Signature Validation Token

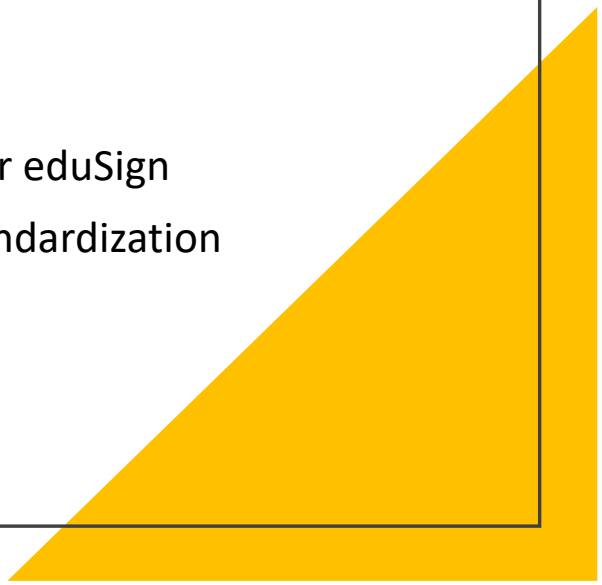
Security Dispatch IETF 109

Stefan Santesson
stefan@aaa-sec.com

Russ Housley
housley@vigilsec.com

Signature Validation Token History

- Swedish government funded research project for Archiviable electronic signatures
- Adopted by the Swedish Agency for Digital Government (DIGG)
- Developed as open source
- Refined and implemented for eduSign
- Approaching the IETF for standardization



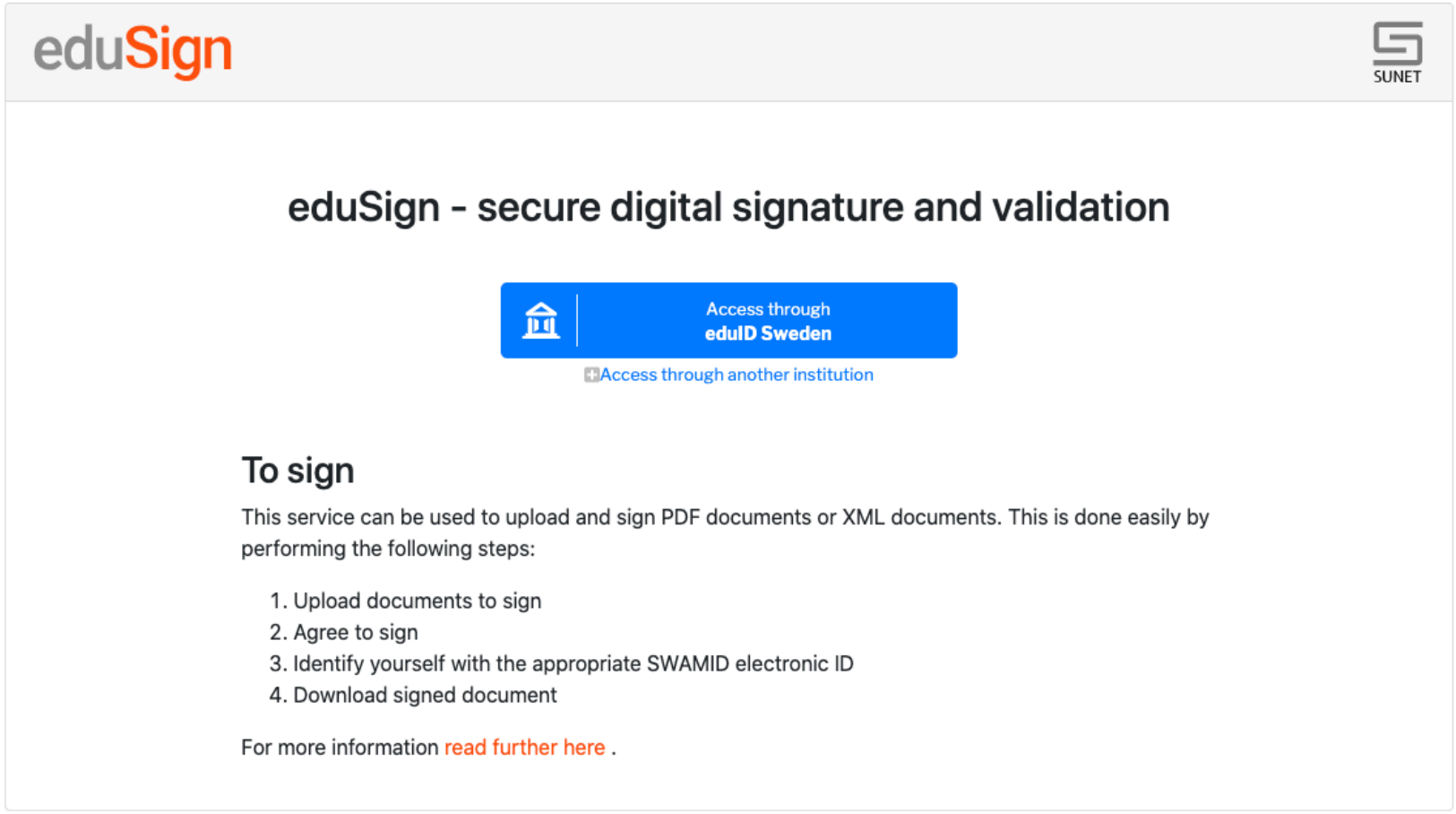
Goal

Simple solution for validating signatures in a distant future

Important requirements

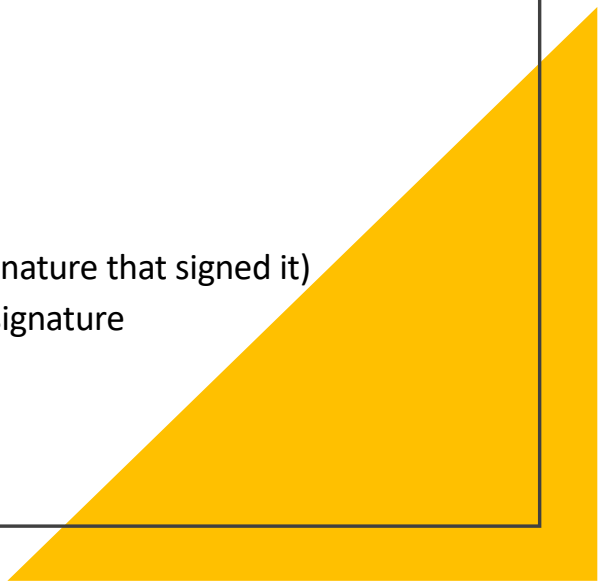
- Predictable outcome of future signature validation
- Avoid cascading evidence collection
- Avoid size explosion
- Avoid repeated storage of large common validation data
- Easy to implement
- Evidence renewal without significant increase of complexity
- Fast verification
- Off-line : Possibility to validate without access to external on-line services
- Compatible with current document parsers and signature validation software.

Running Code - In production



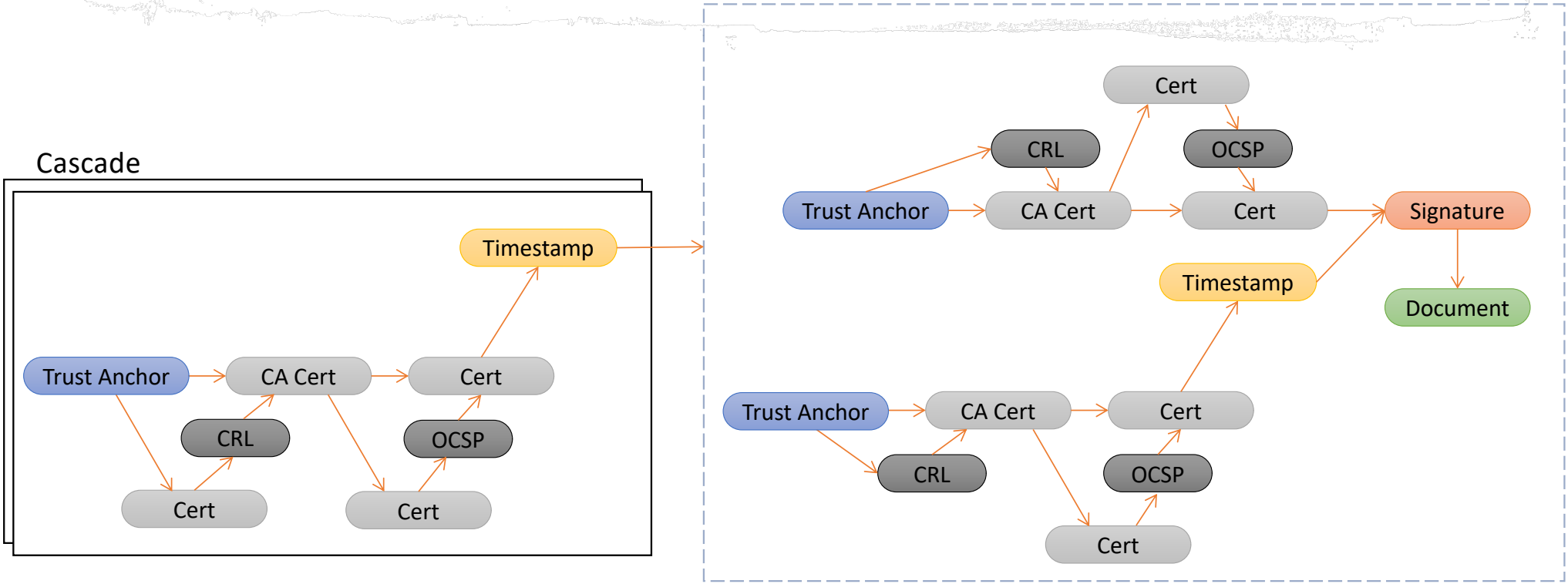
Signature validation requires supporting evidence

- **While signature certificate is valid:**
  - Is certificate revoked? And if revoked:
    - When was certificate revoked?
    - Was signature created before revocation time?
- **After certificate expires:**
  - A time when the signature existed
  - The validity status at that time
- **When algorithms are no longer trusted:**
  - A time when the signature existed
  - The validity status at that time
  - The data that was signed (and the signature that signed it)
  - The certificates used to validate the signature
  - [Results from prior validations]



The R number for evidence reproduction

(When each supporting evidence requires more than one new supporting evidence)

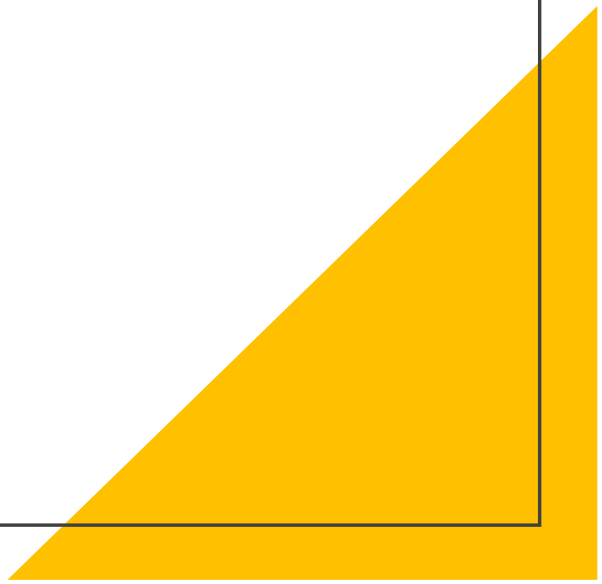


Claim

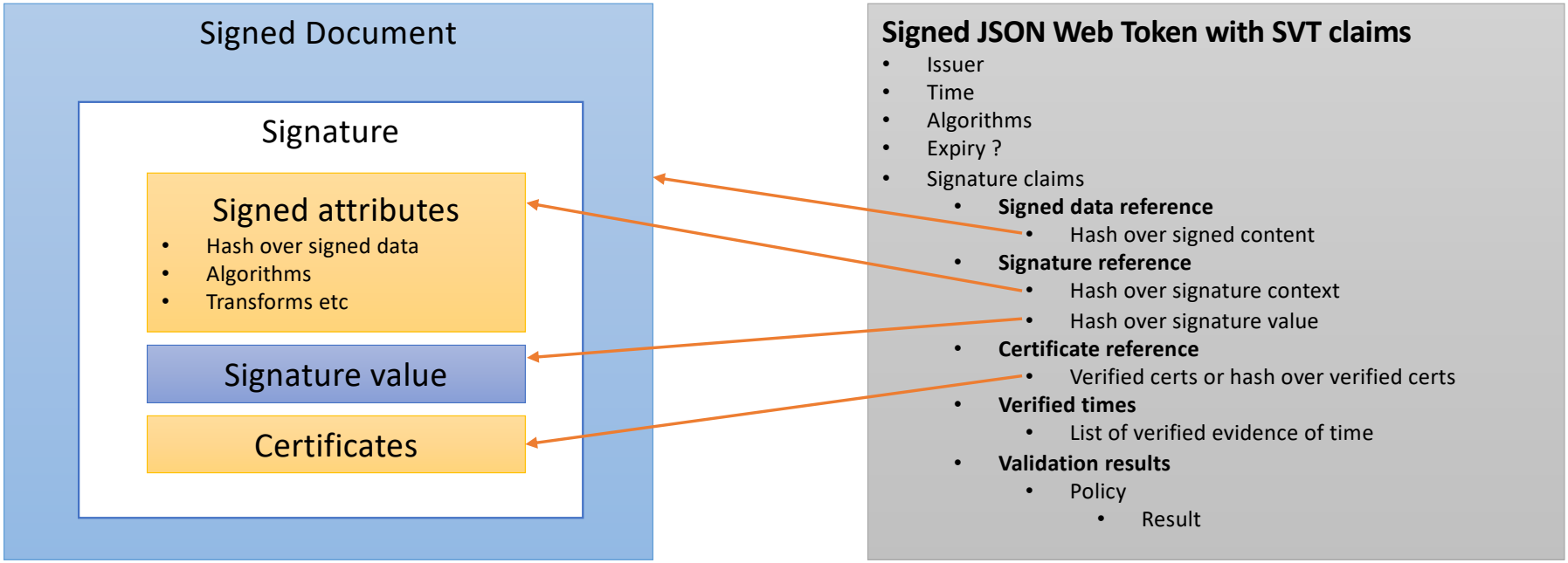
Complexity of long-term signature validation is greatly reduced if we can limit the number of supporting evidence and the evidence R number.

IN FACT….

We can reduce it to one piece of external evidence



Signature Validation Token



SVT JWT Calims

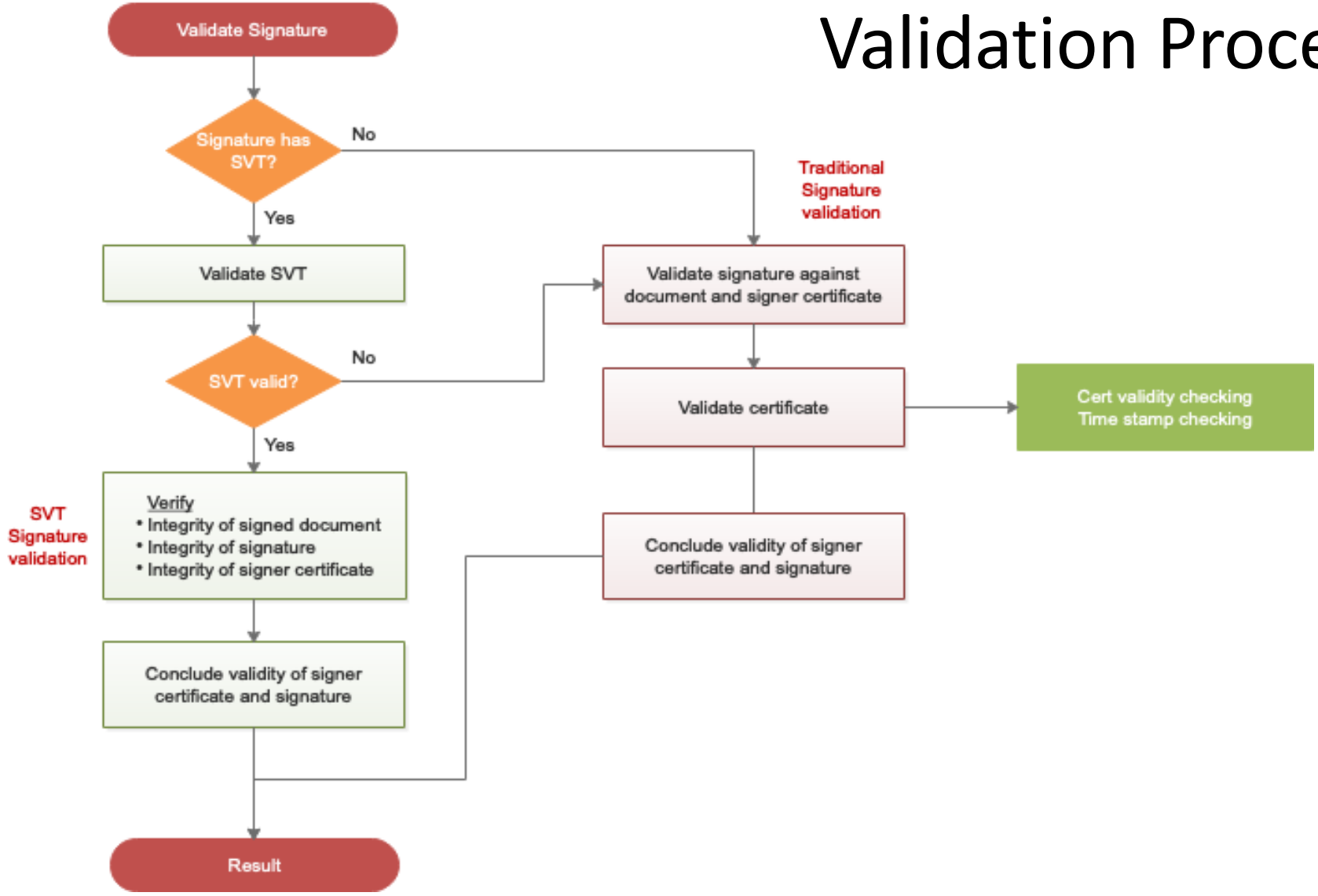
Simple compact format


```
{
 "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"
 }
}
```

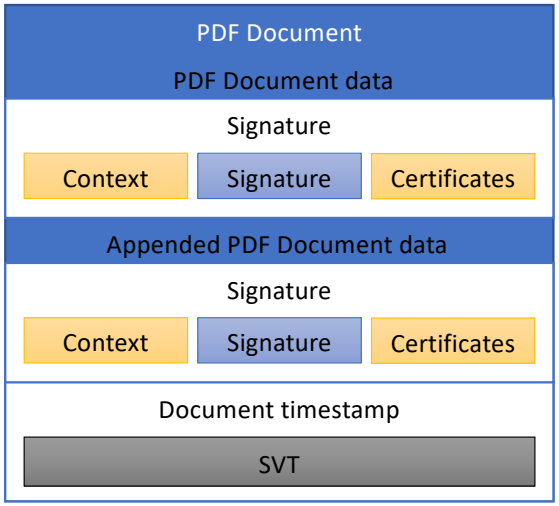
XML SVT example (ECDSA with SHA512)

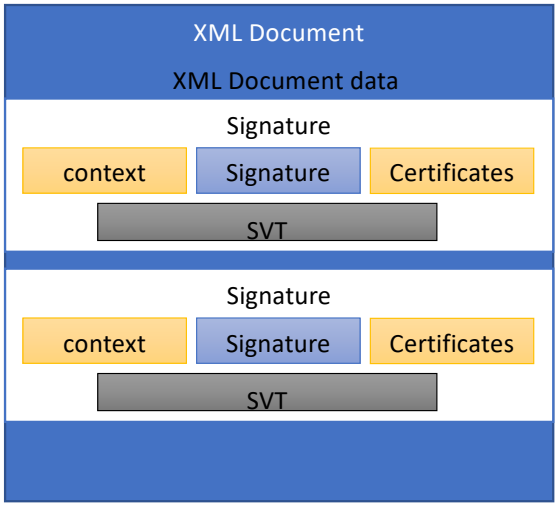
```
<ds:Object>
   <ds:SignatureProperties>
      <ds:SignatureProperty Target="#id-563bcba6778d22b568533aaa4d464e35">
         <svt:SignatureValidationToken xmlns:svt="http://id.swedenconnect.se/svt/1.0/sigprop/ns">
eyJraWQiOiJPZW5JKzQzNEpoYnZmRG50ZlZcLzhyT3hHN0ZrdnlqYUtWSmFWcUlGQlhvaFZoQWU1Zks4YW5vdjFTNjg4cjdLYmFsK2Z2cGFIMWo4aWJnNTJRQnkxUFE9PSI
sInR5cCI6IkpXVCIsImFsZyI6IlJTNTEyIn0.eyJhdWQiOiJodHRwOlwvXC9leGFtcGxlLmNvbVwvYXVkaWVuY2UxIiwiaXNzIjoiaHR0cHM6XC9cL3N3ZWRlbmNvbm5lY3
Quc2VcL3ZhbGlkYXRvciIsImlhdCI6MTYwNTE5OTgyMCwianRpIjoiZjI2MjQ4NWRhNWY3MjMxZjUzZTliNzhiNjRiMzI1ZGYiLCJzaWdfdmFsX2NsYWltcyI6eyJzaWciO
lt7ImV4dCI6bnVsbCwic2lnX3ZhbCI6W3sibXNnIjoiT0siLCJleHQiOm5lbGwsInJlcyI6IlBBU1NFRCIsInBvbCI6Imh0dHA6XC9cL2lkLnN3ZWRlbmNvbm5lY3Quc2Vc
L3N2dFwvc2lndmFsLXBvbGljeVwvdHMtcGtpeFwvMDEifV0sInNpZ19yZWYiOnsic2lnX2hhc2giOiJ3XC9jSVdLb3NBWnRkTFdrS2IxaGM5WWZEYlQzYllPU1hIckFmYUZ
TUEhmaEZFeFVvTUZ3NEs0YUJxT3BZZVhpMTNOZU9CT0NzSG9GaEtiOCtTbHpFNVE9PSIsImlkIjoiaWQtNTYzYmNiYTY3NzhkMjJiNTY4NTMzYWFhNGQ0NjRlMzUiLCJzYl
9oYXNoIjoic3c2OUpzNVZDVjU3YmhkTEp4Q2d5cnh0MnZCbkFDNkY4Z1wvcHI5dWRZRDAxUFNmM3pOWEZmOFFOcENXMjVUbDNyNDd6UnRCSnBCd0drdjNOUlJjcmVnPT0if
Swic2lnbmVyX2NlcnRfcmVmIjp7InJlZiI6WyJsQTVsMjVlK29KVXdlbTlaV2hZUnQ5a1k1T1lKaVB4NEFaa0EzUTd0Mzl0ejcxdlpiaCtEaG1KUWRJS1g3TGVNWEpQWVl4
WHQzRU5mT29SQ2ZXQWc4dz09IiwiXC9UT1h2ZFdcL3ZVYzdDaElFMjk3azdmUm5TdzA5VlpLNk81bGdoTGJmdXpxMWxDSk45T2pQQjlVXC9TbWRtS1dFMXpZZDR0M3FXZ29
STzExelhcL1Z0aitnPT0iLCI1aEJrK2VWY3A5bzZcL2VGS2ZNQzQyWTJ4V3dOZndpcVwvdEtSQlhTSk9aY2J4RUFxeDVvMHRqUW41bUdlTWF0K0cwZHkzQ0RMa1dDSUdYTE
ZjUzhFQlRRPT0iXSwidHlwZSI6ImNoYWluX2hhc2gifSwic2lnX2RhdGFfcmVmIjpbeyJyZWYiOiIiLCJoYXNoIjoiRmNHcE9PZjhpbGNQdDIxR0RkMmNHbkxHRHhSUzVqN
3N2TTRhcHAySDQxZERFTG0yQ3pjZVRZMDJuZGVKZldqaW50bVEzNzZJbFhUT0FyMzF5ell6c2c9PSJ9LHsicmVmIjoiI3hhZGVzLTg1Y2I2MjczOTMzZDQxYzJmZWU4ODYy
ZDJmZjQ5MmNkIiwiaGFzaCI6IllGZ3hwckhTTmhFTjQ2MUlzSjlRM3p1VEYxMmNaaFdrbFFXSmdKMG14TFI5ODNnVmVSOE1rUFByRVwvT1lET0VueWtNU0FPNHIyRHRVbmh
3QllPalgxUT09In1dLCJ0aW1lX3ZhbCI6W119XSwiZXh0IjpudWxsLCJ2ZXIiOiIxLjAiLCJwcm9maWxlIjoiWE1MIiwiaGFzaF9hbGdvIjoiaHR0cDpcL1wvd3d3LnczLm
9yZ1wvMjAwMVwvMDRcL3htbGVuYyNzaGE1MTIifX0.sH273Hi-b1uCSf8RFe4uslfFlktj_GKRBf1DkFKqZv0M-O-cudp4IiCUHH-xF3H1WSOi-VqXhRxFBq6nJG_WxUI4f
ahHoS0I_gYDrsahbQ7ZJvWl7xeVwRhAJ_lb_2oxe4ocEps0P-e8xP4rWFLIbxT5PCZUD18FtI9280arM_pVGPE4YGTlsHELLMzAbk6f-WAzhoaXyLMMzQV3xQVI_uy7qT0-
hVIgKqObUWzu_tlZiLBF5YzHV_bNdaJ_1BJpmdKsVK0Joss99Z-7ez87UwzOCqT-AvrbmCDfvfFwIqK1Iv_GoVMPimHW1SqRE2z0etAkq_b2-SuUNkAJo6yVZRBZAC3QQ2R
XYNPI5IuilH-M6V91-yck-ZI2sSPY4fn4vxVIdTAs7_a4_kARNBGrpp2Zpnm9i9_wq9FGT9FdXdFJ8NaOP3BiuYJpW_fHr81UjqDjfOrkZHcw3JoX-J_S8RcRHBG6AKUm84
Na2g-eBH72MSts-5mOliwHFC6xki_6
         </svt:SignatureValidationToken>
      </ds:SignatureProperty>
   </ds:SignatureProperties>
</ds:Object>
```

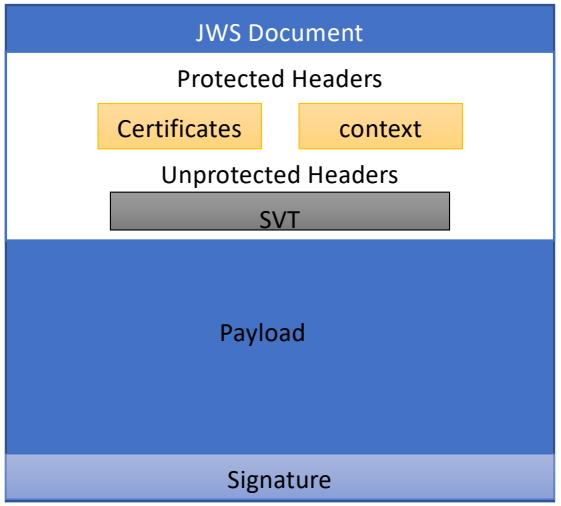
Validation Process



Implementation profiles for PDF, XML, JWS, …







Resources

- Current drafts:
  - https://datatracker.ietf.org/doc/draft-santesson-svt/
  - https://datatracker.ietf.org/doc/draft-santesson-svt-pdf/
  - https://datatracker.ietf.org/doc/draft-santesson-svt-xml/
- IETF Draft development
  - https://github.com/swedenconnect/IETF-SVT
- Open Source
  - Basic SVT library:
    - https://github.com/idsec-solutions/sig-validation-svt
  - Basic library for issuing SVT and signature validation with SVT (Java):
    - https://github.com/idsec-solutions/sig-validation-base
- Test SVT issuing validation service
  - https://sandbox.swedenconnect.se/sigval/

Why IETF?

- Based on the IETF JWT format
- Can support IETF signature formats (CMS, JWS, …)
- No other standards organization is doing this
- IETF has done similar work in the past
- It is a very important subject. Archival of signed electronic documents provide huge cost savings with greatly improved performance.
- We think LAMPS could be a suitable home for this work.

Questions