

SEID v2.0

Nye nasjonale sertifikatprofiler



eIDAS-forordningen

Regulation (EU) No 910/2014 of 23 July 2014

Electronic identification (eID) and Trust Services for my business

eIDAS SOLUTIONS

for electronic
and re

The screenshot shows the LOVDATA website interface. At the top, there is a search bar with the text "Søk etter lover, forskrifter, dommer og stortingsvedtak". Below the search bar, the main content area displays the title of the regulation: "Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektr...". A button labeled "Gå til opprinnelig kunggjort versjon" is visible. The regulation title is repeated in red: "Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester)". Below the title is a table with the following data:

Dato	LOV-2018-06-15-44
Departement	Nærings- og fiskeridepartementet
Ikrafttredelse	15.06.2018
Endrer	LOV-2001-06-15-81
Kunggjort	15.06.2018
Korttittel	Lov om elektroniske tillitstjenester

Below the table, there is a reference to the original law: "Jf. tidligere lov 15. juni 2001 nr. 81. – Jf. EØS-avtalen vedlegg XI nr. 5I (forordning (EU) nr. 910/2014).". The section title is "§ 1. eID og elektroniske tillitstjenester i EØS".



The eSeal logo is shown with the text "eSeal guarantee both the origin and the integrity of a document." Below it, there are three boxes with the following text: "HELPS AVOID FISHING, PROTECTING THE REPUTATION OF YOUR BUSINESS", "REDUCED COSTS AND TIME THROUGH STREAMLINED PROCESSES", and "TRUST IN THE ORIGIN OF THE DOCUMENT". To the right, there is a box labeled "ENHANCED DOCUMENT TRACKING".

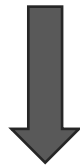
Bakgrunn

- *SEID-prosjektet* definerte i 2005 et sett med anbefalte sertifikatprofiler for person- og virksomhetssertifikater (SEID v1.0) som siden har vært brukt i Norge
- Med innføring av eIDAS-forordningen i 2018 og ny Selvdeklarasjonsforskrift i 2019 ble det identifisert et behov for å tilpasse de noe utdaterte nasjonale sertifikatprofilene med felles europeiske ETSI-standarder
- *SEID-prosjektet* ble videreført gjennom *SEID-samarbeidet* og i 2020 kom de opp med et nytt sett med anbefalte sertifikatprofiler (SEID v2.0) og en definert overgangsordning
- Overgangen fra SEID v1.0 til SEID v2.0 medfører en risiko for at applikasjoner og systemer som benytter person- og virksomhetssertifikater kan «brekke» når sertifikater basert på SEID v2.0 tas i bruk

Sertifikatprofiler i hht «gammelt» regelverk (SEID v1.0)

Kravspesifikasjon for PKI i offentlig sektor Versjon 2.0

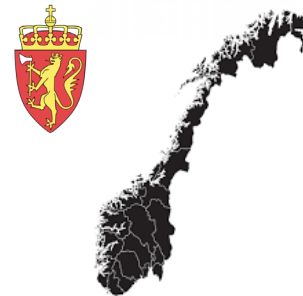
Dette dokumentet er en overordnet, funksjonell kravspesifikasjon for selvdeklarerer og anskaffelse av PKI-basert eID som skal benyttes i forbindelse med elektronisk kommunikasjon med og i offentlig sektor i Norge.



SEID-Prosjektet

Leveranse oppgave 1

Anbefalte sertifikatprofiler for
personsertifikater og virksomhetssertifikater



Subject	9578-4050-10000406, MADS ...
Public key	RSA (2032 Bits)

SERIALNUMBER = 9578-4050-10000406
CN = MADS EGIL HENRIKSVEEN
C = NO



Subject	983163327, BUYPASS AS, BUY...
Public key	RSA (2048 Bits)

SERIALNUMBER = 983163327
CN = BUYPASS AS
O = BUYPASS AS
C = NO

Sertifikatprofiler i hht «nytt» regelverk (SEID v2.0)

Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester)

Dato	LOV-2018-06-15-44
Departement	Kommunal- og moderniseringsdepartementet
Ikrafttredelse	15.06.2018



ETSI EN 319 412-2 V2.2.1 (2020-07)



EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI);
Certificate Profiles;
Part 2: Certificate profile for certificates issued
to natural persons



Subject UN:NO-9578-4050-10000406,...

Public key RSA (2032 Bits)

SERIALNUMBER = UN:NO-9578-4050-10000406
CN = MADS EGIL HENRIKSVEEN
G = MADS EGIL
SN = HENRIKSVEEN
C = NO



valid to onsdag 27. mars 2024 00:59:00

Subject NTRNO-983163327, BUYPASS ...

Public key RSA (3072 Bits)

2.5.4.97 = NTRNO-983163327
CN = BUYPASS AS
O = BUYPASS AS
C = NO

Ulikheter i profilene



Subject 9578-4050-10000406, MADS ...
Public key RSA (2032 Bits)

SERIALNUMBER = 9578-4050-10000406
CN = MADS EGIL HENRIKSVEEN
C = NO

Subject UN:NO-9578-4050-10000406,...
Public key RSA (2032 Bits)

SERIALNUMBER = UN:NO-9578-4050-10000406
CN = MADS EGIL HENRIKSVEEN
G = MADS EGIL
SN = HENRIKSVEEN
C = NO



Subject 983163327, BUYPASS AS, BUY...
Public key RSA (2048 Bits)

SERIALNUMBER = 983163327
CN = BUYPASS AS
O = BUYPASS AS
C = NO

valid to onsoag 27. mars 2024 00:59:00
Subject NTRNO-983163327, BUYPASS ...
Public key RSA (3072 Bits)

2.5.4.97 = NTRNO-983163327
CN = BUYPASS AS
O = BUYPASS AS
C = NO

SEID v2.0

- Utarbeidet av Buypass i samarbeid med de andre sertifikatutstederne
- Sertifikatprofiler for personsertifikater og virksomhetssertifikater
- Harmonisert med eIDAS sertifikatprofiler i ETSI EN 319 412-x
 - Noen få, men vesentlige endringer fra SEID v1.0
- Overgangsordning fra SEID v1.0 til SEID v2.0
- Godkjent av SEID-samarbeidet november 2020
- Publisert av Nkom 8.mars 2021

ETSI EN 319 412-x

ETSI EN 319 412-1 V1.4.1 (2020-06)



Electronic Signatures and Infrastructures (ESI);
Certificate Profiles;
Part 1: Overview and common data structures

ETSI EN 319 412-2 V2.2.1 (2020-07)



Electronic Signatures and Infrastructures (ESI);
Certificate Profiles;
Part 2: Certificate profile for certificates issued
to natural persons

ETSI EN 319 412-3 V1.2.1 (2020-07)



Electronic Signatures and Infrastructures (ESI);
Certificate Profiles;
Part 3: Certificate profile for certificates issued
to legal persons

ETSI EN 319 412-4 V1.1.1 (2016-02)



Electronic Signatures and Infrastructures (ESI);
Certificate Profiles;
Part 4: Certificate profile for web site certificates

ETSI EN 319 412-5 V2.3.1 (2020-04)



Electronic Signatures and Infrastructures (ESI);
Certificate Profiles;
Part 5: QCStatements

Virksomhetssertifikater

SEID v2.0

Anbefalt profil for virksomhetssertifikater

- Sertifikatprofil til bruk for virksomhetssertifikater utstedt til juridiske personer som er registrert i Enhetsregisteret i Norge
 - Profilen kan også brukes for virksomheter som ikke er registrert i Enhetsregisteret
- Profilen er anvendelig for alle virksomhetssertifikater, herunder kvalifiserte sertifikater for elektronisk segl, hvor sertifikatet inneholder informasjon direkte knyttet til virksomhetens identitet i Enhetsregisteret

Sertifikatinnehaver (Subject)

- **Følgende attributter er obligatoriske:**

- countryName (C) = 'NO'
- organizationIdentifier – skal unikt identifisere den juridiske personen
 - OrganizationIdentifier er et nytt attributt sammenliknet med bruken av SerialNumber i SEID v1.0 som tidligere har vært brukt for å identifisere den juridiske personen unikt.
 - Sertifikatutsteder kan velge å inkludere SerialNumber i tillegg til organizationIdentifier, men det er sistnevnte som vil identifisere den juridiske personen i sertifikatet i hht ETSI EN 319 412-3.
- organizationName (O) – fullt (se nedenfor) navn på den juridiske personen slik denne er registrert i Enhetsregisteret
- commonName (CN) – navn som sertifikatinnehaver foretrekker å bruke i sertifikatet

- **I tillegg kan sertifikatfeltet inneholde andre attributter, for underenheter kan det for eksempel være mulig å bruke:**

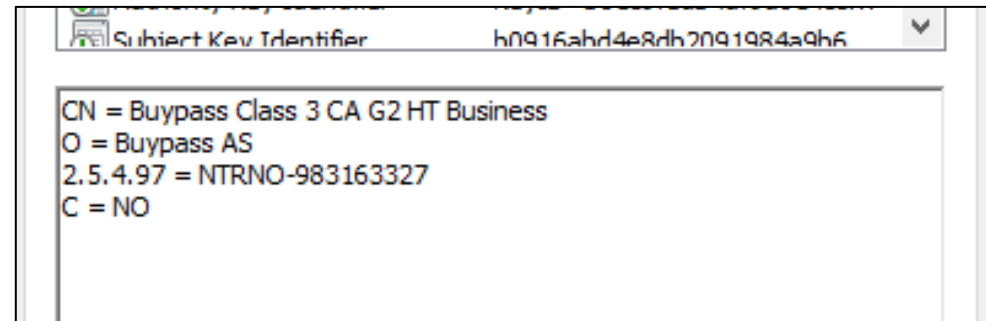
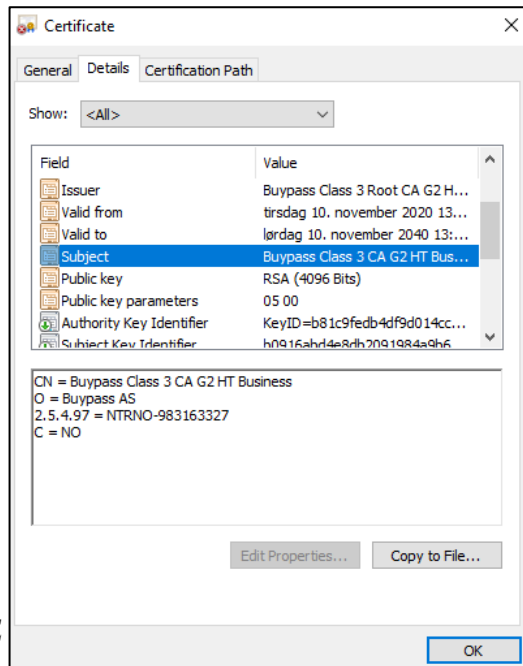
- organizationalUnit (OU) – navn og organisasjonsnummer på underenhet

- **ETSI EN 319 412-3 tillater at O, CN og OU inneholder flere tegn enn det som er spesifisert i RFC 5280 (alle 64 tegn)**

- Dersom en sertifikatutsteder velger å gå utover disse grenseverdiene, så er det greit å være oppmerksom på at dette kan føre til kompatibilitetsproblemer med applikasjoner som forholder seg strengt til RFC-en.
- Regler for forkortelse av navn – ikke definert for virksomhetssertifikater

Samordnet bruk av organizationIdentifiser

- For å sikre harmonisering etter europeiske standarder anbefales det å inkludere en semantisk identifikator i hht ETSI EN 319 412-1 for juridiske personer registrert i Enhetsregisteret:
 - **NTRNO**-<organisasjonsnummer i hht Enhetsregisteret>



Sertifikatets bruksområder

- Key Usage benyttes for å angi bruksområde

ETSI EN 319 412-2 V2.2.1 (2020-07)



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.

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

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.

- Følger ETSI-standardens anbefaling

- Autentisering: Key Usage = digitalSignature
- Signering: Key Usage = nonRepudiation (også kalt contentCommitment)
- Kryptering: Key Usage = keyEncipherment eller keyAgreement

Qualified Certificate Statements



- **Sertifikater som utstedes som kvalifiserte sertifikater for elektronisk segl skal inneholde EU QCStatements i hht ETSI EN 319 412-5:**
 - esi4-qcStatement-1 (EU qualified certificate compliance)
 - esi4-qcStatement-6 (EU qualified certificate of a particular type)
 - id-etsi-qct-eseal -> EU qualified certificate for electronic seal
- **Dersom, og kun dersom, sertifikatet brukes med kvalifisert elektronisk seglframstillingssystem, det vil si at det understøtter kvalifisert elektronisk segl, skal sertifikatet inneholde følgende EU QCStatement i hht ETSI EN 319 412-5:**
 - esi4-qcStatement-4 (EU qualified signature/seal compliance)
- **Det er kun sertifikater med bruksområde Signering som kan merkes som et kvalifisert sertifikat for elektronisk segl**
 - *Men det er lagt inn en åpning for bruksområde Autentisering i tillegg*

Endringer fra SEID v1.0

6.5 Endringer fra SEID-sertifikatprofil v1.0

Sertifikatfelt eller utvidelse	SEID v1.0	SEID v2.0
Subject	countryName (C)=NO organizationName (O): Organisasjonens fulle navn iht. Enhetsregisteret serialNumber: Organisasjonsnummer fra Enhetsregisteret commonName (CN): Navn som sertifikatinneholder foretrekker å bruke i sertifikatet	countryName (C)=NO organizationName (O): Organisasjonens fulle navn iht. Enhetsregisteret organizationIdentifier=Organisasjonsnummer fra Enhetsregisteret formattet iht. 6.2.1 commonName (CN): Navn som sertifikatinneholder foretrekker å bruke i sertifikatet
Underenhet	organizationalUnitName (OU): <organisasjonsnavn>'.<organisasjonsnummer> for underenhet som registrert i Enhetsregisteret	organizationalUnitName (OU): <organisasjonsnavn>'.<organisasjonsnummer> for underenhet som registrert i Enhetsregisteret
KeyUsage	Følgende verdier anbefalt for bruksområde Signering: <ul style="list-style-type: none"> • nonRepudiation, eller • digitalSignature, eller • nonRepudiation + digitalSignature Følgende verdier anbefalt for bruksområde kryptering: <ul style="list-style-type: none"> • keyEncipherment • dataEncipherment 	Følgende verdier anbefalt for bruksområde Signering: <ul style="list-style-type: none"> • nonRepudiation Følgende verdier anbefalt for bruksområde kryptering: <ul style="list-style-type: none"> • keyEncipherment, eller • keyAgreement Følgende verdier anbefalt for bruksområde autentisering: <ul style="list-style-type: none"> • digitalSignature Flere bruksområder kan kombineres i ett sertifikat
qcStatements		Virksomhets sertifikater kan utstedes som ikke-kvalifiserte sertifikater ⁵ Kun sertifikater med bruksområde Signering (og/eller Autentisering) bør merkes som kvalifisert sertifikat. For alle sertifikater, indikasjon på bruk av semantisk identifikator: <ul style="list-style-type: none"> • id-etsi-qcs-semanticId-Legal For kvalifiserte sertifikater i tillegg følgende EU QC Statements: <ul style="list-style-type: none"> • esi4-qcStatement-1 • esi4-qcStatement-6 <ul style="list-style-type: none"> ◦ id-etsi-qct-eseal For sertifikater som understøtter kvalifisert segl, i tillegg: <ul style="list-style-type: none"> ◦ esi4-qcStatement-4

I SEID v1.0 er lengden på O, CN og OU begrenset iht. RFC 5280, mens for SEID v2.0 er det tillatt å gå utover disse grensene for å inkludere fullt navn i disse attributtene. Sjekk med sertifikatutsteders policy for å se hva som gjelder.

Overgangsordning

- Sertifikater som følger de opprinnelige SEID-sertifikatprofilene er fortsatt i utstrakt bruk i det norske markedet.
- For å sikre en smidig overgang fra bruk av SEID-sertifikatprofiler v1.0 til SEID-sertifikatprofiler v2.0 som er bedre harmonisert med felles europeiske ETSI-sertifikatprofiler, er det innført en overgangsordning som skal sikre at sertifikatutstedere kan utstede sertifikater under SEID-sertifikatprofiler v1.0 i en overgangsperiode samtidig som markedets aktører tilpasser sine løsninger til SEID-sertifikatprofiler v2.0.
- Forskjellene mellom SEID-sertifikatprofiler v1.0 og SEID-sertifikatprofiler v2.0 blir tydelig beskrevet som en del av det aktuelle sertifikatfelt og profil i kapittel 5 og 6.
- **Overgangsperioden varer frem til 1. juni 2022.** Dette betyr at sertifikatutstedere kan utstede sertifikater iht. SEID-sertifikatprofiler v1.0 gjennom overgangsperioden. Etter at overgangsperioden er over, skal sertifikatutstedere utstede sertifikater iht. SEID-sertifikatprofiler v2.0.
- Sertifikatutstederne står fritt til å utstede sertifikater iht. SEID-sertifikatprofiler v2.0 i hele overgangsperioden, men bør gjøre en risikovurderingen for at applikasjoner og tjenester ikke støtter disse ennå.
- **Tjeneste-/programvare-leverandører og sertifikatmottakere må være forberedt på å håndtere sertifikater iht. SEID-sertifikatprofiler v2.0 fra 1. september 2021.** Dersom det viser seg at dette forsårsaker feil eller på andre måter gjør at sertifikatene ikke fungerer, bør sertifikatutstederne varsles om dette forholdet og problemet løses i tjenesten/applikasjonen. Dette må være fullført i løpet av overgangsperioden.
- Med en slik overgangsordning vil det kunne være aktive sertifikater i bruk utstedt under SEID v1.0 i lang tid etter overgangsperiodens slutt, dvs. inntil sertifikatene utstedt i overgangsperioden utløper. Med for eksempel en levetid på tre år, vil det kunne være aktive sertifikater basert på SEID v1.0 frem til 1. juni 2025.

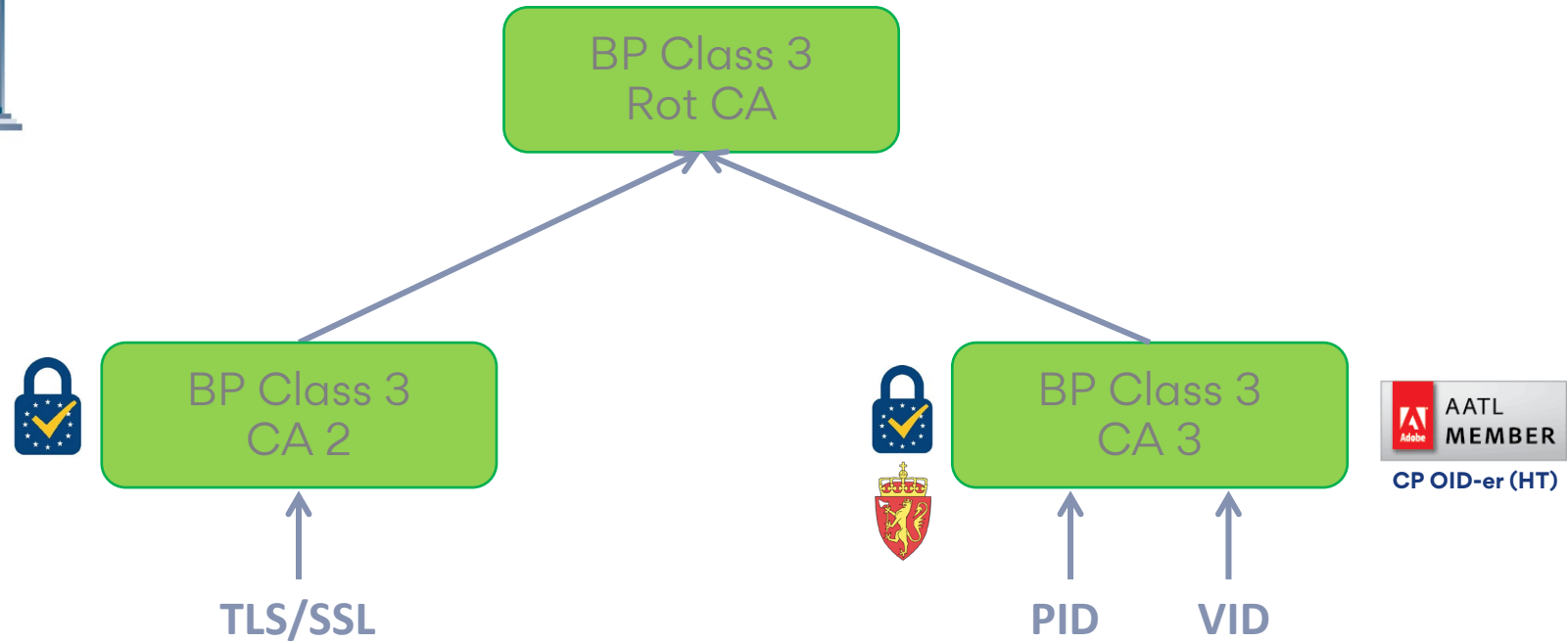
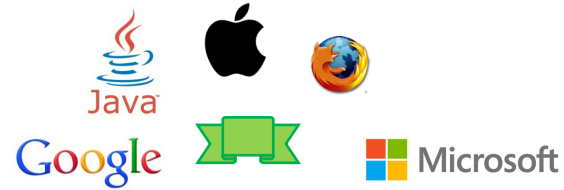
Buypass og SEID v2.0

Plan for innføring

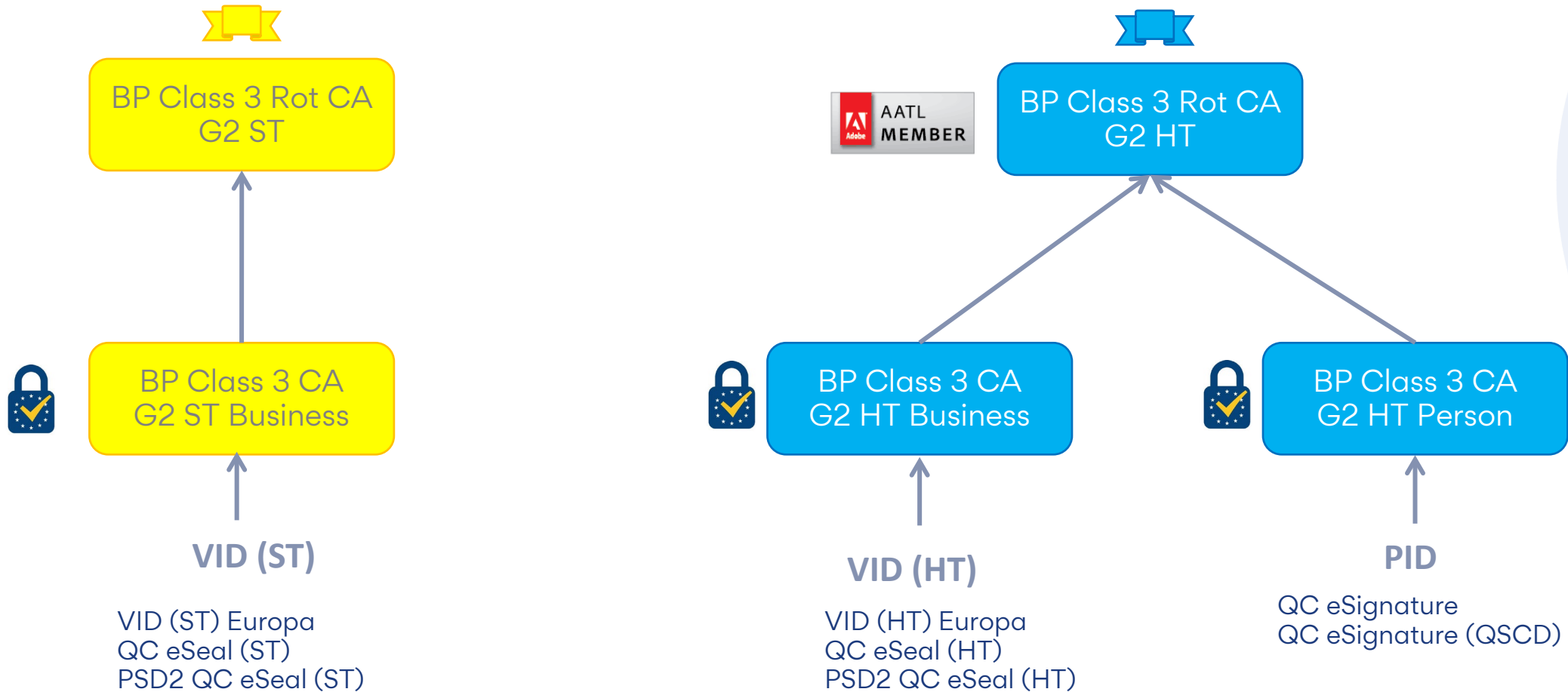
Buypass plan for overgang til SEID v2.0

- Koordinere overgangen med å ta i bruk nye «G2 CA-er»
- Og samtidig ta i bruk «sterkere» kryptografi
 - RSA 3072 bits eller
 - Elliptisk kurve kryptografi (ECC) med NIST P-256
- Tilby sertifikater for test i Q2 2021
- Starte utrulling i produksjon fra Q3 2021

Generasjon 1 (G1) CA-er



Generasjon 2 (G2) CA-er



ST = SoftToken

HT = HardToken

Endringer som følge av G2 CA-er

- **G2 CA-ene er ikke inkludert i «alle» rotsertifikatprogram**
 - Og dermed ikke underlagt regler som gjelder i disse
 - Men de er da heller ikke tilgjengelig i «standard OS og applikasjoner»
- **G2 CA-er som tillitsankre**
 - Defineres eksplisitt, eller
 - Bruke EU TL for å definere tillitsankre 
- **Nye tjenesteadresser for OCSP- og CRL-tjenestene**
 - CRL
 - `crl.buypass.no => crl.buypassca.com`
 - OCSP
 - `ocsp.buypass.no => ocsp[ps|bs].buypassca.com`

«Sterkere» kryptografi


Security strength (Also "bits of security")	A number associated with the amount of work (i.e., the number of operations) that is required to break a cryptographic algorithm or system. In this Recommendation, the security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256}. Note that a security strength of 80 bits is no longer considered sufficiently secure.
--	---

Table 2: Comparable strengths

Security Strength	Symmetric key algorithms	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
≤ 80	2TDEA ²¹	$L = 1024$ $N = 160$	$k = 1024$	$f = 160-223$
112	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224-255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256-383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384-511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$


Europeiske anbefalinger

ETSI TS 119 312 V1.3.1 (2019-02)



TECHNICAL SPECIFICATION

**Electronic Signatures and Infrastructures (ESI);
Cryptographic Suites**



SOG-IS Crypto Working Group

SOG-IS Crypto Evaluation Scheme
Agreed Cryptographic Mechanisms

Document purpose: specify the requirements of the SOG-IS Crypto Evaluation Scheme related to the selection of cryptographic mechanisms. This document is primarily intended for developers and evaluators.

Version 1.2
January 2020

«Sterkere» kryptografi

- Basert på gjeldende anbefalinger og det faktum at våre sertifikater har 3 års levetid, ønsker vi å øke den «kryptografiske styrken» i våre sertifikater
- **Virksomhetssertifikater**
 - Tilby 3072 bits RSA som standard i stedet for 2048 bits RSA
 - Tilby støtte for elliptisk kurve kryptografi (ECC) basert på NIST P-256
- **Personsertifikater**
 - TBD – bla pga begrensinger i gjeldende smartkort teknologi

Hva må du gjøre?

- **Som sertifikatinnhaver**

- Spesielt viktig dersom du skaffer deg nytt sertifikat i 2.halvår 2021 eller senere
- Forsikre deg om at sertifikatet fungerer i fagsystemer og applikasjoner som sertifikatet skal brukes i
 - Ved tvil, ta kontakt med aktuelle leverandører

- **Som leverandør av fagsystemer og applikasjoner som benytter sertifikater**

- Sjekk at systemene/applikasjonene dine aksepterer sertifikater som er
 - basert på SEID v2.0
 - utstedt under nye CA-er
 - håndterer sterkere kryptografi (spesielt 3072 bits RSA, men også ECC P-256)
- Sjekk at validering av sertifikater skjer mot nye tillitsankre (G2 CA-er) og har tilgang til nye tjenesteadresser (CRL/OCSP)

- **Som tilbyder av tjenester som benytter sertifikater**

- Forsikre deg om at tjenestene dine aksepterer sertifikater som angitt over
- Ta evt kontakt med leverandører av fagsystemer og applikasjoner

Mer informasjon

- <https://www.buypass.no/ressurser/fagartikler/seid-2-0>
- <https://www.nkom.no/internett/elektronisk-id-og-tillitstjenester/seid-prosjektet>

