Proposal 0 – original proposal rejected in the bug.	NSS no OCSP[1]		NSS OCSP fail soft[1]																						NIST?[3]		EV[5]
Certificate Type																											
Leaf Cert with no AIA, no crlDp	G	G	G	G	G	G	G	G	G	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Leaf Cert with AIA, no crlDp	G	O	O	G	O	O	G	O	O	F	O+	O+	F	O+	O+	F	O+	O+	F	O+	O+	F	O+	O+	F	O+	O+
Leaf Cert with no AIA, crlDp	G	G	G	C	C	C	C	C	C	F	F	F	C+	C+	C	C+	C	C	F	F	F	C+	C+	C+	C+	C+	C+
Leaf Cert with AIA, crlDp	G	O	O	C	E	E	C	E	E	F	O+	O+	C+	E+	E+	C+	E+	E+	F	O+	O+	C+	E+	E+	C+	C+	E+
Intermediate Cert with no AIA, no crlDp	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	F	F	F	F	F	F	F	F	F
Intermediate Cert with AIA, no crlDp	G	G	O	G	G	O	G	G	O	G	G	O	G	G	O	G	G	O	F	F	O+	F	F	O+	F	F	O+
Intermediate Cert with no AIA, crlDp	G	G	G	G	G	G	C	C	C	G	G	G	G	G	G	C	C	C	F	F	F	F	F	F	C+	C+	C+
Intermediate Cert with AIA, crlDp	G	G	O	G	G	O	C	C	E	G	G	O	G	G	O	C	C	E	F	F	O+	F	F	O+	C+	C+	E+
CERT_REV_OCSP_LEAF_ONLY	0	1	X	0	1	X	0	1	X	0	1	X	0	1	X	0	1	X	0	1	X	0	1	X	0	1	X
CERT_REV_OCSP	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1
CERT_REV_CRL_LEAF_ONLY	0	0	0	1	1	1	X	X	X	0	0	0	1	1	1	X	X	X	0	0	0	1	1	1	X	X	X
CERT_REV_CRL	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	1	1	1
CERT_REV_REQUIRE_LEAF_ONLY	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	X	X	X	X	X	X	X	X	X
CERT_REV_REQUIRE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1

Proposal 1 – This is essentially the same as the proposed changes, except the semantics of CERT_REV_REQUIRE is changed to 'require if present'.	NSS no OCSP[1]		NSS OCSP fail soft[1]							NSS OCSP fail hard.[2]															NIST?[4]		EV[6]
Certificate Type																											
Leaf Cert with no AIA, no crlDp	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Leaf Cert with AIA, no crlDp	G	O	O	G	O	O	G	O	O	G	O+	O+	G	O+	O+	G	O+	O+	G	O+	O+	G	O+	O+	G	O+	O+
Leaf Cert with no AIA, crlDp	G	G	G	C	C	C	C	C	C	G	G	G	C+	C+	C	C+	C	C	G	G	G	C+	C+	C+	C+	C+	C+
Leaf Cert with AIA, crlDp	G	O	O	C	E	E	C	E	E	G	O+	O+	C+	E+	E+	C+	E+	E+	G	O+	O+	C+	E+	E+	C+	C+	E+
Intermediate Cert with no AIA, no crlDp	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G
Intermediate Cert with AIA, no crlDp	G	G	O	G	G	O	G	G	O	G	G	O	G	G	O	G	G	O	G	G	O+	G	G	O+	G	G	O+
Intermediate Cert with no AIA, crlDp	G	G	G	G	G	G	C	C	C	G	G	G	G	G	G	C	C	C	G	G	G	G	G	G	C+	C+	C+
Intermediate Cert with AIA, crlDp	G	G	O	G	G	O	C	C	E	G	G	O	G	G	O	C	C	E	G	G	O+	G	G	O+	C+	C+	E+
CERT_REV_OCSP_LEAF_ONLY	0	1	X	0	1	X	0	1	X	0	1	X	0	1	X	0	1	X	0	1	X	0	1	X	0	1	X
CERT_REV_OCSP	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1
CERT_REV_CRL_LEAF_ONLY	0	0	0	1	1	1	X	X	X	0	0	0	1	1	1	X	X	X	0	0	0	1	1	1	X	X	X
CERT_REV_CRL	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	1	1	1
CERT_REV_REQUIRE_LEAF_ONLY	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	X	X	X	X	X	X	X	X	X
CERT_REV_REQUIRE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1

Proposal 2 Use a single 'leaf only' flag, Require is permissive	NSS no OCSP[1]				NIST?[4]	EV[6]		NSS OCSP fail soft[1]			NSS OCSP fail hard[1]		
Certificate Type													
Leaf Cert with no AIA, no crlDp	G	G	G	G	G	G	G	G	G	G	G	G	G
Leaf Cert with AIA, no crlDp	G	O	G	O	O+	G	O+	O	G	O	O+	G	O+
Leaf Cert with no AIA, crlDp	G	G	C	C	G	C+	C+	G	C	C	G	C+	C+
Leaf Cert with AIA, crlDp	G	O	C	E	O+	C+	E+	O	C	E	O+	C+	E+
Intermediate Cert with no AIA, no crlDp	G	G	G	G	G	G	G	G	G	G	G	G	G
Intermediate Cert with AIA, no crlDp	G	O	G	O	O+	G	O+	G	G	G	G	G	G
Intermediate Cert with no AIA, crlDp	G	G	C	C	G	C+	C+	G	G	G	G	G	G
Intermediate Cert with AIA, crlDp	G	O	C	E	O+	C+	E+	G	G	G	G	G	G
CERT_REV_OCSP	0	1	0	1	1	0	1	1	0	1	1	0	1
CERT_REV_CRL	0	0	1	1	0	1	1	0	1	1	0	1	1
CERT_REV_REQUIRE	X	0	0	0	1	1	1	0	0	0	1	1	1
CERT_REV_LEAF_ONLY	X	0	0	0	0	0	0	1	1	1	1	1	1

KEY:

G = Always Good
F = Always Fail (revoked)l
O= Check OCSP, Unknown or Responder failure == good
C= Check CRL, crl not present == good
E= Check either OCSP or CRL, if can't get status check the other, if neither gives a status return good.
O+= Check OCSP, Unknown or Responder failure == revoked
C+= Check CRL, crl not present == revoked
E+= Check either OCSP or CRL, if can't get status check the other, if neither gives a status return revoked.

General notes:

If a default OCSP responder is enabled, then treat all certs as if they have an AIA extension which points to that responder.
If a CRL is preloaded, treat any cert for which the CRL is preloaded as having a crlDp.
A completely unwound table, with all possibilities will be quite large, An attempt was made to reduce of the combinations and describe them in these notes.

1 Current NSS is modeled here as only supporting OCSP. In fact NSS currently also supports CRLs, but not fetching them from the crlDP. In fact the crlDP is ignored in certificates. This exact semantic is not available by any of the flag combinations. If we need to support it, we may need to add a new flag such as CERT_REV_NSS_CRL. Such a flag is only useful if applications cannot tolerate on of the other approximations (CERT_REV_FLAG_OCSP, CERT_REV_FLAG_CRL).
2 Need to check, does NSS treat and explicit “UNKNOWN” as revoked if hard failure is on?
3 Need to check. This will be true if NIST requires CRLs whether or not crlDP is present. If this is true, then we will need to have a 'hard' Authentication Required flag and proposals 1 & 2 will not work.
4 Need to check. This is the inverse of the previous case. If NIST does not require crlDP's, then proposal 0 is insufficient, but proposals 1 & 2 will work.
5 This is the true definition of EV according to the spec.
6 This is an acceptable processing of an EV chain. The reason is there will be no valid EV chain that does not have at least a crlDP or AIA (or both) extension.

Things none of these proposals can do:

1. Hard failure on OCSP, but soft for CRL. (Certs with crlDP's only will succeed even best effort while certs with AIA won't)

2. Hard failure on CRL, but soft for OCSP (NIST + OCSP in previous incarnations of the spec).

3. Since we don't have crlDP processing, Technically we need to reject chains which do not have AIA's on each cert for EV. Only proposal 0 provides that capability. It may be in practice we don't want to have such a strict understanding, then proposals 1 & 2 may work.

4. There is no way to specify that the leaf cert must fail if AIA is not present, intermediates must pass AIA's that are present, intermediates without AIA's succeed. This is a potential corner semantic one may wish to use to process our EV certificates.

Certificate Type	1	2	3	4
Leaf Cert with no AIA, no crlDp	G	G	F	F
Leaf Cert with AIA, no crlDp	O+	O	O+	O+
Leaf Cert with no AIA, crlDp	C	C+	F	F
Leaf Cert with AIA, crlDp	O+	C+	O+	O+
Intermediate Cert with no AIA, no crlDp	G	G	F	G
Intermediate Cert with AIA, no crlDp	O+	O	O+	O+
Intermediate Cert with no AIA, crlDp	C	C+	F	G
Intermediate Cert with AIA, crlDp	O+	C+	O+	O+

To solve these, we would need to expand the flags, this will generate a difficulty in describing the meaning of each flag, as well as creating many more non-sense bit combinations.

This can be managed by providing a few predefined revocation policies applications are expected to use. Full documentation of the minute meaning of each bit would live in a document like this one up on a wiki. Programmers not happy with the predefined policies can create their own from the primitive bits.