

BUYPASS CLASS 3 CERTIFICATES



PUBLIC

Version: 10.0
Document date: 05.03.2019

History of changes

Version	Date	Status	Description
1.0	06.05.2005	Approved	Initial version
1.1	06.06.2006	Approved	New chapter : 1.2 Bypass Class 3 Enterprise certificate profile
1.2	07.03.2008	Approved	New chapter: 1.3 Bypass Class 3 SSL EV certificate profile
1.2.1	05.04.2008	Approved	Updated chapter 1.3 and added new chapter 1.4 Bypass Class 3 SSL certificate profile
1.2.2	20.08.2008	Approved	Updated chapter 1.4
1.2.3	26.10.2009	Approved	Changed OCSP URL for SSL from https to http
1.2.4	17.11.2009	Approved	Changed name of the document
1.2.5	01.03.2010	Approved	Added DNS name to Subject Alternative Names for the SSL certificate profiles
1.2.6	09.06.2010	Approved	Changed encoding of Business Categories according to ballot 43 CABForum
1.3	18.10.2010	Approved	Changes due to new CA structure, support for SHA256 and longer keys
1.4	22.02.2011	Approved	Changed URLs for CA1
1.5	01.07.2012	Approved	Included support for BR and changes in CA structure
2.0	01.12.2012	Approved	Changes related to new CA-structure
3.0	11.06.2013	Approved	Included Enterprise certificates provided as hard tokens
4.0	28.04.2014	Approved	Maximum lifetime of Qualified Certificates changed from 3 years to 5 years
5.0	09.09.2014	Approved	Product name Bypass Business SSL Certificates changed name to Bypass Business Plus SSL Certificates
6.0	05.01.2015	Approved	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	Approved	Lifetime of Bypass Enterprise Certificates changed from <= 38 months to <= 42 months due to expanded renewal period.
8.0	11.01.2016	New version	Added CABF EV OID in EV Certificates.
9.0	15.03.2018	New version	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	New version	Included EKU, and Key Usage for Enterprise certificates where subscriber generates private key

Table of content

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)	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
1.3	Buypass SSL Evident certificate profile	8
1.3.1	Certificate profile according to CA/Browser Forum EV Guidelines	8
1.3.2	Certificate profile according to Regulation (EU) No 910/2014 (eIDAS)	10
1.4	Buypass SSL Business Plus certificate profile	11
1.5	CRL profile	13
2	Certificate and CRL profiles for CA certificates	13
2.1	Buypass Class 3 CA certificate profile	13
2.1.1	Root CA certificate	13
2.1.2	Intermediate CA certificates	14
2.2	CRL profile	15
3	Revocation status information	15
3.1	CRL	15
3.2	OCSP	15

1 Certificate and CRL profiles for Subscriber certificates

1.1 Bypass 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	CN=Buypass Class 3 CA 3 O= Buypass AS-983163327 C=NO	M	B	
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 2.16.578.1.26.1.3.6	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%203%20CA%203?certificateRevocationList URL = http://crl.buypass.no/crl/BPClass3CA3.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/BPClass3CA3 [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	M	N	
Key Usage	Digital Signature, Key Encipherment, Data Encipherment, Key Agreement (0xB8)	M	C	Certificate 1
	Non-Repudiation (0x40)	M	C	Certificate 2

Field	Value	1)	2)	Comment
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	
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 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
Issuer	CN=Buypass Class 3 CA 3 O= Buypass AS-983163327 C=NO	M	B	
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 2.16.578.1.26.1.3.6	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%203%20CA%203?certificateRevocationList URL = http://crl.buypass.no/crl/BPClass3CA3.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/BPClass3CA3 [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	M	N	

Field	Value	1)	2)	Comment
Key Usage	Digital Signature, Key Encipherment (0xA0)	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	
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.bypass.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

1.2 Bypass 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	CN=Bypass Class 3 CA 3 O= Bypass AS-983163327 C=NO	M	B	
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=Organization number	M	B	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	

Field	Value	1)	2)	Comment
CRL Distribution Point	URL=ldap://ldap.bypass.no/dc=Buypass,dc=NO,CN=Buypass%20Class%203%20CA%203?certificateRevocationList URL = http://crl.bypass.no/crl/BPClass3CA3.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.bypass.no/ocsp/BPClass3CA3 [2]Authority Info Access Access Method= Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL = http://crl.bypass.no/crt/BPClass3CA3.cer	M	N	
Key Usage	Digital Signature, Key Encipherment, Data Encipherment (0xB0)	M	C	CA generated Private Keys, Certificate 1
	Non-Repudiation (0x40)	M	C	CA generated Private Keys, Certificate 2
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, (0xE0)	M	C	Subscriber generated Private Key
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
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)

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 3 O= Buypass AS-983163327 C=NO	M	B	
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	According to an authoritative source
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	

Field	Value	1)	2)	Comment
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	URL=ldap://ldap.bypass.no/dc=Buypass,dc=NO,CN=Buypass%20Class%203%20CA%203?certificateRevocationList URL = http://crl.bypass.no/crl/BPClass3CA3.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://ocspec.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/BPClass3CA3.cer	M	N	
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
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment, (0xE0)	M	C	Subscriber generated Private Key
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
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) Mandatory or Optional field
 2) Basic, Critical or Non-Critical extensions

1.3 Bypass 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)

Field	Value	1)	2)	Comment
				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 <= 825 days
Subject	C=<country>	M	B	According to QGR
	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	Domain name owned or controlled by Subscriber. Wild card not allowed.
	SerialNumber=Organization number	M	B	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
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.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://crl.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	
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 Extention	(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 <= 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 QGR
	OU=<Subscriber Department>	O	B	
	CN=<Domain name>	M	B	Domain name owned or controlled by Subscriber. Wild card not allowed.
	SerialNumber=Organization number	M	B	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
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= 2.16.578.1.26.1.3.3 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.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 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 Extention	(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)

- 1) Mandatory or Optional field
 2) 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	M	B	

Field	Value	1)	2)	Comment
	C=NO			
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 825 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 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= 2.16.578.1.26.1.3.4 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	
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 Extensioin	(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

1.5 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 3 CA <ca no> O= Buypass AS-983163327 C=NO	M	B	<ca no> 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	

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 Buypass Class 3 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 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	

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	
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 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 no> O= Buypass AS-983163327 C=NO	M	B	<ca no> 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	

- 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 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	

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>

3.2 OCSP

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

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

Buypass Class 3 CA 3:

- <http://ocsp.buypass.no/ocsp/BPClass3CA3>
- <http://ocspec.buypass.com> – for Qualified Enterprise certificates according to Regulation (EU) No 910/2014 (eIDAS)