19. Certificate Issuance of End Entity Certificates with Sub-standard Key Sizes

Issuance of End Entity Certificates with sub-standard key sizes SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the CA to perform a certificate signing operation.

Sub-standard key size is defined as less than 2048 bits[1]. End Entity Certificates with sub-standard key sizes MUST NOT be issued except in the following cases:

1. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates);
2. Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA; and
3. Subscriber Certificates, provided that:
   a. The Applicant's application was deployed prior to the Effective Date;
   b. The CA follows a documented process to establish that the Applicant's application is in active use by the Applicant and the Certificate's use is required by a substantial number of Relying Parties;
   c. The CA follows a documented process to determine that the Applicant's application does not rely on web server access via web browsers;
   d. The CA follows a documented process to determine that the Applicant's application poses no known security risks to Relying Parties using web browsers; and
   e. The CA documents that the Applicant's application cannot be patched or replaced without substantial economic outlay.

Such certificates MUST NOT contain the CA's policy OID indicating compliance with the Baseline Requirements (defined in Section 9.3.4), in order to signal non-compliance with all other parts of these requirements.

[1] When a 2048-bit key is generated with the most significant bit set to zero, some certificate parsing software will report the size as 2047 bits. For the purposes of this document, such keys are considered to be 2048 bits in length.