

HOTP Standalone Client Profile



OATH Certification –

HOTP Standalone Client Profile

v1.0

03/01/2010

Authors:

1 Overview

This profile defines the technical requirements for a standalone OTP client application to become compliant with OATH Client Certification.

An OTP client application typically interacts with the following entities.

- A. An OTP token ID
- B. An OTP algorithm and related algorithm parameters
- C. A way to communicate its OTP secret key to an OTP validation server

OATH Standalone Client Profile defines criteria for each of the above aspect for a client. In a nutshell, the HOTP Standalone Client Profile requires the following.

- A. The OTP token ID **MUST** be compliant with OATH Token ID Specification
- B. The OTP algorithm **MUST** be the HOTP algorithm as defined in RFC4226
- C. Client applications **MUST** support PSKC [PSKC] to communicate OTP secret keys to an OTP validation server

In the following sections, the detail specifications for the profiles are given.

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 Specification

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

- a. Token ID format must meet the specifications outlined at <http://www.openauthentication.org/oath-id>.
 - OMP is registered at <http://www.openauthentication.org/oath-id/prefixes>
 - Please list your OMP
- b. Each token is assigned a unique Token ID
 - Please describe how you manage the assignment of Token IDs to each token, and ensure that each token has a unique identifier
- c. Token ID is printed on the token or displayed in UI
 - Please include a screen shot/picture of the Token showing the Token ID

3 OTP Algorithm Compliance Specification

The client application MUST implement the HOTP algorithm according to RFC 4226. It should meet the following criteria.

- a. MUST pass the test vectors defined in the RFC 4226
- b. MUST be able to generate a sequence of valid OTPs
- c. OTP length MUST be 6 or 8 numeric digits
- d. OTP secret key size MUST be at least 20 bytes
- e. The client application MUST increment the internal HOTP counter exactly by one after each successful generation of an OTP
- f. The client application MUST be able to make generated OTP visible or accessible.

4 OTP Credential Transport Compliance Specification

The provider of the HOTP Standalone Client MUST provide the OTP credentials in the PSKC credential transport data format, as defined in [PSKC]. The PSKC MUST conform to the following.

- a. MUST use one of the following key protection methods and algorithms to protect the OTP credential values in a PSKC <KeyContainer>
 - Pre-shared AES key for key encryption. The key encryption algorithm MUST be AES-128-CBC as defined in Section 6.1 of [PSKC]
 - PSKC file protected with PBE encryption as defined in Section 6.2 of [PSKC]. The password length is up to 64 characters.
- b. Use Key Algorithm URI for HOTP algorithm as defined in [PSKC]
- c. MUST specify token ID with the key Id attribute <KeyContainer>/<KeyPackage>/<Key>/@Id.
- d. Supply a non-negative value for the initial HOTP counter carried in the element <KeyContainer>/<KeyPackage>/<Key>/<Data>/<Counter>

5 References

[OTIS] OATH Token Identifier Specification, <http://www.openauthentication.org/oath-id/>
[OMP] OATH Manufacturer Prefixes, <http://www.openauthentication.org/oath-id/prefixes>

HOTP Standalone Client Profile

[HOTP] HOTP: An HMAC-Based One-Time Password Algorithm,
<http://www.ietf.org/rfc/rfc4226.txt>

[PSKC] Portable Symmetric Key Container, <http://tools.ietf.org/html/draft-ietf-keyprov-pskc-05>

[XMLENC] "XML Encryption Syntax and Processing", W3C Recommendation, December 2002,
<http://www.w3.org/TR/2002/REC-xmlenc-core-20020212/>

[AESKWV] Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm,
<http://tools.ietf.org/html/rfc5649>

[FIPS197-AES] National Institute of Standards and Technology, "Specification for the Advanced Encryption Standard (AES)", FIPS 197, November 2001,
<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>