Independent Compliance Check against RFC6238

of the following target:

C202 – TOTP Hardware Token

Applicant:
TOKEN2 Switzerland
Chemin du Pré-Colomb 10
CH-1290 Versoix (Genève)

Report Number:
048-001-020_Independent-Compliance-Check _v1-0.pdf

Official release
May 29, 2020

Assessor
K. Marty

This assessment report is subject to the confidentiality rules agreed between the CertX and the client and, without prejudice of any of those closes, should only be reproduced in full.

Documentation purpose

CertX[1], as a certification body and considered as an independent assessor in the scope of this project, has check the compliance the C202 TOTP Hardware Token product from Token2[2] against RFC6238[3] requirements.

This document summarizes the result of the independent compliance check of the product mentioned above against relevant algorithm requirements based on documentation analysis.

Independent compliance check – Results

Token2 has delivered a sufficient amount of evidences to evaluate the compliance of the C202 TOTP Hardware Token product and its related processes. Rationale and justification of compliance are described in a separate document[4].

Req	Requirements (extracted from *RFC6238*)	Methods	Status
[R1]	The prover (e.g., token, soft token) and verifier (authentication or validation server) MUST know or be able to derive the current Unix time (i.e., the number of seconds elapsed since midnight UTC of January 1, 1970) for OTP generation. See [UT] for a more detailed definition of the commonly known "Unix time". The precision of the time used by the prover affects how often the clock synchronization should be done; see Section 6.	Documentation review	Checked
[R2]	The prover and verifier MUST either share the same secret or the knowledge of a secret transformation to generate a shared secret.	Documentation review	Checked
[R3]	The algorithm MUST use HOTP [RFC4226] as a key building block.	Documentation review	Checked (without testing validation)
[R4]	The prover and verifier MUST use the same time-step value X.	Documentation review	Checked
[R5]	There MUST be a unique secret (key) for each prover.	Documentation review	Checked
[R6]	The keys SHOULD be randomly generated or derived using key derivation algorithms.	Documentation review	Checked
[R7]	The keys MAY be stored in a tamper-resistant device and SHOULD be protected against unauthorized access and usage.	Documentation review	Checked

Conclusion

Token2 has proven the addressing of the entire set of RFC6238 requirements through the assessment of their C202 TOTP Hardware Token product. The documentation provided in the scope of this compliance check was sufficient to validate the compliance of the targeted product on documentation level.

[1] *https://certx.com/*
[2] *https://www.token2.com/home*
[3] *https://tools.ietf.org/html/rfc6238*
[4] *048-001-020_Independent-Compliance-Check-Report_v3-0.pdf*