Business Certificates – an introduction v1.3

This document describes the concept of a *Business Certificate*, a digital certificate issued to a legal entity. A Business Certificate is issued from a Certificate Authority (CA) controlled by a Trust Service Provider (TSP).

A Business Certificate may be used for different purposes (e.g. authentication, encryption, signing/sealing) and at different levels of trust (Qualified, non-Qualified etc.).

This document describes Business Certificates and relevant aspects for those considering to start using Business Certificates for securing communication between legal persons.

Business Certificates may be distributed by means of using *the Business Certificate Publisher (BCP)* service (to be named CertPub in the future). This could be an effective way of distributing Business Certificates to support many-to-many communication. However, the BCP is out of the scope of this document.

Definitions

By **eIDAS** we mean '*Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*'.

Terms and definitions from the eIDAS regulation:

- **Trust Service:** means an electronic service normally provided for remuneration which consists of:
  a) the creation, verification, and validation of electronic signatures, *electronic seals* or electronic time stamps, electronic registered delivery services and *certificates related to those services*, or
  b) the creation, verification and validation of certificates for website authentication; or
  c) the preservation of electronic signatures, seals or certificates related to those services;
- **Qualified Trust Service:** means a Trust Service that meets the applicable requirements laid down in this Regulation
- **Trust Service Provider (TSP):** means a natural or a legal person who provides one or more Trust Services either as a Qualified or as a non-qualified Trust Service Provider
- **Qualified Trust Service Provider (QTSP):** means a Trust Service Provider who provides one or more Qualified Trust Services and is granted the qualified status by the supervisory body
- **Electronic Seal (eSeal)[1]:** means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
- **Advanced Electronic Seal (AdES):** means an Electronic Seal, which meets the requirements set out in Article 36;
- **Qualified Electronic Seal (QES):** means an Advanced Electronic Seal, which is created by a qualified electronic seal creation device, and that is based on a Qualified Certificate for Electronic Seal;
- **Certificate for Electronic Seal (Cert eSeal):** means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;

- **Qualified Certificate for Electronic Seal (QC eSeal)**: means a Certificate for an Electronic Seal, that is issued by a Qualified Trust Service Provider and meets the requirements laid down in Annex III;

[1)] The concept of *electronic seal* is similar to *electronic signature*. However, a legal person generates an electronic seal while a natural person generates an electronic signature. These concepts are legal concepts as defined by eIDAS and both are typically implemented by means of *digital signature* as technology.

Other terms and definitions:

- **Certificate**: an electronic document that uses a digital signature to bind a Public Key and an identity
- **Business Certificate**: a Certificate where the identity represents a legal person
- **Certificate Authority (CA):** The entity confirming the binding between a Public Key and an identity by generating a digital signature on a Certificate using the CA Private Key. The term applies equally to both Root CAs and Subordinate CAs. The term is often used about the organization that is responsible for the creation, issuance, revocation, and management of Certificates. However, we prefer to use the term TSP for this purpose.
- **Private Key**: The key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
- **Public Key:** The key of a key pair that MAY be publicly disclosed by the holder of the corresponding Private Key and that is used by a relying party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key

Business Certificate

A digital certificate is an electronic document that binds a Public Key to an identity. The identity may be the identity of a natural person, a legal person, a system etc. For a Business Certificate the identity always represents a legal person.

The Public Key included in a Certificate corresponds to a Private Key controlled by the legal person identified as Subject in the Certificate.

Certificate Quality levels – QCP, NCP and LCP

The strength of the binding between the Public Key and the identity and thus the trust and confidence a relaying party may have in the Certificate depends on the controls taken by the Trust Service Provider (TSP) when issuing the Certificate.

These controls are defined in terms of certificate policies (CP) and there are defined different qualities of certificate polices.

The quality levels relevant for Business Certificates (and supported by BCP) are:

- A **Qualified Certificate Policy (QCP)** is a policy for EU qualified certificates offering the level of quality defined in Regulation (EU) No 910/2014 (eIDAS). For legal persons the QCP satisfies the requirements for Qualified Certificates for electronic seals (QC eSeals).

- A **Normalized Certificate Policy (NCP)** which meets general recognized best practice for TSPs issuing Certificates used in support of any type of transaction. This includes Business Certificates for several purposes, e.g. authentication, signing/sealing and encryption.

- A **Lightweight Certificate Policy (LCP)** offering a quality of service less onerous than the NCP (requiring less demanding policy requirements) for use where a risk assessment does not justify the additional burden of meeting all requirements of the NCP (e.g. physical presence), for Certificates used in support of any type of transaction (such as digital signatures, web authentication).

Requirements for each Certificate Quality level

For each quality level, there exists a set of requirements that a TSP must comply with when issuing a Certificate at that specific quality level.

All certificates must comply with common standards and best practices, but the main difference between the quality levels are the controls performed when issuing the Certificate. The legal effect of the Certificate may also be different, e.g. a Qualified Certificate has a legal effect as defined by the eIDAS regulation.

Some main differentiators are how to verify the authenticity of a certificate request and how to perform the identity control of a legal person (e.g. by means of physical presence).

For legal persons (organizations) registered in Norway, the organization must be registered in the "Brønnøysundregistrene" and any natural person registered with a role related to the organization in the register, may act as the authorized representative for the organization.

Requirements for QCP

Certificates issued according to QCP must satisfy the requirements for qualified certificates according to eIDAS.

This requires that the identity of the legal person and, if applicable, any specific attributes of the person, shall be verified

a) by the physical presence of an authorized representative of the legal person; or
b) using methods which provide equivalent assurance in terms of reliability to the physical presence of an authorized representative of the legal person and for which the TSP can prove the equivalence

A TSP may use different methods to implement identity verification for legal persons. Electronic identifications means based on Qualified Certificates for electronic signatures used by an authorized representative is accepted in addition to any other traditional method for implementing physical presence.

A Qualified Certificate should be used for Electronic Seal (signing) only and not for encryption.

Requirements for NCP

"Virksomhetssertifikater" according to "Kravspesifikasjonen for PKI i offentlig sector" is compliant with this level of quality.

The identity of the legal person, or other organizational entity identified in association with a legal person, shall be checked against a duly mandated subscriber either directly, by physical presence of a

person allowed to represent the legal person, or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

The requirements for the NCP are less restrictive with respect to who is allowed to represent the legal person at identity verification compared to the QCP, but physical presence is still required.

A certificate at this quality level may be used for all transactions including Electronic Seal (signing), authentication and encryption.

Requirements for LCP

This quality level does not require physical presence (or similar) and may be used in cases where a risk assessment does not justify the additional burden of meeting all requirements of the NCP.

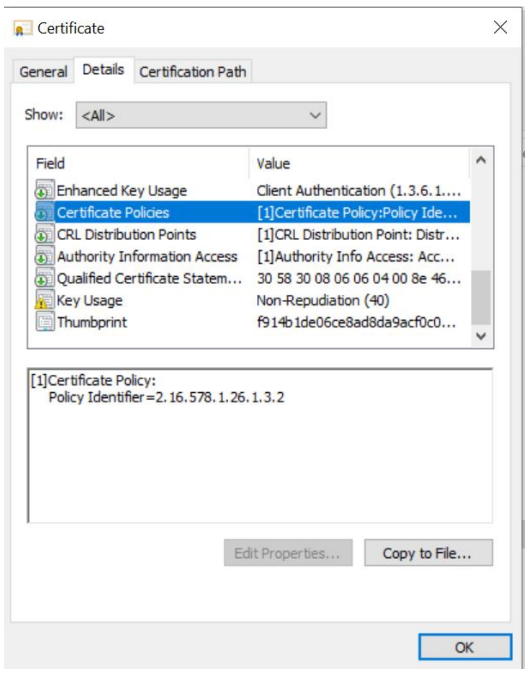
A certificate at this quality level may be used for all transactions including Electronic Seal (signing), authentication and encryption.

How to identify the Certificate Quality level

A Business Certificate is issued from a CA controlled by a TSP.

For the quality level QCP, the TSP must be a QTSP and registered on the EU Trusted List as a provider of Qualified Certificates for Electronic Seal. The EU Trust List includes information on the CA used by the QTSP for issuing different types of Qualified Certificates (see https://www.nkom.no/teknisk/tillitstjenester/kvalifiserte-tilbydere/tillitsliste for more information on the Norwegian national trusted list).

The Certificate Quality Level (or policy level) is defined by the QTSP in its Certificate Policy (CP) and Certification Practice Statement (CPS) and available as Certificate Policy Object Identifiers (CP OID) in an attribute in the certificate as shown below:



Consult the QTSP documentation to understand how to map their CP OIDs to the defined Certificate Quality Levels.

Purpose of certificates

A Business Certificate may be used for different purposes, the typical purposes are:

- Authentication
- Encryption
- Signing or sealing

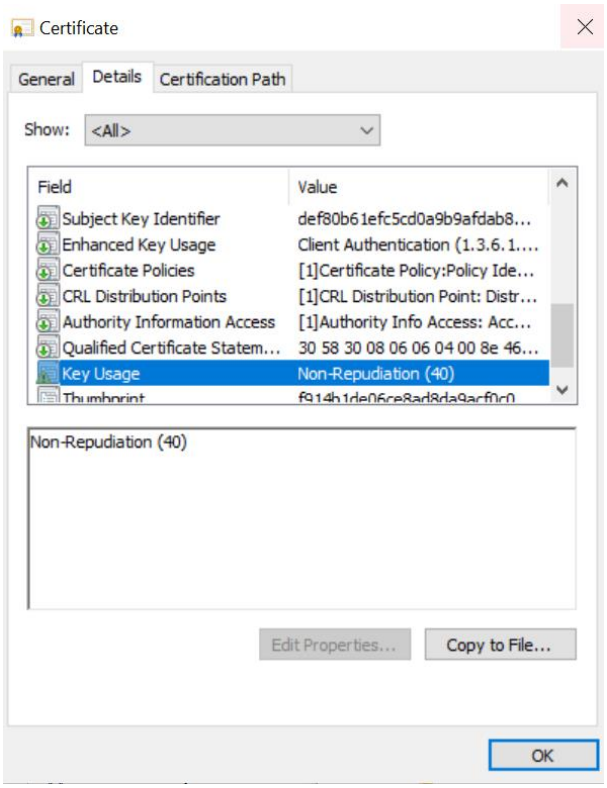
We prefer to use the legal term electronic seal (eSeal) and not electronic signature in the context of Business Certificates. An electronic seal is a digital signature generated by a legal person, while a natural person generates an electronic signature.

Digital signature is the underlying technology used in both cases, and it is used for some of the other purposes introduced above (e.g. authentication) as well. Be aware of this difference in purpose, legal terms and technology.

The eIDAS regulation defines Electronic Seal and the generation of Certificates for Electronic Seals as a Trust Service. However, the concept of Certificates for authentication and encryption is not defined as Trust Services according to eIDAS.

Business Certificates may be issued for the purpose of authentication and encryption as well as electronic seals. However, Qualified Certificates according to eIDAS, will typically only be issued for the purpose of electronic seal.

The purpose of a certificate is defined by the Key Usage extension in the certificate (see https://tools.ietf.org/html/rfc5280#section-4.2.1.3) as shown below:



ETSI defines requirements for certificate profiles complying with eIDAS.ETSI EN 319 412-2 v2.2.1 and ETSI EN 319 412-3 v1.2.1 defines six (6) different combinations of Key Usages:

Table 1: Key usage settings

Type	Non-Repudiation (Bit 1)	Digital Signature (Bit 0)	Key Encipherment or Key Agreement (Bit 2 or 4)
A	X		
B	X	X	
C		X	
D		X	X
E			X
F	X	X	X

The key usage extension shall be present and shall contain one (and only one) of the key usage settings defined in table 1 (A, B, C, D, E or F). Type A, C, or E should be used to avoid mixed usage of keys.

Certificates used to validate commitment to signed content (e.g. documents, agreements and/or transactions) shall be limited to type A, B or F. Of these alternatives, type A should be used (see the security note 2 below).

EXAMPLE:

> *Digital signatures which are aimed to be used as advanced electronic signatures as defined in Regulation (EU) No 910/2014 [i.5] are considered to signal commitment to signed content.*

Certificates used to validate digital signatures over content (e.g. documents, agreements and/or transactions) that provide evidence of origin and integrity of the content shall be limited to type A, B or F. Of these alternatives, type A should be used (see the security note 2 below).

EXAMPLE:

> *Digital signatures which are aimed to be used as advanced electronic seals as defined in Regulation (EU) No 910/2014 [i.3] are considered to provide evidence of origin and integrity of the content.*

NOTE 1:
The X.509 standard [i.3] has renamed the nonRepudiation bit to "contentCommitment". IETF RFC 5280 [1] has kept the original name nonRepudiation for backwards compatibility reasons. These bits are equivalent in function and meaning regardless of their different names.

NOTE 2: [security note]
Combining the non-repudiation bit (bit 1) in the keyUsage certificate extension with other keyUsage bits can have security implications depending on the security environment in which the certificate is to be used.

> *If the subject's environment can be fully controlled and trusted, then there are no specific security implications.*
>
> *If the subject's environment is not fully controlled or not fully trusted, then unintentional signing of commitments is possible.*

It is for the QTSP to decide which Key Usages to use for the specific purposes, but we will recommend the following Key Usage for the identified purposes:

- Authentication: Key Usage = Digital Signature (type C)
- Encryption: Key Usage = Key Encipherment or Key Agreement (type E)
- Signing or sealing: Key Usage = Non-Repudiation (type A)

A QTSP may also combine several purposes in a single certificate.

Consult the QTSP documentation to understand how the specific purposes may be identified in their Business Certificates.

Overview purpose and key usage

The table below gives an overview of terms used to describe purpose and key usage, as seen from the legislation (eIDAS) and standard (ETSI) point of view as well as implementation point of view (Windows).

Scope - terms	**Authentication**	**Encryption**	**Signing/Sealing**
Subject is a natural person	Authentication	Encryption	Signing
- Norwegian	Autentisering	Kryptering	Signering
Subject is a legal person	Authentication	Encryption	Sealing
- Norwegian	Autentisering	Kryptering	Forsegling
Key usage x.509 i.3	Digital Signature	Key Encipherment	Content Commitment
Key usage x.509 i.1-2x	Digital Signature	Key Encipherment	Non-Repudiation
Key usage Windows 10	Digital Signature	Key Encipherment	Non-Repudiation
- Norwegian	Digital signatur	Nøkkelchiffrering	Ikke-avvisning
Key usage ETSI EN 319 412-2 V2.1.1	Digital Signature	Key Encipherment	Non-Repudiation
Key usage in ETSI (set bit)	Bit 0 (80)	Bit 2 (20)	Bit 1 (40)
eIDAS legal term: Subject is a natural person	Electronic identification	Not defined	Electronic signature [1)] (eSignature)
eIDAS legal term: Subject is a legal person	Electronic identification	Not defined	Electronic seal [1)] (eSeal)

[1)] May be an advanced electronic signature/seal or a qualified electronic signature/seal according to the eIDAS regulation.