Annex X: KMIP Profile for FC-SP-2 EAP-GPSK
(Normative)

X.1 Scope

While this annex specifies no normative behavior for the protocols specified in this standard, it is an optional but normative KMIP 1.0 Profile, to which key servers may choose to conform in support of implementations of this standard.

X.2 Overview

This standard specifies several protocols that use shared-key cryptographic algorithms. Practical use of shared-key cryptography in the expected applications of this standard may also require a centralized key management and distribution service. While key management services are out of scope of this standard, its informative annexes include guidelines for its integration with standard key management services.

Annex C provides guidelines for using RADIUS authentication services to support the DH-CHAP protocol specified by this standard. This annex offers guidelines for using OASIS KMIP 1.0 compliant key servers in support of the EAP-GPSK protocol as specified in this standard.

NOTE 1 – Certain limitations of the RADIUS protocol preclude its use in support of FC-SP-2 with EAP-GPSK. These include dependence on the cryptographically weak MD5 hash algorithm, inability to support bi-directional authentication, and inability to cryptographically bind the authentication to subsequent protocols.

NOTE 2 – The OASIS KMIP work group has active but incomplete work on an enhancement release that would offer opportunities for better specification of some features that may be useful to FC-SP-2, especially concerning key location and access control. Because it is incomplete, this work is not reflected here.

The KMIP standard formalizes application-specific functionality specifications as “profiles”. A profile specifies a subset of the optional features in the KMIP Specification that would be useful and sufficient for some class of applications. In KMIP version 1.0, profiles are specified only for servers. Profile-conformant clients implicitly do not depend on any KMIP feature not required by the profile, and do not use any KMIP feature prohibited by the profile.

KMIP profiles each comprise a pairing of an Authentication Suite and a Conformance Clause. An Authentication Suite specifies how a secure relationship is maintained between the KMIP client and the KMIP server. A Conformance Clause specifies the optional features of the KMIP Specification that are required and permitted for profile-conformant servers.

This annex specifies a KMIP Profile for FC-SP-2 EAP-GPSK shared-key management. The OASIS KMIP work group has been consulted on the format and technical content of the profile, and their recommendations are reflected in this annex.

X.3 KMIP profile specification

X.3.1 FC-SP-2 EAP-GPSK Profile

The FC-SP-2 EAP-GPSK Profile consists of the tuple (FC-SP-2 EAP/GPSK Key Foundry and Server Conformance Clause, FC-SP-2 EAP-GPSK Authentication Suite).
X.3.2 FC-SP-2 EAP-GPSK Authentication Suite

X.3.2.1 Protocol

KMIP servers conformant to this Authentication Suite shall support TLSv1.2 (see RFC 5246)

KMIP servers conformant to this Authentication Suite:

a) shall use TLSv1.2 to establish and maintain channel confidentiality and integrity, and provide assurance of server authenticity for KMIP messaging;

b) shall use TLSv1.2 to provide assurance of mutual authenticity for KMIP messaging, with the exception of the Query operation; and

c) should not use TLSv1.2 to provide assurance of client authenticity for the Query operation.

KMIP servers conformant to this Authentication Suite shall support the following cipher suites (see NIST SP 800-57 Part 3 (December 2009)):

a) TLS_RSA_WITH_AES_256_CBC_SHA256; and

b) TLS_RSA_WITH_AES_128_CBC_SHA256.

KMIP servers conformant to this Authentication Suite may support the cipher suites listed in tables 4-1 through 4-4 of NIST SP 800-57 Part 3 (December 2009) with the exception of NULL ciphers.

KMIP servers conformant to this Authentication Suite shall not support any other cipher suites.

X.3.2.2 Client Authenticity

For authenticated services (all operations save Query) KMIP servers conformant to this Authentication Suite shall require the use of TLSv1.2 channel mutual authentication to provide assurance of client authenticity.

X.3.2.3 Client Identity

KMIP servers conformant to this Authentication Suite shall use the identity derived from the TLS channel authentication as the client identity.

If a KMIP server conformant to this Authentication Suite receives a Message Structure in which the Request Header contains an Authentication structure (see KMIP-Spec 7.1), the KMIP server shall reply with a Response message that contains only a Response Header and a single Response Batch Item. The Response Batch Item shall contain:

a) no Operation field;

b) a Result Status field set to Operation Failed; and

c) a Result Reason Enumeration set to Authentication Not Successful.
X.3.2.4 Object Creator

If a KMIP request creates a new managed object, then KMIP servers conformant to this Authentication Suite shall set the client identity derived from the TLS session that carried the request as the creator of the managed object.

X.3.2.5 Access Policy

KMIP servers conformant to this Authentication Suite shall support access control policies that restrict access to a specified symmetric key to a specified set of sharing entities. Sets of sharing entities of greater than one member shall be supported. The means of defining and applying such access control policies are not within the scope of this profile.

X.3.3 FC-SP-2 EAP/GPSK Key Foundry and Server Conformance Clause

An implementation that conforms to this Conformance Clause:

a) Shall support the conditions required by the KMIP Server conformance clauses. (see KMIP-Spec 12.1)

b) Shall support the following additional objects:

   A) Symmetric Key (see KMIP-Spec 2.2.2)

c) Shall support the following additional client-to-server operations:

   A) Create (see KMIP-Spec 4.1)

d) Shall support the following additional attributes:

   A) Block Cipher Mode (see KMIP-Spec 3.6)

   B) Process Start Date (see KMIP-Spec 3.20)

   C) Protect Stop Date (see KMIP-Spec 3.21)

e) Shall support the following subsets of enumerated attributes:

   A) Cryptographic Algorithm (see KMIP-Spec 3.4 and 9.1.3.2.12)

      aa) AES

      bb) HMAC-SHA256

   B) Block Cipher Mode (see KMIP-Spec 3.6 and 9.1.3.2.13)

      aa) CBC

      bb) CMAC

   C) Object Type (see KMIP-Spec 3.3 and 9.1.3.2.11)

      aa) Symmetric Key
D) Cryptographic Length (see KMIP-Spec 3.5 and 9.1.3.2.12)
   aa) 128
   bb) 256

E) Cryptographic Usage Mask (see KMIP-Spec 3.14 and 9.1.3.3.1)
   aa) Encrypt
   bb) Decrypt
   cc) MAC Generate
   dd) MAC Verify
   ee) Derive Key

f) Shall support the following subsets of enumerated objects:
   A) Key Format Type (see KMIP-Spec 3.4 and 9.1.3.2.3)
      aa) Raw
      bb) Transparent Symmetric Key

   g) Shall reject Requests containing the following additional Message Header fields:
      A) Authentication (see KMIP-Spec 6.6)

h) May support any feature within KMIP-Spec that is not listed above; and

i) May support extensions outside the scope of KMIP-Spec (e.g., vendor extensions, conformance clauses) that do not contradict any KMIP requirements or requirements of this profile.