Elektroniska underskrifter
Signering och Validering

SUNET dagarna 2020-10-25

Stefan Santesson

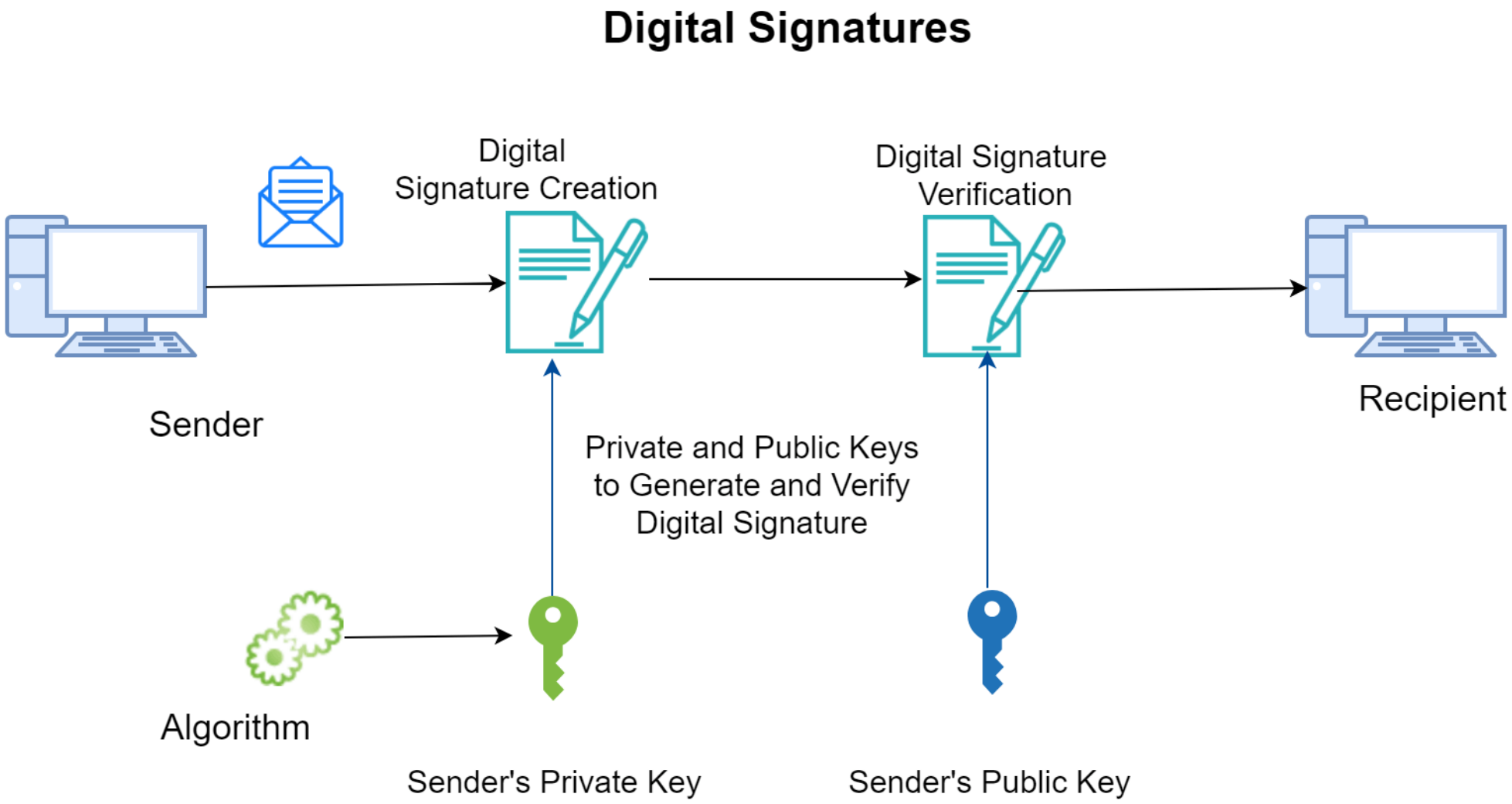
(stefan@idsec.se)

Innehåll

- Hur hamnade vi här
- Fristående underskriftstjänst
- Underskriftsformat
- Validering av underskrifter
- Valideringsintyg
- Frågor

Vägen till fristående underskriftstjänst

Basteknik

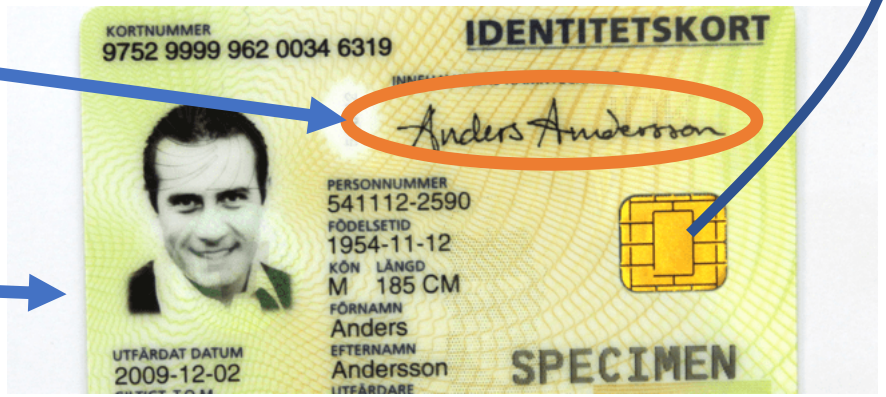

Digital Signatures
Digital
Signature Creation
Digital Signature
Verification
Sender
Recipient
Private and Public Keys
to Generate and Verify
Digital Signature
Algorithm
Sender's Private Key
Sender's Public Key

Traditionell analogi

Privat underskriftsnyckel

Publik nyckel

Certifikat



Utfärdande av eID med underskriftsfunktion

Användare kontrollerar underskriftsfunktionen

MEN …

- PIN inmatning i osäker miljö
- Omöjligt för kortet att kontrollera vad som egentligen skrivs under
- Formfaktor
  - Kräver kortläsare
  - Ej mobilstöd
- Spärrning och glömda koder
- Begränsande och dyr lösning

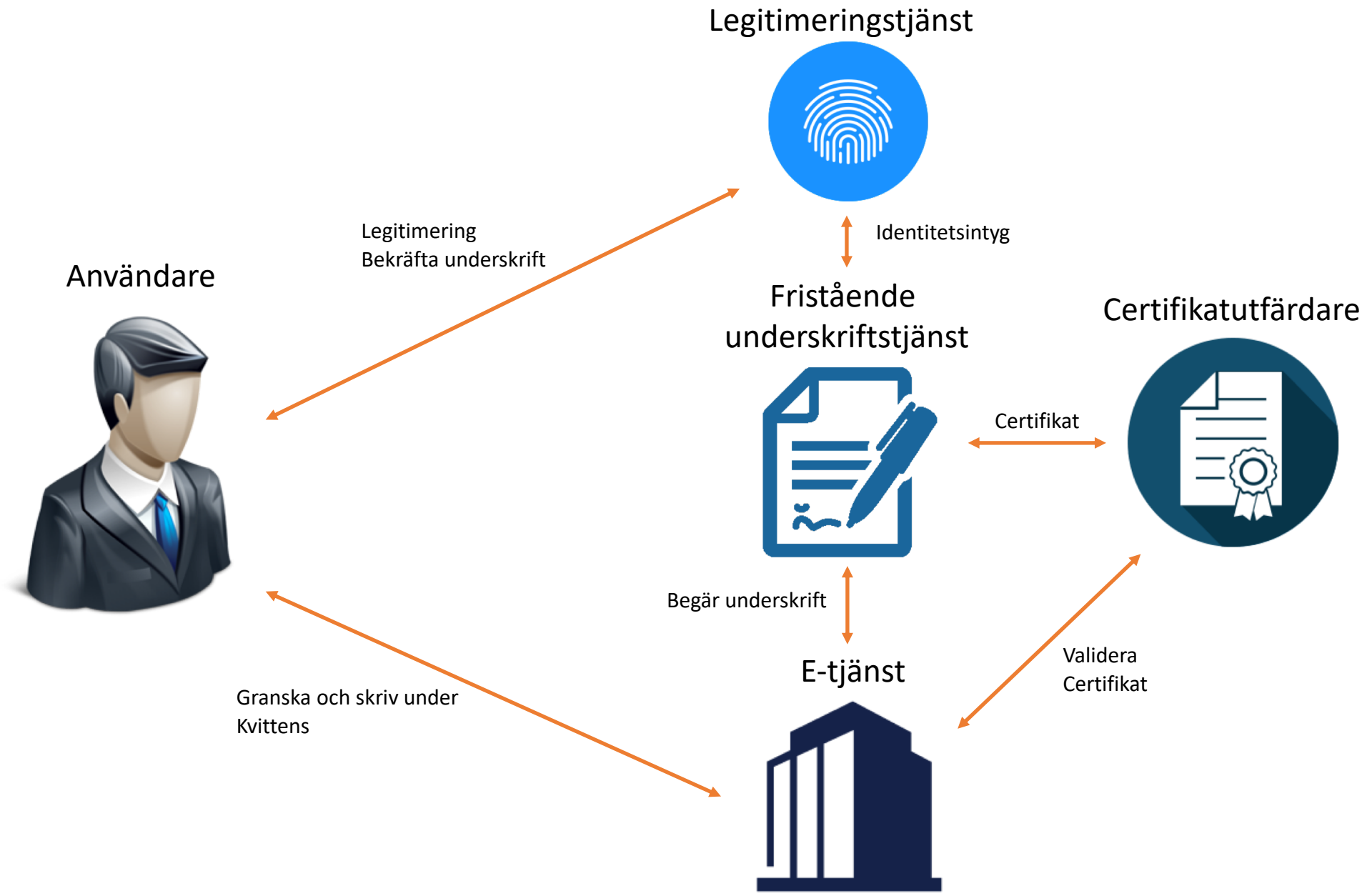
Underskrift – Vad det egentligen är

- Manifestation av ett avtal
- Avtalet är bindande, inte underskriften
- Tekniken är sekundär
  - Handslag / Muntligt
  - Handskriven underskrift
  - Elektronisk underskrift
- Undertecknaren utför en verifierbar handling som manifesterar avsikten att ingå avtal

Ett nytt e-legitimationssystem 2010 - 2020

- Federativ lösning med fristående legitimeringstjänster (Sweden Connect)
- SAML
- Metadata
- Valfrihetssystemet
- Teknikneutral eID
- Tillitsramverk styr
- eID måste inte ha underskriftsfunktion
- Tillkomsten av fristående underskriftstjänst

Fristående underskriftstjänst


Legitimeringstjänst
Användare
Legitimering
Bekräfta underskrift
Identitetsintyg
Fristående
underskriftstjänst
Certifikatutfärdare
Certifikat
Begär underskrift
E-tjänst
Validera
Certifikat
Granska och skriv under
Kvittens

Var lagras underskriftsnyckeln

eID

Underskriftstjänst
Statisk nyckel

Användarens tjänst
Användarens format och trust
Användaren ansvarar för WYSIWYS

Domängräns

Legitimeringstjänst

E-tjänst

Underskriftstjänst
Genererad nyckel

E-tjänstens tjänst
E-tjänstens format och trust
E-tjänsten ansvarar för WYSIWYS

Jämförelse

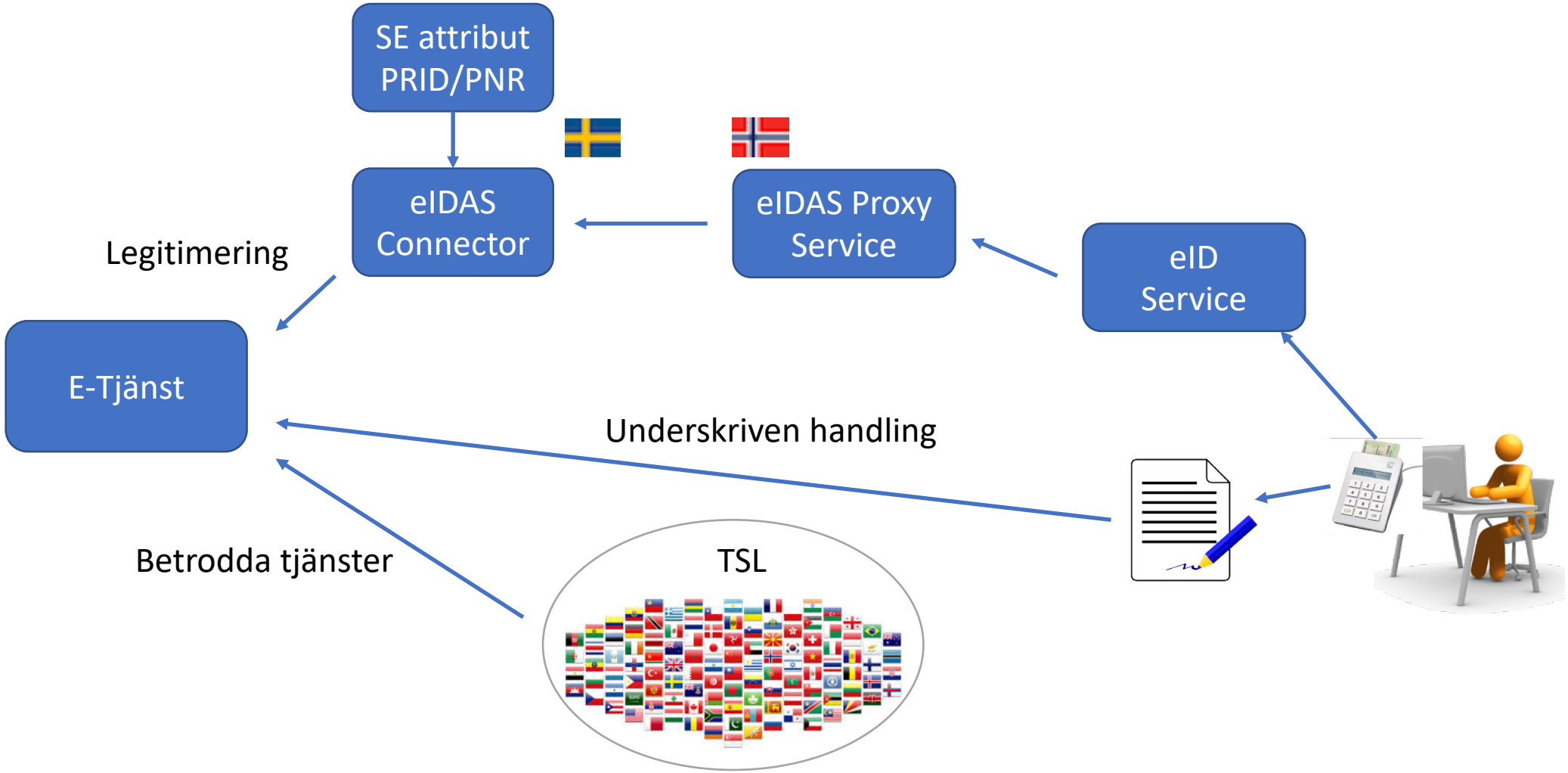
Fristående underskriftstjänst

- E-tjänsten tillhandahåller
- Ny nyckel för varje underskrift
- Nytt certifikat för varje underskrift
- Anpassningsbar identitet
- Ny giltighetstid varje gång
- Automatisk tidsstämpling
- Ingen/liten spärrning
- Valfritt eID

Användarens tjänst/funktion

- Användaren anskaffar
- Statisk nyckel
- Statiskt certifikat
- Statisk identitet
- Certifikatet kan löpa ut snart
- Behöver tidsstämplas
- Omfattande spärrlistor
- Låst till eID

Vem har skrivit under?

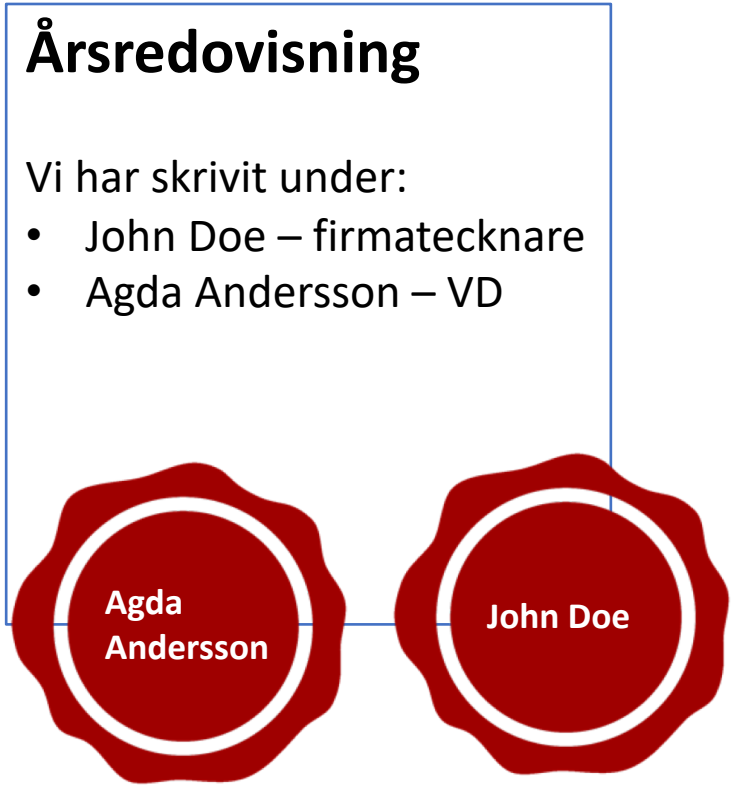


Avancerade elektroniska underskrifter Artikel 26

- Knuten till undertecknaren
- Undertecknaren skall kunna identifieras genom den
- Den ska vara skapad på grundval av uppgifter för skapande av elektroniska underskrifter som undertecknaren med hög grad av tillförlitlighet kan använda uteslutande under sin egen kontroll
- Den ska vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas

Avancerade elektroniska underskrifter Artikel 26

- Vems avancerade underskrift?



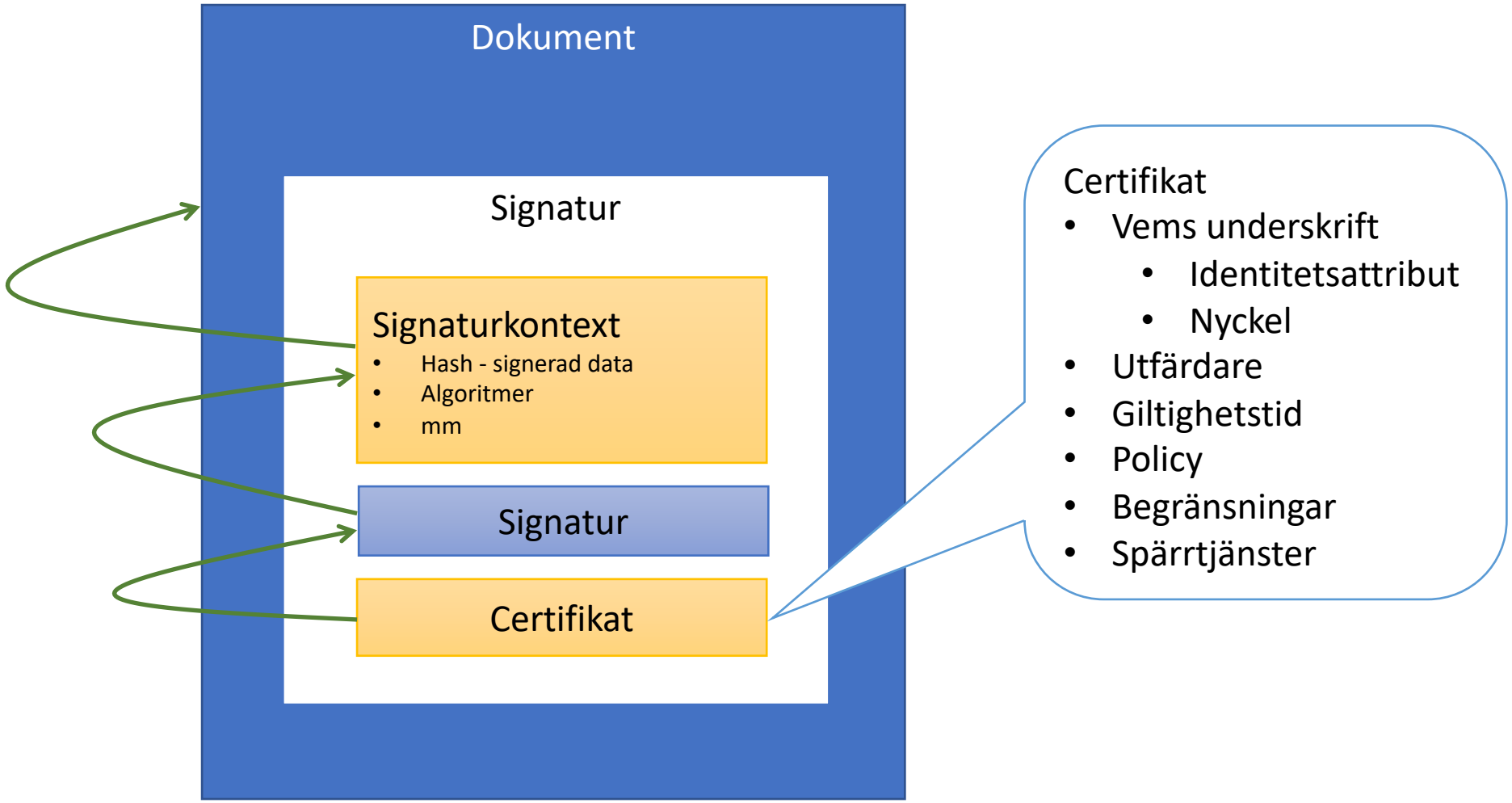
Eller

Fristående underskriftstjänst - sammanfattning

- Skapar undertecknarens avancerade underskrift enligt eIDAS
- E-tjänsten ansvarar för hela underskriftsflödet
  - Användaren accepterar att skriva under med underskriftstjänsten som en del i att man godkänner användande av e-tjänsten
  - Format och betrodda nycklar för verifiering
  - Identitetsinformation som knyts till underskriften
  - Säkerhetsnivå
  - Validering
- Användaren deklarerar avsikt att skriva under i sin e-legitimeringsfunktion

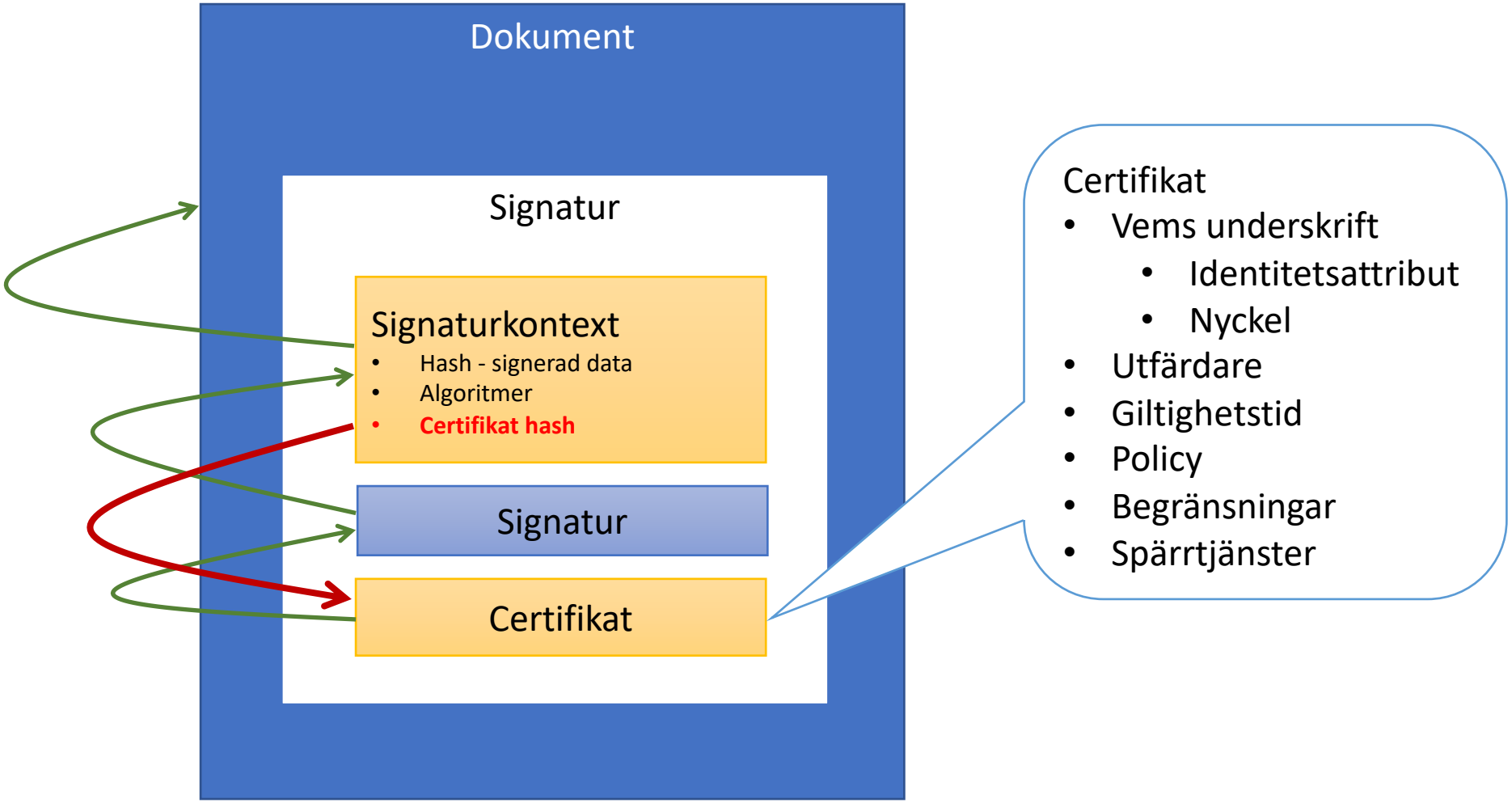
Underskriftformat

Underskriven handling



ETSI formaten för avancerade underskrifter

En tankevurpa



ETSI formaten

- Övertolkning av formulering i signaturdirektivet och eIDAS regleringen
  - **Undertecknaren skall kunna identifieras genom underskriften**
- Sammanblandning mellan identitet och person
  - Samma person har olika identiteter
  - Underskrift knyts till person
  - Handlingen och omständigheterna definierar roll och innebörd
  - Förlitande part bestämmer vem som är trovärdig att intyga vem undertecknaren är

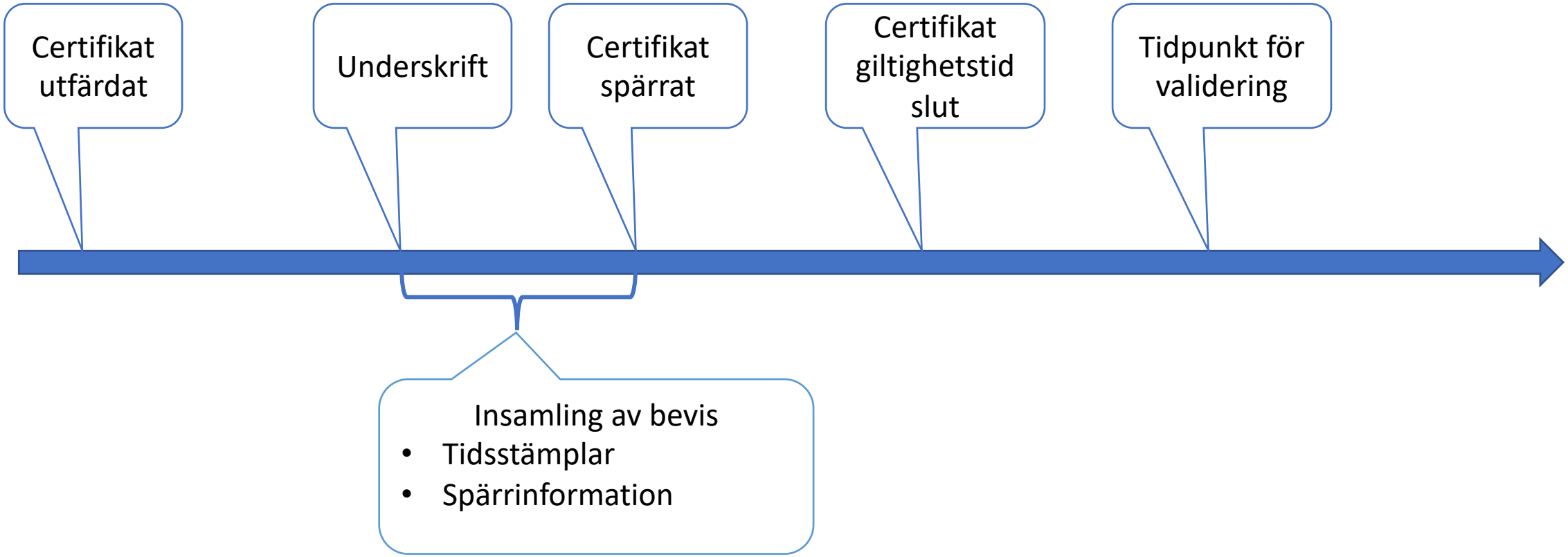
ETSI formaten - konsekvenser

- Krävs av eIDAS
- Resten av världen använder inte formaten, men kan tolerera dom
- ETSI signaturer kan byggas ut för långtidsvalidering
  - Men bara om dom skapats enligt ETSI formaten

- Används när:
  - Dokumenten valideras i andra EU länder
  - Mottagaren kan vilja bygga ut till ETSI långtidsvalideringsformat

Validering

Validering tidsaxel



Signaturvalidering kräver stöd från externt bevismaterial

Under certifikatets giltighetstid:

- Är certifikatet spärrat? Och om spärrat:
  - När spärrades certifikatet?
  - Skapades underskriften innan certifikatet spärrades?

Efter att giltighetstiden löpt ut

- Tidpunkt när underskriften existerade under certifikatets giltighetstid
- Certifikatets spärrstatus vid den tidpunkten

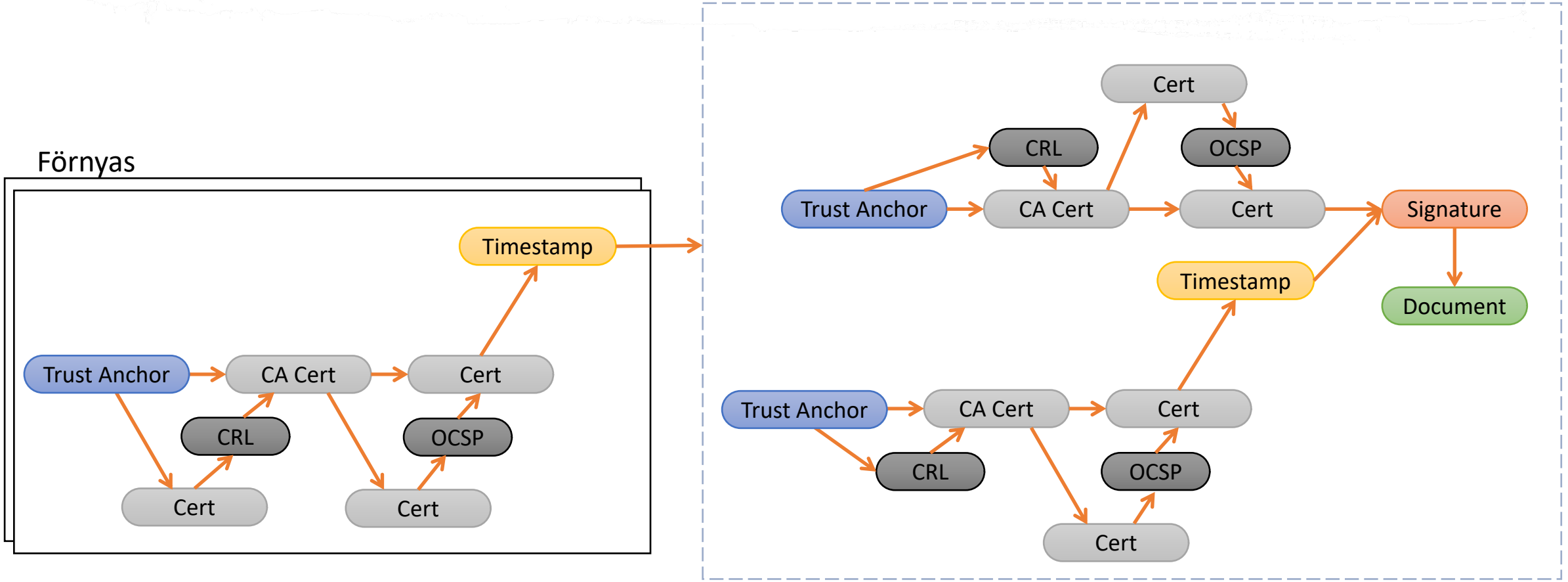
När algoritmer eller nycklar inte längre är säkra

- Tidpunkt när underskriften existerade under certifikatets giltighetstid
- Certifikatets spärrstatus vid den tidpunkten
- Dokumentet som skrevs under (och dess underskrift)
- Alla certifikat som krävs för att validera underskriften
- [Resultat från tidigare validering]

Tidsstämplingsmetoden

R talet för bevisreproduktion

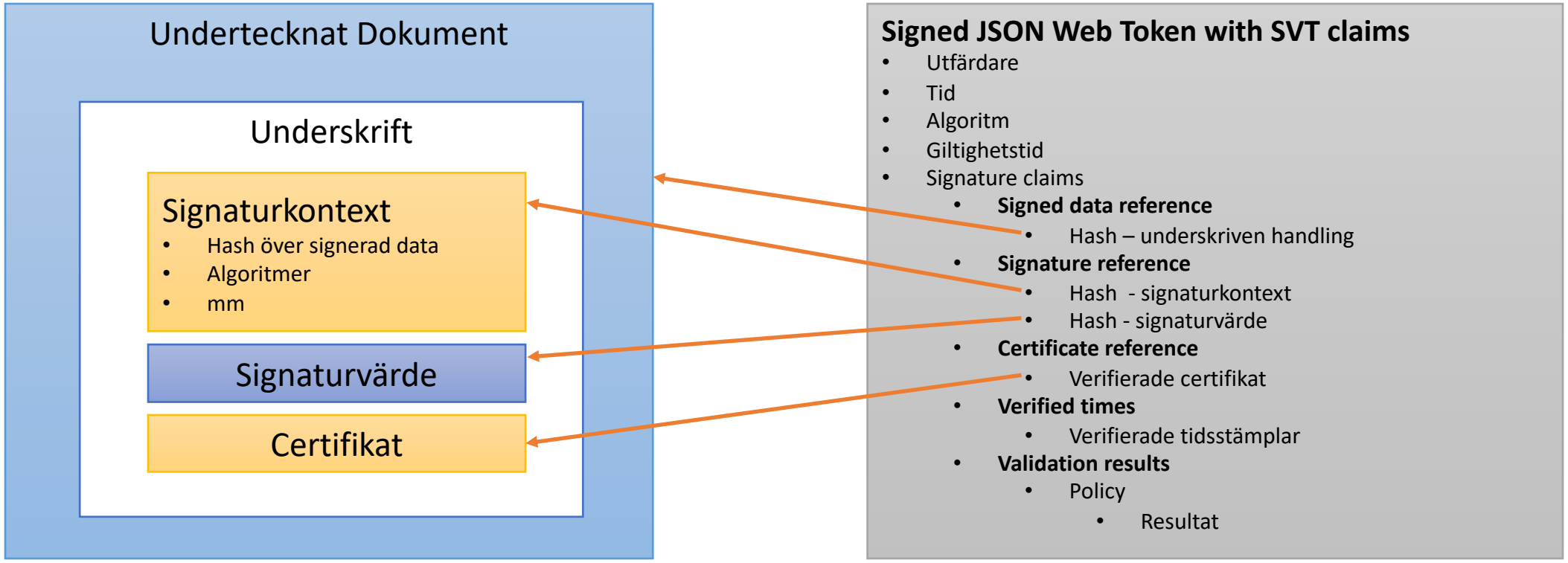
(När varje bevis kräver stöd av mer än 1 nytt bevis)



Valideringsintyg

Ett intyg som ersätter alla bevisfragment i tidsstämplingsmetoden

Valideringsintyg (Signature Validation Token)

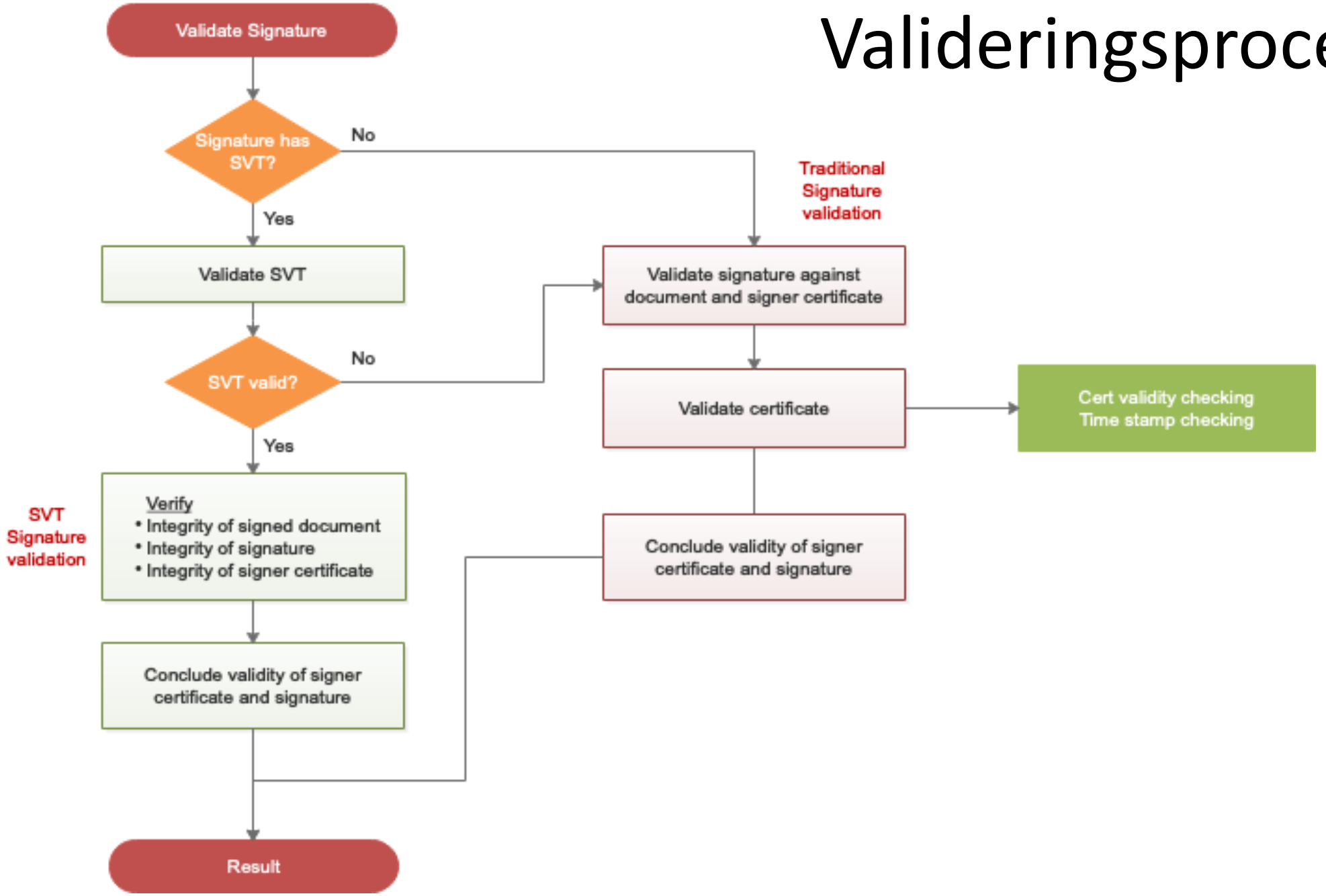


SVT JWT Calims

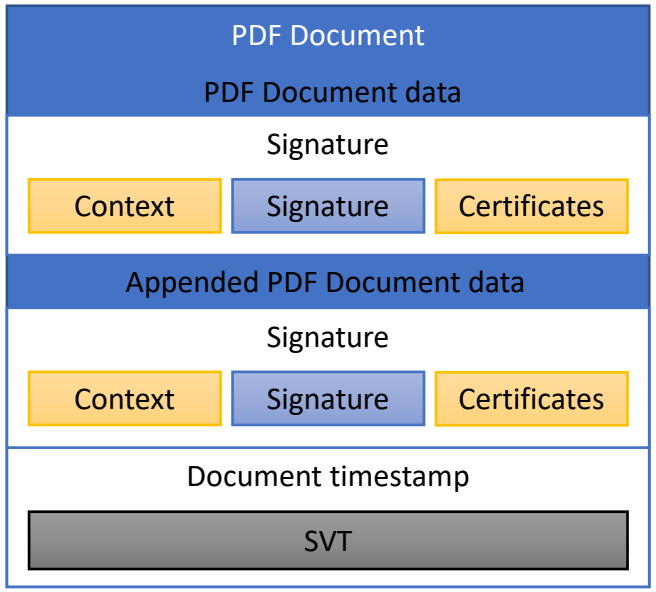
Enkelt kompakt format

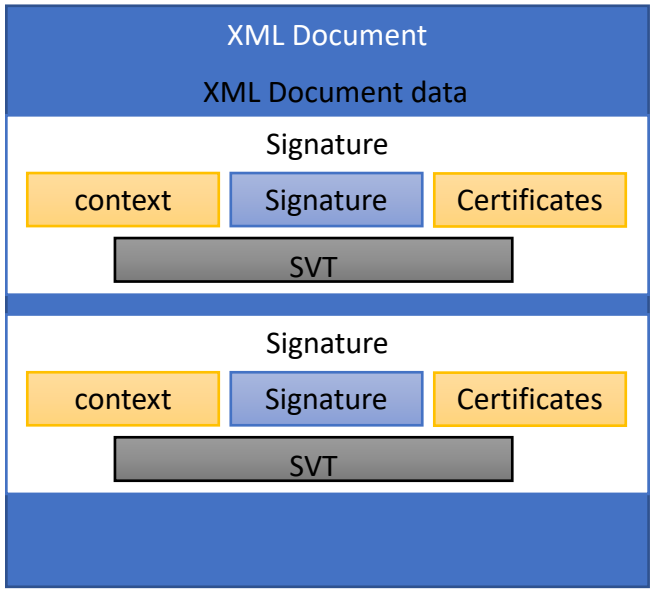

```
{
 "aud" : "http://example.com/audience1",
 "iss" : "https://swedenconnect.se/validator",
 "iat" : 1584703056,
 "jti" : "45d4f765d1f981f7f0c304615ad9491",
 "sig_val_claims" : {
  "sig" : [ {
   "sig_val" : [ {
    "msg" : "Passed basic signature validation",
    "res" : "PASSED",
    "pol" : "http://id.swedenconnect.se/svt/sigval-policy/chain/01"
   } ],
   "sig_ref" : {
    "sig_hash" : "mC0ReA...Vqdw==",
    "sb_hash" : "DNn...aXg=="
   },
   "signer_cert_ref" : {
    "ref" : [ "fIdr...UnoA==" ],
    "type" : "chain_hash"
   },
   "sig_data_ref" : [ {
    "ref" : "0 74697 79699 37821",
    "hash" : "qmIjbB...5ihujvw=="
   } ],
   "time_val" : [ ]
  } ],
  "ver" : "1.0",
  "profile" : "PDF",
  "hash_algo" : "http://www.w3.org/2001/04/xmlenc#sha512"
 }
}
```

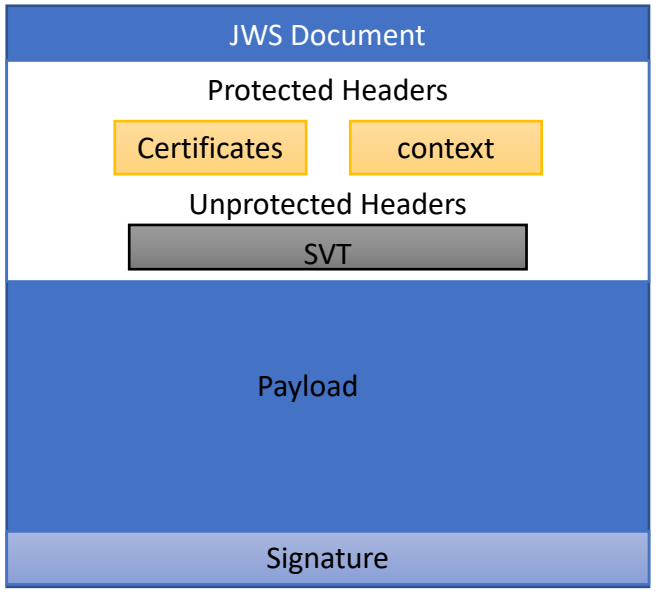
Valideringsprocess



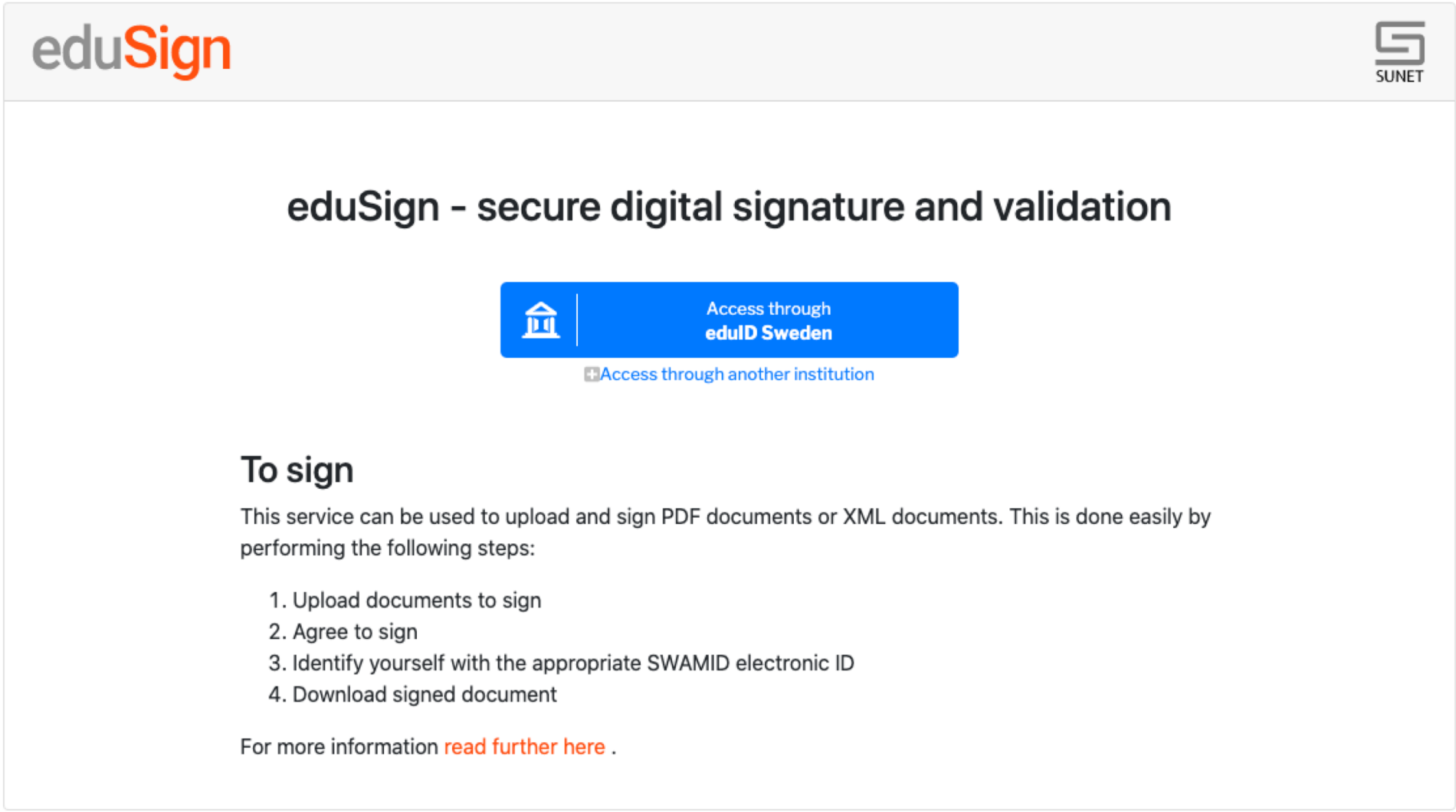
Implementations profiler för PDF, XML, JWS, …







Running Code - In production



Resurser

Nuvarande specifikationer

https://docs.swedenconnect.se/technical-framework/index.html#sigval

IETF drafts

https://github.com/swedenconnect/IETF-SVT

Open Source

SVT library:

- https://github.com/idsec-solutions/sig-validation-svt

Lib för SVT baserad validering och utfärdande av valideringsintyg(Java):

- https://github.com/idsec-solutions/sig-validation-base

eduSign validation service

https://validator.edusign.sunet.se

Frågor