The TPMKEY URI Scheme
draft-mavrogiannopoulos-tpmuri-01

Abstract

   This memo specifies a TPMKEY Uniform Resource Identifier (URI) Scheme
   for identifying cryptographic keys stored in TPM chips and accessed
   using the TCG Software Stack (TSS). The URI is based on how TPM keys
   are identified in the TSS specification.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Trusted Platform Module (TPM) is a trusted piece of hardware
built into many current devices that has been specified by the
Trusted Computing Group (TCG) [TPMMAIN]. In addition to the chip
itself, the TCG defined one standard way to interface with a TPM,
called the TCG Software Stack (TSS) [TSS].

The TSS defines several layers. The most important ones in the
context of this document are the TCG Service Provider (TSP) and the
TCG Core Services (TCS). The TSP provides the TCG services to
applications, which in turn provide access to the TPM. Each
application accesses a single TSP and there is only one TCS for
several TSPs. The task of the TCS is to provide a common set of
services per platform for all TSPs.

TPM keys can be stored either in the TSP (called "user space") or in
the TCS (called "system space"). Furthermore, the TSS assigns a UUID
to each key. That UUID is unique for a specific key hierarchy on a
specific platform. Last, keys can also be stored in so called key
blobs, which are basically files.

The URI scheme defined in this document is designed with a mapping to
TPM keys that are accessed via the TSS in mind. The URI uses only
the scheme and the path components which are required by the Uniform
Resource Identifier generic syntax [RFC3986]. The URI scheme does
not use the hierarchical element for a naming authority in the path
since the authority part could not be mapped to TPM key elements.
The URI scheme does not use the optional query and fragment elements.

2. TPMKEY URI Scheme Definition

In accordance with [RFC4395], this section provides the information
required to register the TPMKEY URI scheme.

2.1. TPMKEY URI Scheme Name

tpmkey

2.2. TPMKEY URI Scheme Status

Provisional.

2.3. TPMKEY URI Scheme Syntax

The TPMKEY URI scheme is a sequence of attribute value pairs
separated by a semicolon. In accordance with [RFC3986], the data
should first be encoded as octets according to the UTF-8 character

encoding [RFC3629]; then only those octets that do not correspond to
characters in the unreserved set or to permitted characters from the
reserved set should be percent-encoded. Rules "unreserved" and "pct-
encoded" in the TPMKEY specification below were imported from
[RFC3986]. As a special case, note that according to [RFC3986], a
space must be percent-encoded.

A TPMKEY URI takes the form (for explanation of Augmented BNF, see
[RFC5234]):

```
    tpmkey-URI            = "tpmkey" ":" tpmkey-identifier
    tpmkey-identifier     = *1(tpmkey-attr *(";" tpmkey-attr))
    tpmkey-attr           = tpmkey-uuid / tpmkey-file / pk11-storage
    tpmkey-reserved-avail = ":" / "[" / "]" / "@" / "!" / "$" /
                             "&" / "'" / "(" / ")" / "*" / "+" /
                             "," / "="
    tpmkey-char           = unreserved / tpmkey-reserved-avail /
                             pct-encoded
    tpmkey-file           = "file" "=" *tpmkey-char
    tpmkey-uuid           = "uuid" "=" UUID
    tpmkey-storage        = "storage" "=" *1("user" / "system")
```

More specifically, the attribute "uuid" represents a unique
identifier of a TPM key and its structure is defined in [RFC4122].
The attribute "storage" corresponds to the storage subsystem used
(user or system). The attribute "file" represents a filename and
corresponds to a file that contains a BER-encoded blob in accordance
with the ASN.1 data definitions in the Portable Data section of the
Trusted Computing Group Software Stack Specification Version 1.2.

2.4. TPMKEY URI scheme semantics

The TPMKEY URI scheme is used to reference TPM keys through the TSS.
The allowed operations on the URI are defined by the TSS
specification.

2.5. Applicability of the TPMKEY URI scheme

The TPMKEY URI scheme is relevant to applications and protocols that
need to identify TPM keys that are accessed through TSS.

3. Examples of TPMKEY URI Schemes

One of the simplest forms is from a key stored in the TSP.

    tpmkey:uuid=7f468c16-cb7f-11e1-824d-b3a4f4b20343;storage=user

A TPM key that is stored in a system's file.

        tpmkey:file=/path/to/file

4. IANA Considerations

This document registers a URI scheme. The registration template can
be found in Section 2 of this document.

5. Security Considerations

There are security considerations for URI schemes discussed in
[RFC3986].

Given that the TPMKEY URI is also supposed to be used in command line
arguments to running programs, and those arguments can be world
readable on some systems, the URI intentionaly does not allow for
specifying the TPM key password as a URI attribute.

6. Acknowledgements

This document derives from [I-D.pechanec-pkcs11uri]. Furthermore the
authors want to thank Greg Kazmierczak for early feedback.

7. References

7.1. Normative References

[RFC3986]   Berners-Lee, T., Fielding, R., and L.
                          Masinter, "Uniform Resource Identifier
                          (URI): Generic Syntax", STD 66, RFC 3986,
                          January 2005.

[RFC4395]   Hansen, T., Hardie, T., and L. Masinter,
                          "Guidelines and Registration Procedures for
                          New URI Schemes", BCP 35, RFC 4395,
                          February 2006.

[RFC3629]   Yergeau, F., "UTF-8, a transformation
                          format of ISO 10646", STD 63, RFC 3629,
                          November 2003.

[RFC4122]   Leach, P., Mealling, M., and R. Salz, "A
                          Universally Unique IDentifier (UUID) URN
                          Namespace", RFC 4122, July 2005.

[TPMMAIN]   TCG, "TPM Main Specification Version 1.2",
                          March 2011.

[TSS]   TCG, "TCG Software Stack (TSS)
                              Specification Version 1.2", March 2007.

7.2. Informative References

[RFC5234]   Crocker, D. and P. Overell, "Augmented BNF
                              for Syntax Specifications: ABNF", STD 68,
                              RFC 5234, January 2008.

[I-D.pechanec-pkcs11uri] Pechanec, J. and D. Moffat, "The PKCS#11
                              URI Scheme", draft-pechanec-pkcs11uri-07
                              (work in progress), December 2012.

Authors' Addresses

    Carolin Latze
    Swisscom Switzerland Ltd
    Ostermundigenstrasse 93
    Bern,   3008
    Switzerland

    EMail: carolin.latze@swisscom.com

    Nikos Mavrogiannopoulos
    ESAT/SCD/COSIC KU Leuven - IBBT
    Kasteelpark Arenberg 10, bus 2446
    Leuven-Heverlee,   B-3001
    Belgium

    EMail: nikos.mavrogiannopoulos@esat.kuleuven.be