Technical information about each root certificate

SSL Validation Type	DV, OV Is the CA ever allowed to issue SSL certificates without verifying the identity of the certificate subscriber? Buypass response: The existence of the certificate subscriber is always verified, even for DV certificates through the registered domain owner. Only Norwegian domain owners are currently supported and their existence is verified.	OV, EV

Verification Policies and Practices

Email Address Verification Procedures	If you are requesting to enable the Email Trust Bit, then please provide all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices Buypass response: The Email Trust Bit is never set for any SSL certificate.
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices From email of 9/16: "Buypass use two-factor smartcard authentication for logging in." Who does this apply to? RA? CA? Is it documented in the CP or CPS? If not, can you add this information? (can be done while request is in the queue for discussion) Buypass response: All RA- and CA trusted personnel use their personal two factor authentication token (i.e. a smartcard) to access their accounts. This is partly mentioned in chpt. 5.1 in the CPS. We will evaluate if this is sufficient /clear enough and update accordingly in time before the public discussion.
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices From email of 9/16: <Network Security Review> "Carried out without any signs or traces of intrusion or compromise." Is there information in your CP or CPS regarding pentetration testing, checking for mis-issuance of certificates, flagging high-profile domains, etc? If not, can you add this information? (can be done while request is in the queue for discussion) Buypass response: All actions listed are performed. This kind of testing, etc. is partly mentioned in chpt. 6.5 and 6.6, but we will evaluate if this is sufficient /clear enough and update accordingly in time before the public discussion.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Document Handling of IDNs in CP/CPS	Buypass response: No
Verifying Email Address Control	? Buypass response: No – email address is not allowed in any SSL certificate
DNS names go in SAN	? Buypass response: Yes, all DNS names go in SAN.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Wildcard DV SSL certificates	Are wildcard SSL certs allowed? Buypass response: Yes, however wildcard certs are only allowed for OV certificates
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification. Buypass response: No email address prefixes are used. Only the email address listed in the administrative contact field of the domain's WHOIS record
Delegation of Domain / Email validation to third parties	External RAs? Buypass response: No
Distributing generated private keys in PKCS#12 files	? Buypass response: No
Certificates referencing hostnames or private IP addresses	? Buypass response: Yes, hostnames may only be referenced in an OV certificate (SSL Domain Plus).
Issuing SSL Certificates for Internal Domains	? Buypass response: No