TOTP Standalone Client Profile

Version 1.1

02/11/2011

1 Overview

This document defines the technical requirements for compliance with a TOTP Standalone Client profile for OATH Certification.

An OTP client application typically is comprised of the following entities.
1. An OTP token ID
2. An OTP algorithm and related algorithm parameters
3. A way to communicate its OTP secret key to an OTP validation server

OATH Standalone TOTP Client Profile defines criteria for each of the above aspects of a client. In summary, the TOTP Standalone Client requires the following.
1. The OTP token ID MUST comply with OATH Token ID Specification.
2. The OTP algorithm MUST be as defined in TOTP: Time-based One-time Password Algorithm draft-IETF specification [TOTP].
3. Client application providers MUST supply a PSKC [RFC 6030] file to communicate OTP secret keys to an OTP validation server

The detailed specifications for the TOTP Standalone Client profile are contained Section 2.

1.1 Conventions

Throughout this document, normative requirements are highlighted by use of capitalized key words as described below.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]:

- MUST - This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

- MUST NOT - This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

- SHOULD - This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

- SHOULD NOT - This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

- MAY - This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular

marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

2   Token ID Compliance

A compliant OTP client application must use a Token ID that meets the following criteria.

a. The Token ID format SHOULD meet the specifications outlined in the OATH Token Identifier specification [OTIS].
   ➢ OATH Manufacturer Prefix (OMP) MUST be registered at http://www.openauthentication.org/oath-id/prefixes
b. Each Standalone Client TOTP token MUST be assigned a unique Token ID
c. Token ID MUST be printed on the token or displayed in UI

3   Support for TOTP algorithm

The client application MUST implements the TOTP algorithm according to [TOTP]. It should meet the following criteria.

a. The Time-based OTP (TOTP) value calculated MUST be based on the TOTP algorithm defined [TOTP] where TOTP = HOTP (K, T), and T is a time-based integer and K is a symmetric shared secret.
b. The time-based counter (T) MUST be calculated as the number of time steps (X) from T0 (UNIX epoch) to the current UNIX time [TOTP].
c. The length of the time step X SHOULD be 30 seconds.
d. The default floor function MUST be used in the computation of T. For example, with T0 = 0 and time step X = 30, T = 1 if the current UNIX time is 59 seconds and T = 2 if the current UNIX time is 60 seconds [TOTP].
e. OTP length MUST be 6 OR 8 numeric digits
f. The secret K MUST be unique for each token.
g. The client implementation MUST use HMAC-SHA-1 OR HMAC-SHA-256 for the computation.
h. The secret key size MUST be at least 20 bytes if HMAC-SHA-1 is used for computation. The secret key size MUST be at least 32 bytes if HMAC-SHA-256 is used for the computation.
i. The client application MUST be able to make generated OTP visible and/or accessible.

4 OTP Credential Transport

The TOTP Standalone Client provider MUST make the OTP credentials available in the PSKC credential transport data format as defined in [RFC 6030]

a. The PSKC MUST use one of the following key protection methods and algorithms to protect the OTP credential values in the PSKC `<KeyContainer>` element:
  ➢ Pre-shared AES key for key encryption. The key encryption algorithm MUST be AES-128-CBC as defined in Section 6.1 of [RFC 6030]
  ➢ PSKC file protected with PBE encryption as defined in Section 6.2 of [RFC 6030]. The password length is up to 64 characters.
b. The PSKC MUST use the Key Algorithm URI for TOTP as defined in [ALG]
c. The PSKC MUST specify the Token ID within the key Id attribute
`<KeyContainer>/<KeyPackage>/<Key>/@Id`
d. The PSKC file MUST contain a Time element representing the value of the time step.
e. The PSKC Time element value MUST be a non-negative value.
f. The PSKC Time Interval element value MUST be 30 seconds.
g. The PSKC file SHOULD contain integrity checks for the values (ValueMAC)

5 References

[TOTP]   TOTP: Time-based One-time Password Algorithm draft
              http://tools.ietf.org/html/draft-mraihi-totp-timebased-05
[RFC 6030]   Portable Symmetric Key Container
              http://tools.ietf.org/search/rfc6030
 [OTIS]   OATH Token Identifier specification
              http://www.openauthentication.org/oath-id/
[ALG]   Additional PSKC Algorithm Profiles
              http://tools.ietf.org/id/draft-hoyer-keyprov-pskc-algorithm-profiles-01.txt