Bugzilla ID: 477028
Bugzilla Summary: Add Buypass AS root certificates

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	Data
CA Name	Buypass AS
Website URL (English version)	www.buypass.no
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	?
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	Buypass has over 2 million customers in Norway and is a provider of secure solutions for electronic identification, electronic signature, and payment. 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 has a license from the Ministry of Finance as e-money business pursuant to the Act on e-money.

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data	Data
Certificate Name	Buypass Class 2 CA 1	Buypass Class 3 CA 1
Cert summary / comments	Buypass Class 2 certificates are issued to persons or enterprises and 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.	The Buypass Class 3 certificates are either issued to persons or enterprises. 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 SSL certificates will be issued exclusively

		by Class 3 CA.
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=361508	https://bugzilla.mozilla.org/attachment.cgi?id=361508
SHA-1 fingerprint.	a0:a1:ab:90:c9:fc:84:7b:3b:12:61:e8:97:7d:5f:d3:22:61:d3:cc	61:57:3a:11:df:0e:d8:7e:d5:92:65:22:ea:d0:56:d7:44:b3:23:71
Valid from	10/13/2006	5/9/2005
Valid to	10/13/2016	5/9/2015
Cert Version	3	3
Modulus length	2048	2048
CRL • URL • Update frequency: What is the nextUpdate in the CRL for end-entity certificates?	http://crl.prod.buypass.no/crl/BPClass2CA1.crl 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.prod.buypass.no/crl/BPClass3CA1.crl 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 (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf Section 26(b): "If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days."	https://ocsp.prod.buypass.no/BPClass2 Class 2 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.	https://ocsp.prod.buypass.no/BPClass23 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.

List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.)	Please provide a CA hierarchy description and/or diagram. Are there any internally operated subordinate CAs chaining up to this root? For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CP/CPS, and that any audit covers them as well as the root.	Please provide a CA hierarchy description and/or diagram. Are there any internally operated subordinate CAs chaining up to this root? For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CP/CPS, and that any audit covers them as well as the root.
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited.	For the subordinate CAs that are operated by third parties, please provide a general description and explain how the CP/CPS and audits ensure the third parties are in compliance. If applicable, please see https://wiki.mozilla.org/CA:SubordinateCA_checklist	For the subordinate CAs that are operated by third parties, please provide a general description and explain how the CP/CPS and audits ensure the third parties are in compliance. If applicable, please see https://wiki.mozilla.org/CA:SubordinateCA_checklist Are any of the sub-CAs that are operated by third-parties are or will be EV enabled? If the answer is yes, then please refer to http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf section 7.b.1 and section 37b.
List any other root CAs that have issued cross-signing certificates for this root CA	Has this root been involved in cross-signing with another root?	Has this root been involved in cross-signing with another root?
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites Email From Buypass: Both CA certificates issues certificates for SSL-enabled servers and digitally signed or encrypted email. None of them issues certificates for signing executable code objects.	
If SSL certificates are issued within the hierarchy rooted at this root CA certificate:	OV Class 2 SSL CP section 4.1.1 Initial Application	OV, EV Class 3 SSL CP section 4.1.1, Initial Application:

• Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (DV.) • Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber in addition to verifying the domain name. (OV) • Whether verification of the certificate subscriber conforms to the Extended Validation Certificate Guidelines issued by the CAB Forum. (EV)	The controls and procedures used to verify the Certificate Application SHALL establish: i. that the Certificate Application is accurate and complete. ii. 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). iii. that the Certificate Applicant and Certificate Approver are Authorised Subscriber Representatives according to the requirements described in section 3.2. iv. that the Subscriber is a registered holder or has control of the domain name to be included in the SSL Certificate.	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: i. that the Certificate Application is accurate and complete. ii. that the Subscriber is registered in the Norwegian Central Coordinating Register for Legal Entities and the National Register of Business Enterprises (Private Organizations only) and that Subscriber information registered conform with information provided in the Certificate Application (see section 3.1.1). iii. that the Certificate Applicant, Certificate Approver and Contract Signer are Authorised Subscriber Representatives according to the requirements described in section 3.2. iv. that the Contract Signer has signed the Subscriber Agreement. v. that the Certificate Applicant has signed the Certificate Application (for EV Certificates only). vi. that the Subscriber is a registered holder or has exclusive control of the domain name to be included in the SSL Certificate.
EV policy OID(s)	NOT EV	EV OID: 2.16.578.1.26.1.3.3
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. • For SSL certificates this should also include URLs of one or more web servers using the certificate(s). • There should be at least one example certificate for each of the major types of certificates	Buypass CA test-certs https://bugzilla.mozilla.org/attachment.cgi?id=361509	

issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV. • Note: mainly interested in SSL, so OK if no email example.	
CP/CPS	CP and CPS: http://www.buypass.no/Bedrift/Produkter+og+tjenester/SSL/SSL%20dokumentasjon Buypass Class 2 SSL Certificate Policy in English http://www.buypass.no/_binary?download=true&id=1270 Buypass Class 2 SSL Certificate Practice Statement in English http://www.buypass.no/_binary?download=true&id=1272 Buypass Class 3 SSL Certificate Policy in English http://www.buypass.no/_binary?download=true&id=1271 Buypass Class 3 SSL Certificate Practice Statement in English http://www.buypass.no/_binary?download=true&id=1273 Please review the potentially problematic practices list at http://wiki.mozilla.org/CA:Problematic_Practices. For relevant items, provide further information.
AUDIT	Audit Type: WebTrust CA Auditor: KPMG Auditor website: www.kpmg.com Audit Report and Management's Assertions: https://cert.webtrust.org/SealFile?seal=848&file=pdf (12/22/2008) This is the WebTrust CA audit for • Buypass Class 2 SSL and Class 3 SSL Certificates • Buypass Class 3 Enterprise Certificates Please provide the url to the WebTrust EV audit. Audit Type: WebTrust EV

	Auditor: KPMG Auditor website: www.kpmg.com Audit Report and Management's Assertions: ? From Buypass: Webtrust for CA and EV SSL (readiness). Link to the Webseal: https://cert.webtrust.org/ViewSeal?id=848

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify the domain referenced in an SSL cert is owned/controlled by the subscriber. In addition to verification of subscriber's legal identity.
    - Class 2 SSL CP
        - Section 2.1.1: 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 4.1.1: The controls and procedures used to verify the Certificate Application SHALL establish: … that the Subscriber is a registered holder or has control of the domain name to be included in the SSL Certificate.
        - Section 4.4.1: A Certificate SHALL be revoked if: … The CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the Certificate, or that the Subscriber has failed to renew its domain name;
    - Class 3 SSL CP
        - Section 2.1.1: 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 4.1.1: For EV Certificates, the contents of the Subscriber Agreement SHALL comply with the requirements of the CA/Browser Forum Guidelines [10].
        - Section 4.1.1: 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 Subscriber is a registered holder or has exclusive control of the domain name to be included in the SSL Certificate.
        - Section 4.4.1: : A Certificate SHALL be revoked if: …The CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the Certificate, or that the Subscriber has failed to renew its domain name;
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - I haven't found email verification information yet. Perhaps this is in the CP/CPS for "Buypass Class 3 Enterprise Certificates"?
- Verify identity info in code signing certs is that of subscriber
    - Not Applicable, not requesting code signing trust bit for either root.

- Make sure it's clear which checks are done for which context (cert usage)
- All documents supplied as evidence should be publicly available and must be addressed in any audit. Any substantial omissions submitted afterwards may need to be confirmed by auditor, at Mozilla's discretion.

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
  - SSL certs are OV and EV.
  - 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. If the validity period exceeds twelve months, the CA SHALL revalidate Subscriber information every twelve months for as long as the Certificate is still valid, see [10].
- Wildcard DV SSL certificates
  - SSL certs are OV and EV.
- Delegation of Domain / Email validation to third parties
  - Class 2 and Class 3 SSL CPS section 4.1.1: Buypass does not use external RAs.
- Issuing end entity certificates directly from roots
  - Based on the test certs, it looks like SSL certs are issued directly from roots. Need hierarchy description to confirm.
- Allowing external entities to operate unconstrained subordinate CAs
  - ?
- Distributing generated private keys in PKCS#12 files
  - Class 2 and Class 3 SSL CP section 4.2: The CA SHALL ensure that the Subscriber has possession of the Private Key associated with the Public Key presented for certification.
- Certificates referencing hostnames or private IP addresses
  - ?
- OCSP Responses signed by a certificate under a different root
  - ?
- CRL with critical CIDP Extension
  - CRLs imported into Firefox without error.

Verify Audits

(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that they did indeed issue this report.
    - Posted on cert.webtrust.org
- For EV CA's, verify current WebTrust EV Audit done.
    - Need EV audit report url
- Review Audit to flag any issues noted in the report
    - No issues noted in WebTrust CA audit report.