TOTP Validation Server Profile

Version 1.1

02/11/2011

1 Overview

This document defines the technical requirements for compliance with a TOTP Validation Server profile for OATH Certification.

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 TOTP Validation Server Specification

For a server to be compliant with the TOTP Validation Server Specification, the server MUST correctly respond to all test data for this specification (published by OATH and updated periodically),

The suites of test data will ensure the compliance in the following functional areas:

2.1 Support for TOTP algorithm

The server application MUST implement the TOTP algorithm according to [TOTP]

1. Repeat validation attempts of the same OTP MUST give an error or incorrect response.
2. The Time-based OTP (TOTP) value calculated MUST be based on the TOTP algorithm defined in [TOTP] where TOTP = HOTP(K, T), and T is a time-based integer and K is a symmetric shared secret.
3. The time-based counter for the specific token (T) used by the server MUST be calculated as the number of time steps from T0 (UNIX epoch) to the current UNIX time [TOTP].
4. 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].
5. The default length of the time step X MUST be 30 seconds.
6. The length of the time step X SHOULD be configurable on a per token basis so that tokens with differing time step values can coexist within the same validation server.
7. The server MUST accept OTP lengths of 6 AND 8 numeric digits.
8. The server implementation MUST support both HMAC-SHA-1 AND HMAC-SHA-256 for the computation.
9. 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.
10. The secret K MUST be unique for each token profile stored in the server.

2.2 Validation

1. A validation server MUST have a configurable validation window, defined as the number of time steps before or after the current timestamp.
2. The validation server MUST compare OTPs not only with the receiving timestamp, but also the past time steps that are within the range of the validation window
3. The validations server MUST reject an OTP if it is used more than once.

2.3 OTP Credential Import

The Server that is compliant with this profile MUST support the import of OTP credentials in the PSKC credential transport data format as defined in [RFC 6030].

The validation server MUST check the PSKC file against the following rules. If an element defined as MUST is not present, the validation server MUST reject it.

PSKC Key Protection & Integrity

The server MUST support the following PSKC import profiles:

a. PSKC file protected with AES-128-CBC pre shared key as defined in Section 6.1 of [RFC 6030]
b. PSKC file protected with PBE encryption as defined in Section 6.2 of [RFC 6030]
   - ➢ During import the server MUST accept passwords that are between 5 and 64 characters (both inclusive) in length.

If a PSKC file contains integrity checks for the values (ValueMAC) the server MUST check the correct ValueMAC and MUST NOT import records where the ValueMAC does not match the data.

Token ID Compliance

The PSKC MUST specify the Token ID within the key Id attribute
`<KeyContainer>/<KeyPackage>/<Key>/@Id`

During import the OATH Token Identifier SHOULD be validated for conformance with the OATH Token Identifier Specification [OTIS]. This validation SHOULD be performed in terms of format (length and potentially characters used).

Other

a. The PSKC MUST use Key Algorithm URI for TOTP algorithm as defined in [ALG]

b. The PSKC MUST supply a `<Time>` element. The value SHOULD be non-negative.

c. The PSKC MUST supply a `<TimeInterval>` element. The value SHOULD be 30 seconds.

d. The PSKC MUST contain `<ResponseFormat>` element.
   - ➢ The value of ‘`Encoding`’ Attribute MUST be ‘`DECIMAL`’ and value of ‘`Length`’ attribute MUST be ‘`6`’ or ‘`8`’.

3 References

[TOTP] TOTP: Time-based One-time Password Algorithm draft-IETF specification
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