--Motion—

1) Replace Section 3.2.2.5 with the following:

3.2.2.5. Authentication for an IP Address

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of an IP Address listed in the Certificate.

The CA SHALL confirm that, as of the date the Certificate issues, either the CA or a Delegated Third Party has validated each IP Address listed in the Certificate using at least one of the methods listed below.

Completed confirmations of Applicant authority may be valid for the issuance of multiple certificates over time. In all cases, the confirmation must have been initiated within the time period specified in the relevant requirement (such as Section 3.3.1 of this document) prior to certificate issuance. For purposes of IP Address validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

Note: IP Addresses are listed in Subscriber Certificates using iPAddress in the subjectAltName extension or in Subordinate CA Certificates via iPAddress field in the permittedSubtress in the Name Constraints extension.

3.2.2.5.1 Validating the Applicant as the IP Address Owner

If using this method, the CA SHALL verify the Applicant's control over an IP Address by obtaining documentation of IP address assignment to the Applicant directly from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC). This method may only be used the CA authenticates the Applicant's identity under BR Section 3.2.2.1 and the authority of the Applicant Representative under BR Section 3.2.5

3.2.2.5.2 [Reserved]

3.2.2.5.3 [Reserved]

3.2.2.5.4 [Reserved]

3.2.2.5.5 [Reserved]

3.2.2.5.6 Agreed-Upon Change to Website

If using this method, the CA SHALL confirm the Applicant's control over the requested IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of validating control of Domain Names or IP addresses, on the IP Address that is accessible by the CA via HTTP/HTTPS over an Authorized Port. The Request Token or Random Value MUST NOT appear in the request.

If a Random Value is used, the CA or Delegated Third Party SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 3.3.1 of these Requirements).

Note: Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; (ii) a hash of the Subject Public Key Info [X.509]; and (iii) a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests. This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. E.g. echo date -u +%Y%m%d%H%M sha256sum

3.2.2.5.7 [Reserved]

3.2.2.5.8 Reverse Address Lookup

If using this method, the CA SHALL verify the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the Domain Name using a method permitted under Section 3.2.2.4.

3.2.2.4.9 Test Certificate

If using this method, the CA SHALL confirm the Applicant's control over the requested IP Address by confirming the presence of a non-expired Test Certificate issued by the CA on the IP Address and which is accessible by the CA via TLS over an Authorized Port for the purpose of issuing a Certificate with the same Public Key as in the Test Certificate.

3.2.2.4.10 TLS Using a Random Number

If using this method, the CA SHALL confirm the Applicant's control over the requested IP Address by confirming the presence of a Random Value within a Certificate on the IP Address which is accessible by the CA via TLS over an Authorized Port.

3.2.2.5.11 Delegated Control Over a Device

If using this method, the CA SHALL verify the Applicant's control over an IP Address by 1) the CA accessing a device located at the requested IP Address, 2) the CA authenticating to the device using credentials provided by the Applicant or created by the CA, and 3) the CA adding a Request Token or Random Value to a file on the device at a location determined by the CA.