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	www.buypass.no
Organizational type	Public corporation
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	2006-10-13	2005-05-09

Valid to	2016-10-13	2015-05-09
Cert Version	3	3
Modulus length	2048	2048
CRL URL Update frequency 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 Responder URL	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	There is no subordinate CA. This root signs end-entity certificates directly.	There is no subordinate CA. This root signs end-entity certificates directly.
	Comment #9 from Frank Hecker: My position on this is as follows: As noted in our problematic practices document, we do think that issuing end-entity certificates directly from a root is not a good practice, and that a better practice would be to issue EE certificates from a subordinate CA that can act as the issuing CA. However there is nothing in our current CA policy that prohibits issuing EE certificates directly from a root. I've also looked through the EV guidelines, and I can't see anything there that prohibits issuing EE certificates directly from the root. So: I urge Buypass to consider establishing a subordinate CA to issue EV certificates, instead of continuing to issue them directly from the root, and to operate the root in an off-line mode (where it will issue only subordinate CA certificates). However I don't see a justification for delaying its request until this change is made. Comment #11 from Buypass: Buypass established the CA activity in 2005 (Buypass Class 3 CA 1) and the focus was issuance of certificates in the Norwegian market. One of the main design principles was simplicity and as a new actor in a immature Norwegian certificate market the simple, yet sufficient solution with one single CA was a natural choice. We established the Buypass Class 2 CA 1 in 2006 in order to add some more flexibility to our certificate product range. We fully understand the advantages of having a CA hierarchy and our current strategy is to revise our CA structure when we are to replace the Buypass Class 3 CA 1, no later then 2012. During this revision of our CA structure, a CA hierarchy with one or more offline root CAs and separate issuing CAs will most probably be the preferred choice. Furthermore, we had a discussion on the topic with our auditors before starting the WebTrust engagement and learned that the EV Guidelines does not require certificates being issued from a subordinate issuing CA under a Root. Buypass has taken adequate measures to secure the private key of the issuing CA (being also the root).	

Subordinate CAs operated by third parties	None	None
List any other root CAs that have issued cross-signing certificates for this root CA	None	None
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites 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. Comment #11 from Buypass: The Email (S/MIME) trust bit should not be enabled.	
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV Class 2 SSL CP section 4.1.1 Initial Application 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.	OV, EV Class 3 SSL CP section 4.1.1, Initial Application: 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).	https://domain.ssl.buypass.no/ssl/domain/ Buypass CA test-certs https://bugzilla.mozilla.org/attachment.cgi?id=361509	https://evident.ssl.buypass.no/ssl/evident/
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	
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 (2008-12-22) This is the WebTrust CA audit for • Buypass Class 2 SSL and Class 3 SSL Certificates • Buypass Class 3 Enterprise Certificates	

	Audit Type: WebTrust EV Readiness Audit Auditor: KPMG Auditor website: www.kpmg.com Audit Report and Management's Assertions: https://bugzilla.mozilla.org/attachment.cgi?id=371230 (2008-12-22, for Buypass Class 3 CA) > From: Paling, Patrick <Paling.Patrick@kpmg.nl> > Subject: RE: Verifying Authenticity of Audit Report provided by Buypass > Date: Thursday, April 23, 2009, 3:43 AM Kathleen, Thank you for your e-mail. I am the engagement manager for the WebTrust for CA and WebTrust EV SSL audits for Buypass and I can confirm that the report was issued to Buypass AS by KPMG Advisory NV, The Netherlands. Furthermore, I want to give you some more background on our reporting practices for EV SSL. Buypass has succesfully completed the first phase of the EV SSL audit, focussing on the design of the practices and procedures (also referred to as a Readiness Audit). However, this has been audited by us at a specific point in time (as specified in the report). Of course, we did not yet complete the next phase (auditing the operating effectiveness, where we test the EV SSL controls over a longer period in time), as Buypass will have to be in operation for a number of months. Responding to your remark on publishing the reports on the Internet: it is our Dutch firm's practice to only publish an assurance report and make it available to the general public / the Internet after the audit on operating effectiveness has been completed. Once Buypass has succesfully completed the audit on operating effectiveness, we will issue the report on the cert.webTrust website and provide Buypass the accompanying webseal. Best regards, Patrick Paling

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.
    - Not Applicable, not requesting email trust bit for either root.
- 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
    - **Both of these roots issue end-entity certificates directly. See info in table above.**
- Allowing external entities to operate unconstrained subordinate CAs

    - No externally-operated sub-CAs.
- Distributing generated private keys in PKCS#12 files
    - Comment #7: all SSL certificates are issued on keys generated by the subscriber.
- Certificates referencing hostnames or private IP addresses
    - No
- OCSP Responses signed by a certificate under a different root
    - No
- 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.
    - WebTrust CA audit is posted on cert.webtrust.org
    - WebTrust EV Readiness audit is attached in bugzilla – KPMG has confirmed the authenticity of the report.
- For EV CA's, verify current WebTrust EV Audit done.
    - Current.
- Review Audit to flag any issues noted in the report
    - No issues noted in either audit report.