

CSC API V1 Implementation Profile

Version 7 – June 2023

This specification contains a synthetic list of requirements and constraints related to Adobe Acrobat Sign's implementation of the Cloud Signature Consortium's API V1.

This is only intended to develop a test suite for the CSC Conformity Checker tool.

1. Adobe Acrobat Sign does support CSC API V1 v.1.0.4.0.
2. Requires the "specs" parameter from the response of the "info" method to be "1.0.4.0" or "1.0.3.0".
3. Requires the "logo" parameter from the response of the "info" method to link to a bitmap logo image file with at least 64-pixel height and a maximum width of 256 pixel.
4. Requires returning the "description" field in the response from the info method.
5. Supports only OAuth 2.0 usage for service authorization:
 - a. With Authorization Code flow (authType = oauth2code) for human interactive cloud signatures.
 - b. With Client Credentials flow (authType = oauth2client) for machine automated electronic seals.
 - c. Supports the refresh token flow only for reauthenticating within the same working session.
6. The oauth2 parameter returned by the "info" method can contain or not the "/oauth2" path fragment in the URI.
7. Requires the Service access token to be valid for at least 1800 seconds (30 minutes).
8. Adobe Acrobat Sign does not support HTTP basic authentication for service authorization.
9. Supports all types of credential authorization modes: Explicit, Implicit and OAuth.
 - a. For Explicit authMode it requires the client application to provide either a PIN or an OTP, or both.
 - b. When an OTP is used, both online and offline OTP types are supported.
 - c. For Electronic Seals, only Explicit authMode with a PIN is supported.
10. Supports localized strings for the following User Interface elements used when Explicit credentials authorization is used:
 - a. PIN/label
 - b. PIN/description
 - c. OTP/label
 - d. OTP/description
11. Supports credentials with both SCAL 1 and SCAL 2.
12. Requires the Credentials access token (SAD) to be valid between 60 and 1800 seconds (1 to 30 minutes).
13. Requires implementing the oauth2/revoke method, which is called at the end of every signing session.

14. Adobe Acrobat Sign does support multiple signatures with a single authorization.
 - a. The “multisign” parameter returned in the response of the credentials/info method is honored, with an upper limit of 10 signatures per authorization.
 - b. Multiple signatures are only supported via the credentials/extendTransaction method.
 - c. Sending an array of hashes with a single credential authorization and signHash call is not supported.
15. Requires that error descriptions exactly match the texts provided in the CSC API specification.
16. Supports the following signature algorithms:
 - a. RSASSA with PKCS#1 v1.5 with key size from 2048 up to 8192 bits. The recommended key size is 3072 bits. The default algorithm is RSAwithSHA256 (OID: 1.2.840.113549.1.1.11).
 - b. RSASSA-PSS encoding with MGF1 with SHA256 (OID: 1.2.840.113549.1.1.10).
 - The “signAlgoParams” must contain the following Base64-encoded value:
“MDmgDzANBglghkgBZQMEAgEFAKEcMBoGCSqGSib3DQEBCDANBglghkgBZQMEAgEFAKIDAgEgowMCAQE=”
 - c. ECDSA with NIST elliptic curves, with key size from 256 up to 521 bits. The default algorithm is ECDSA with P-256 and SHA256 (OID: 1.2.840.10045.4.3.2)
 - d. SHA-2 hashing algorithms, with SHA256 as default. SHA-3 is not yet supported.
17. The signing certificate chain must be AATL and/or EUTL-trusted. The full certificate chain is always required when calling the credentials/info method.
18. Recommends returning the “description” field in the response from the credentials/info method. This value is visible to the Signer.
19. Adobe Acrobat Sign does not support the signatures/timestamp method. Instead, a standard RFC3161 timestamp service is always used with any cloud signature.
20. Recommends implementing the “account_token” parameter for service authorization based on public eID schemes or other mechanisms with restricted access.
 - a. The accountID parameter should be registered between the TSP and authorized customers.
21. The “state” parameter is included in all API method calls and must be returned in all API responses.
22. The “clientData” parameter is never included in any API method calls.
23. Requires the BaseURI endpoint to be protected with a publicly trusted TLS certificate, supporting TLS version 1.2 and at least one of the cipher suites listed below:
 - a. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - b. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - c. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - d. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - e. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
 - f. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 - g. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
 - h. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384.

For any additional information, please contact adobetsp@adobe.com