End Entity Certificate Templates

⚠ **C0 Public Document**
Nexus property.

Identification of the document		
No pages: 11	**State:** Final	**Reference:** LoA-End-Cert-Template
Creation date: 5/7/2024	**Last updated:** 12/11/2025	**Version:** 1.2

Version history			
Version	**Author**	**Date**	**What changes were made, where**
V1	Rubina Akram, Christian Dahlberg	2024-05-07	Initial Draft
V1.1	Christian Dahlberg	2024-06-17	Adjusted naming convention customer issuing CA Official Version
V1.2	Linh Pham	2025-12-11	Minor change in CA naming convention
		Click or tap to enter a date.	
		Click or tap to enter a date.	
		Click or tap to enter a date.	

Table of Contents

1 End Entity Person Certificates

1.1 Authentication certificate

Field	Value	Comments	Source
Version	V3		CA
Serial Number	Unique number		CA
Issuer Signature Algorithm	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)		CA
Issuer Distinguished Name	Unique X.500 CA DN. CN = SEE RIGHT -> O = [Customer_Org] C = [Customer_Country]	CN=[Customer] Issuing CA G[N]* [Customer] Employee Issuing CA G[N]**	CA
Validity Period	Up to 60 months expressed in UTC format		Certificate Management System based on CA templates
Subject Distinguished Name			
SerialNumber	Subject:serialNumber (2.5.4.5)	This field MUST contain the Subject's full Swedish social security number (or equal) Social Security Number will be given in the following format: YYYYMMDDXXXX	From customer but must comply with SPAR
Given Name	subject:givenName (2.5.4.42)	This field MUST contain the Subject's marked Given Name IF it exists OR All Given Names of the subject if marking of Given Name is absent and First Names exists This field is empty if Given Name and First Names are absent	From customer but must comply with SPAR
Sur Name	subject: surname (2.5.4.4)	This field MUST contain all of the Subject's surnames.	From customer but must comply with SPAR
Common Name	subject:commonName (2.5.4.3) cn = Common name	This field MUST contain the Subject's common name.	Combination of Given Name and Surname
Organization	subject:organizationName (2.5.4.10)	This field MUST contain the Subject's full legal organization name as listed in the official records.	Companies Registration Office and Central Bureau of Statistics
OrganizationIdentifier	subject:organizationIdentifier	This field MUST contain the Subject's full legal organization number as listed in the official records in the following format: XXXXXXXXXX.	Companies Registration Office and Central Bureau of Statistics
Country	subject:countryName (2.5.4.6)	This field MUST contain the country code for the Subject's organization as listed in the official records. In ISO3166 format	Companies Registration Office and Central Bureau of Statistics

Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)		CA
Issuer's Signature	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)		CA
Extension	**Value**		
Authority Key Identifier	Octet String – Same as Issuer's subject key identifier	Contains 20 byte SHA-2 hash of the CA Public Key	CA
Subject Key Identifier	Octet String – Calculated by CA from public key in PKCS#10	Contains 20 byte SHA-2 hash of the subjectPublicKey in this certificate	CA
1.2.752.34.2.1 Card Number Extension	10 digits	This field MUST contain 10 digits.	Identity Management System
Key Usage	Critical=TRUE; Digital Signature, Key Encipherment (a0)	Critical	CA
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2), Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	This field MUST contain Client Authentication AND contain the smartCardLogon.	Certificate Management System based on CA templates
1.3.6.1.4.1.311.25.2	Octetstring (max 28)	IF present this field contain the Subject SID (Security Identifier) from customers active directory.	Customers Active directory
Certificate Policies	[1]Certificate Policy: Policy Identifier= SEE RIGHT-> : https://pki.nexusgroup.com	[Customer] Issuing CA G[n] - OID 1.2.752.274.1.1.3 [Customer] Employee Issuing CA G[n]	Certificate Management System based on CA templates
Subject Alternative Name	UPN = XXXXXXXXXXX@[customer].xx OR Not present	IF present this field CAN contain The Subject's User Principal Name formatted as the subject's e-mail address	Certificate Management System based on CA templates
CRL Distribution Point	CRL HTTP URL = SEE RIGHT -> (2.5.29.31)	http://dp.eid.prod.go.nexusgroup.com/crl/customer-issuing-ca-g1.crl OR http://dp.prod.go.nexusgroup.com/crl/customer-client-issuing-ca-g1.crl	CA
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.go.nexusgroup.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= SEE RIGHT->	http://dp.eid.prod.go.nexusgroup.com/aia/customer-issuing-ca-g1.cer OR http://dp.prod.go.nexusgroup.com/aia/customer-client-issuing-ca-g1.cer	CA

*CA for LoA3 qualified certificates
**CA for non-qualified certificates
G[n] denotes the Generation number (e.g., G1, G[N], G3, etc.). This designation is used to illustrate the evolution or versioning of the PKI chain over time.

1.2 Signing certificate

Field	Value	Comments	Source
Version	V3		CA
Serial Number	Unique number		CA
Issuer Signature Algorithm	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)		CA
Issuer Distinguished Name	Unique X.500 CA DN. CN = SEE RIGHT -> O = [Customer_Org] C = [Customer_Country]	CN=[Customer] Issuing CA G[n]* [Customer] Employee Issuing CA G[n]*	CA
Validity Period	Up to 60 months expressed in UTC format		Certificate Management System based on CA templates
Subject Distinguished Name			
Given Name	subject:givenName (2.5.4.42)	This field MUST contain the Subject's marked Given Name IF it exists OR All Given Names of the subject if marking of Given Name is absent and First Names exists This field is empty if Given Name and First Names are absent	From customer but must comply with SPAR
Sur Name	subject: surname (2.5.4.4)	This field MUST contain all of the Subject's surnames.	From customer but must comply with SPAR
Common Name	subject:commonName (2.5.4.3) cn = Common name	This field MUST contain the Subject's common name.	Combination of Given Name and Surname
Organization	subject:organizationName (2.5.4.10)	This field MUST contain the Subject's full legal organization name as listed in the official records.	Companies Registration Office and Central Bureau of Statistics
OrganizationIdentifier	subject:organizationIdentifier	This field MUST contain the Subject's full legal organization number as listed in the official records in the following format: XXXXXX-XXXX.	Companies Registration Office and Central Bureau of Statistics
Country	subject:countryName (2.5.4.6)	This field MUST contain the country code for the Subject's organization as listed in the official records. In ISO3166 format	Companies Registration Office and Central Bureau of Statistics
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)		CA
Issuer's Signature	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)		CA
Extension	**Value**		
Authority Key Identifier	Octet String – Same as Issuer's subject key identifier	Contains 20 byte SHA-2 hash of the CA Public Key	CA
Subject Key Identifier	Octet String – Calculated by CA from public key in PKCS#10	Contains 20 byte SHA-2 hash of the subjectPublicKey in this certificate	CA

1.2.752.34.2.1 Card Number Extension	10 digits	This field MUST contain 10 digits.	Identity Management System
Key Usage	critical=TRUE; nonRepudiation (40)	Critical	CA
Extended Key Usage	Document Signing (1.3.6.1.4.1.311.10.3.12)	This field MUST contain Document Signing	CA
Certificate Policies	[1]Certificate Policy: Policy Identifier= SEE RIGHT-> : https://pki.nexusgroup.com	[Customer] Issuing CA G[n] - OID 1.2.752.274.1.1.3 [Customer] Employee Issuing CA G[n]	Certificate Management System based on CA templates
CRL Distribution Point	CRL HTTP URL = SEE RIGHT -> (2.5.29.31)	http://dp.eid.prod.go.nexusgroup.com/crl/customer-issuing-ca-g1.crl OR http://dp.prod.go.nexusgroup.com/crl/customer-client-issuing-ca-g1.crl	CA
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.go.nexusgroup.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= SEE RIGHT->	http://dp.eid.prod.go.nexusgroup.com/aia/customer-issuing-ca-g1.cer OR http://dp.prod.go.nexusgroup.com/aia/customer-client-issuing-ca-g1.cer	CA

*CA for LoA3 qualified certificates
**CA for non-qualified certificates

2 End Entity Mobile ID Certificates

2.1 Authentication certificate

Field	Value	Comments	Source
Version	V3		CA
Serial Number	Unique number		CA
Issuer Signature Algorithm	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)		CA
Issuer Distinguished Name	Unique X.500 CA DN. CN = SEE RIGHT -> O = [Customer_Org] C = [Customer_Country]	CN=[Customer] Issuing CA G[n]* [Customer] Employee Issuing CA G[n]**	CA
Validity Period	Up to 24 months expressed in UTC format		Certificate Management System based on CA templates
Subject Distinguished Name			
SerialNumber	Subject:serialNumber (2.5.4.5)	This field MUST contain the Subject's full Swedish social security number (or equal) Social Security Number will be given in the following format: YYYYMMDDXXXX	From customer but must comply with SPAR
Given Name	subject:givenName (2.5.4.42)	This field MUST contain the Subject's marked Given Name IF it exists OR All Given Names of the subject if marking of Given Name is absent and First Names exists This field is empty if Given Name and First Names are absent	From customer but must comply with SPAR
Sur Name	subject: surname (2.5.4.4)	This field MUST contain all of the Subject's surnames.	From customer but must comply with SPAR
Common Name	subject:commonName (2.5.4.3) cn = Common name	This field MUST contain the Subject's common name.	Combination of Given Name and Surname
Organization	subject:organizationName (2.5.4.10)	This field MUST contain the Subject's full legal organization name as listed in the official records.	Companies Registration Office and Central Bureau of Statistics
OrganizationIdentifier	subject:organizationIdentifier	This field MUST contain the Subject's full legal organization number as listed in the official records in the following format: XXXXXX-XXXX.	Companies Registration Office and Central Bureau of Statistics

Country	subject:countryName (2.5.4.6)	This field MUST contain the country code for the Subject's organization as listed in the official records. In ISO3166 format	Companies Registration Office and Central Bureau of Statistics
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)		CA
Issuer's Signature	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)		CA
Extension	**Value**		
Authority Key Identifier	Octet String – Same as Issuer's subject key identifier	Contains 20 byte SHA-2 hash of the CA Public Key	CA
Subject Key Identifier	Octet String – Calculated by CA from public key in PKCS#10	Contains 20 byte SHA-2 hash of the subjectPublicKey in this certificate	CA
1.2.752.34.2.1 Card Number Extension	9 digits	This field MUST contain 9 digits.	Identity Management System
Key Usage	Critical=TRUE; Digital Signature, Key Encipherment (a0)	Critical	CA
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2)	This field MUST contain Client Authentication.	Certificate Management System based on CA templates
1.3.6.1.4.1.311.25.2	Octetstring (max 28)	IF present this field contain the Subject SID (Security Identifier) from customers active directory.	Customers Active directory
Certificate Policies	[1]Certificate Policy: Policy Identifier= SEE RIGHT-> : https://pki.nexusgroup.com	[Customer] Issuing CA G[n] - OID 1.2.752.274.1.1.3 [Customer] Employe Issuing CA G[n]	Certificate Management System based on CA templates
Subject Alternative Name	UPN = XXXXXXXXXXX@organization. xx OR Not present	IF present this field CAN contain The Subject's User Principal Name formatted as the subject's full Swedish social security number (or equal) OR mailbox and the agency domain name OR Not present	Certificate Management System based on CA templates
CRL Distribution Point	CRL HTTP URL = SEE RIGHT -> (2.5.29.31)	http://dp.eid.prod.go.nexusgroup.com/crl/customer-issuing-ca-g1.crl OR http://dp.prod.go.nexusgroup.com/crl/customer-client-issuing-ca-g1.crl	CA
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.go.nexusgroup.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= SEE RIGHT->	http://dp.eid.prod.go.nexusgroup.com/aia/customer-issuing-ca-g1.cer OR http://dp.prod.go.nexusgroup.com/aia/customer-client-issuing-ca-g1.cer	CA

*CA for LoA3 qualified certificates
**CA for non-qualified certificates

2.2 Signing certificate

Field	Value	Comments	Source
Version	V3		CA
Serial Number	Unique number		CA
Issuer Signature Algorithm	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)		CA
Issuer Distinguished Name	Unique X.500 CA DN. CN = SEE RIGHT -> O = [Customer_Org] C = [Customer_Country]	CN=[Customer] Issuing CA G[n]* [Customer] Employee Issuing CA G[n]**	CA
Validity Period	Up to 24 months expressed in UTC format		Certificate Management System based on CA templates
Subject Distinguished Name			
Title	subject:title (2.5.4.12)		Certificate Management System
Given Name	subject:givenName (2.5.4.42)	This field MUST contain the Subject's marked Given Name IF it exists OR All Given Names of the subject if marking of Given Name is absent and First Names exists This field is empty if Given Name and First Names are absent	From customer but must comply with SPAR
Sur Name	subject: surname (2.5.4.4)	This field MUST contain all of the Subject's surnames.	From customer but must comply with SPAR
Common Name	subject:commonName (2.5.4.3) cn = Common name	This field MUST contain the Subject's common name.	Combination of Given Name and Surname
Organization	subject:organizationName (2.5.4.10)	This field MUST contain the Subject's full legal organization name as listed in the official records.	Companies Registration Office and Central Bureau of Statistics
OrganizationIdentifier	subject:organizationIdentifier	This field MUST contain the Subject's full legal organization number as listed in the official records in the following format: XXXXXX-XXXX.	Companies Registration Office and Central Bureau of Statistics
Country	subject:countryName (2.5.4.6)	This field MUST contain the country code for the Subject's organization as listed in the official records. In ISO3166 format	Companies Registration Office and Central Bureau of Statistics
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)		CA
Issuer's Signature	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)		CA

Extension	Value		
Authority Key Identifier	Octet String – Same as Issuer's subject key identifier	Contains 20 byte SHA-2 hash of the CA Public Key	CA
Subject Key Identifier	Octet String – Calculated by CA from public key in PKCS#10	Contains 20 byte SHA-2 hash of the subjectPublicKey in this certificate	CA
1.2.752.34.2.1 Card Number Extension	9 digits	This field MUST contain 9 digits	Identity Management System
Key Usage	critical=TRUE; nonRepudiation (40)	Critical	CA
Extended Key Usage	Document Signing (1.3.6.1.4.1.311.10.3.12)	This field MUST contain Document Signing	CA
Certificate Policies	[1]Certificate Policy: Policy Identifier= SEE RIGHT-> : https://pki.nexusgroup.com	[Customer] Issuing CA G[n] - OID 1.2.752.274.1.1.3 [Customer] Employee Issuing CA G[n]	Certificate Management System based on CA templates
CRL Distribution Point	CRL HTTP URL = SEE RIGHT -> (2.5.29.31)	http://dp.eid.prod.go.nexusgroup.com/crl/customer-issuing-ca-g1.crl OR http://dp.prod.go.nexusgroup.com/crl/customer-client-issuing-ca-g1.crl	CA
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.go.nexusgroup.com [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= SEE RIGHT->	http://dp.eid.prod.go.nexusgroup.com/aia/customer-issuing-ca-g1.cer OR http://dp.prod.go.nexusgroup.com/aia/customer-client-issuing-ca-g1.cer	CA

*CA for LoA3 qualified certificates
**CA for non-qualified certificates