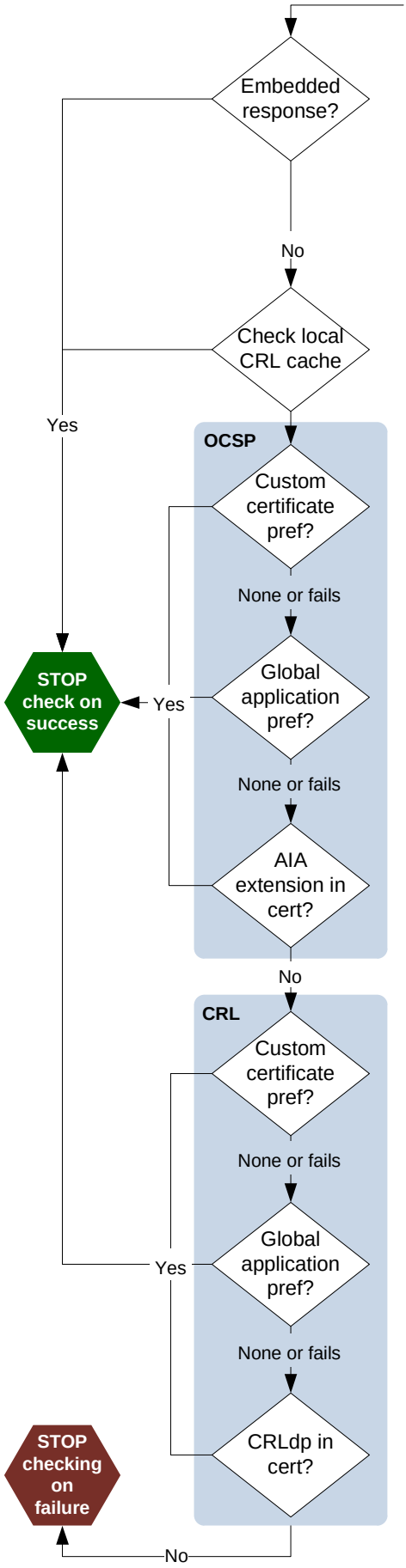
REVOCATION CHECKING QUICK KEY



Get service providers: Both OCSP and CRL service providers are available by default. Configurable via cRevocationCheckers.

Check for embedded revocation data: First check Document Security Store (DSS) added post signing[1], then check if signer embedded the data in the signature. Configurable via iUseArchivedRevInfo and UI. UI string is:

10.x and earlier: *Include signature's revocation status when signing*.

11.0 and later: *Automatically add verification information when saving signed PDF*.

Refer to the Signature Size and Long Term Validation (LTV) Quick Key for additional information about LTV and DSS configuration.

Check local CRL cache: If no embedded data, check to see if a CRL is stored in the application's local cache. For example, at C:\Documents and Settings\<user>\Application Data\Adobe\<product>\<version>\Security\CRLCache.

Check remote OCSP: iReqRevCheck (See [2 or 3] for all preferences) reference specifies whether the check is required to succeed and what should happen if it doesn't. The check occurs as follows:

- If there is a custom certificate preference, use those settings (e.g. look at iURLToConsult and use value in sURL).
- If no custom certificate preference, use Adobe_OCSPRevChecker setting (e.g. look at iURLToConsult and use value in sURL).
- If no registry preference, use the AIA extension in the certificate.
- Administrators can lock revocation checking behavior via bReqRevCheck.

Note: Revocation checking cannot be disabled for certified documents.

REFERENCES

[1] *ETSI PAdES standard*
[2] *Digital Signatures documentation*
[3] *Preference Reference for Acrobat and Reader*

Retrieve a remote CRL: iReqRevCheck preference specifies whether the check is required to succeed and what should happen if it doesn't. The check occurs as follows:

- If there is a custom certificate preference, use those settings (e.g. if no sURL and sLDAP is set, search LDAP server).
- If no custom certificate preference, use Adobe_CRLRevChecker setting (e.g. if no sURL and sLDAP is set, search LDAP server).
- If no registry preference, use the CRLdp extension in the certificate.
- If there are multiple CRLdp's, the CRLs are checked in the order listed in the CRLdp extension. Checking stops after finding the first good CRL.

CHANGES ACROSS RELEASES

9.0: Default: Revocation data not embedded. Can be enabled via UI or registry.

9.1: Default: Revocation data embedded. Can be disabled via UI or registry.

9.2: Revocation data can be added to DSS after signing and by someone other than the signer. Certificate cannot be self signed or already trusted.

10.0: iSendNonce replaces bSendNonce for OCSP checks.