SURFconext Key rollover

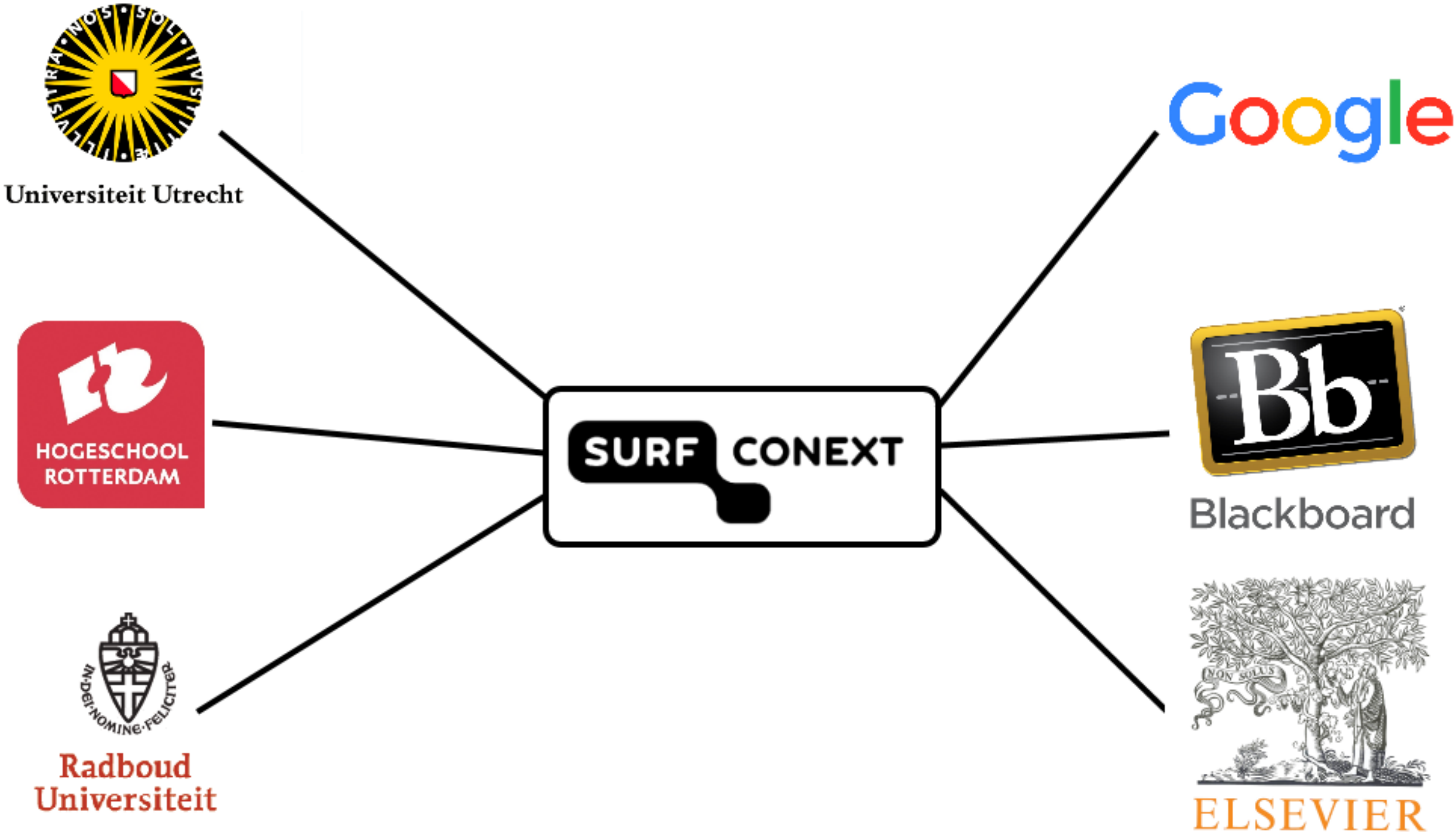
NIEUWE METADATA EN VERIFICATIESLEUTELS VOOR SURFCONEXT

Joost van Dijk

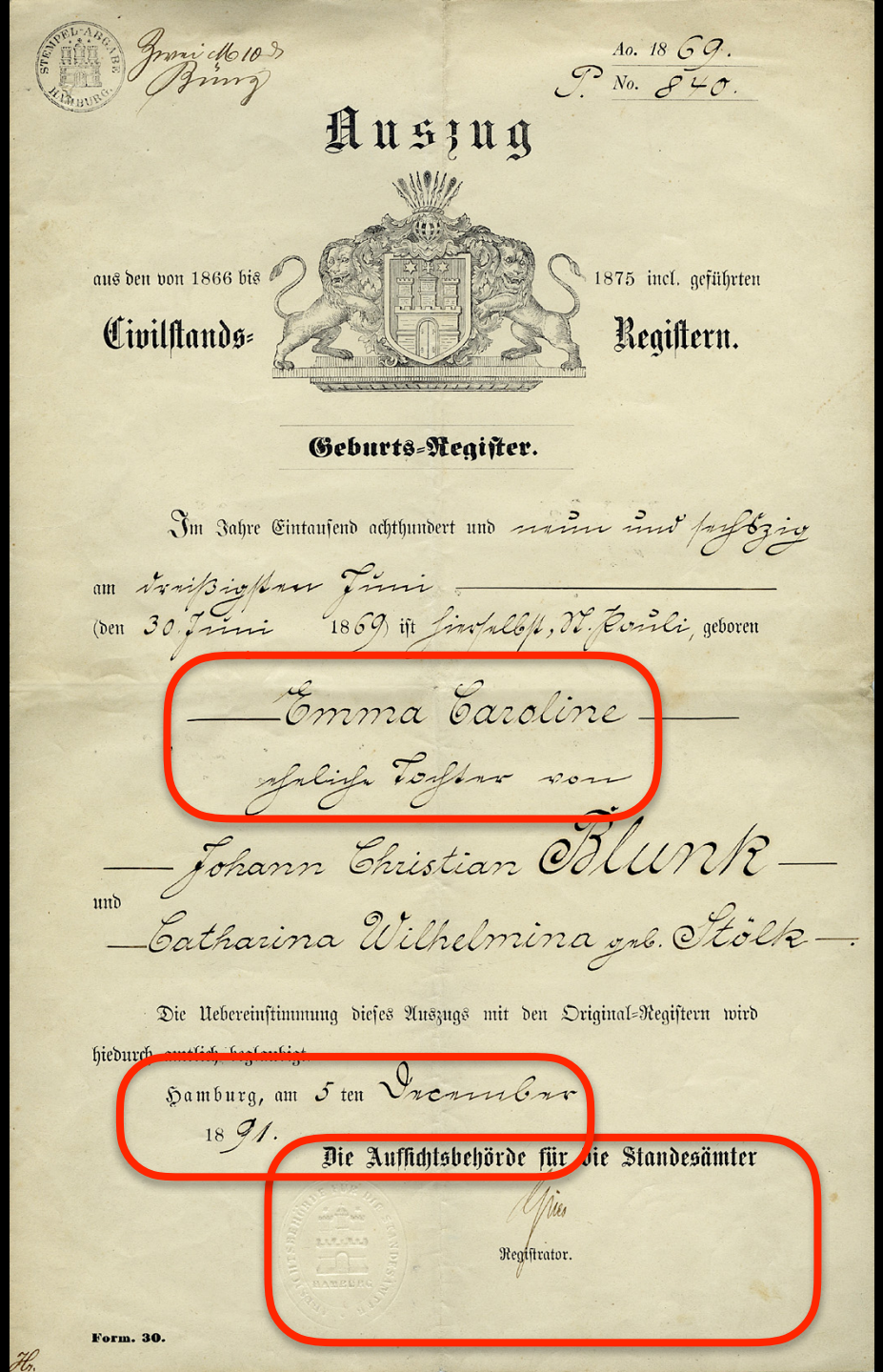
9 april 2019 - What's next @ SURFconext?

Inhoud

- Wat is een key rollover?
- Wat gaat er veranderen?
- Waarom eigenlijk?


Universiteit Utrecht
HOGESCHOOL ROTTERDAM
Radboud Universiteit
SURF CONEXT
Google
Bb
Blackboard
ELSEVIER

SAML assertion anno 1869



Ao. 18 69.
P. No. 840.

Auszug

aus den von 1866 bis 1875 incl. geführten

Civilstands-Registern.

Geburts-Register.

Im Jahre Eintausend achthundert und neun und sechzig

am dreißigsten Juni

(den 30 Juni 1869) ist hierselbst, N. Neuer, geboren

Emma Caroline

ehelige Tochter von

Johann Christian Blunk

und

Catharina Wilhelmina geb. Stölk.

Die Uebereinstimmung dieses Auszugs mit den Original-Registern wird hiedurch amtlich bescheinigt.

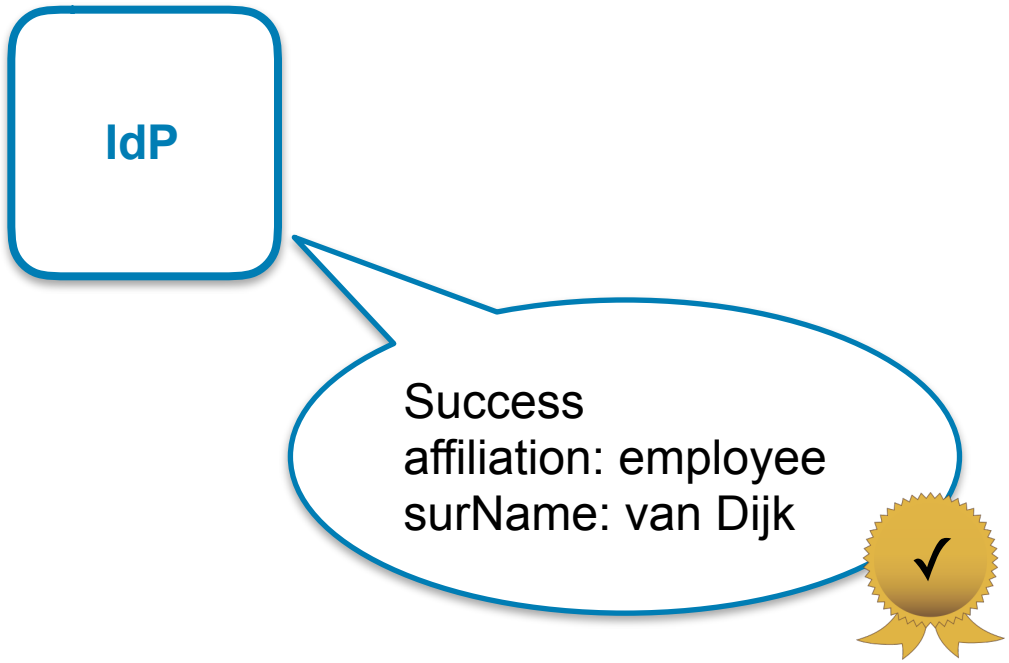
Hamburg, am 5 ten December 1891.

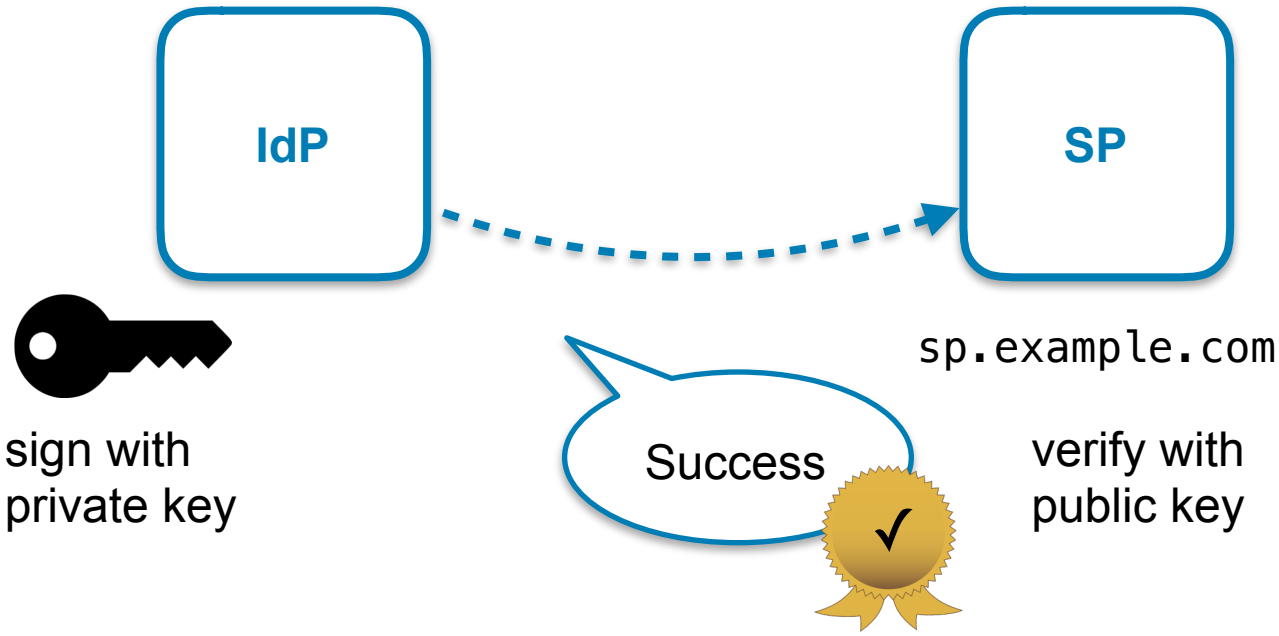
Die Aufsichtsbehörde für die Standesämter

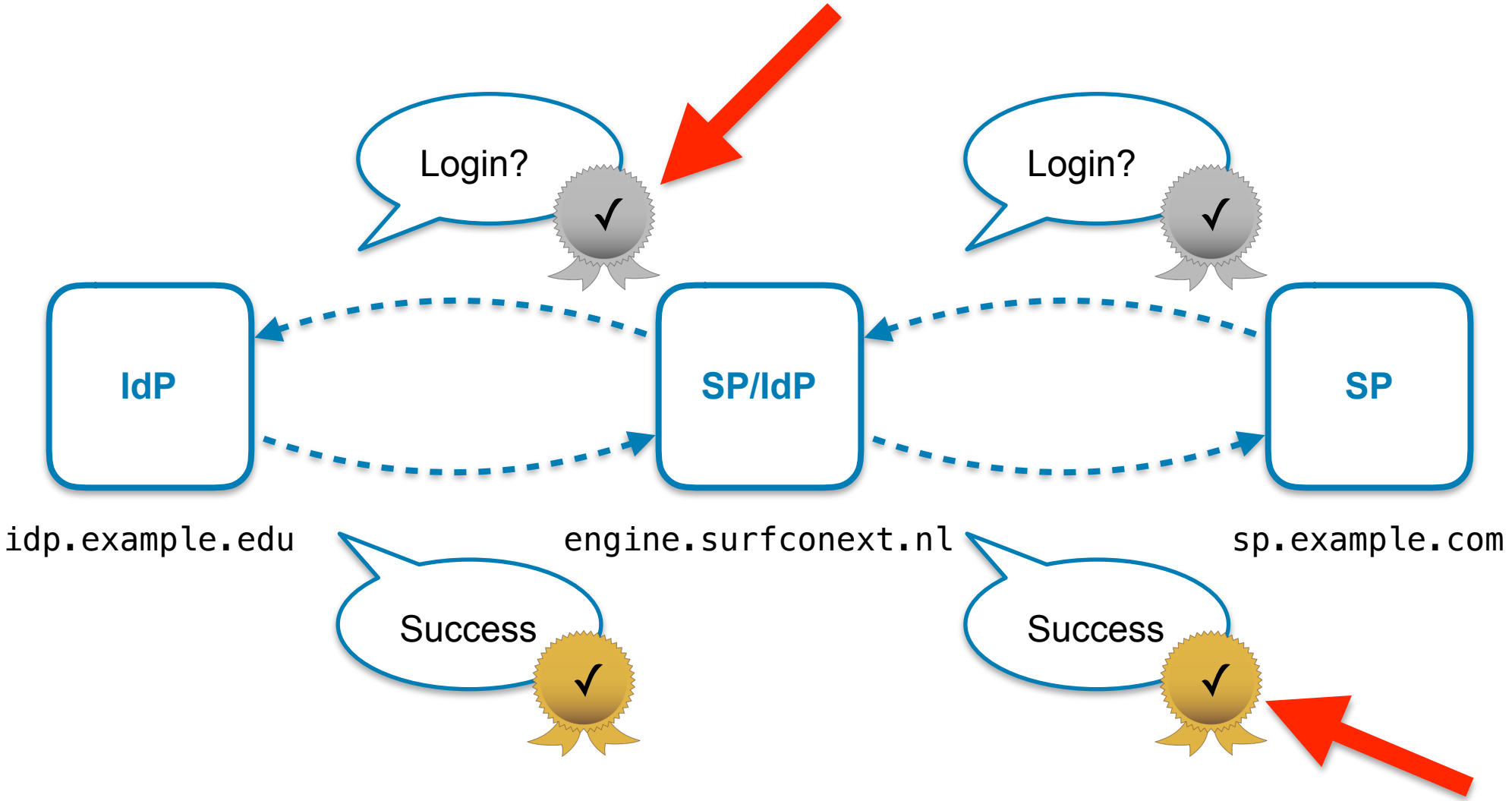
Registrator.

Form. 30.

SAML assertion anno 2019




IdP
SP
sp.example.com
sign with
private key
Success
verify with
public key


Login?
Login?
IdP
SP/IdP
SP
idp.example.edu
engine.surfconext.nl
sp.example.com
Success
Success

Metadata

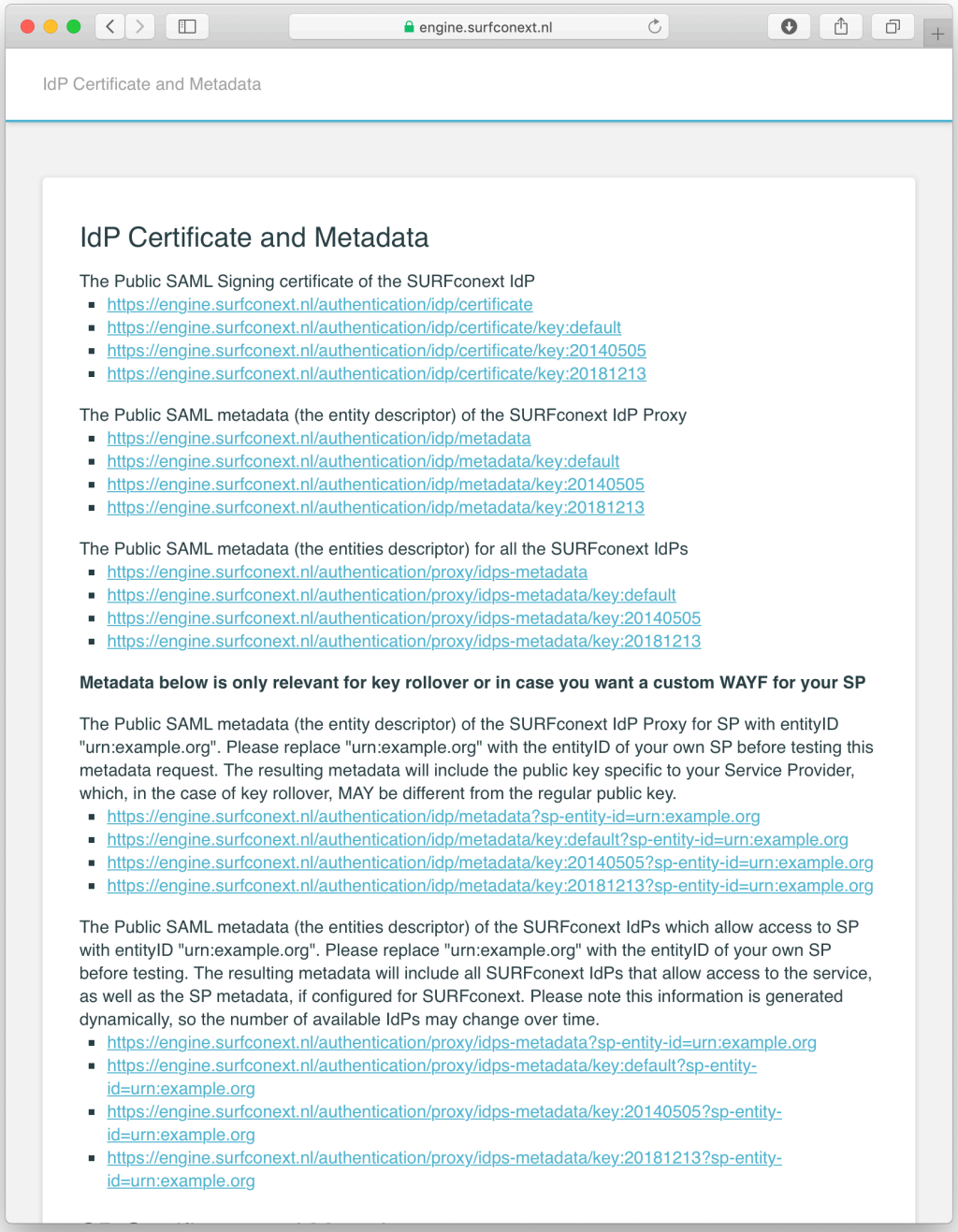
naam: SURFconext

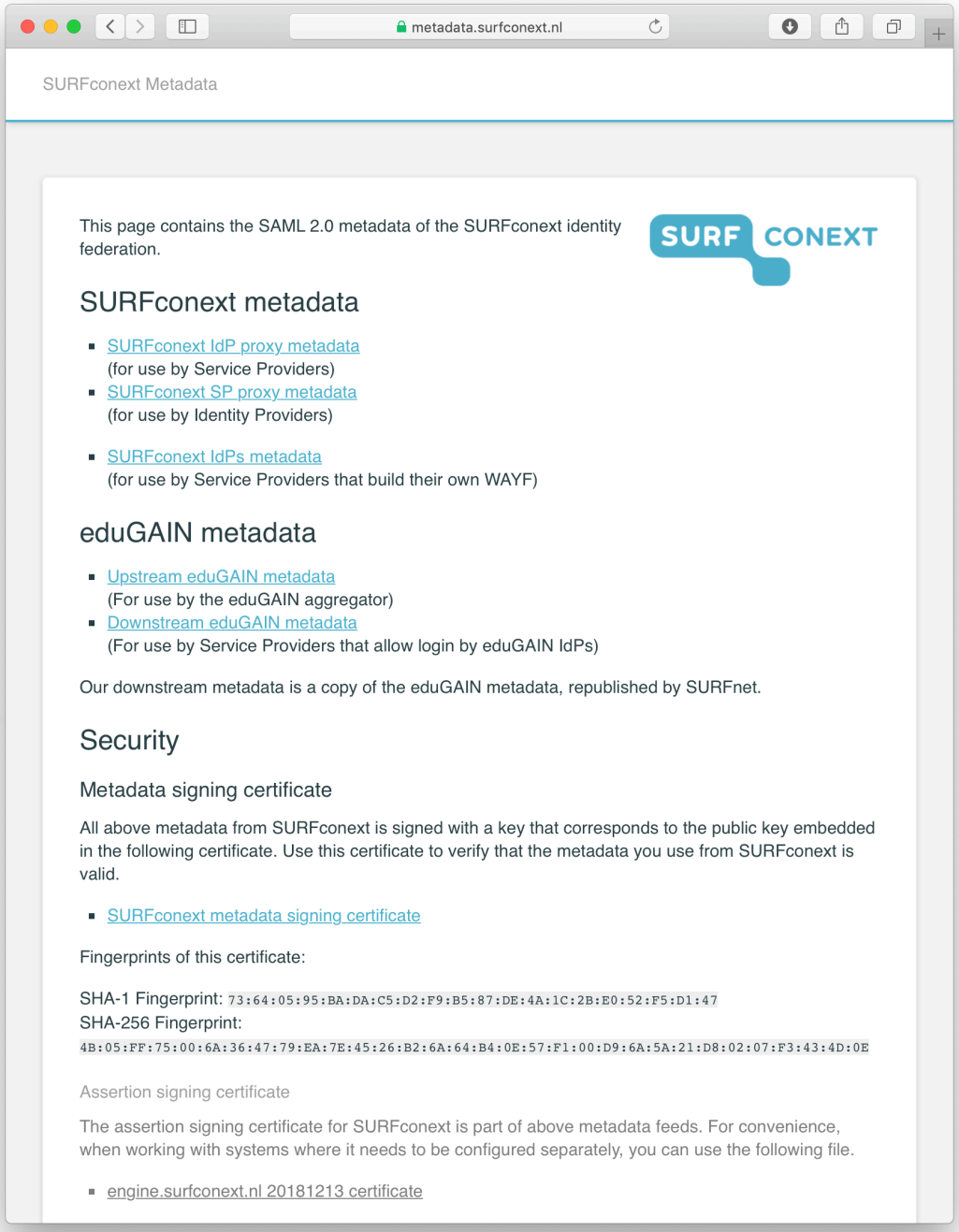
ID: https://engine.surfconext.nl/authentication/idp/metadata

Location: https://engine.surfconext.nl/authentication/idp/single-sign-on/key:20181213

certificaat:

Wat verandert er?





https://engine.surfconext.nl

https://metadata.surfconext.nl

This page contains the SAML 2.0 metadata of the SURFconext identity federation.

SURFconext metadata

- SURFconext IdP proxy metadata
  (for use by Service Providers)
- SURFconext SP proxy metadata
  (for use by Identity Providers)

- SURFconext IdPs metadata
  (for use by Service Providers that build their own WAYF)

eduGAIN metadata

- Upstream eduGAIN metadata
  (For use by the eduGAIN aggregator)
- Downstream eduGAIN metadata
  (For use by Service Providers that allow login by eduGAIN IdPs)

Our downstream metadata is a copy of the eduGAIN metadata, republished by SURFnet.

Security

Metadata signing certificate

All above metadata from SURFconext is signed with a key that corresponds to the public key embedded in the following certificate. Use this certificate to verify that the metadata you use from SURFconext is valid.

- SURFconext metadata signing certificate

Fingerprints of this certificate:

SHA-1 Fingerprint: `73:64:05:95:BA:DA:C5:D2:F9:B5:87:DE:4A:1C:2B:E0:52:F5:D1:47`
SHA-256 Fingerprint: `4B:05:FF:75:00:6A:36:47:79:EA:7E:45:26:B2:6A:64:B4:0E:57:F1:00:D9:6A:5A:21:D8:02:07:F3:43:4D:0E`

Assertion signing certificate

The assertion signing certificate for SURFconext is part of above metadata feeds. For convenience, when working with systems where it needs to be configured separately, you can use the following file.

engine.surfconext.nl 20140505

Subject Name
- Country or Region NL
- County Utrecht
- Locality Utrecht
- Organisation SURFnet B.V.
- Organisational Unit SURFconext
- Common Name engine.surfconext.nl 20140505

Issuer Name
- Country or Region NL
- County Utrecht
- Locality Utrecht
- Organisation SURFnet B.V.
- Organisational Unit SURFconext
- Common Name engine.surfconext.nl 20140505

Serial Number 00 C5 42 F7 19 F5 65 FB 2E
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
- Parameters None

Not Valid Before Monday, 5 May 2014 at 16:22:35 Central European Summer Time
Not Valid After Sunday, 5 May 2019 at 16:22:35 Central European Summer Time

Public Key Info
- Algorithm RSA Encryption (1.2.840.113549.1.1.1)
- Parameters None
- Public Key 256 bytes: AB 61 30 36 C1 D2 32 87 ...
- Exponent 65537
- Key Size 2.048 bits
- Key Usage Any

Signature 256 bytes: 2F 0B F4 3E BB 0B 12 21 ...

engine.surfconext.nl 20181213

Subject Name
- Country or Region NL
- County Utrecht
- Locality Utrecht
- Organisation SURFnet B.V.
- Organisational Unit SURFconext
- Common Name engine.surfconext.nl 20181213

Issuer Name
- Country or Region NL
- County Utrecht
- Locality Utrecht
- Organisation SURFnet B.V.
- Organisational Unit SURFconext
- Common Name engine.surfconext.nl 20181213

Serial Number 00 88 0C AA 73 18 67 EB 7A
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
- Parameters None

Not Valid Before Thursday, 13 December 2018 at 16:29:20 Central European Standard Time
Not Valid After Wednesday, 13 December 2023 at 16:29:20 Central European Standard Time

Public Key Info
- Algorithm RSA Encryption (1.2.840.113549.1.1.1)
- Parameters None
- Public Key 256 bytes: B3 CE 19 2F 9F 04 44 5F ...
- Exponent 65537
- Key Size 2.048 bits
- Key Usage Verify

Signature 256 bytes: 57 87 99 7C BB E9 DC 3D ...

engine.surfconext.nl 20140505

Subject Name
- Country or Region NL
- County Utrecht
- Locality Utrecht
- Organisation SURFnet B.V.
- Organisational Unit SURFconext
- Common Name engine.surfconext.nl 20140505

Issuer Name
- Country or Region NL
- County Utrecht
- Locality Utrecht
- Organisation SURFnet B.V.
- Organisational Unit SURFconext
- Common Name engine.surfconext.nl 20140505

Serial Number 00 C5 42 F7 19 F5 65 FB 2E
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
- Parameters None

Not Valid Before Monday, 5 May 2014 at 16:22:35 Central European Summer Time
Not Valid After Sunday, 5 May 2019 at 16:22:35 Central European Summer Time

Public Key Info
- Algorithm RSA Encryption (1.2.840.113549.1.1.1)
- Parameters None
- Public Key 256 bytes: AB 61 30 36 C1 D2 32 87 ...
- Exponent 65537
- Key Size 2.048 bits
- Key Usage Any

Signature 256 bytes: 2F 0B F4 3E BB 0B 12 21 ...

SURFconext metadata signer

Issuer Name
- Country or Region NL
- Organisation SURFnet
- Common Name SURFconext Root CA

Serial Number 6D 76 C3 A4 2A 6B 26 00 5A 7B 71 0C DE 7D 75 4D
Version 1
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
- Parameters None

Subject Name
- Country or Region NL
- County Utrecht
- Organisation SURFnet
- Organisational Unit SURFconext
- Common Name SURFconext metadata signer

Not Valid Before Monday, 14 January 2019 at 17:39:05 Central European Standard Time
Not Valid After Thursday, 18 January 2024 at 17:39:05 Central European Standard Time

Public Key Info
- Algorithm RSA Encryption (1.2.840.113549.1.1.1)
- Parameters None
- Public Key 256 bytes: C7 24 17 2A 97 CD 6E DD ...
- Exponent 65537
- Key Size 2.048 bits
- Key Usage Any

Signature 512 bytes: 8E F2 57 5E 4C 4E AA 1D ...

Waarom eigenlijk?

engine.surfconext.nl 20140505

Subject Name
- Country or Region NL
- County Utrecht
- Locality Utrecht
- Organisation SURFnet B.V.
- Organisational Unit SURFconext
- Common Name engine.surfconext.nl 20140505

Issuer Name
- Country or Region NL
- County Utrecht
- Locality Utrecht
- Organisation SURFnet B.V.
- Organisational Unit SURFconext
- Common Name engine.surfconext.nl 20140505

Serial Number 00 C5 42 F7 19 F5 65 FB 2E
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
- Parameters None

Not Valid Before Monday, 5 May 2014 at 16:22:35 Central European Summer Time
Not Valid After Sunday, 5 May 2019 at 16:22:35 Central European Summer Time

Public Key Info
- Algorithm RSA Encryption (1.2.840.113549.1.1.1)
- Parameters None
- Public Key 256 bytes: AB 61 30 36 C1 D2 32 87 ...
- Exponent 65537
- Key Size 2.048 bits
- Key Usage Any

Signature 256 bytes: 2F 0B F4 3E BB 0B 12 21 ...

CVE-2014-0160

Leena Snidate / Codenomicon [CC0]


CryptoServer Se-Series Gen2
Mode: Operational OK Temp.: 27,0 °C
Trans./min.: 13 Clients: 0
Load: 0 %
EXIT
OK
USB Host
USB CS
utimaco
CryptoServer Se-Series Gen2
Mode: Operational OK Temp.: 29,2 °C
Trans./min.: 0 Clients: 0
Load: 0 %
EXIT
OK
USB Host
USB CS
utimaco
Luna SA
SafeNet

Samengevat

- Nieuwe Assertion Signing key
  - Geldig tot 18 december 2024
- Nieuwe metadata locatie
  - metadata.surfnet.nl
- Nieuwe Metadata Signing key
  - opgeslagen in HSM
  - Ieder uur ververst
  - Certificaat uitgegeven door offline root
- Deadline voor migratie: **1 Mei 2019**
- Documentatie: https://edu.nl/keyrollover

Joost.vanDijk@surfnet.nl

@joostd

joostd@hotmail.com

https://www.linkedin.com/in/joostd/

SURF NET