsulated to the UID generated from the IDRi payload or extracted from the IDRuidi payload according to 3GPP TS 33.179 [TS33179] subclause F.2.1.

3. IANA Considerations

This document defines new values for registration of the Type field of the General Extensions Payload Field in RFC 3830 [RFC3830], the ID Role field in RFC 6043 [RFC6043] and the ID Scheme field in RFC 6509 [RFC6509] required to support MCPTT, are detailed. The IANA registrations for these new values are described in the following sections.

3.1. Registration of Type field values for MCPTT

This document defines two new Type field values to support MCPTT as described in section Section 2.1. The following changes have been made to the Type field in the General Extensions Payload registry of the MIKEY Payload Name Spaces:

Value	ID Role	Reference
TBD1	SAKKE-to-self	[RFCxxxx]
TBD2	GMK associated parameters	[RFCxxxx]

Note to RFC Editor: Please replace RFC XXXX with the RFC number of this specification.

3.2. Registration of ID Role values for MCPTT

This document defines two new ID Role values to support MCPTT, indicating the generator of the UID as described in section Section 2.2. The following changes have been made to the ID Role registry of the MIKEY Payload Name Spaces:

Value	ID Role	Reference
TBD3	MCPTT user/group (IDRuidr)	[RFCxxxx]
TBD4	GMS URI (IDRuidi)	[RFCxxxx]

Note to RFC Editor: Please replace RFC XXXX with the RFC number of this specification.

3.3. Registration of ID Scheme values for MCPTT

This document defines two new ID Scheme values to support MCPTT, indicating the scheme of the SAKKE Payload, as described in section Section 2.3. The following changes have been made to the ID Scheme registry of the MIKEY Payload Name Spaces:

Value	ID Role	Reference
TBD5	MCPTT ID scheme	[RFCxxxx]
TBD6	MCPTT SAKKE-to-self	[RFCxxxx]

Note to RFC Editor: Please replace RFC XXXX with the RFC number of this specification.

4. Security Considerations

3GPP TS 33.179 [TS33179] defines the Group Services and System Aspects for the Security of Mission Critical Push-To-Talk (MCPTT). This document introduces no new security considerations beyond those defined in RFC 6509 [RFC6509].

5. Acknowledgements

Ivo Sedlacek provided input and feedback on the details around the definition of the new values for these fields.

6. References

6.1. Normative References

[RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, DOI 10.17487/RFC3830, August 2004, <http://www.rfc-editor.org/info/rfc3830>.

[RFC6043] Mattsson, J. and T. Tian, "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)", RFC 6043, DOI 10.17487/RFC6043, March 2011, <http://www.rfc-editor.org/info/rfc6043>.

[RFC6509] Groves, M., "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)", RFC 6509, DOI 10.17487/RFC6509, February 2012, <http://www.rfc-editor.org/info/rfc6509>.

6.2. Informative References

[TS24381] 3GPP TS 24.381, "Mission Critical Push-To-Talk (MCPTT) Group Management", March 2016.

[TS33179] 3GPP TS 33.178, "Security of Mission Critical Push-To-Talk (MCPTT)", March 2016.

Authors' Addresses

Mary Barnes
TX
US

Email: mary.ietf.barnes@gmail.com

Andrew Allen
Blackberry
1200 Sawgrass Corporate Parkway
Sunrise, FL 33323
US

Email: aallen@blackberry.com