Version: 1.0
Document date: 25.09.2023

PUBLIC

Certificate and CRL Profiles

Buypass Class 3 BCSS Certificates

HISTORY OF CHANGES

Version	Date	Description
1.0	2023-10-01	First version.

TABLE OF CONTENTS

1 Certificate and CRL profiles for Subscriber certificates

1.1 Buypass Class 3 Person BCSS certificates

The certificate profiles in this section are for the BCSS certificates where the certificate is issued to a natural person which has been authenticated by using an already issued eID means. The certificate attributes in the Subject field are retrieved from identity attributes from the eID means and may be different across different eID means.

The certificate attributes in the Subject field are defined in section 1.1.3.

1.1.1 Certificate profile for short-term signing certificates

This profile is used for short-term non-qualified certificates issued to natural persons 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	Buypass Class 3 CA G2 HT Person BCSS	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Validity of the certificate <= 8 hours
Subject	*See section 1.1.3 below.*	*M*	*B*	
Subject Public Key Info	Subject Public Key	M	B	ECDSA using NIST P-256
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	M	N	
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 = 2.16.578.1.26.1.3.8	M	N	Buypass CP OID for BCSS
	Policy OID = 0.4.0.2042.1.2	M	N	ETSI OID NCP+
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/BPCl3CaG2HTPSBCSS.cer	M	N	CA certificate
Key Usage	Non-Repudiation (0x40)	M	C	
Short-term certificate	ext-etsi-valassured-ST-certs= 0.4.0.194121.2.1	M	N	ETSI extension indicating the validity of the certificate is assured because the certificate is a "short-term certificate".
eID means reference	2.16.578.1.26.2.2 + eIDMeansType + eIDMeansValue	M	N	Buypass extension with eID means reference: urn:no:buypass:cert:serial_number:<cert.serial.no>
Qualified Certificate Statements	qcStatement-2 id-etsi-qcs-semanticsId-Natural nameRegistrationAuthoritites {id-etsi-qcs-semanticsId-Legal }	M	N	Semantic Identifiers. The legal person identifier is only included if Subject.OrganizationIdentifier is present.

1.1.2 Certificate profile for qualified short-term signing certificates

This profile is used for short-term qualified certificates issued to natural persons 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	Buypass Class 3 CA G2 HT Person BCSS	M	B	
Validity	notBefore<time> notAfter<time>	M	B	Validity of the certificate <= 8 hours
Subject	*See section 1.1.3 below.*	*M*	*B*	
Subject Public Key Info	Subject Public Key	M	B	ECDSA using NIST P-256
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	M	N	
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 = 2.16.578.1.26.1.3.8	M	N	Buypass CP OID for BCSS
	Policy OID = 0.4.0.194112.1.2	M	N	ETSI OID QCP-n-qscd
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/BPCl3CaG2HTPSBCSS.cer	M	N	CA certificate
Key Usage	Non-Repudiation (0x40)	M	C	
Short-term certificate	ext-etsi-valassured-ST-certs= 0.4.0.194121.2.1	M	N	ETSI extension indicating the validity of the certificate is assured because the certificate is a "short-term certificate".
eID means reference	2.16.578.1.26.2.2 + eIDMeansType + eIDMeansValue	M	N	Buypass extension with eID means reference: urn:no:buypass:cert:serial_number:<cert.serial.no>
Qualified Certificate Statements	qcStatement-2 id-etsi-qcs-semanticsId-Natural nameRegistrationAuthoritites {id-etsi-qcs-semanticsId-Legal}	M	N	Semantic Identifiers. The legal person identifier is only included if Subject.OrganizationIdentifier is present.
	esi4-qcStatement-1	M	N	EU Qualified Certificate (QC)
	esi4-qcStatement-4	M	N	The private key resides in a QSCD
	esi4-qcStatement-6 id-etsi-qct-esign	M	N	EU QC for electronic signature
	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 Certificate attributes for Subject field based on eID means

1.1.3.1 Buypass ID in mobile and Buypass ID on smartcard

These attributes are extracted from the certificates used in the eID means.

Field	Value	1)	2)	Comment
Subject	C=NO	M	B	
	SerialNumber=UN:NO-9578-4050-<BuypassId>	M	B	<BuypassId>: unique Buypass identifier for Subject
	Surname	M	B	LastName according to FREG
	GivenName	M	B	FirstName + MiddleName according to FREG
	CommonName	M	B	Subject preferred name

1.1.3.2 Buypass ID FIDO2

These attributes are extracted from identity attributes from tokens retrieved when using the eID means.

Field	Value	1)	2)	Comment
Subject	C=NO	M	B	
	SerialNumber=BP:NO-578-0001-Base64Enc(<uniqueIdentifier>)	M	B	Unique identifier = sha256(FNR/DNR)
	Surname	M	B	LastName according to FREG
	GivenName	M	B	FirstName + MiddleName according to FREG
	CommonName	M	B	Subject preferred name

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

1.2 CRL profile

Buypass Class 3 CA G2 HT Person BCSS

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 HT Person BCSS
	O = Buypass AS
	OrganizationIdentifier = NTRNO-983163327
	C = NO
		M	B	

This Update	UTCTime	M	B	Time of CRL generation
Next Update	UTCTime	M	B	Latest time the next CRL will be 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 certificates profile

2.1.1 Root CA certificate

Buypass Class 3 Root CA G2 HT:

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	Validity of the certificate <= 25 years

Subject	CN = Buypass Class 3 Root CA G2 HT
	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	N	
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 G2 HT Person BCSS:

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	Validity of the certificate <= 20 years

Subject	CN = Buypass Class 3 CA G2 HT Person BCSS
	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

Field	Value	1)	2)	Comment
Basic Constraints	Subject Type=CA Path Length Constraint=None	M	N	
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/BPCl3RootCaG2HT.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/BPCl3RootCaG2HT.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	

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

2.2 CRL profile

Buypass Class 3 Root CA G2 HT:

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 HT
	O = Buypass AS
	OrganizationIdentifier = NTRNO-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 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 G2 HT: http://crl.buypassca.com/BPCl3RootCaG2HT.crl
Buypass Class 3 CA G2 HT Person BCSS: http://crl.buypassca.com/BPCl3CaG2HTPSBCSS.crl