**11.1.3 Wildcard Domain Validation**

Before issuing a certificate with a wildcard character (\*) in a CN or subjectAltName of type DNS-ID, the CA MUST establish and follow a documented procedure† that determines if the wildcard character occurs in the first label position to the left of a public “registry-controlled” label (e.g. “\*.com”, “\*.co.uk”). CAs may consult with “public suffix lists” to identify public “registry-controlled” domains. See RFC 6454 Section 8.2 for further explanation).

If a wildcard would fall within the label immediately to the left of a public “registry-controlled” domain†, CAs MUST refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs MUST NOT issue “\*.co.uk” or “\*.com”, but MAY issue “\*.example.com” to Example Co.). Domains registered to cloud service providers or Internet hosting service providers are not considered to be public if the provider maintains reasonable controls to monitor its Domain Namespace for fraudulent activities and remove any fraudulent Subdomains.

Prior to September 1, 2013, each CA MUST revoke any valid certificate that does not comply with this section of the Requirements.

†Determination of what is “registry-controlled” versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a “public suffix list” such as http://publicsuffix.org/. If the process for making this determination is standardized by an RFC, then such a procedure SHOULD be preferred.

**13.1.5 Reasons for Revoking a Subscriber Certificate**

The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;

2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;

3. The CA obtains evidence that the Subscriber’s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (also see Section 10.2.4) or no longer complies with the requirements of Appendix A;

4. The CA obtains evidence that the Certificate was misused;

5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the

Subscriber or Terms of Use Agreement;

6. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant’s right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name, except when the Subscriber is a cloud service provider. The CA SHALL revoke a Wildcard Certificate issued to cloud service provider within *nn* days if the cloud service provider do not provide evidence of the following:

1. Maintains a process that identifies potentially misleading subordinate domain names for additional approval
2. Regularly monitors the Domain Namespace for fraudulent activities
3. The fraudulent activities has been removed, or will investigate and remove the fraudulent activities within *nn* hours upon notification by the CA
4. Asserts that the Private Key corresponding to the Public Key in the Wildcard Certificate has not been compromised

8. The CA is made aware of a material change in the information contained in the Certificate;

9. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA’s Certificate Policy or Certification Practice Statement;

10. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;

11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

12. The CA’s right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;

13. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;

14. Revocation is required by the CA’s Certificate Policy and/or Certification Practice Statement; or

15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).