Token Type	Level	Token Requirements	Verifier Requirements
Device		higher.[21]	least 64 bits of entropy.[20]
MF Software Cryptographic Token	Level 3	The cryptographic module shall be validated at FIPS 140-2 Level 1 or higher.[21] Each authentication shall require entry of the password or other activation data and the unencrypted copy of the authentication key shall be erased after each authentication.	Verifier generated token input (e.g., a nonce or challenge) has at least 64 bits of entropy.[20]
MF OTP Hardware Token	Level 4	Cryptographic module shall be FIPS 140-2 validated Level 2 or higher; with physical security at FIPS 140-2 Level 3 or higher.[21] The one-time password shall be generated by using an Approved block cipher or hash function to combine a symmetric key stored on a personal hardware device with a nonce to generate a one-time password. The nonce may be a date and time, a counter generated on the device. Each authentication shall require entry of a password or other activation data through an integrated input mechanism.	The one-time password shall have a limited lifetime of less than 2 minutes.
MF Hardware Cryptographic Token	Level 4	Cryptographic module shall be FIPS 140-2 validated, Level 2 or higher; with physical security at FIPS 140-2 Level 3 or higher.[21] Shall require the entry of a password, PIN, or biometric to activate the authentication key. Shall not allow the export of authentication keys.	Verifier generated token input (e.g., a nonce or challenge) has at least 64 bits of entropy.[20]

6.3.1.2. Multi-Token Authentication

When two of the token types are combined for a multi-token authentication scheme, Table 7 shows the highest possible assurance level that can be achieved by the combination.[22]

[22] Note that the table displays tokens that exhibit the properties of "something you have" and "something you know".