

Certificate and CRL Profiles

Buypass Class 3 Certificates

HISTORY OF CHANGES

Version	Date	Description
1.0	06.05.2005	Initial version
1.1	06.06.2006	New chapter : 1.2 Buypass Class 3 Enterprise certificate profile
1.2	07.03.2008	New chapter: 1.3 Buypass Class 3 SSL EV certificate profile
1.2.1	05.04.2008	Updated chapter 1.3 and added new chapter 1.4 Buypass Class 3 SSL certificate profile
1.2.2	20.08.2008	Updated chapter 1.4
1.2.3	26.10.2009	Changed OCSP URL for SSL from https to http
1.2.4	17.11.2009	Changed name of the document
1.2.5	01.03.2010	Added DNS name to Subject Alternative Names for the SSL certificate profiles
1.2.6	09.06.2010	Changed encoding of Business Categories according to ballot 43 CABForum
1.3	18.10.2010	Changes due to new CA structure, support for SHA256 and longer keys
1.4	22.02.2011	Changed URLs for CA1
1.5	01.07.2012	Included support for BR and changes in CA structure
2.0	01.12.2012	Changes related to new CA-structure
3.0	11.06.2013	Included Enterprise certificates provided as hard tokens
4.0	28.04.2014	Maximum lifetime of Qualified Certificates changed from 3 years to 5 years
5.0	09.09.2014	Product name Buypass Business SSL Certificates changed name to Buypass Business Plus SSL Certificates
6.0	05.01.2015	EBR (European Business Register) included for SSL Certificates. Certificate Transparency included for EV SSL Certificates. RSA 1024 bits removed for all Certificates.
7.0	11.05.2015	Lifetime of Buypass Enterprise Certificates changed from <= 38 months to <= 42 months due to expanded renewal period.
8.0	11.01.2016	Added CABF EV OID in EV Certificates.
9.0	15.03.2018	Adapted to new ETSI profiles. Removed SHA-1 and CA1. Reduced validity period. Added certificate and CRL profiles for CA certificates. Added revocation status information.
10.0	05.03.2019	Included EKU, and Key Usage for Enterprise certificates where subscriber generates private key
11.0	26.03.2019	Included EKU in Buypass Class 3 CA 2.
12.0	02.06.2019	Included profiles for PSD2 Certificates, added UPN and Smartcard logon.
13.0	12.07.2019	Included Key Usage Digital Signature, Non-Repudiation (OxCO) for PSD2 QC eSeal.
14.0	04.02.2020	Included cabfOrganizationIdentifier for PSD2 QWACs.
15.0	03.03.2020	Included NCP and NCP+ (ETSI profiles). Included SerialNumber as an option in Enterprise Certificates with ETSI profile.
16.0	01.09.2020	Maximum TLS certificate validity period of 398 days.
17.0	01.12.2020	Included generation 2 (G2) of Root CAs and issuing CAs.
17.1	22.02.2021	Included support for ECC in TLS certificates.
17.2	03.05.2021	Maximum validity period for PSD2 QWAC set to 825 days

Contents

1	Certificate and CRL profiles for Subscriber certificates	4
1.1	Buypass Class 3 Qualified certificate profile	4
1.1.1	Certificate profile according to National legislation	4
1.1.2	Certificate profile according to Regulation (EU) No 910/2014 (eIDAS).....	4
1.1.3	CA specific details	5
1.2	Buypass Class 3 Enterprise certificate profile	6
1.2.1	Certificate profile according to National legislation	6
1.2.2	Certificate profile according to Regulation (EU) No 910/2014 (eIDAS).....	7
1.2.3	PSD2 Certificate profile according to Regulation (EU) No 389/2018 (RTS).....	9
1.2.4	CA specific details	10
1.3	Buypass SSL Evident certificate profile	11
1.3.1	Certificate profile according to CA/Browser Forum EV Guidelines.....	11
1.3.2	Certificate profile according to Regulation (EU) No 910/2014 (eIDAS).....	12
1.3.3	PSD2 Certificate profile according to Regulation (EU) No 389/2018 (RTS).....	13
1.3.4	QWAC Certificate profile according to Regulation (EU) No 910/2014 (eIDAS).....	14
1.3.5	PSD2 QWAC Certificate profile according to Regulation (EU) No 389/2018 (RTS).....	16
1.4	Buypass SSL Business Plus certificate profile.....	17
1.5	CRL profile	18
2	Certificate and CRL profiles for CA certificates	19
2.1	Buypass Class 3 CA certificate profile	19
2.1.1	Root CA certificate	19
2.1.2	Intermediate CA certificates	20
2.2	CRL profile	23
3	Revocation status information	24
3.1	CRL.....	24
3.2	OCSP	24

1 Certificate and CRL profiles for Subscriber certificates

1.1 Buypass Class 3 Qualified certificate profile

1.1.1 Certificate profile according to National legislation

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	<CA specific>	M	B	See 1.1.3
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 5 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 2032 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 = 2.16.578.1.26.1.3.1 or Policy OID = 2.16.578.1.26.1.3.6	M	N	Private keys in smart card or Private keys in HSM
Subject Alternative Name	RFC822Name=<Subject email address> Other Name: Principal Name=<User Principal Name>	O	N	
CRL Distribution Point	<CA specific>	M	N	See 1.1.3
Authority Information Access	<CA specific>	M	N	See 1.1.3
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	Client Authentication (1.3.6.1.5.5.7.3.2), Secure Email (1.3.6.1.5.5.7.3.4)	M	N	
	Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	O	N	
Qualified Certificate Statement	esi4-qcStatement-1	M	N	

1.1.2 Certificate profile according to Regulation (EU) No 910/2014 (eIDAS)

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

Field	Value	1)	2)	Comment
				OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	<CA specific>	M	B	See 1.1.3
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 5 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	
	Surname	M	B	LastName
	GivenName	M	B	FirstName + MiddleName
	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 2032 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 = 2.16.578.1.26.1.3.1 or Policy OID = 2.16.578.1.26.1.3.6	M	N	Private keys in smart card or Private keys in HSM
	Policy OID = 0.4.0.194112.1.0	O	N	ETSI QCP-n (QC only)
Subject Alternative Name	RFC822Name=<Subject email address> Other Name: Principal Name=<User Principal Name>	O	N	
CRL Distribution Point	<CA specific>	M	N	See 1.1.3
Authority Information Access	<CA specific>	M	N	See 1.1.3
Key Usage	Digital Signature, Key Encipherment (OxAO)	M	C	Certificate 1
	Non-Repudiation (Ox40)	M	C	Certificate 2
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2), Secure Email (1.3.6.1.5.5.7.3.4)	M	N	
	Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	O	N	
Qualified Certificate Statements	esi4-qcStatement-1	M	N	EU Qualified Certificate (QC)
	esi4-qcStatement-6 id-etsi-qct-esign	M	N	EU QC for electronic signatures
	esi4-qcStatement-5 <PdsLocation url= https://www.buypass.no/pds/pds_en.pdf language="en"/>	M	N	URL to PKI Disclosure Statement (PDS)

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

1.1.3 CA specific details

Buypass Class 3 CA 3:

Issuer	CRL Distribution Point	Authority Information Access
CN = Buypass Class 3 CA 3 O = Buypass AS-983163327 C = NO	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.buypass.no/crl/BPClass3CA3.crl	[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/BPClass3CA3
	[2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.buypass.no/dc=Buypass,dc=	[2]Authority Info Access Access Method= Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name:

Issuer	CRL Distribution Point	Authority Information Access
	NO,CN=Buypass Class 3 CA 3 ?certificateRevocationList (ldap://ldap.buypass.no/dc=Buypass,dc=NO, CN=Buypass%20Class%203%20CA%203? certificateRevocationList)	URL = http://crt.buypass.no/crt/BPClass3CA3.cer

Buypass Class 3 CA HT PS:

Issuer	CRL Distribution Point	Authority Information Access
CN = Buypass Class 3 CA G2 HT Person O = Buypass AS OrganizationIdentifier = NTRNO- 983163327 C = NO	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.buypassca.com/BPCI3CaG2HTTPS.crl	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocspps.buypassca.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://crt.buypassca.com/BPCI3CaG2HTTPS.cer

1.2 Buypass Class 3 Enterprise certificate profile

1.2.1 Certificate profile according to National legislation

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	<CA specific>	M	B	See 1.2.4
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 42 months
Subject	C=NO	M	B	
	O=<Subscriber Name>	M	B	According to 'Enhetsregisteret'
	OU=<Subscriber Department>	O	B	
	CN=<Subject name>	M	B	Subject name as defined by Subscriber (e.g. subscriber name, system name, application name)
SerialNumber		M	B	Organization number according to 'Enhetsregisteret'
Subject Public Key Info	Subject Public Key	M	B	RSA key size is at least 2048 bits for Soft Tokens and 2032 bits for Hard Tokens
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 = 2.16.578.1.26.1.3.2 or Policy OID = 2.16.578.1.26.1.3.5	M	N	Soft Token or Hard Token
Subject Alternative Name	RFC822Name=<Subject email address>	O	N	
CRL Distribution Point	<CA specific>	M	N	See 1.2.4
Authority Information Access	<CA specific>	M	N	See 1.2.4
Key Usage	Digital Signature, Key Encipherment, Data Encipherment (0xBO)	M	C	CA generated Private Keys, Certificate 1

Field	Value	1)	2)	Comment
	Non-Repudiation (0x40)	M	C	CA generated Private Keys, Certificate 2
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2), Secure Email (1.3.6.1.5.5.7.3.4)	M	N	CA generated Private Keys
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, (0xE0) or Non-Repudiation (0x40)	M	C	Subscriber generated Private Key
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2), Secure Email (1.3.6.1.5.5.7.3.4)	M	N	Subscriber generated Private Key

1.2.2 Certificate profile according to Regulation (EU) No 910/2014 (eIDAS)

In case Bypass generates the private keys, Certificates may be issued as combinations of Non-Qualified Certificates (similar to Certificates according to national legislation) or combinations of Qualified and Non-Qualified Certificates. For the latter case, the Qualified Certificate is always issued with KeyUsage=nonrepudiation.

Non-Qualified 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	<CA specific>	M	B	See 1.2.4
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 42 months
Subject	C=NO	M	B	
	O=<Subscriber Name>	M	B	According to an authoritative source
	OU=<Subscriber Department>	O	B	
	CN=<Subject name>	M	B	Subject name as defined by Subscriber (e.g. subscriber name, system name, application name)
	SerialNumber	O	B	Organization number according to an authoritative source
Subject Public Key Info	Organization Identifier	M	B	According to an authoritative source
	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 = 2.16.578.1.26.1.3.2 or Policy OID = 2.16.578.1.26.1.3.5	M	N	Soft Token or Hard Token
	Policy OID = 0.4.0.2042.1.1 or Policy OID = 0.4.0.2042.1.2	O	N	ETSI NCP or ETSI NCP+
Subject Alternative Name	RFC822Name=<Subject email address>	O	N	
CRL Distribution Point	<CA specific>	M	N	See 1.2.4
Authority Information Access	<CA specific>	M	N	See 1.2.4
Key Usage	Digital Signature, Key Encipherment (0xA0)	M	C	CA generated Private Keys, Certificate 1
	Non-Repudiation (0x40)	M	C	CA generated Private Keys, Certificate 2
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2), Secure Email (1.3.6.1.5.5.7.3.4)	M	N	CA generated Private Keys

Field	Value	1)	2)	Comment
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, (0xEO) or Non-Repudiation (0x40)	M	C	Subscriber generated Private Key
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2), Secure Email (1.3.6.1.5.5.7.3.4)	M	N	Subscriber generated Private Key

Qualified 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	<CA specific>	M	B	See 1.2.4
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 42 months
Subject	C=NO	M	B	
	O=<Subscriber Name>	M	B	According to an authoritative source
	OU=<Subscriber Department>	O	B	
	CN=<Subject name>	M	B	Subject name as defined by Subscriber (e.g. subscriber name, system name, application name)
	SerialNumber	O	B	Organization number according to an authoritative source
Subject Public Key Info	Organization Identifier	M	B	According to an authoritative source
	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 = 2.16.578.1.26.1.3.2 or Policy OID = 2.16.578.1.26.1.3.5	M	N	Soft Token or Hard Token
	Policy OID = 0.4.0.194112.1.1	O	N	ETSI QCP-I
Subject Alternative Name	RFC822Name=<Subject email address>	O	N	
CRL Distribution Point	<CA specific>	M	N	See 1.2.4
Authority Information Access	<CA specific>	M	N	See 1.2.4
Key Usage	Non-Repudiation (0x40)	M	C	CA generated Private Keys
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2), Secure Email (1.3.6.1.5.5.7.3.4)	M	N	CA generated Private Keys
Key Usage	Non-Repudiation (0x40)	M	C	Subscriber generated Private Key
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2), Secure Email (1.3.6.1.5.5.7.3.4)	M	N	Subscriber generated Private Key
Qualified Certificate Statements	esi4-qcStatement-1	M	N	EU Qualified Certificate (QC)
	esi4-qcStatement-6 id-etsi-qct-eseal	M	N	EU QC for electronic seals
	esi4-qcStatement-5 <PdsLocation url= https://www.bypass.no/pds/pds_en.pdf language="en"/>	M	N	URL to PKI Disclosure Statement (PDS)

1.2.3 PSD2 Certificate profile according to Regulation (EU) No 389/2018 (RTS)

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	<CA specific>	M	B	See 1.2.4
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 42 months
Subject	C=NO	M	B	
	O=<Subscriber Name>	M	B	According to an authoritative source
	OU=<Subscriber Department>	O	B	
	CN=<Subject name>	M	B	Subject name as defined by Subscriber (e.g. subscriber name, system name, application name)
Organization Identifier		M	B	PSD2 Authorization Number according to an NCA (formatted according to ETSI TS 119 495)
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 = 2.16.578.1.26.1.3.2 or Policy OID = 2.16.578.1.26.1.3.5	M	N	Soft Token or Hard Token
	Policy OID = 0.4.0.194112.1.1	O	N	ETSI QCP-I (QC only)
Subject Alternative Name	RFC822Name=<Subject email address>	O	N	
CRL Distribution Point	<CA specific>	M	N	See 1.2.4
Authority Information Access	<CA specific>	M	N	See 1.2.4
Key Usage	Non-Repudiation (0x40) or Digital Signature, Non-Repudiation (0xC0)	M	C	
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2), Secure Email (1.3.6.1.5.5.7.3.4)	M	N	CA generated Private Key
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2), Secure Email (1.3.6.1.5.5.7.3.4)	M	N	Subscriber generated Private Key
Qualified Certificate Statements	esi4-qcStatement-1	M	N	EU Qualified Certificate (QC)
	esi4-qcStatement-6 id-etsi-qct-eseal	M	N	EU QC for electronic seals
	esi4-qcStatement-5 <PdsLocation url= https://www.bypass.no/pds/pds_en.pdf language="en"/>	M	N	URL to PKI Disclosure Statement (PDS)
	etsi-psd2-qcStatement	M	N	PSD2QcType ::= SEQUENCE { rolesOfPSP RolesOfPSP, nCAName NCAName, nCAId NCAId }

1) Mandatory or Optional field

2) Basic, Critical or Non-Critical extensions

1.2.4 CA specific details

Buypass Class 3 CA 3 (according to National legislation):

Issuer	CRL Distribution Point	Authority Information Access
CN=Buypass Class 3 CA 3 O= Buypass AS-983163327 C=NO	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.buypass.no/crl/BPClass3CA3.crl</p> <p>[2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.buypass.no/dc=Buypass,dc=NO,CN=Buypass Class 3 CA 3 ?certificateRevocationList (ldap://ldap.buypass.no/dc=Buypass,dc=NO, CN=Buypass%20Class%203%20CA%203? certificateRevocationList)</p>	<p>[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/BPClass3CA3</p> <p>[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/BPClass3CA3.cer</p>

Buypass Class 3 CA 3 (according to Regulation (EU) No 910/2014 (eIDAS)):

Issuer	CRL Distribution Point	Authority Information Access
CN=Buypass Class 3 CA 3 O= Buypass AS-983163327 C=NO	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.buypass.no/crl/BPClass3CA3.crl</p>	<p>[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL = http://ocspec.buypass.com</p> <p>[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/BPClass3CA3.cer</p>

Buypass Class 3 CA ST Business:

Issuer	CRL Distribution Point	Authority Information Access
CN = Buypass Class 3 CA G2 ST Business O = Buypass AS OrganizationIdentifier = NTRNO- 983163327 C = NO	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.buypassca.com/BPCI3CaG2STBS.crl</p>	<p>[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocspbs.buypassca.com</p> <p>[2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://crt.buypassca.com/BPCI3CaG2STBS.cer</p>

Buypass Class 3 CA HT Business:

Issuer	CRL Distribution Point	Authority Information Access
CN = Buypass Class 3 CA G2 HT Business O = Buypass AS OrganizationIdentifier = NTRNO- 983163327 C = NO	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.buypassca.com/BPCI3CaG2HTBS.crl</p>	<p>[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocspbs.buypassca.com</p> <p>[2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://crt.buypassca.com/BPCI3CaG2HTBS.cer</p>

1.3 Buypass SSL Evident certificate profile

1.3.1 Certificate profile according to CA/Browser Forum EV Guidelines

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 3 CA 2 O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 398 days
Subject	C=<country>	M	B	According to an authoritative source
	jurisdictionOfIncorporation CountryName=<country>	M	B	OBJECT IDENTIFIER ::= 1.3.6.1.4.1.311.60.2.1.3
	O=<Subscriber Name>	M	B	According to an authoritative source
	OU=<Subscriber Department>	O	B	
	CN=<Domain name>	M	B	Fully qualified domain name. Wild card not allowed.
	SerialNumber	M	B	Organization number according to an authoritative source
	BusinessCategory=["Private Organization" "Government Entity" "Business Entity" "Non-Commercial Entity "]	M	B	Type of Subject
	LocalityName= <City or town – postal area> PostalCode= <postal code>	M	B	Physical location of Subscriber place of Business
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 = 2.16.578.1.26.1.3.3 Policy OID = 2.23.140.1.1	M	N	Buypass SSL Evident (EV) OID CABF EV OID from 11.1.2016
	Policy Qualifier ID = id-qt 1	M	N	Reference to CPS
	Policy Qualifier = https://www.buypass.no/cps	M	N	
CRL Distribution Point	URL = http://crl.buypass.no/crl/BPClass3CA2.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/BPClass3CA2.cer	M	N	
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	RSA keys
	Digital Signature (0x80)	M	C	ECDSA keys
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 Extension	(OID=1.3.5.1.4.1.11129.2.4.3)	M	C	Poison Extension, Precertificate only

1.3.2 Certificate profile according to Regulation (EU) No 910/2014 (eIDAS)

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 3 CA 2 O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 398 days
Subject	C=<country>	M	B	According to an authoritative source
	jurisdictionOfIncorporation CountryName=<country>	M	B	OBJECT IDENTIFIER ::= 1.3.6.1.4.1.311.60.2.1.3
	O=<Subscriber Name>	M	B	According to an authoritative source
	OU=<Subscriber Department>	O	B	
	CN=<Domain name>	M	B	Fully qualified domain name. Wild card not allowed.
	SerialNumber	M	B	Organization number according to an authoritative source
	BusinessCategory=["Private Organization" "Government Entity" "Business Entity" "Non-Commercial Entity"]	M	B	Type of Subject
	LocalityName= <City or town – postal area> PostalCode= <postal code>	M	B	Physical location of Subscriber place of Business
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 = 2.16.578.1.26.1.3.3 Policy OID = 2.23.140.1.1 Policy OID = 0.4.0.194112.1.4	M	N	Buypass SSL Evident (EV) OID CABF EV OID from 11.1.2016 ETSI QCP-w from 3.6.2019
	Policy Qualifier ID = id-qt 1	M	N	Reference to CPS
	Policy Qualifier = https://www.buypass.no/cps	M	N	
	CRL Distribution Point	URL = http://crl.buypass.no/crl/BPClass3CA2.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:	M	N	

Field	Value	1)	2)	Comment
	URL = http://ocsp.bypass.com [2]Authority Info Access Access Method= Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://crt.bypass.no/crt/BPClass3CA2.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	RSA keys
	Digital Signature (0x80)	M	C	ECDSA keys
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 Extension	(OID=1.3.5.1.4.1.11129.2.4.3)	M	C	Poison Extension, Precertificate only
Qualified Certificate Statements	esi4-qcStatement-1	M	N	EU Qualified Certificate (QC)
	esi4-qcStatement-6 id-etsi-qct-web	M	N	EU QC for website authentication
	esi4-qcStatement-5 <PdsLocation url= https://www.bypass.no/pds/pds_en.pdf language="en"/>	M	N	URL to PKI Disclosure Statement (PDS)

1.3.3 PSD2 Certificate profile according to Regulation (EU) No 389/2018 (RTS)

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 3 CA 2 O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 398 days
Subject	C=<country>	M	B	According to an authoritative source
	jurisdictionOfIncorporation CountryName=<country>	M	B	OBJECT IDENTIFIER ::= 1.3.6.1.4.1.311.60.2.1.3
	O=<Subscriber Name>	M	B	According to an authoritative source
	OU=<Subscriber Department>	O	B	
	CN=<Domain name>	M	B	Fully qualified domain name. Wild card not allowed.
	SerialNumber	M	B	Organization number according to an authoritative source
	Organization Identifier	M	B	PSD2 Authorization Number according to an NCA (formatted according to ETSI TS 119 495)
	BusinessCategory=["Private Organization" "Government Entity" "Business Entity" "Non-Commercial Entity "]	M	B	Type of Subject
	LocalityName= <City or town - postal area> PostalCode= <postal code>	M	B	Physical location of Subscriber place of Business
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)

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= 2.16.578.1.26.1.3.3 Policy OID= 2.23.140.1.1 Policy OID=0.4.0.194112.1.4	M	N	Buypass SSL Evident (EV) OID CABF EV OID ETSI QCP-w
	Policy Qualifier ID = id-qt 1	M	N	Reference to CPS
	Policy Qualifier = https://www.buypass.no/cps	M	N	
CRL Distribution Point	URL = http://crl.buypass.no/crl/BPClass3CA2.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/BPClass3CA2.cer	M	N	
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	RSA keys
	Digital Signature (0x80)	M	C	ECDSA keys
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	
cabfOrganizationIdentifier	OID: 2.23.140.3.1	M	N	PSD2 Authorization Number formatted according to EV Guidelines, from 1.2.2020
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 Extension	(OID=1.3.5.1.4.1.11129.2.4.3)	M	C	Poison Extension, Precertificate only
Qualified Certificate Statements	esi4-qcStatement-1	M	N	EU Qualified Certificate (QC)
	esi4-qcStatement-6 id-etsi-qct-web	M	N	EU QC for website authentication
	esi4-qcStatement-5 <PdsLocation url= https://www.buypass.no/pds/pds_en.pdf language="en"/>	M	N	URL to PKI Disclosure Statement (PDS)
	etsi-psd2-qcStatement	M	N	PSD2QcType ::= SEQUENCE { rolesOfPSP RolesOfPSP, nCAName NCAName, nCAId NCAId }

1.3.4 QWAC Certificate profile according to Regulation (EU) No 910/2014 (eIDAS)

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 3 CA G2 QC WA O = Buypass AS	M	B	

Field	Value	1)	2)	Comment
	OrganizationIdentifier = NTRNO-983163327 C = NO			
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 398 days
Subject	C=<country>	M	B	According to an authoritative source
	jurisdictionOfIncorporation CountryName=<country>	M	B	OBJECT IDENTIFIER ::= 1.3.6.1.4.1.311.60.2.1.3
	O=<Subscriber Name>	M	B	According to an authoritative source
	OU=<Subscriber Department>	O	B	
	CN=<Domain name>	M	B	Fully qualified domain name. Wild card not allowed.
	SerialNumber	M	B	Organization number according to an authoritative source
	BusinessCategory=["Private Organization" "Government Entity" "Business Entity" "Non-Commercial Entity"]	M	B	Type of Subject
	LocalityName= <City or town - postal area> PostalCode= <postal code>	M	B	Physical location of Subscriber place of Business
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 = 0.4.0.194112.1.4 Policy OID = 2.16.578.1.26.1.3.7	M	N	ETSI QCP-w Buypass Qualified Website Authentication Certificate OID
	Policy Qualifier ID = id-qt 1	M	N	Reference to CPS
	Policy Qualifier = https://www.buypass.no/cps	M	N	
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.buypassca.com/BPCI3CaG2QCWA.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://ocspwa.buypassca.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://crl.buypassca.com/BPCI3CaG2QCWA.cer	M	N	
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	RSA keys
	Digital Signature (0x80)	M	C	ECDSA keys
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	
Qualified Certificate Statements	esi4-qcStatement-1	M	N	EU Qualified Certificate (QC)
	esi4-qcStatement-6 id-etsi-qct-web	M	N	EU QC for website authentication
	esi4-qcStatement-5	M	N	URL to PKI Disclosure Statement (PDS)

Field	Value	1)	2)	Comment
	<PdsLocation url= https://www.buypass.no/pds/pds_en.pdf language="en"/>			

1.3.5 PSD2 QWAC Certificate profile according to Regulation (EU) No 389/2018 (RTS)

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 3 CA G2 QC WA O = Buypass AS OrganizationIdentifier = NTRNO-983163327 C = NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 825 days
Subject	C=<country>	M	B	According to an authoritative source
	jurisdictionOfIncorporation CountryName=<country>	M	B	OBJECT IDENTIFIER ::= 1.3.6.1.4.1.311.60.2.1.3
	O=<Subscriber Name>	M	B	According to an authoritative source
	OU=<Subscriber Department>	O	B	
	CN=<Domain name>	M	B	Fully qualified domain name. Wild card not allowed.
	SerialNumber	M	B	Organization number according to an authoritative source
	Organization Identifier	M	B	PSD2 Authorization Number according to an NCA (formatted according to ETSI TS 119 495)
	BusinessCategory=["Private Organization" "Government Entity" "Business Entity" "Non-Commercial Entity"]	M	B	Type of Subject
	LocalityName= <City or town - postal area> PostalCode= <postal code>	M	B	Physical location of Subscriber place of Business
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=0.4.0.19495.3.1 Policy OID = 2.16.578.1.26.1.3.7	M	N	ETSI QCP-w-psd2 Buypass Qualified Website Authentication Certificate OID
	Policy Qualifier ID = id-qt 1	M	N	
	Policy Qualifier = https://www.buypass.no/cps	M	N	Reference to CPS
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.buypassca.com/BPCI3CaG2QCWA.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:	M	N	

Field	Value	1)	2)	Comment
	URL= http://ocspwa.buypassca.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://crt.buypassca.com/BPCI3CaG2QCWA.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	RSA keys
	Digital Signature (0x80)	M	C	ECDSA keys
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	
cabfOrganizationIdentifier	OID: 2.23.140.3.1	M	N	PSD2 Authorization Number formatted according to EV Guidelines, from 1.2.2020
Qualified Certificate Statements	esi4-qcStatement-1	M	N	EU Qualified Certificate (QC)
	esi4-qcStatement-6 id-etsi-qct-web	M	N	EU QC for website authentication
	esi4-qcStatement-5 <PdsLocation url= https://www.buypass.no/pds/pds_en.pdf language="en"/>	M	N	URL to PKI Disclosure Statement (PDS)
	etsi-psd2-qcStatement	M	N	PSD2QcType ::= SEQUENCE { rolesOfPSP RolesOfPSP, nCAName NCAName, nCAId NCAId }

1) Mandatory or Optional field2) Basic, Critical or Non-Critical extensions

1.4 Buypass SSL Business 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	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 3 CA 2 O= Buypass AS-983163327 C=NO	M	B		
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 398 days	
Subject	C=<country>	M	B	According to an authoritative source	
	O=<Subscriber Name>	M	B	According to an authoritative source	
	OU=<Subscriber Department>	O	B		
	CN=<Domain name>	M	B	Fully qualified domain name	
	SerialNumber		M	B	Organization number according to an authoritative source
	LocalityName= <City or town - postal area> PostalCode= <postal code>		M	B	Physical location of Subscriber place of Business
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		

Field	Value	1)	2)	Comment
Certificate Policies	Policy OID= 2.16.578.1.26.1.3.4 Policy OID = 2.23.140.1.2.2	M	N	Buypass SSL Business Plus OID CABF BR OV OID
CRL Distribution Point	URL = http://crl.buypass.no/crl/BPClass3CA2.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/BPClass3CA2.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
Key Usage	Digital Signature, Key Encipherment (0xA0)	M	C	RSA key
	Digital Signature (0x80)	M	C	ECDSA keys
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 Extension	(OID=1.3.5.1.4.1.11129.2.4.3)	M	C	Poison Extension, Precertificate only

1) Mandatory or Optional field2) Basic, Critical or Non-Critical extensions

1.5 CRL profile

Buypass Class 3 CA 3 and Buypass Class 3 CA 2:

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 3 CA <ca id> O= Buypass AS-983163327 C=NO	M	B	<ca id> is 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 non-expired revoked certificates	O	B	

Buypass Class 3 CA G2 HT Person, Buypass Class 3 CA G2 HT Business, Buypass Class 3 CA G2 ST Business and Buypass Class 3 CA G2 QC WA:

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 3 CA G2 <ca id> O = Buypass AS	M	B	<ca id> is 'HT Person', 'HT Business', 'ST Business' or 'QC WA'.

Field	Value	1)	2)	Comment
	OrganizationIdentifier = NTRNO-983163327 C = NO			
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
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 Bypass Class 3 CA certificate profile

2.1.1 Root CA certificate

Bypass Class 3 CA Root CA:

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 3 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 3 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	

Bypass Class 3 Root CA G2 HT, Bypass Class 3 Root CA G2 ST and Bypass Class 3 Root CA G2 QC:

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	Sha512WithRSAEncryption	M	B	Sha512WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 }
Issuer	CN = Buypass Class 3 Root CA G2 <ca id> O = Buypass AS	M	B	<ca id> is 'HT', 'ST' or 'QC'.

Field	Value	1)	2)	Comment
	OrganizationIdentifier = NTRNO-983163327 C = NO			
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 25 years
Subject	CN = Buypass Class 3 Root CA G2 <ca id> O = Buypass AS OrganizationIdentifier = NTRNO-983163327 C = NO	M	B	<ca id> is 'HT', 'ST' or 'QC'.
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	
Qualified Certificate Statement	id-qcs-pkixQCSyntax-v2 id-etsi-qcs-SemanticsId-Legal	M	N	

2.1.2 Intermediate CA certificates

Buypass Class 3 CA 3 and Buypass Class 3 CA 2:

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 3 Root CA O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 20 years
Subject	CN=Buypass Class 3 CA <ca id> O= Buypass AS-983163327 C=NO	M	B	<ca id> is 2 or 3
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 3 CA 2 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 3 CA 2 only

Buypass Class 3 CA G2 HT Person and Buypass Class 3 CA G2 HT Business:

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	Sha512WithRSAEncryption	M	B	Sha512WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 }
Issuer	CN = Buypass Class 3 Root CA G2 HT O = Buypass AS OrganizationIdentifier = NTRNO-983163327 C = NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 20 years
Subject	CN = Buypass Class 3 CA G2 HT <ca id> O = Buypass AS OrganizationIdentifier = NTRNO-983163327 C = NO	M	B	<ca id> is 'Person' or 'Business'
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	
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	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.buypassca.com/BPCI3RootCaG2HT.crl	M	N	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://crt.buypassca.com/BPCI3RootCaG2HT.cer	M	N	
Key Usage	Certificate Signing, CRL Signing (0x06)	M	C	
Qualified Certificate Statement	id-qcs-pkixQCSyntax-v2 id-etsi-qcs-SemanticsId-Legal	M	N	

Buypass Class 3 CA G2 ST Business:

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	Sha512WithRSAEncryption	M	B	Sha512WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 }
Issuer	CN = Buypass Class 3 Root CA G2 ST O = Buypass AS OrganizationIdentifier = NTRNO-983163327 C = NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 20 years
Subject	CN = Buypass Class 3 CA G2 ST Business O = Buypass AS OrganizationIdentifier = NTRNO-983163327 C = NO	M	B	

Field	Value	1)	2)	Comment
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	
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	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.buypassca.com/BPCI3RootCaG2ST.crl	M	N	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://crl.buypassca.com/BPCI3RootCaG2ST.cer	M	N	
Key Usage	Certificate Signing, CRL Signing (0x06)	M	C	
Qualified Certificate Statement	id-qcs-pkixQCSyntax-v2 id-etsi-qcs-SemanticsId-Legal	M	N	

Buypass Class 3 CA G2 QC WA:

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	Sha512WithRSAEncryption	M	B	Sha512WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 }
Issuer	CN = Buypass Class 3 Root CA G2 QC O = Buypass AS OrganizationIdentifier = NTRNO-983163327 C = NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 20 years
Subject	CN = Buypass Class 3 CA G2 QC WA O = Buypass AS OrganizationIdentifier = NTRNO-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	
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	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.buypassca.com/BPCI3RootCaG2QC.crl	M	N	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	M	N	

Field	Value	1)	2)	Comment
	Alternative Name: URL= http://crt.bypassca.com/BPCI3RootCaG2QC.cer			
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	
Qualified Certificate Statement	id-qcs-pkixQCSyntax-v2 id-etsi-qcs-SemanticsId-Legal	M	N	

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

2.2 CRL profile

Buypass Class 3 Root CA:

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 3 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	

Buypass Class 3 Root CA G2 HT, Buypass Class 3 Root CA G2 ST and Buypass Class 3 Root CA G2 QC:

Field	Value	1)	2)	Comment
Version	X509 version 2 CRL	M	B	
Signature Algorithm	Sha512WithRSAEncryption	M	B	Sha512WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 }
Issuer	CN = Buypass Class 3 Root CA G2 <ca id> O = Buypass AS OrganizationIdentifier = NTRNO-983163327 C = NO	M	B	<ca id> is 'HT', 'ST' or 'QC'.
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
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 3 Root CA: <http://crl.buypass.no/crl/BPClass3RootCA.crl>

Buypass Class 3 CA 2: <http://crl.buypass.no/crl/BPClass3CA2.crl>

Buypass Class 3 CA 3: <http://crl.buypass.no/crl/BPClass3CA3.crl>

Buypass Class 3 Root CA G2 HT: <http://crl.buypassca.com/BPCI3RootCaG2HT.crl>

Buypass Class 3 CA G2 HT Person: <http://crl.buypassca.com/BPCI3CaG2HTPS.crl>

Buypass Class 3 CA G2 HT Business: <http://crl.buypassca.com/BPCI3CaG2HTBS.crl>

Buypass Class 3 Root CA G2 ST: <http://crl.buypassca.com/BPCI3RootCaG2ST.crl>

Buypass Class 3 CA ST Business: <http://crl.buypassca.com/BPCI3CaG2STBS.crl>

Buypass Class 3 Root CA G2 QC: <http://crl.buypassca.com/BPCI3RootCaG2QC.crl>

Buypass Class 3 CA QC WS: <http://crl.buypassca.com/BPCI3CaG2QCWA.crl>

3.2 OCSP

Buypass Class 3 Root CA and Buypass Class 3 CA 2:

- <http://ocsp.buypass.com>

Buypass Class 3 CA 3:

- <http://ocsp.buypass.no/ocsp/BPClass3CA3> – for certificates according to National legislation
- <http://ocspec.buypass.com>

Buypass Class 3 CA G2 HT Person:

- <http://ocspbs.buypassca.com>

Buypass Class 3 CA G2 HT Business and Buypass Class 3 CA ST Business:

- <http://ocspbs.buypassca.com>

Buypass Class 3 CA QC WS:

- <http://ocspwa.buypassca.com>