CERTIFICATE AND CRL PROFILES

Buypass Class 3 Certificates

PUBLIC

Version: 1.2.3
Document date: 26.10.2009

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

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 Buypass Class 3 Enterprise certificate profile
1.2	07.03.2008	Approved	New chapter: 1.3 Buypass Class 3 SSL EV certificate profile
1.2.1	05.04.2008	Approved	Updated chapter 1.3 and added new chapter 1.4 Buypass 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

Table of content

1 Certificate and CRL profiles 4
1.1 Buypass Class 3 certificate profile 4
1.2 Buypass Class 3 Enterprise certificate profile 5
1.3 Buypass Class 3 SSL EV certificate profile 6
1.4 Buypass Class 3 SSL certificate profile 7
1.5 CRL profile 8

1 Certificate and CRL profiles

1.1 Buypass Class 3 certificate profile

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	sha-1WithRSAEncryption	M	B	sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
Issuer	CN=Buypass Class 3 CA 1 O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 3 years
Subject	C=NO	M	B	
	O=<Subscriber Name>-<Subscriber Id>	O	B	Subscriber 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 (min.1024 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	M	N	
Subject Alternative Name	RFC822Name=<Subject email address> Other Name: Principal Name=<UPN>	O	N	Subject emailaddress User Principal Name
CRL Distribution Point	URL=ldap://ldap.prod.buypass.no/dc=Buypass,dc=NO,CN=Buypass%20Class%203%20CA%201?certificateRevocationList URL=http://crl.prod.buypass.no/crl/BPClass3CA1.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=https://ocsp.prod.buypass.no/BPClass23	M	N	
Key Usage	Digital Signature, Key Encipherment, Data Encipherment, Key Agreement (0xB8)	M	C	Certificate 1

Field	Value	1)	2)	Comment
	Non-Repudiation (0x40)	M	C	Certificate 2
Extended Key Usage		O	N	
Card Number	Reference to smartcard	O	N	id-seis-pe-cn OID: 1.2.752.34.2.1
Qualified Certificate Statement	esi4-qcStatement-1	M	N	
Thumbprint algorithm	sha1	M		
Thumbprint		M		

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

1.2 Buypass Class 3 Enterprise certificate profile

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	sha-1WithRSAEncryption	M	B	sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
Issuer	CN=Buypass Class 3 CA 1 O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <= 3 years
Subject	C=NO	M	B	
	O=<Subscriber Name>	M	B	According to 'Enhetsregisteret'
	OU=<Subscriber Department>	O	B	
	CN=<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 (min.1024 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	Policy OID= 2.16.578.1.26.1.3.2	M	N	

Field	Value	1)	2)	Comment
Policies				
Subject Alternative Name	RFC822Name=<Subject email address> Other Name: Principal Name=<UPN>	O	N	Subject emailaddress Subject Principal Name
CRL Distribution Point	URL=ldap://ldap.prod.buypass.no/dc=Buypass,dc=NO,CN=Buypass%20Class%203%20CA%201?certificateRevocationList URL=http://crl.prod.buypass.no/crl/BPClass3CA1.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=https://ocsp.prod.buypass.no/BPClass23	M	N	
Key Usage	Digital Signature, Key Encipherment, Data Encipherment (0xB0)	M	C	Certificate 1
	Non-Repudiation (0x40)	M	C	Certificate 2
Extended Key Usage		O	N	
Thumbprint algorithm	sha1	M		
Thumbprint		M		

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

1.3 Buypass Class 3 SSL EV certificate profile

Field	Value	1)	2)	Comment
Version	X509 version 3 certificates	M	B	
Serial number	Unique certificate serial number	M	B	
Signature Algorithm	sha-1WithRSAEncryption	M	B	sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
Issuer	CN=Buypass Class 3 CA 1 O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate=1 year
Subject	C=NO	M	B	
	jurisdictionOfIncorporation CountryName=NO	M	B	OBJECT IDENTIFIER ::= 1.3.6.1.4.1.311.60.2.1.3
	O=<Subscriber Name>	M	B	According to 'Enhetsregisteret'
	OU=<Subscriber Department>	O	B	
	CN=<Domain name>	M	B	Domain name owned or controlled by the Subject. Wild card not allowed.
	SerialNumber=Organization number	M	B	According to 'Enhetsregisteret'.

Field	Value	1)	2)	Comment
	BusinessCategory=[“V1.0, Clause 5.(b)” | “V1.0, Clause 5.(c)” | “V1.0, Clause 5.(d)”]	M	B	Type of Subject: b => Private Organisation c => Government Entity d => Business Entity (N/A)
	LocalityName= <City or town – postal area>	M	B	Physical location of Subjects place of Business
	PostalCode= <postal code>	M	B	
Subject Public Key Info	Subject Public Key	M	B	RSA (min.1024 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= 2.16.578.1.26.1.3.3	M	N	BP Class 3 CA SSL EV OID
	Policy Qualifier ID = id-qt 1 [RFC 3280]	M	N	Reference to CPS
	Policy Qualifer = <URI to CPS>	M	N	
CRL Distribution Point	URL=http://crl.prod.buypass.no/crl/BPClass3CA1.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.prod.buypass.no/BPClass23	M	N	
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	
Thumbprint algorithm	sha1	M		
Thumbprint		M		

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

1.4 Buypass Class 3 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	sha-1WithRSAEncryption	M	B	sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)

Field	Value	1)	2)	Comment
				5 }
Issuer	CN=Buypass Class 3 CA 1 O= Buypass AS-983163327 C=NO	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Lifetime of certificate <=3 years
Subject	C=NO	M	B	
	O=<Subscriber Name>	M	B	According to 'Enhetsregisteret'
	OU=<Subscriber Department>	O	B	
	CN=<Domain name>	M	B	Domain name owned or controlled by the Subject.
	SerialNumber=Organization number	M	B	According to 'Enhetsregisteret'.
Subject Public Key Info	Subject Public Key	M	B	RSA (min.1024 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	M	N	BP Class 3 CA SSL OID
CRL Distribution Point	URL=http://crl.prod.buypass.no/crl/BPClass3CA1.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.prod.buypass.no/BPClass23	M	N	
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	
Thumbprint algorithm	sha1	M		
Thumbprint		M		

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

1.5 CRL profile

Field	Value	1)	2)	Comment
Version	X509 version 2 CRL	M	B	
Signature Algorithm	sha-1WithRSAEncryption	M	B	sha-1WithRSAEncryption OBJECT IDENTIFIER ::=

Field	Value	1)	2)	Comment
				{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
Issuer	CN=Buypass Class 3 CA 1 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 revoked certificates	O	B	Present if any certificates are currently revoked

Each entry in the RevokedCertificates list has the following content:

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