

# SURF secure ID(P)

EEN VEILIGE IDP: BEST BELANGRIJK



Thijs Kinkhorst

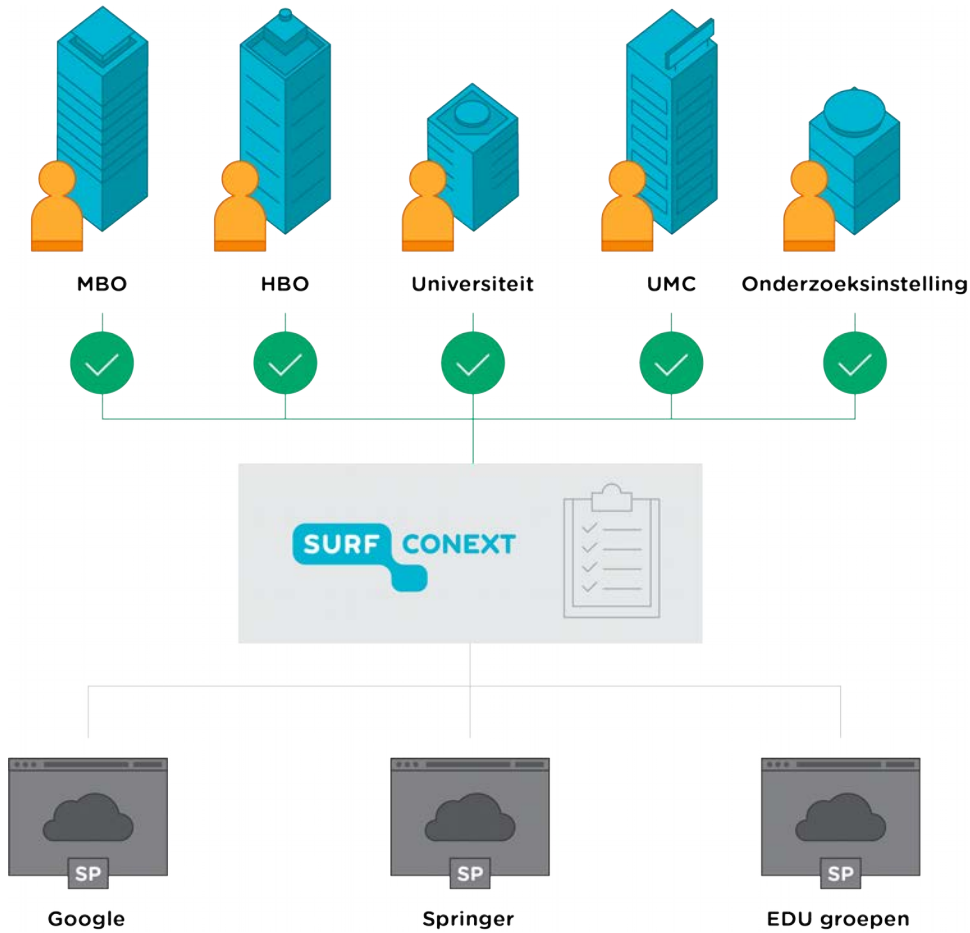


# Even voorstellen

- Thijs Kinkhorst
- Technisch Product Manager SURFconext & kernel-lid SURFcert

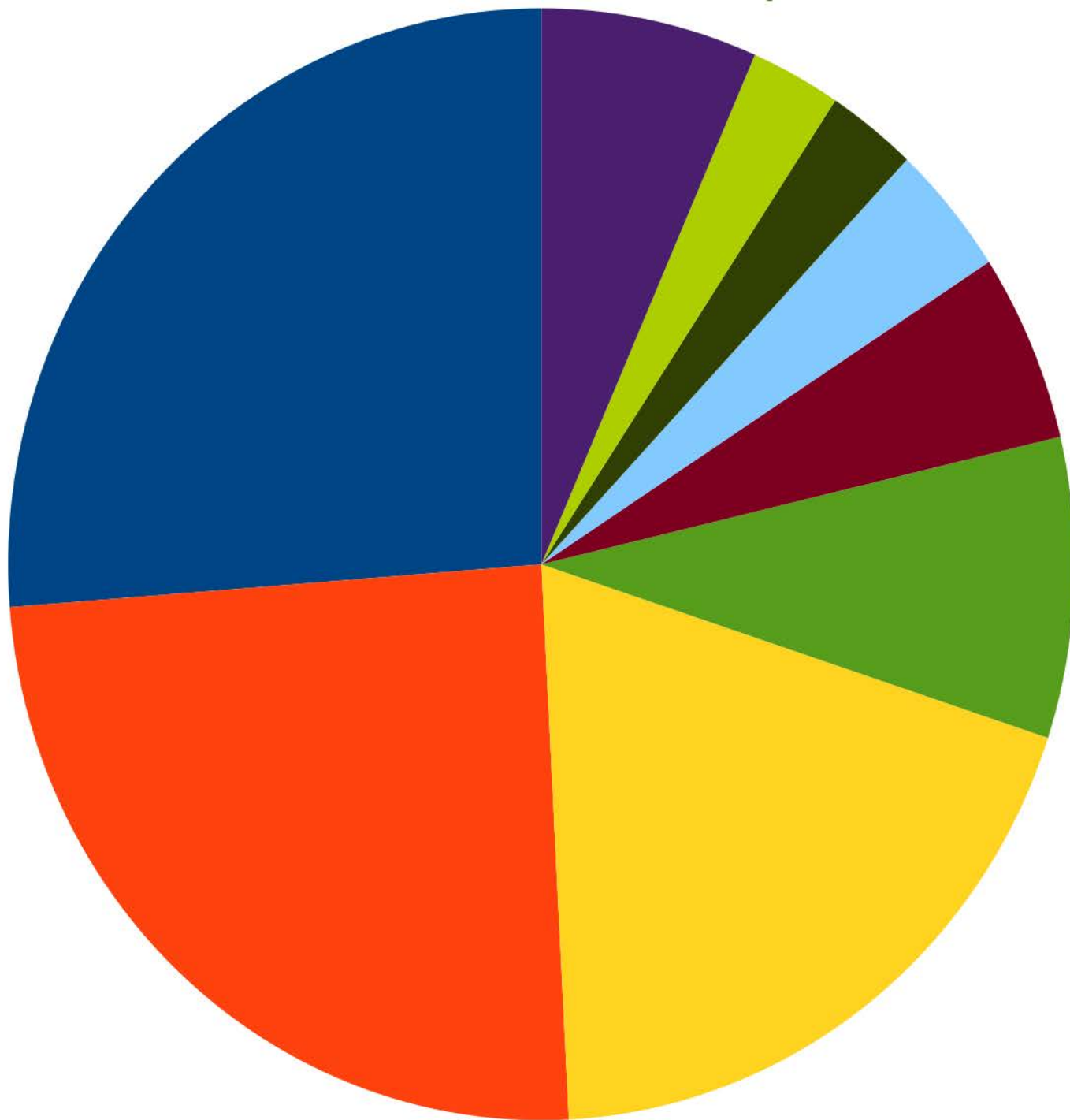


# De Identity Provider: basis van het federatievertrouwen



# Identity Providers in SURFconext

191































































































































































- Researchinstellingen
- BVE-instellingen
- HBO-instellingen
- Universiteiten
- Ziekenhuizen
- Klant SURFconext
- Bibliotheken
- Overig Hoger Onderwijs
- Overige

# Identity Providers in SURFconext

#	%	Product
130	69%	MS ADFS
33	17%	SimpleSAMLphp
11	6%	NetIQ/Novell AM
5	3%	Oracle AM / OpenSSO
3	2%	Shibboleth
1	1%	Google

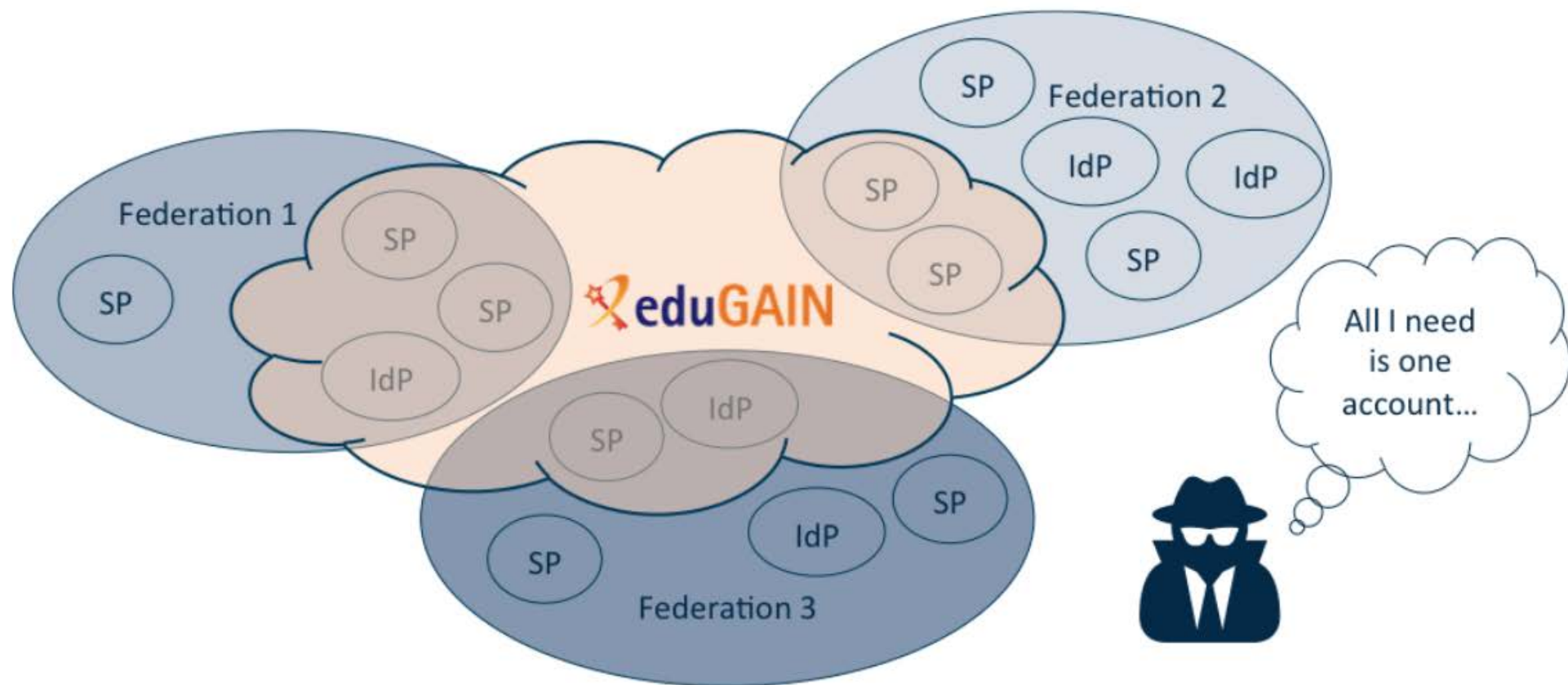
#	%	Product
1	1%	Onegini
1	1%	Mujina
1	1%	OpenConext
1	1%	OpenASelect
1	1%	Overig
1	1%	CAS

 Academisch Medisch Centrum	 Hogeschool Tio	 Meertens Instituut (KNAW)	 Politeiaacademie	 Sociaal en Cultureel Planbureau	 Universiteit van Tilburg
 Academisch Ziekenhuis Maastricht	 Hogeschool Utrecht	 MefrogGroup Nederland	 Radboud Universiteit	 Social ID   Oregon	 Universiteit voor Humanistiek
 Aeres Groep - Vliertum	 Hogeschool van Amsterdam	 Ministerie van Defensie - NLDA	 Radboudumc	 SOMT University (Stichting Opleidingen Musculoskeletale Therapie)	 University of Curaçao
 AMOLF	 Hogeschool van Arnhem en Nijmegen	 Naturalis Biodiversity Center	 Rathenau Instituut (KNAW)	 SRON Netherlands Institute for Space Research	 Viaa Gereformeerde Hogeschool Zwolle
 Amphia Ziekenhuis	 Hogeschool Van Hall Larenstein	 rboi biblio	 Rijksinstituut voor Volksgezondheid en Milieu	 STC Group	 Vrije Universiteit Amsterdam
 Amsterdamsche Hogeschool voor de Kunsten	 HKU Hogeschool voor de Kunsten Utrecht	 Nederlands Herseninstituut (KNAW)	 Rijksmuseum Amsterdam	 STC Group - Edu	 VUmc medisch centrum
 Antoni van Leeuwenhoek - Nederlands Kanker Instituut	 Hogeschool Windesheim	 Nederlands Instituut voor Ecologie NIOO (KNAW)	 Rijksuniversiteit Groningen	 Stenden Hogeschool	 Wageningen University & Research (WUR)
 ArEZ Hogeschool voor de Kunsten	 Hogeschool The Hague	 Nederlands Instituut voor onderzoek van de gezondheidszorg (NIVEL)	 rijkslijst	 Stichting Kennisnet	 Wellantcollege
 ASTRON	 Hubrecht Institute (KNAW)	 Nederlands Interdisciplinair Demografisch Instituut (KNAW)	 ROC Abcde College	 Stichting Landstede (LandstedeMBO, Menso Afling, Thomas a Kempis, Jeroen Centre for Sports & Education en Startcollege)	 Westerdijk Fungal Biodiversity Institute (CBS - KNAW)
 Avans Hogeschool	 Huygens Instituut (KNAW)	 Netherlands eScience Center	 ROC Alfa college	 Stichting Sint Antonius Ziekenhuis	 Zadkine
 Bezoeksbureau Humanitiescluster KNAW	 HZ University of Applied Sciences	 Netherlands Institute for Advanced Study in the Humanities and Social Sciences	 ROC Arcaus College	 Stichting Studielink	 Zeeuwse Bibliotheek
 Biblotek Groningen	 IHE Delft Institute for Water Education	 NHL Hogeschool	 ROC Aventis	 Stichting Wetenschappelijk Onderzoek Verkeersveiligheid SWOV	 Zuyd Hogeschool
 Bureau (KNAW)	 Integraal Kankercentrum Nederland	 NHL-Stenden	 ROC Da Vinci	 Sunma College	
 Catharinacollege	 Internationaal Instituut voor Sociale Geschiedenis (KNAW)	 NHTV internationaal hoger onderwijs Breda	 ROC Friese Poort	 SURF	
 Centraal Bureau voor de Genetiek	 IRIMA Guest I&P   Privacy by Design Foundation	 Nikhef	 ROC Glade Opleidingen	 SURFmarkt	
 Centraal Planbureau	 Katholieke Pabo Zwolle	 Nimeto	 ROC Horizon College	 SURFiana	
 Centrum Wetkunde & Informatie	 KNAW	 NIOO instituut voor oorlogs-, holocaust- en genocidestudies (KNAW)	 ROC Leeuwenborgh	 Technische Universiteit Delft	
 Christelijke Hogeschool Ede (CHE)	 Koning Willem I College	 Nova College	 ROC Leiden	 Technische Universiteit Eindhoven	
 Cbap	 Koninklijk Conservatorium	 NSCR	 ROC Meldan Nederland	 Technologiesichting STW	
 Cdo	 Koninklijk Nederlands Instituut voor Onderzoek der Zee (NIOZ)	 Nuclear Research and Consultancy Group	 ROC Mondriaan	 Thomas More Hogeschool	
 Cluzus College	 Koninklijke Academie van Beziende Kunsten	 Nuffic	 ROC Nijmegen	 TNO Innovation for life	
 COG Vellei & Gelderland - Midden	 Koninklijke Bibliotheek	 NWO	 ROC Noorderpoort	 Tinboes Instituut	
 Data Archiving and Networked Services (KNAW)	 Leeds Universitair Medisch Centrum	 Nyenrode Business Universiteit	 ROC Regio College	 UMC Groningen	
 De Haagse Hogeschool (HHS)	 Leidse Onderwijsinstellingen	 Onderwijsgroep Noord	 ROC TOP	 United ID   United ID Services	
 Deltares	 Lentiz Onderwijsgroep	 Onderwijsgroep Tilburg	 ROC van Amsterdam Flevoland en VOVa	 Universitair Medisch Centrum Utrecht	
 Deltona College	 Maastricht School of Management	 Open Juridische Hogeschool, Netwerk Open Hogeschool Informatica, Schakel2 NOHI	 ROC van Twente	 Universiteit Leiden	
 Design Academy Eindhoven	 Marx Academie	 Open Universiteit	 Royal Netherlands Institute of Southeast Asian and Caribbean Studies	 Universiteit Maastricht	
 DIFFER	 Max Planck Instituut voor Psychologie	 Openbare Bibliotheek Amsterdam (OBA)	 SaNS Expertisecentrum	 Universiteit Twente	
 Digital Humanities HumanitiesCluster (KNAW)	 MBO Amersfoort	 OpenConex monitoring I&P	 Saxion	 Universiteit Utrecht	
Drenthe College	MBO Utrecht	Planbureau voor de Leefomgeving	SivLucas	Universiteit van Amsterdam	

1.312.508  
gebruikers



# EduGAIN vergroot de uitdaging





# Een veilige IdP: best belangrijk!



# Een veilige IdP: de aspecten

- Een veilige verbinding
- De juiste accounts en attributen
- Handelen bij incidenten

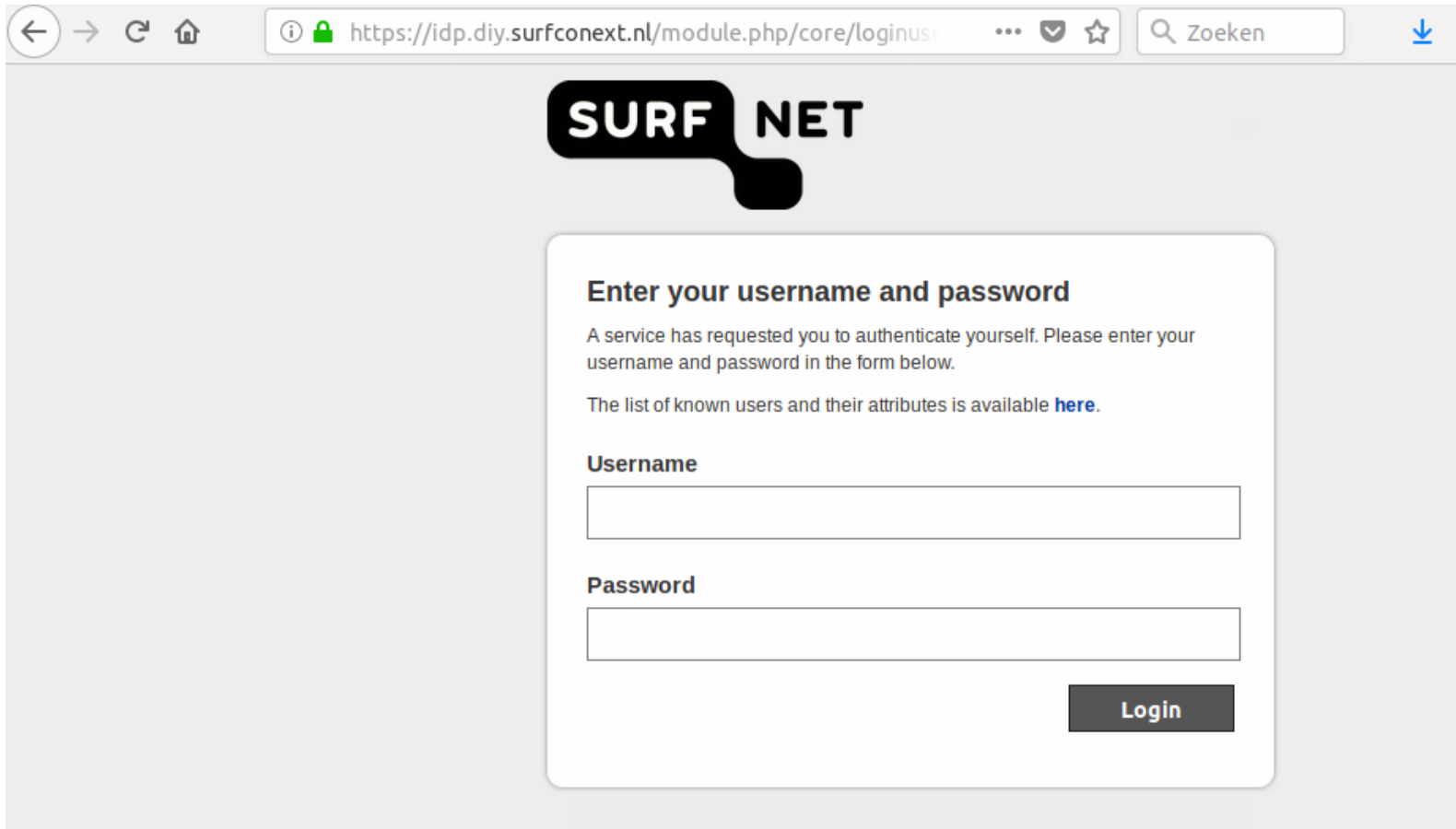
# Een veilige IdP: de aspecten

Een veilige verbinding

38 %



# HTTPS



← → ↻ 🏠 🔒 https://idp.diy.surfconext.nl/module.php/core/loginuse ... 📄 ☆ 🔍 Zoeken ⬇️

## SURF NET

**Enter your username and password**

A service has requested you to authenticate yourself. Please enter your username and password in the form below.

The list of known users and their attributes is available [here](#).

**Username**

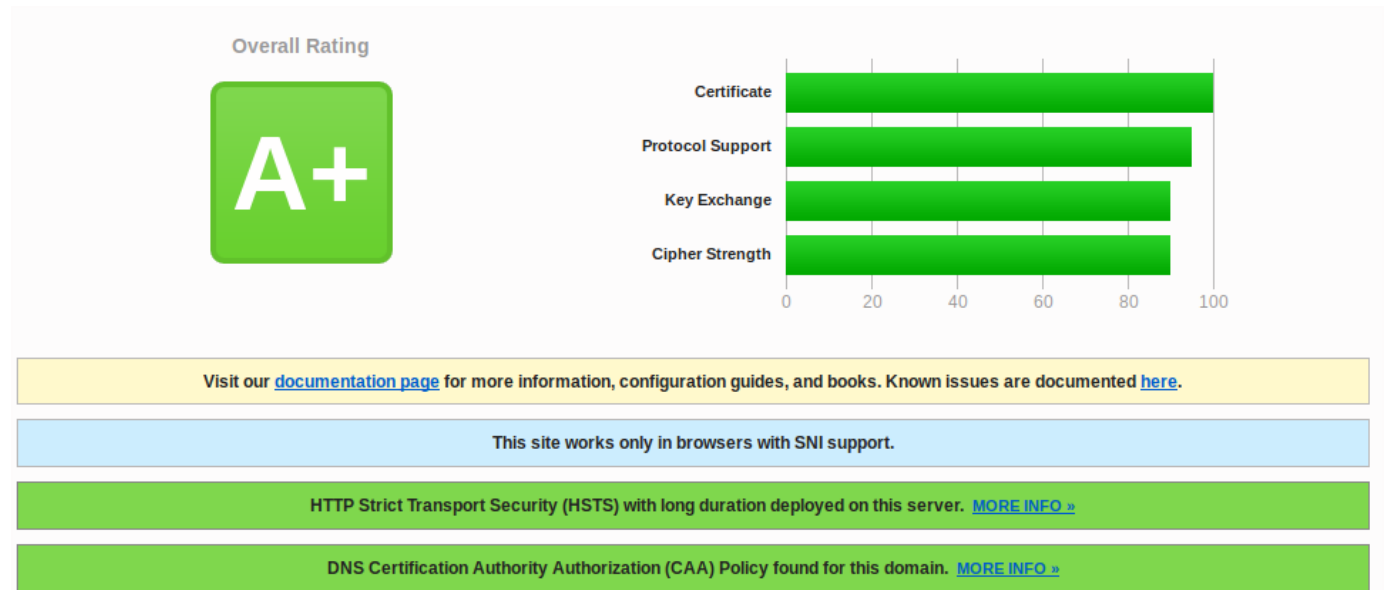
**Password**

**Login**

# HTTPS: een te compleet protocol

- Dat het werkt maakt het nog niet veilig.
- 29% van de IdP's gebruikt onveilige ciphers

- <https://ssllabs.com>
- <https://internet.nl>



# HTTPS: domeinnamen, eerste label

```
41 adfs
16 sts
12 login
12 idp
 8 federation
 7 sso
 7 fs
 6 federatie
 6 adfs2
 3 signon
 3 secure
 3 saml
 2 sclogin
 2 namidp
 2 fed
```

# HTTPS: domeinnamen, eerste label

```
1 wayf          1 dans          1 login-edu
1 teamwerk      1 conext        1 kitlv
1 tcs02         1 ccidfederation 1 inloggen
1 surfspot     1 bureau        1 iisg
1 surf          1 beta          1 idservice
1 stsip        1 auth          1 idp01
1 stsfed       1 adfsv2        1 huygens
1 rathenau     1 adfs-p        1 huc
1 onegini      1 adfs-differ  1 glr-adfs
1 niod         1 adfs3prod     1 gatekeeper2
1 nidi         1 adfs3host     1 fsa
1 nias         1 adfs20        1 fides
1 nam-id       1 adfs1         1 fedlogin
1 meertens     1 adfs01        1 federate
1 mdb-vw-adfs  1 accounts      1 engine
1 logon        1 access        1 demeter
```





## Extended Validation

  Triodos Bank N.V. (NL) | <https://bankieren.triodos.nl/it>

  Cooperatieve Rabobank U.A. (NL) | <https://bankie>

  SURFnet bv (NL) | <https://engine.surfconext.nl>

  Coöperatie SURF U.A. (NL) | <https://surfdrive.surf.nl/files>

  Magazijn \"De Bijenkorf\" B.V. (NL) | <https://www.debijenkorf.nl>

# Een veilige verbinding

- De IdP is dé plek voor een veilig login-schermbul>- Verzorgd en mobiel-vriendelijk
- DNSSEC
- HTTPS met een goede configuratie
- Extended Validation
- Regel het één keer goed: koppel zoveel mogelijk aan je mooie loginschermbul

# Een veilige IdP: de aspecten

De juiste accounts en attributen

# De juiste accounts

- Alleen natuurlijke gebruikers
- Die vallen binnen de doelgroep
- Identificeerbaar wie het is
  
- Wachtwoordbeleid?

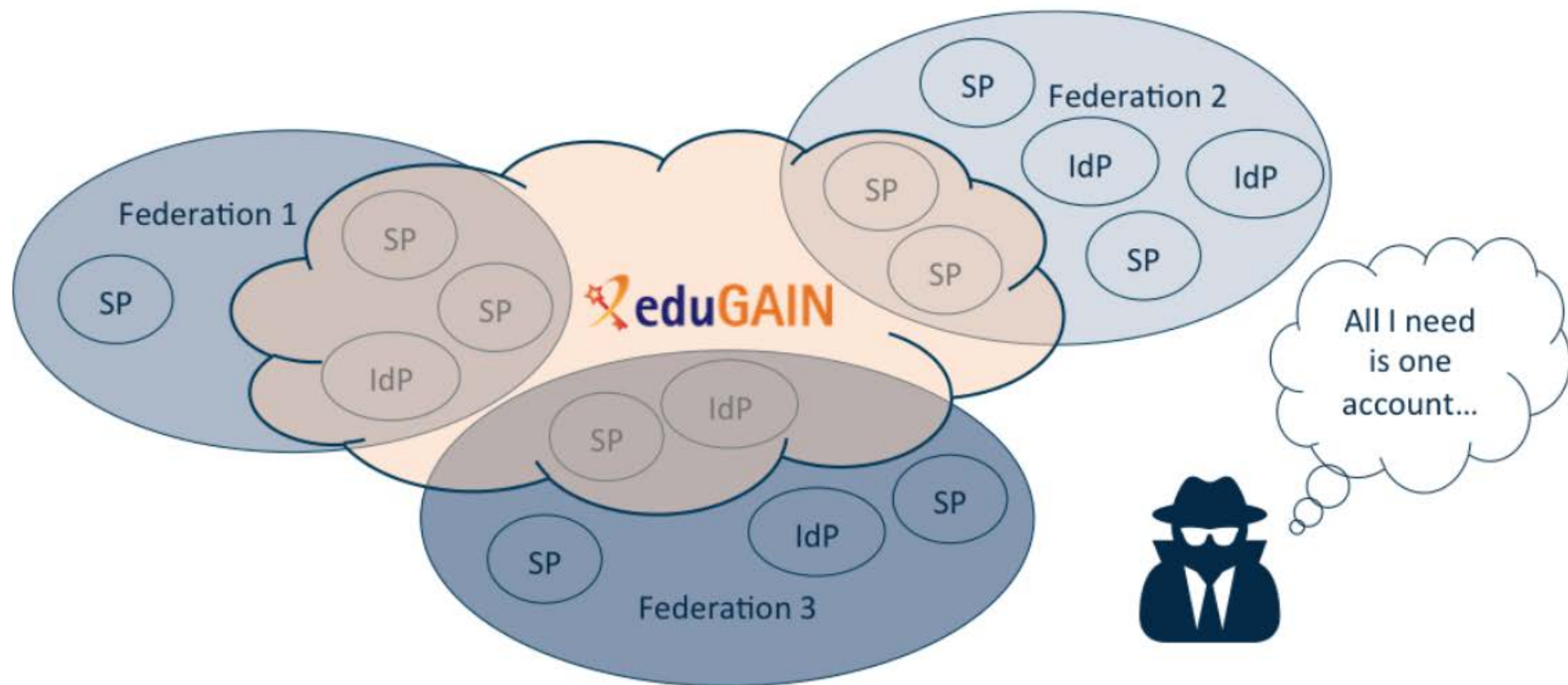
# De juiste attributen

- Attribuutwaarden moeten kloppen
- Naam, betrekking (student of medewerker)
- SURFconext gaat twee attributen checken:
  - SchachHomeOrganization (“univharderwijk.nl”)
  - EduPersonPrincipalName (“\*@univharderwijk.nl”)

# Een veilige IdP: de aspecten

Handelen bij incidenten

# EduGAIN vergroot de uitdaging



# Handelen bij incidenten

- Bij een incident snel kunnen handelen, ook internationaal
- The Security Incident Response Trust Framework for Federated Identity: **SIRTFI**

```
-<md:ContactPerson contactType="other" remd:contactType="http://refeds.org  
/metadata/contactType/security">  
  <md:GivenName>SURFcert</md:GivenName>  
  <md:EmailAddress>mailto:cert@surfnet.nl</md:EmailAddress>  
</md:ContactPerson>
```



# Handelen bij incidenten

- Gebruikers/logins moeten effectief traceerbaar zijn.
- Wees in contact met je lokale CERT/CSIRT: zorg dat jullie elkaar weten te vinden.
- Een keer 'oefenen' kan erg leerzaam zijn!



Einde



EEN VEILIGE IDP:  
EEN VEILIG IDEE!

