Bugzilla ID: 685128
Bugzilla Summary: Add Buypass Root certificates

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	Buypass AS
Website URL	http://www.buypass.no
Organizational type	Public corporation
Primark Market / Customer Base	Buypass AS is a public corporation and a leading supplier of secure solutions for electronic identification, electronic signatures and payment in the Nordic countries. Our solutions are delivered via the Internet, mobile phones, POS terminals and company internal networks. Buypass has issued electronic IDs to over 2 million of Norway's 4.9 million inhabitants. Buypass is registered with the Post and Telecommunications Authority as the issuer of the qualified ID according to the law on electronic signature. The company is the market leading ID supplier within e-Government services in Norway, provides identification services to all government departments, over 70% of the country's primary health care services and the entire customer base of the Norsk Tipping (the Norwegian national Lottery). We have the last few years made significant investment in SSL certificates for the European market. Buypass root certificates have been included in most of the browsers (Mozilla, IE, Safari/IOS and Opera) and we currently support 99.5% of customers' and partners' browsers. We are a member of the international CA/Browser Forum.
CA Contact Information	CA Email Alias: policy@buypass.no CA Phone Number: 47 23 14 59 00 Title / Department:

Technical information about each root certificate

Certificate Name	Buypass Class 2 Root CA	Buypass Class 3 Root CA
Certificate Summary	The Buypass Class 2 certificates are issued to natural persons not registered in the Norwegian National Registry of Persons and the merchant certificates are issued to organizations. The Buypass Class 2 certificates have the same basic usage areas as Class 3 certificates. The Class 2 CP has, however, less strict requirements with respect to identification of the requesting party than Class 3 certificates. "Domain" and" Domain+" -SSL certificates are issued exclusively by Class 2 CA. All certificates are issued to the general public.	The Buypass Class 3 qualified certificates are issued to natural persons and the enterprise certificates are issued to organizations. The certificates may be used for authentication purposes, encryption/decryption and/or electronic signatures (non-repudiation). The certificates are part of an infrastructure provided by Buypass AS enabling electronic commerce in Norway. The certificates are used by many different service providers ranging from purely commercial companies to governmental and other public institutions including the health sector. Extended Validation and Business SSL certificates are issued exclusively by the Buypass Class 3 CA. All certificates are issued to the general public.

Root Cert URL	http://www.buypass.no/cert/BPClass2RootCA-sha2.cer	http://www.buypass.no/cert/BPClass3RootCA-sha2.cer
SHA1	49:0A:75:74:DE:87:0A:47:FE:58:EE:F6:C7:6B:EB:C6:0B:12:40:99	DA:FA:F7:FA:66:84:EC:06:8F:14:50:BD:C7:C2:81:A5:BC:A9:64:57
Valid From	2010-10-26	2010-10-26
Valid To	2040-10-26	2040-10-26
Cert Version	3	3
Cert Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption	PKCS #1 SHA-256 With RSA Encryption
Modulus	4096	4096
Test Website	https://valid.domainplus.ca22.ssl.buypass.no/CA2Class2	https://valid.evident.ca23.ssl.buypass.no/CA2Class3
CRL URL	http://crl.buypass.no/crl/BPClass2CA2.crl (NextUpdate: 25 hrs) Class 2 SSL CP Section 4.4.9: The CRL service SHALL at least issue CRLs every 24 hours and each CRL SHALL have a maximum expiration time of 48 hours.	http://crl.buypass.no/crl/BPClass3CA2.crl (NextUpdate: 25 hrs) Class 3 SSL CP Section 4.4.9: The CRL service SHALL at least issue CRLs every 24 hours and each CRL SHALL have a maximum expiration time of 48 hours.
OCSP URL	http://ocsp.buypass.no/ocsp/BPClass2CA2	http://ocsp.buypass.no/ocsp/BPClass3CA2 Class 3 SSL CP Section 4.4.11: The OCSP service SHALL be updated at least every 24 hours, and OCSP responses from this service SHALL have a maximum expiration time of 48 hours.
Requested Trust Bits	Websites (SSL/TLS)	Websites (SSL/TLS)
SSL Validation Type	OV	OV, EV
EV Policy OID(s)	Not EV	2.16.578.1.26.1.3.3

CA Hierarchy

CA Hierarchy	https://bugzilla.mozilla.org/attachment.cgi?id=558776 Buypass Class 2 Root CA has two internally-operated subCAs.	https://bugzilla.mozilla.org/attachment.cgi?id=558776 Buypass Class 3 Root CA has two internally-operated subCAs.
Externally Operated SubCAs	None	None
Cross-Signing	None	None

Verification Policies and Practices

Policy Documentation	Documents are provided in English. Class 2 CP: http://www.buypass.no/bedrift/kundeservice/dokumentasjon/ca-dokumenter-juridisk/_attachment/8957 Class 2 CPS: http://www.buypass.no/bedrift/kundeservice/dokumentasjon/ca-dokumenter-juridisk/_attachment/8961 Class 3 CP: http://www.buypass.no/bedrift/kundeservice/dokumentasjon/ca-dokumenter-juridisk/_attachment/8960 Class 3 CPS: http://www.buypass.no/bedrift/kundeservice/dokumentasjon/ca-dokumenter-juridisk/_attachment/8963
Audits	Auditor: KPMG (KPMG Advisory N.V.) Auditor Website: www.kpmg.com Audit Document URL(s): https://cert.webtrust.org/ViewSeal?id=1139 (2010.11.30) Point-in-time WebTrust for CA and EV SSL audit report and management assertions for the new CA (CA2): http://www.buypass.no/Bedrift/Produkter-og-tjenester/SSL-sertifikat/_attachment/10607 (2010.11.30)

Class 2 SSL Cert Organization And Domain Name Verification Procedures	Class 2 SSL Certificate Policy Section 2.1.1: The CA SHALL warrant that the identity of the Subscriber that appears in an issued Buypass Domain Plus SSL Certificate is accurate and correct at the time of issuance. The CA SHALL warrant that an issued Buypass Domain Plus SSL Certificate is linked to one (1) unique organization registered in the Norwegian Central Coordinating Register for Legal Entities. The CA SHALL warrant that the Subscriber is in possession of the Subject Private Key that corresponds to the Public Key in that Certificate. The CA SHALL warrant that Subscriber named in the Class 2 SSL Certificate has the right to use the domain name(s) listed in the Certificate. Section 2.1.2: An RA operating under the Certificate Policy for Buypass Class 2 SSL Certificates [14] SHALL: receive Certificate Applications from Subscribers, both initial applications (see 4.1.1) and rekey applications (see 4.1.2) verify all information submitted by Subscribers, both for initial applications and for rekey applications and if such verification is successful, submit a request to the CA for the issuance of a Buypass Class 2 SSL Certificate Section 3.1.1: a) The following Subscriber information SHALL be obtained by the RA during initial registration: name of the Subscriber. For Buypass Domain Plus SSL Certificates: full name of the Subscriber as defined in the Norwegian Central Coordinating Register for Legal Entities the Subscribers' Organization Number as defined in the Norwegian Central Coordinating Register for Legal Entities for Buypass SSL Domain Plus Certificates the address and telephone number of Subscriber's Place of Business contact information of Subscriber representatives acting as Certificate Approver name and Contact information of Subscriber representative acting as Certificate Applicant b) All information provided SHALL be verified according to section 4.1.1. Section 3.1.2: The RA SHALL be able to identify Certificate Applicants and Certificate Approvers as Authorized Subscriber Representatives; a) Authorized Certificate Approvers are: Subscriber representative authorised to sign contracts on behalf of the Subscriber Certificate Approvers already authorized by the Subscriber under the Certificate Policy for Buypass Class 3 SSL Certificates [16] administration or technical contact for the given domain name(s) whenever organization information is not included in the Certificate b) Accepted ways of confirming a Certificate Approver's SSL Authority are: an internal verification by Buypass that the person already possesses a Certificate Approver role for the Subscriber under the Certificate Policy for Buypass Class 3 SSL Certificates [16] an independent confirmation obtained from the Norwegian Central Coordinating Register for Legal Entities that the Certificate Approver is entitled to bind the Subscriber organization by signature an independent confirmation from the Subscriber that the Certificate Approver is a Subscriber representative authorised to sign contracts on behalf of the Subscriber administration or technical contact for the given domain name(s) in an official domain name registry whenever organization information is not included in the Certificate c) A Certificate Application SHALL be expressly approved by a Certificate Approver.

	d) An authorized Certificate Approver is by definition also an authorized Certificate Applicant. Section 4.1.1: d) In the event that external RAs are used, the CA SHALL verify that application data is exchanged with recognized RAs, whose identity is authenticated. e) The controls and procedures used to verify the Certificate Application SHALL establish: □ that the Certificate Application is accurate and complete □ that the Subscriber is registered in the Norwegian Central Coordinating Register for Legal Entities and that Subscriber information registered conform with information provided in the Certificate Application (see section 3.1.1) for Buypass Domain Plus SSL Certificates □ that the Certificate Applicant and Certificate Approver are Authorized Subscriber Representatives according to the requirements described in section 3.1.2 □ that the Subscriber is a registered holder or has control of the domain name to be included in the SSL Certificate
Class 3 SSL Cert Organization And Domain Name Verification Procedures	Class 3 SSL Certificate Policy Section 2.1.1: The CA SHALL warrant that the identity of the Subscriber that appears in an issued SSL Certificate is accurate and correct at the time of issuance. The CA SHALL warrant that an issued SSL Certificate is linked to one (1) unique organization registered in the Norwegian Central Coordinating Register for Legal Entities. The CA SHALL warrant that the Subscriber that is named in a Certificate is in possession of the Subject Private Key that corresponds to the Public Key in that Certificate. The CA SHALL warrant that Subscriber named in the SSL Certificate has the exclusive right to use the domain name(s) listed in the SSL Certificate. Section 2.1.2: An RA operating under the Certificate Policy for Buypass Class 3 SSL Certificates [15] SHALL: □ receive Certificate Applications from Subscribers, both initial applications (see 4.1.1) and rekey applications (see 4.1.2) □ verify all information submitted by Subscribers, both for initial applications and for rekey applications and if such verification is successful, submit a request to the CA for the issuance of a Buypass Class 3 SSL Certificate Section 3.1.1: a) The following Subscriber information SHALL be obtained by the RA during initial registration: □ full name and legal status of the Subscriber as defined in the Norwegian Central Coordinating Register for Legal Entities □ the Subscribers' Organization Number as defined in the Norwegian Central Coordinating Register for Legal Entities □ the address of Subscriber's Place of Business as defined in the Norwegian Central Coordinating Register for Legal Entities and the main telephone number □ name and contact information of all Subscriber Representatives authorized to operate as either Certificate Applicant, Certificate Approver, Certificate Manager or Contract Signer b) All information provided SHALL be verified according to section 4.1.1. Section 3.1.2: The RA SHALL be able to identify Certificate Applicants, Certificate Approvers, Certificate Managers and Contract Signers as Authorized Subscriber Representatives; {Acceptable documents are listed, and the CAB Forum EV Guidelines are referenced.} Section 4.1.1:

	The Certificate Applicant, Certificate Approver, Certificate Manager and Contract Signer SHALL register with an RA as Authorized Subscriber Representatives either prior to, or at the time of, applying for a Certificate. Section 3.1 defines necessary requirements for identification, authentication and authorization. a) The Certificate Applicant, Certificate Approver and Contract Signer SHALL register with an RA as Authorized Subscriber Representatives either prior to, or at the time of, applying for a Certificate. Section 3.1 defines necessary requirements for identification, authentication and authorization. b) The Subscriber SHALL provide to the RA: □ all Subscriber information as defined in section 3.1 □ a Certificate Application signed by a Certificate Applicant □ a legally enforceable Subscriber Agreement signed by a Contract Signer that specifies the rights and responsibilities of the parties c) For EV Certificates, the contents of the Subscriber Agreement SHALL comply with the requirements of the CA/Browser Forum Guidelines [10]. d) The confidentiality and integrity of application data SHALL be protected, especially when exchanged between the Subscriber and RA or between distributed RA/CA system components. The Certificate Applicant, Certificate Manager and/or Certificate Approver SHALL be able to establish the identity of the RA. e) In the event that external RAs are used, the CA SHALL verify that application data is exchanged with recognized RAs, whose identity is authenticated. f) The controls and procedures used to verify the Certificate Application SHALL conform to the information verification requirements defined by the CA/Browser Forum Guidelines [10] and SHALL establish: □ that the Certificate Application is accurate and complete □ that the Subscriber is registered in the Norwegian Central Coordinating Register for Legal Entities and that Subscriber information registered conform with information provided in the Certificate Application (see section 3.1.1) □ that the Certificate Applicant, Certificate Approver, Certificate Manager and Contract Signer are Authorized Subscriber Representatives according to the requirements described in section 3.1.2 □ that the Contract Signer has signed the Subscriber Agreement □ that the Certificate Applicant has signed the Certificate Application (for EV Certificates only) □ that the Subscriber is a registered holder or has exclusive control of the domain names to be included in the SSL Certificate g) The Certificate Application SHALL be rejected if any of the verification steps in f) fails. In this case the Certificate Applicant SHALL be notified without undue delay that the Certificate Application has been rejected. h) Auditable controls SHALL be in place to ensure separation of duties such that no person single- handedly can both validate and authorize the issuance of an SSL Certificate.
Email Address Verification Procedures	N/A – Not requesting the email trust bit.
Code Signing Subscriber Verification Procedures	N/A – Not requesting the Code Signing trust bit.
Multi-factor Authentication	Comment #3: 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	Comment #3: All actions listed are performed. In both CPS documents sections 6.5, 6.6, and 6.7 describe computer security controls, lifecycle technical controls, and network security controls.

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

Publicly Available CP and CPS	Yes
CA Hierarchy	These root certificates sign internally-operated subordinate CAs. They do not directly sign end-entity subscriber certificates.
Audit Criteria	Yes
Document Handling of IDNs in CP/CPS	N/A
Revocation of Compromised Certificates	Yes
Verifying Domain Name Ownership	Yes
Verifying Email Address Control	N/A
Verifying Identity of Code Signing Certificate Subscriber	N/A
DNS names go in SAN	Yes, all DNS names go in SAN.
Domain owned by a Natural Person	Yes
OCSP	Yes

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

Long-lived DV certificates	Class 2 SSL CP Section 4.2: The validity period for a Class 2 SSL Certificate SHALL NOT exceed three years. Class 3 SSL CP Section 4.2: The validity period for an EV Certificate SHALL NOT exceed twenty seven months.
Wildcard DV SSL certificates	No wildcard DV SSL certs are allowed. Wildcard SSL certs are only allowed for OV.
Email Address Prefixes for DV Certs	Comment #3: 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	Domain verification is not delegated to third parties.
Issuing end entity certificates directly from roots	No
Allowing external entities to operate subordinate CAs	No
Distributing generated private keys in PKCS#12 files	No
Certificates referencing hostnames or private IP addresses	Comment #3: Yes, hostnames may only be referenced in an OV certificate (SSL Domain Plus).
Issuing SSL Certificates for Internal Domains	No
OCSP Responses signed by a certificate under a different root	No
CRL with critical CIDP Extension	No
Generic names for CAs	No