

BUYPASS CLASS 2 CERTIFICATES



PUBLIC

Version: 7.0
Document date: 15.03.2018

History of changes

Version	Date	Status	Description
0.8	24.08.2006	Draft	Draft based on Bypass Class 3 doc
1.0	20.08.2008	Approved	New chapter: 1.3 Bypass Class 2 SSL certificate profile
1.0.1	26.10.2009	Approved	Changed ocsf URLs for SSL from https to http
1.0.2	17.11.2009	Approved	Changed name of the document
1.0.3	01.03.2010	Approved	Added DNS name to Subject Alternative Names for the SSL certificate profile
1.0.4	09.06.2010	Approved	Introducing 2 SSL certificate profiles; Domain and Domain Plus. The latter is the same as the original SSL certificate profile
1.1	18.10.2010	Approved	Introducing Merchant certificates and changes due to new CA structure, support for SHA256 and longer keys
1.2	22.02.2011	Approved	Including wildcard and support for Exchange. Changed URLs for CA1
1.3	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	28.04.2014	Approved	Maximum lifetime of Merchant Certificates changed from 3 years to 5 years
4.0	09.09.2014	Approved	Product name Bypass Domain Plus SSL Certificates changed name to Bypass Business SSL Certificates
5.0	08.01.2015	New version	EBR (European Business Register) included for SSL Certificates. RSA 1024 bits removed for all Certificates.
6.0	11.01.2016	New version	Removed option for internal domain names and/or server names in SSL Business.
7.0	15.03.2018	New version	Removed profiles for certificates not chaining to Class 2 Root CA. Removed SHA-1 and CA1. Added profile for Go SSL. Reduced validity period. Added certificate and CRL profiles for CA certificates. Added revocation status information.

Table of content

1	Certificate and CRL profiles for Subscriber certificates	4
1.1	Buypass SSL Business certificate profile	4
1.2	Buypass SSL Domain certificate profile	5
1.3	Buypass Go SSL certificate profile	6
1.4	CRL profile.....	7
2	Certificate and CRL profiles for CA certificates	8
2.1	Buypass Class 2 CA certificate profile	8
2.1.1	Root CA certificate	8
2.1.2	Intermediate CA certificates.....	8
2.2	CRL profile.....	9
3	Revocation status information.....	10
3.1	CRL.....	10
3.2	OCSP.....	10

1 Certificate and CRL profiles for Subscriber certificates

1.1 Bypass 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=Bypass Class 2 CA 2 O= Bypass 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	Bypass SSL Business OID CABF BR OV OID
CRL Distribution Point	URL = http://crl.bypass.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.bypass.no/ocsp/BPOcsp before December 2016 and URL = http://ocsp.bypass.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.bypass.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 Extention	(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 Bypass 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=Bypass Class 2 CA 2 O= Bypass 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	Bypass SSL Domain OID CABF BR DV OID
CRL Distribution Point	URL = http://crl.bypass.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.bypass.no/ocsp/BPOcsp before December 2016 and URL = http://ocsp.bypass.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.bypass.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
<i>Poison Extention</i>	(OID=1.3.5.1.4.1.11129.2.4.3)	M	C	<i>Poison Extension, Precertificate only</i>

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

1.3 Bypass 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.bypass.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.bypass.com [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/crl/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 Extention	(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 Bypass 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=Bypass Class 2 Root CA O= Bypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 30 years
Subject	CN=Bypass Class 2 Root CA O= Bypass 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=Bypass Class 2 Root CA O= Bypass 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=Bypass Class 2 CA <ca no> O= Bypass 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 Bypass Class 3 CA 2 and Bypass Class 3 CA 5 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=Bypass Class 2 Root CA O= Bypass 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