



OATH Certification –

HOTP Validation Server Profile

V1.0

03/01/2010

Authors:

1 Overview

This profile defines the technical requirements for a HOTP validations server to become compliant with OATH Validation Server 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 HOTP Validation Server Specification

For a server to be compliant to the HOTP 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 RFC 4226 HOTP algorithm - MANDATORY

1. Repeat validation attempt of the same OTP MUST give an error or incorrect response
 - a. The counter for the specific device stored by the server MUST be incremented if the right OTP was presented
 - b. The counter for the specific device MUST not be incremented if an incorrect OTP was presented
2. The server MUST accept OTP lengths of 6 AND 8 numeric digits

2.2 Validation Look Ahead Value (VLAV)- MANDATORY

1. During validation of a proposed OTP the server MUST support a window for the HOTP event counter (window defined as all possible counter values between the current stored counter C and C + VLAV that will be accepted as valid OTPs)
2. It MUST be possible to set the VLAV to any positive integer value
3. Any OTP within the windows MUST generate correct validation
 - a. The stored counter MUST be incremented to reflect the next expected OTP
 - b. The OTP MUST obey all rules set out in Section 2.1
 - c. Once the OTP has been validated it MUST NOT be possible to validate any 'older' OTP (with lower HOTP counter values) For example:

VLAV set to '10'

OTP1 (Counter = 0) -> Validates

OTP2 (Counter = 11) -> does NOT validate

OTP3 (Counter = 6) -> Validates

OTP4 (Counter = 4 hence 'older than counter=6) -> does NOT validate

2.3 PSKC – import - MANDATORY

1. PSKC profile (format) – 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 [PSKC]
 - b. PSKC file protected with PBE encryption as defined in Section 6.2 of [PSKC]
 1. During import the server MUST accept passwords that MUST be longer than 5 characters and up to 64 characters (included) long
2. During import the OATH TokenID SHOULD be validated for conformance with the OATH TokenId Specification [OTIS] this validation SHOULD be performed in terms of format (length and potentially characters used).
3. 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.

3 References

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

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

[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>