CERTIFICATE AND CRL PROFILES

Buypass Class 2 Certificates

PUBLIC

Version: 3.0
Document date: 15.03.2014

Buypass AS
Nydalsveien 30A, PO Box 4364 Nydalen
N-0402 Oslo, Norway
Tel.: +47 23 14 59 00
Fax: +47 23 14 59 01
E-mail: kundeservice@buypass.no
VAT: NO 983 163 327
www.buypass.no

Table of content

1 Certificate and CRL profiles 3
1.1 Buypass Class 2 Person certificate profile 3
1.2 Buypass Class 2 Domain Plus certificate profile 4
1.3 Buypass Class 2 Domain certificate profile 6
1.4 Buypass Class 2 Merchant certificate profile 7
1.5 CRL profile 8

1 Certificate and CRL profiles

1.1 Buypass Class 2 Person certificate profile

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption	M	B	sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 } sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	CN=Buypass Class 2 CA <ca no> O= Buypass AS-983163327 C=NO	M	B	<ca no> is 1 or 3
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 3 years
Subject	C=NO	M	B	
	O=<Subscriber Name>-<Subscriber Id>	O	B	Subscriber Name and Id according to Enhetsregisteret
	OU=<Subscriber Department>	O	B	
	CN=<Subject Name>	M	B	FirstName + MiddleName + LastName
	SerialNumber=9578-4050-<BuypassId>	M	B	<BuypassId>: unique Buypass identifier for Subject
Subject Public Key Info	Subject Public Key	M	B	RSA key size is at least 1024, from 2011 it will be 2032 or 2048 bits
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	M	B	
Authority Key Identifier	Key Identifier for the CA public key.	M	N	
Subject Key Identifier	Key Identifier for the Subject Public Key	M	N	
Certificate Policies	Policy OID= 2.16.578.1.26.1.2.1	M	N	
Subject Alternative Name	RFC822Name=<Subject email address>	O	N	
CRL Distribution Point	URL=ldap://ldap.buypass.no/dc=Buypass,dc=NO,CN=Buypass%20Class%202%20CA%20<ca no>?certificateRevocationList URL = http://crl.buypass.no/crl/BPClass2CA<ca no>.crl	M	N	<ca no> is 1 or 3

Field	Value	1)	2)	Comment
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL = http://ocsp.buypass.no/ocsp/BPClass2CA<ca no>	M	N	<ca no> is 1 or 3
Key Usage	Digital Signature, Key Encipherment, Data Encipherment, Key Agreement (0xB8)	M	C	Certificate 1
	Non-Repudiation (0x40)	M	C	Certificate 2
Extended Key Usage		O	N	

1) Mandatory or Optional field
2) Basic, Critical or Non-Critical extensions

1.2 Buypass Class 2 Domain Plus certificate profile

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption	M	B	sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 } sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	CN=Buypass Class 2 CA <ca no> O= Buypass AS-983163327 C=NO	M	B	<ca no> is 1 or 2
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <=3 years
Subject	C=NO	M	B	
	O=<Subscriber Name>	M	B	According to 'Enhetsregisteret'
	OU=<Subscriber Department>	O	B	
	CN=<Domain name>	M	B	Fully qualified domain name owned or controlled by the Subject
	SerialNumber=Organization number	M	B	According to 'Enhetsregisteret'
	LocalityName= <City or town – postal area>	M	B	Physical location of Subscriber place of Business
	PostalCode= <postal code>	M	B	
Subject Public Key Info	Subject Public Key	M	B	RSA key size is at least 1024 for certificates with expiry date before 1.1.2014, otherwise at least 2048 bits

Field	Value	1)	2)	Comment
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	M	B	
Authority Key Identifier	Key Identifier for the CA public key.	M	N	
Subject Key Identifier	Key Identifier for the Subject Public Key	M	N	
Certificate Policies	Policy OID= 2.16.578.1.26.1.2.3 Policy OID = 2.23.140.1.2.2	M	N	BP Class 2 Domain Plus OID BR OV OID – only for CA 2
CRL Distribution Point	URL = http://crl.buypass.no/crl/BPClass2CA<ca no>.crl	M	N	<ca no> is 1 or 2
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL = http://ocsp.buypass.no/ocsp/BPClass2CA1 if <ca no> = 1 and URL = http://ocsp.buypass.no/ocsp/BPOcsp if <ca no> = 2 [2]Authority Info Access Access Method= Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://crt.buypass.no/crt/BPClass2CA2.cer	M	N	<ca no> is 1 or 2 The reference to the issuing CA certificate is only used for CA 2
Subject Alternative Name	DNS Name	M	N	Set of fully qualified domain names, where one is equal to Subject.CN. May include internal domain names and/or server names. A single domain name if wildcard.
Key Usage	Digital Signature, Key Encipherment (0xA0)	M	C	
Extended Key Usage	Server Authentication (OID=1.3.6.1.5.5.7.3.1) Client Authentication (OID=1.3.6.1.5.5.7.3.2)	M	N	

1) Mandatory or Optional field
2) Basic, Critical or Non-Critical extensions

1.3 Buypass Class 2 Domain certificate profile

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption	M	B	sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 } sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	CN=Buypass Class 2 CA <ca no> O= Buypass AS-983163327 C=NO	M	B	<ca no> is 1 or 2
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <=3 years
Subject	CN=<Domain name>	M	B	Fully qualified domain name owned or controlled by the Subject
Subject Public Key Info	Subject Public Key	M	B	RSA key size is at least 1024 for certificates with expiry date before 1.1.2014, otherwise at least 2048 bits
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	M	B	
Authority Key Identifier	Key Identifier for the CA public key.	M	N	
Subject Key Identifier	Key Identifier for the Subject Public Key	M	N	
Certificate Policies	Policy OID= 2.16.578.1.26.1.2.4 Policy OID = 2.23.140.1.2.1	M	N	BP Class 2 Domain OID BR DV OID – only for CA 2
CRL Distribution Point	URL = http://crl.buypass.no/crl/BPClass2CA<ca no>.crl	M	N	<ca no> is 1 or 2
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL = http://ocsp.buypass.no/ocsp/BPClass2CA1 if <ca no> = 1 and URL = http://ocsp.buypass.no/ocsp/BPOcsp if <ca no> = 2 [2]Authority Info Access Access Method= Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://crt.buypass.no/crt/BPClass2CA2.cer	M	N	<ca no> is 1 or 2 The reference to the issuing CA certificate is only used for CA 2
Subject Alternative Name	DNS Name	M	N	Set of fully qualified domain name(s), where one is equal to Subject.CN

Field	Value	1)	2)	Comment
Key Usage	Digital Signature, Key Encipherment (0xA0)	M	C	
Extended Key Usage	Server Authentication (OID=1.3.6.1.5.5.7.3.1) Client Authentication (OID=1.3.6.1.5.5.7.3.2)	M	N	

1) Mandatory or Optional field
2) Basic, Critical or Non-Critical extensions

1.4 Buypass Class 2 Merchant certificate profile

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption	M	B	sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 } sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	CN=Buypass Class 2 CA <ca no> O= Buypass AS-983163327 C=NO	M	B	<ca no> is 2 or 3
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 5 years
Subject	C=NO	M	B	
	O=<Subscriber Name>	M	B	According to 'Enhetsregisteret'
	OU=<Merchant Name>	O	B	
	CN=<MerchantID>	M	B	Merchant Identifer; i.e. unique Merchant Identifier assigned to Subject by Buypass
Subject Public Key Info	Subject Public Key	M	B	RSA key size is at least 2048 bits
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	M	B	
Authority Key Identifier	Key Identifier for the CA public key.	M	N	
Subject Key Identifier	Key Identifier for the Subject Public Key	M	N	
Certificate Policies	Policy OID= 2.16.578.1.26.1.2.5	M	N	BP Class 2 Merchant ID OID

Field	Value	1)	2)	Comment
Subject Alternative Name	RFC822Name=<Subject email address>	O	N	
CRL Distribution Point	URL=ldap://ldap.buypass.no/dc=Buypass,dc=NO,CN=Buypass%20Class%202%20CA%20<ca no>?certificateRevocationList URL = http://crl.buypass.no/crl/BPClass2CA<ca no>.crl	M	N	<ca no> is 2 or 3
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL = http://ocsp.buypass.no/ocsp/BPClass2CA<ca no>	M	N	<ca no> is 2 or 3
Key Usage	Digital Signature, Key Encipherment, Data Encipherment (0xB0)	M	C	Certificate 1

1) Mandatory or Optional field
2) Basic, Critical or Non-Critical extensions

1.5 CRL profile

Field	Value	1)	2)	Comment
Version	X509 version 2 CRL	M	B	
Signature Algorithm	sha-1WithRSAEncryption or sha256WithRSAEncryption	M	B	sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 } sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	CN=Buypass Class 2 CA <ca no> O= Buypass AS-983163327 C=NO	M	B	<ca no> is 1, 2 or 3
This Update	UTCTime	M	B	Time of CRL generation
Next Update	UTCTime	M	B	Latest time the next CRL is issued
Revoked Certificates	List of revoked certificates	O	B	Present if any certificates are currently revoked

Each entry in the RevokedCertificates list has the following content:

Field	Value	1)	2)	Comment
Serial Number	Serial Number of the revoked certificate	M	B	
Revocation Date	UTCTime	M	B	Date and time the revocation was registered
Revocation Reason	Reason Code for the revocation	O	N	

1) Mandatory or Optional field
2) Basic, Critical or Non-Critical extensions