CERTIFICATE AND CRL PROFILES

BUYPASS CLASS 2 CERTIFICATES

PUBLIC

Version: 8.0
Document date: 26.03.2019

Buypass AS
Nydalsveien 30A, PO Box 4364 Nydalen
N-0402 Oslo, Norway
Tel.: + 47 22 70 13 00
E-mail: support@buypass.com
VAT: NO 983 163 327
www.buypass.com

Table of content

1 Certificate and CRL profiles for Subscriber certificates

1.1 Buypass SSL Business certificate profile

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	sha256WithRSAEncryption	M	B	sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	CN=Buypass Class 2 CA 2 O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 825 days
Subject	C=<country>	M	B	According to QGR
	O=<Subscriber Name>	M	B	According to QGR
	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 QGR
	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 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= 2.16.578.1.26.1.2.3 Policy OID = 2.23.140.1.2.2	M	N	Buypass SSL Business OID CABF BR OV OID
CRL Distribution Point	URL = http://crl.buypass.no/crl/BPClass2CA2.crl	M	N	
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/BPOcsp before December 2016 and URL = http://ocsp.buypass.com since December 2016 [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	
Subject Alternative Name	DNS Name	M	N	Set of fully qualified domain names and/or wildcard domain names, 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	
Signed Certificate TimeStamp List	(OID=1.3.5.1.4.1.11129.2.4.2)	M	N	2 or 3 Signed Certificate Timestamps from CT-logs embedded in the final certificate
Poison Extentsion	*(OID=1.3.5.1.4.1.11129.2.4.3)*	*M*	*C*	*Poison Extension, Precertificate only*

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

1.2 Buypass SSL 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	sha256WithRSAEncryption	M	B	sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	CN=Buypass Class 2 CA 2 O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <=-825 days
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 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	Buypass SSL Domain OID CABF BR DV OID
CRL Distribution Point	URL = http://crl.buypass.no/crl/BPClass2CA2.crl	M	N	
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/BPOcsp before December 2016 and URL = http://ocsp.buypass.com since December 2016	M	N	

Field	Value	1)	2)	Comment
	[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			
Subject Alternative Name	DNS Name	M	N	Set of fully qualified domain name(s), where one is equal to Subject.CN
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	
Signed Certificate TimeStamp List	(OID=1.3.5.1.4.1.11129.2.4.2)	M	N	2 or 3 Signed Certificate Timestamps from CT-logs embedded in the final certificate
Poison Extentsion	*(OID=1.3.5.1.4.1.11129.2.4.3)*	*M*	*C*	*Poison Extension, Precertificate only*

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

1.3 Buypass Go SSL certificate profile

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	sha256WithRSAEncryption	M	B	sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	CN=Buypass Class 2 CA 5 O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 180 days
Subject	CN=<Domain name>	O	Co	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 2048 bits or ECDSA (only NIST P-256 is accepted)
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= 2.16.578.1.26.1.2.7 Policy OID = 2.23.140.1.2.1	M	N	Buypass Go SSL OID CABF BR DV OID

Field	Value	1)	2)	Comment
CRL Distribution Point	URL = http://crl.buypass.no/crl/BPClass2CA5.crl	M	N	
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.com [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/BPClass2CA5.cer	M	N	
Subject Alternative Name	DNS Name	M	Co	Set of fully qualified domain name(s), where one is equal to Subject.CN if CN is used
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	
Signed Certificate TimeStamp List	(OID=1.3.5.1.4.1.11129.2.4.2)	M	N	2 or 3 Signed Certificate Timestamps from CT-logs embedded in the final certificate
Poison Extentsion	*(OID=1.3.5.1.4.1.11129.2.4.3)*	*M*	*C*	*Poison Extension, Precertificate only*

1) Mandatory or Optional field
2) Basic, Critical, Non-Critical or Conditional extensions (CN critical if present, otherwise SAN critical)

1.4 CRL profile

Field	Value	1)	2)	Comment
Version	X509 version 2 CRL	M	B	
Signature Algorithm	sha256WithRSAEncryption	M	B	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 5
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 non-expired revoked certificates	O	B	

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

Field	Value	1)	2)	Comment
Revocation Reason	Reason Code for the revocation	O	N	

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

2 Certificate and CRL profiles for CA certificates

2.1 Buypass Class 2 CA certificate profile

2.1.1 Root CA certificate

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	sha256WithRSAEncryption	M	B	sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	CN=Buypass Class 2 Root CA O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 30 years
Subject	CN=Buypass Class 2 Root CA O= Buypass AS-983163327 C=NO	M	B	
Subject Public Key Info	Subject Public Key	M	B	RSA key size is at least 4096 bits
Basic Constraints	Subject Type=CA Path Length Constraint=None	M	B	
Subject Key Identifier	Key Identifier for the Root CA public key	M	N	
Key Usage	Certificate Signing, CRL Signing (0x06)	M	C	

2.1.2 Intermediate CA certificates

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	sha256WithRSAEncryption	M	B	sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	CN=Buypass Class 2 Root CA O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 20 years for CA 2 and <= 10 years for CA 5
Subject	CN=Buypass Class 2 CA <ca no> O= Buypass AS-983163327 C=NO	M	B	<ca no> is 2 or 5

Field	Value	1)	2)	Comment
Subject Public Key Info	Subject Public Key	M	B	RSA key size is at least 2048 bits
Basic Constraints	Subject Type=CA Path Length Constraint=None	M	B	
Authority Key Identifier	Key Identifier for the Root CA public key	M	N	
Subject Key Identifier	Key Identifier for the CA Public Key	M	N	
Certificate Policies	Policy OID= <All issuance policies>	M	N	
CRL Distribution Point	URL = http://crl.buypass.no/crl/BPClass3RootCA.crl	M	N	
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.com	M	N	For Buypass Class 2 CA 2 and Buypass Class 2 CA 5 only
Key Usage	Certificate Signing, CRL Signing (0x06)	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	For Buypass Class 2 CA 2 only

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

2.2 CRL profile

Field	Value	1)	2)	Comment
Version	X509 version 2 CRL	M	B	
Signature Algorithm	sha256WithRSAEncryption	M	B	sha256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	CN=Buypass Class 2 Root CA O= Buypass AS-983163327 C=NO	M	B	
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 non-expired revoked CA certificates	O	B	

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

3 Revocation status information

3.1 CRL

Buypass Class 2 Root CA:

- http://crl.buypass.no/crl/BPClass2RootCA.crl

Buypass Class 2 CA 2:

- http://crl.buypass.no/crl/BPClass2CA2.crl

Buypass Class 2 CA 5:

- http://crl.buypass.no/crl/BPClass2CA5.crl

3.2 OCSP

Buypass Class 2 Root CA, Buypass Class 2 CA 2 and Buypass Class 2 CA 5:

- http://ocsp.buypass.com – used since December 2016
- http://ocsp.buypass.no/ocsp/BPOcsp - used before December 2016