v20151201-04

Building Interoperable Global Trust

bridging technology and policy divides

Nikhef

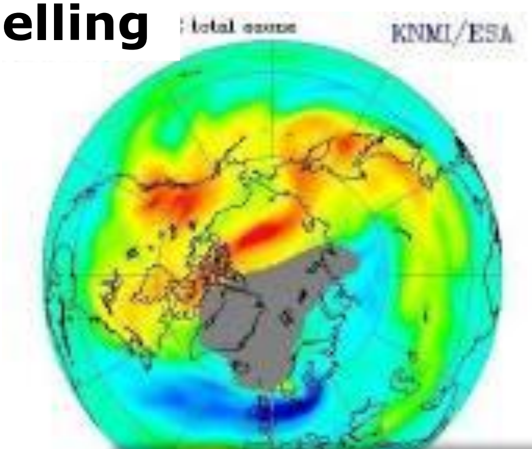
David Groep

EWTI 2015

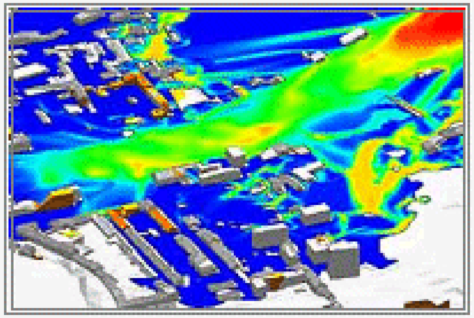
Image by Cristian Bortes, May 2011, CC-BY - https://flic.kr/p/9Uvwng

Research as a global distributed enterprise

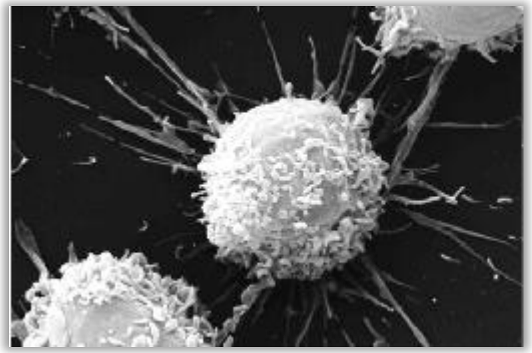
Climate modelling

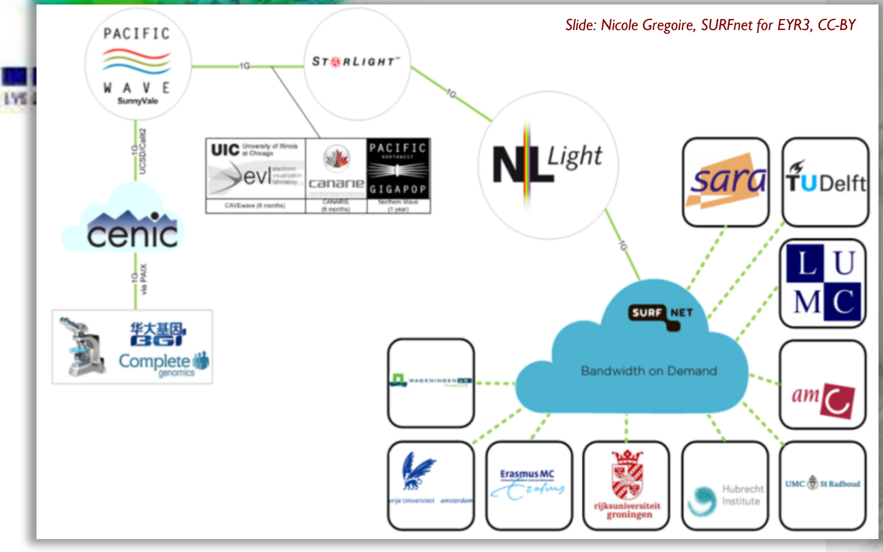


Aerospace
air flow and stress



Flood prediction & disaster mitigation




Slide: Nicole Gregoire, SURFnet for EYR3, CC-BY

Bandwidth on Demand

Global data flows for genomics

The intended outcome …

2x3000 physicists
>10k technical staff
150 institutes
50 countries/areas

2-3 people

2 people

Image source: joint CERN (wLCG) and EGI

Organisations participating in the global collaboration of e-Infrastructures

Even just for wLCG, supporting the CERN LHC programme

More than 200 independent institutes with end-users

More than 50 countries & regions

More than 300 service centres

Handful regional 'service coordination organisations'

300 000 CPU cores, 200+PByte storage

One independent 'policy-bridge' PKI

WLCG
Worldwide LHC Computing Grid

PRAGMA

PRACE

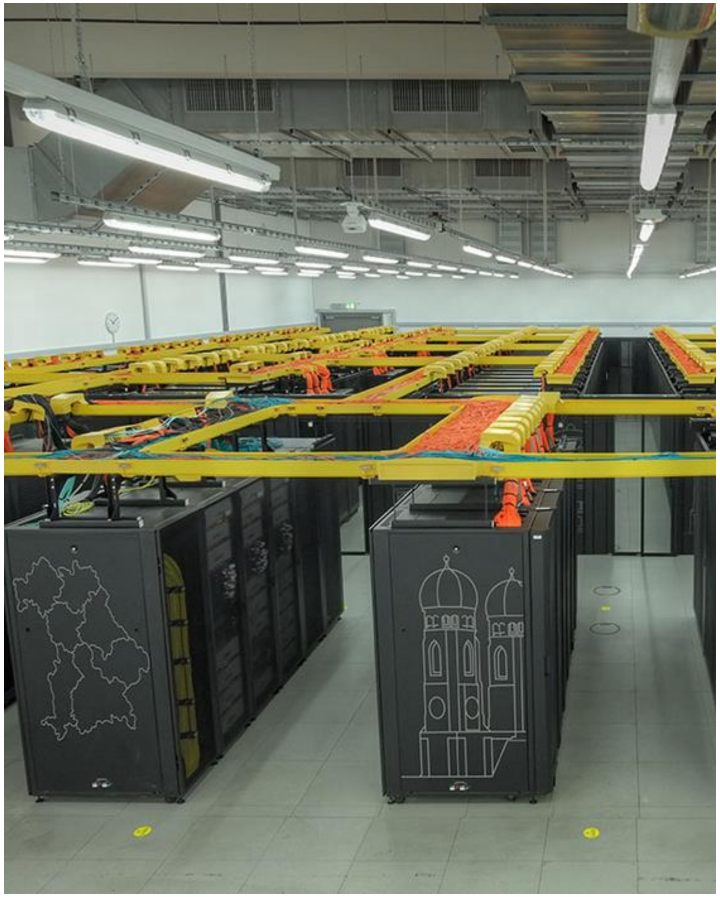
Open Science Grid

egi

XSEDE
Extreme Science and Engineering
Discovery Environment

Building Sustainable Trust

Single Organisation
managerial control over all assets

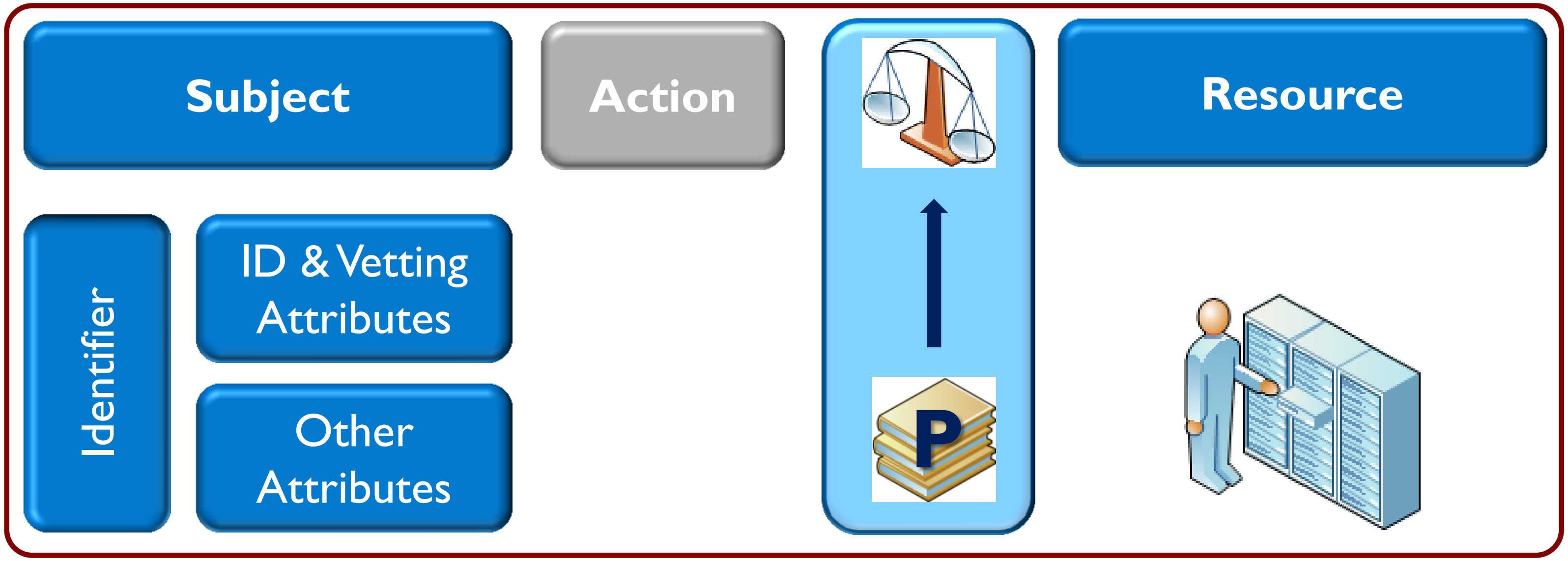


Collaborative Community
distributed responsibility
loose controls
varying jurisdictions

David Groep
Nikhef
Amsterdam
PDP & Grid

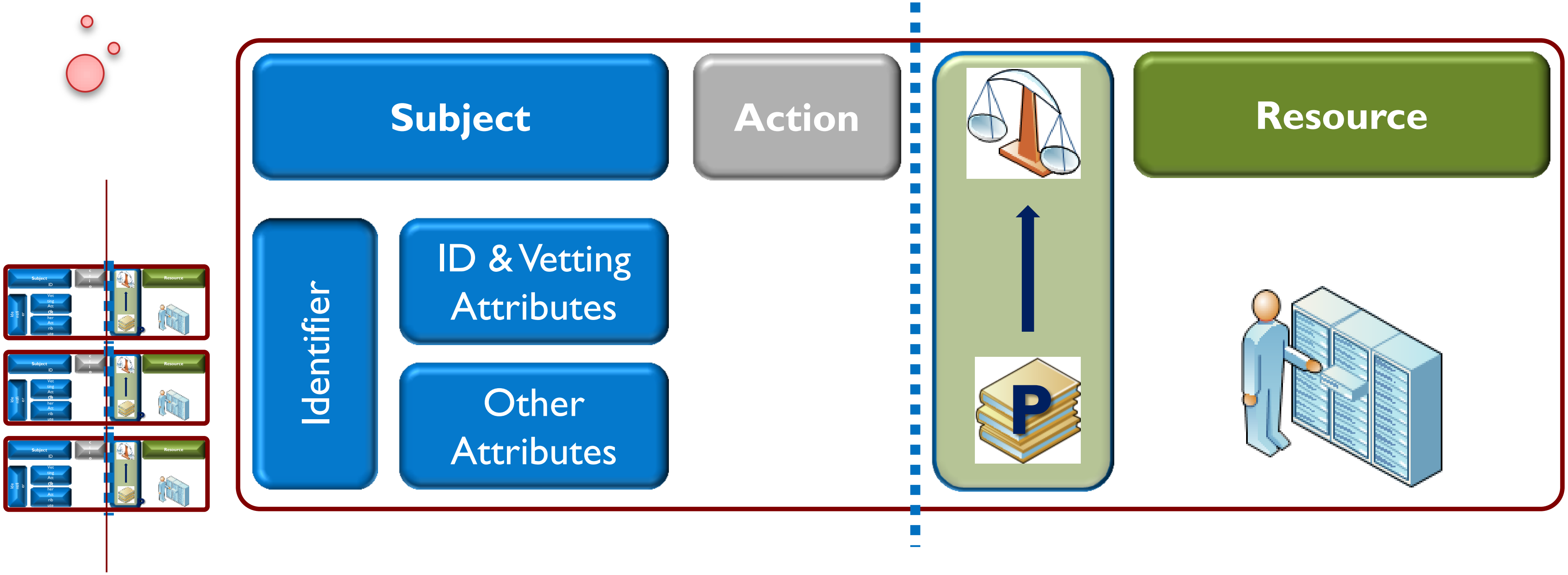
left: the SuperMUC, LRZ, Garching bei München – which is actually also part of the R&E e-Infrastructure …

Identifying participants – classifying risks



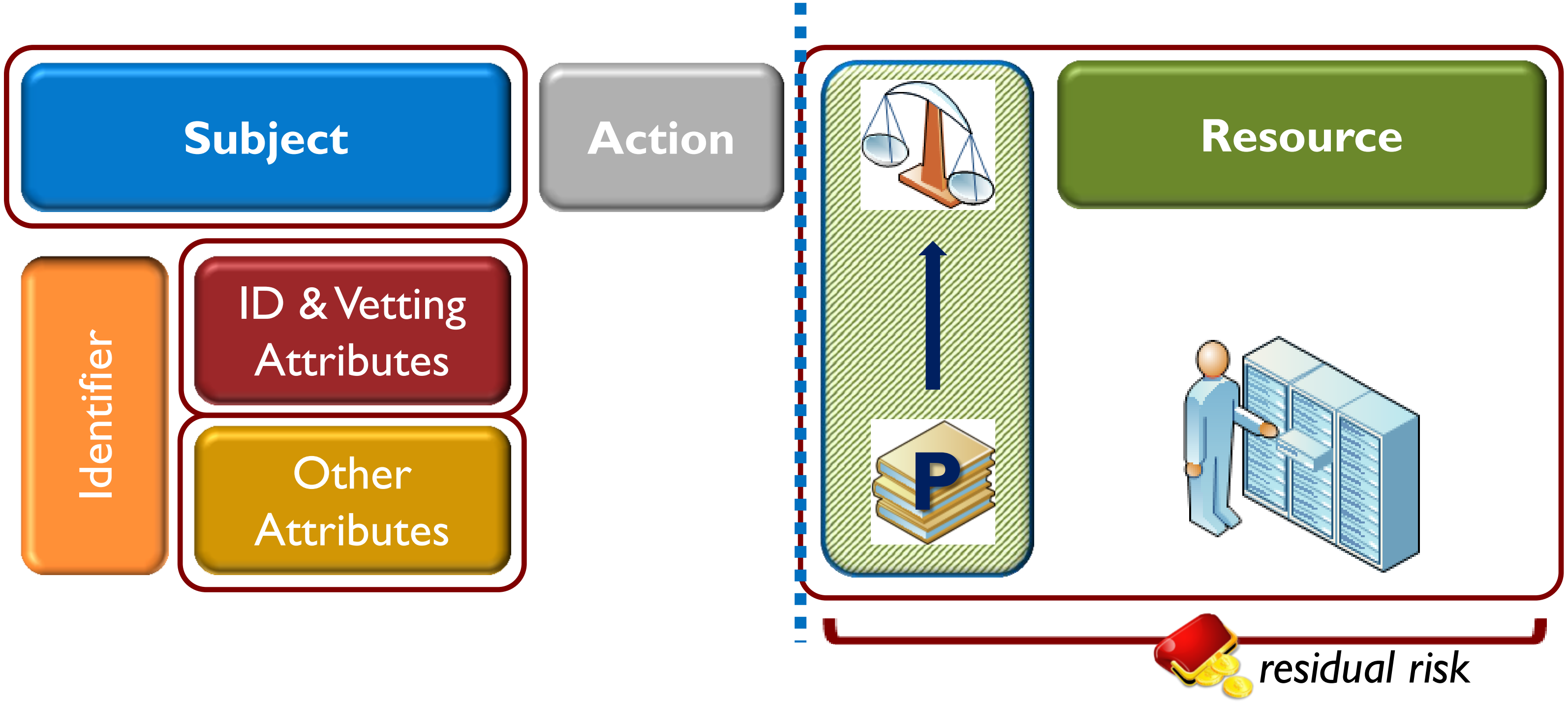
1. Single organisation responsible for entire risk envelope

Identifying participants – classifying risks



1. Single organisation responsible for entire risk envelope
2. Multiple 'monolithic' organisations in **equivalent roles** interwork

Identifying participants – classifying risks



1. Single organisation responsible for entire risk envelope
2. Multiple 'monolithic' organisations in equivalent roles interwork
3. Independent administrative domains collaborate in **distinct roles**

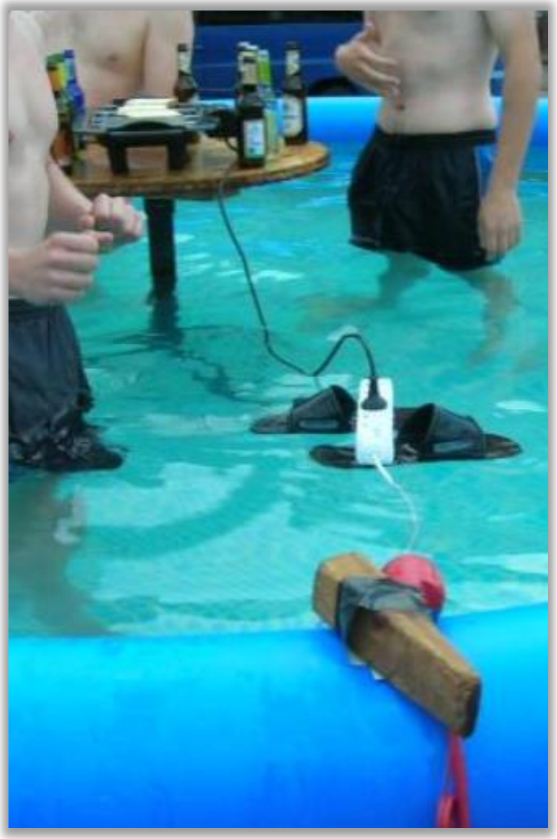
David Groep
Nikhef
Amsterdam
PDP & Grid

Relying Parties as a Defining Element

Service providers ('relying parties') absorb almost all of the residual risk – as they host and manage resources under threat

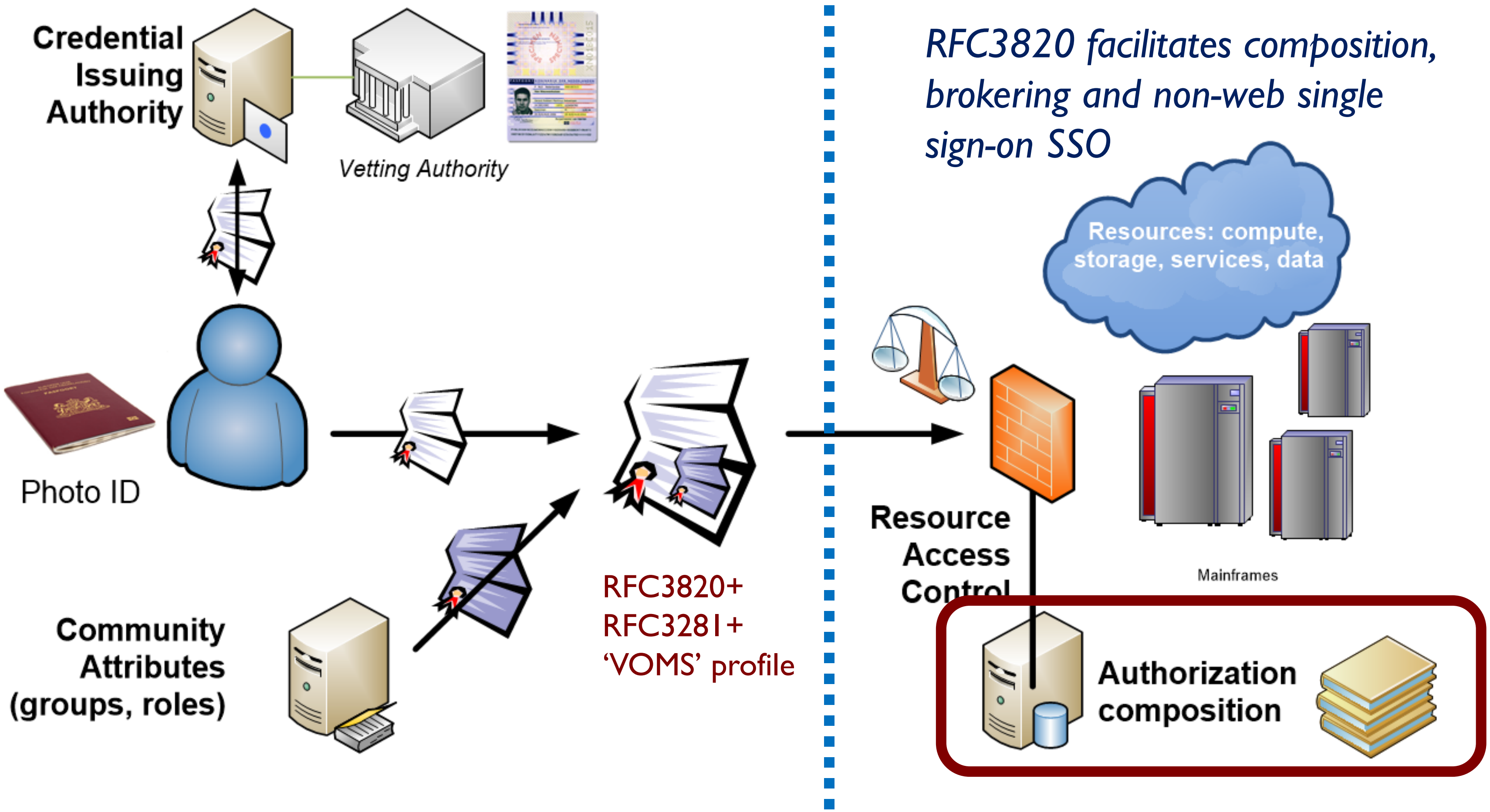
They trust others *for a particular purpose*

- Sources of 'subject authority' should **align with RP interests** to be useful
- RP must have policy controls to **compose sources of authority**
- RP must be **equipped with effective controls** to mitigate risks



source: NorthWood LAN party 7 - http://www.linuxno.de/

Multi-authority access control with PKI in e-Infrastructures using composable policy


Credential Issuing Authority
Vetting Authority
Photo ID
Community Attributes (groups, roles)
RFC3820+
RFC3281+
'VOMS' profile
Resources: compute, storage, services, data
Resource Access Control
Mainframes
Authorization composition

RFC3820 facilitates composition, brokering and non-web single sign-on SSO

VOMS Attribute Certificate Format, https://redmine.ogf.org/dmsf files/10489

Why a dedicated trust fabric for eScience?

'non-alignment'

Specific assurances required for e-Infrastructures

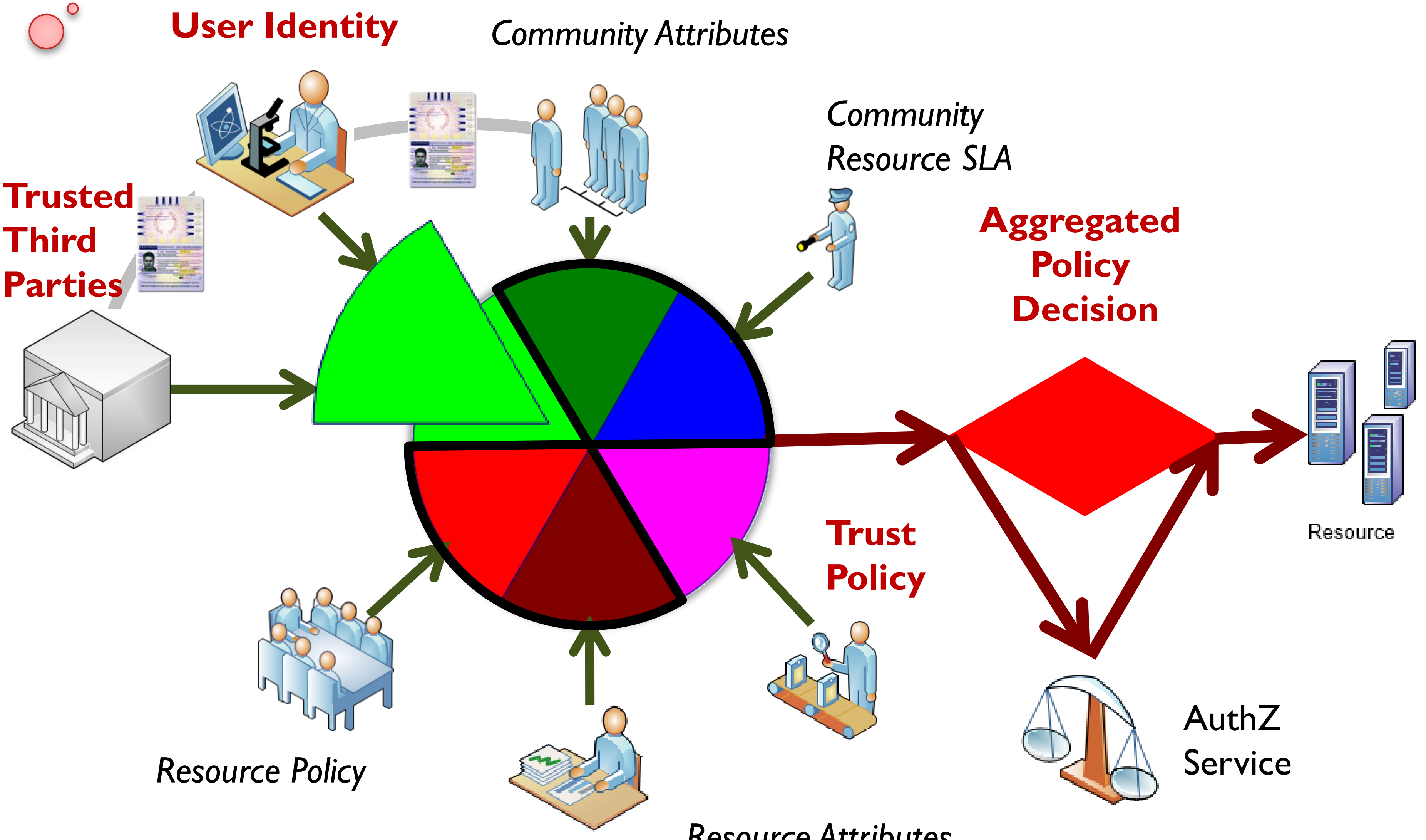
- globally unique, non-reassigned identifiers
- identify end-users as well as networked services
- active participation in incident response at last resort

Issues for e-Infra compared to current browser trust

- 'actual' relying party – end users – are not even encouraged to make trust decisions autonomously - *it's e.g. impossible to consistently remove an individual trust anchor from NSS default set*
- decisions (necessarily) consensus-based, but consensus in a group far larger and with divergent interests from specific cross-enterprise RPs
- public browser trust almost exclusively DNS focused

Not all RPs nor all risks are equal, so ultimately one gets differentiated LoA even in a single federation

Empowering the Relying Party



graphic inspired by OGF OGSA-AuthZ WG, 2005

Establishing PKI interworking: AP EU TAG

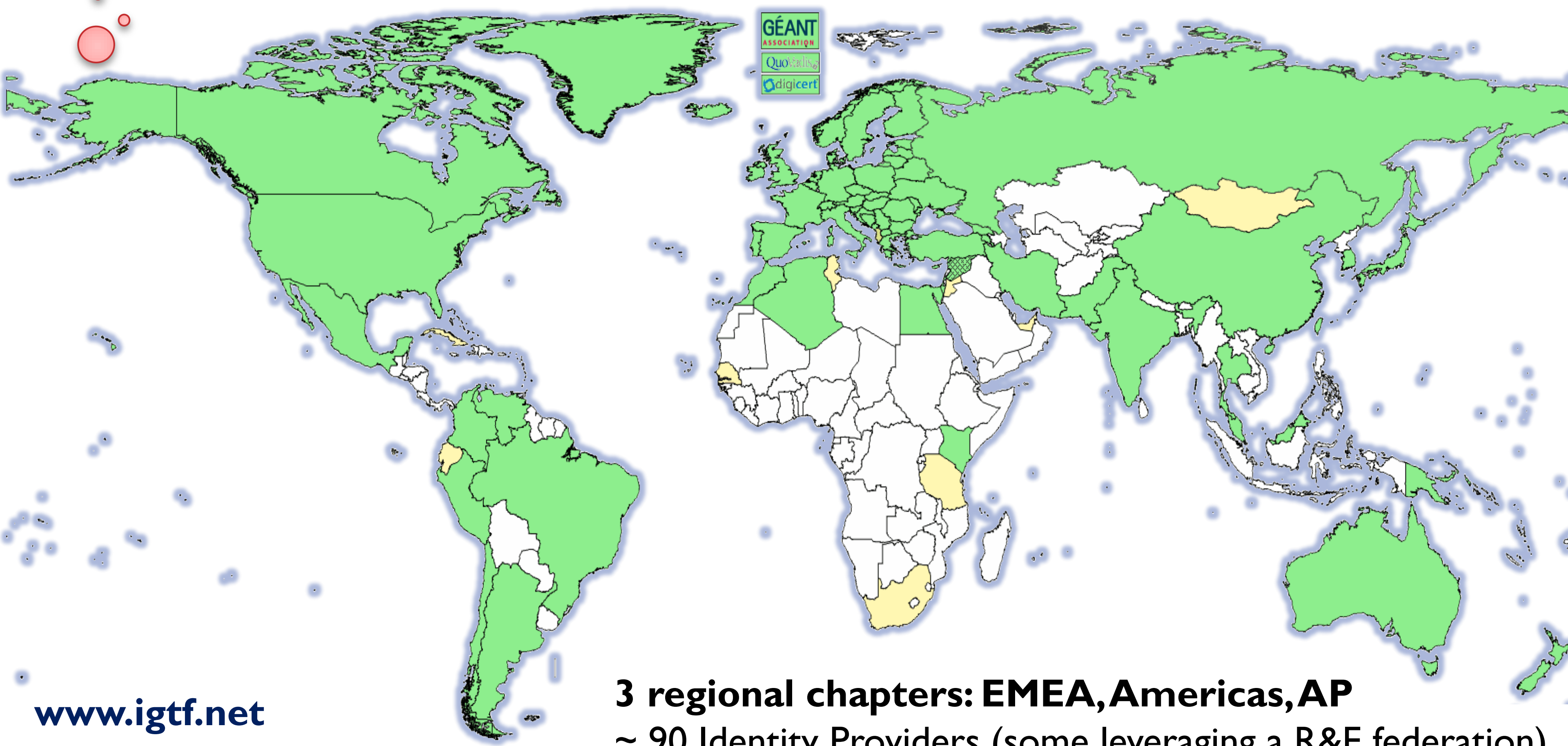
- European resource provider collaboration established first CA Coordination Group for e-Infrastructures in 2000
  - Leveraged on purpose existing PKI CAs where available
  - Global research needs resulted in the 2003 'Tokyo Accord'

- With start of production e-Infrastructures in 2004
  - EUGridPMA: national (e-infra) identity services plus major e-Infrastructures & TERENA
  - APGrid and PRAGMA establish APGridPMA
  - Canada, Latin America and USA establish TAGPMA

IGTF
Interoperable Global Trust Federation
AP|EU|TAG

- bringing together resource providers, communities, IdPs
  - agree on global, shared minimum requirements and assurance levels
  - inspired and coordinated by the needs of relying parties, who frequently *co-support* some of the identity management operations

Interoperable Global Trust Federation



3 regional chapters: EMEA, Americas, AP

~ 90 Identity Providers (some leveraging a R&E federation)

~ 10 international major relying parties

~ 60 countries / economic areas / extra-territorial orgs

> 1000 relying service provider collaborations

www.igtf.net

IGTF
Interoperable Global Trust Federation
AP | EU | TAG

Minimum requirements: assurance profiles

- Federation *minimum requirements* (APs) reflect specific operational and security needs of resource providers
  - ➤differentiated LoA support:
  - classic direct-vetting subscriber services
  - identity services leveraging (R&E) federations with ID vetting
  - 'LoA1+' Identifier-Only Trust Assurance
    – if relying party has other ways to vet its users, allow for lower-assurance identifiers, thus enabling more federations as ID source
- 'research-inspired' trust verification process: self-audits, peer-review, transparent open policies and processes
  - 'meet or exceed' required minimum standards

www.igtf.net/ap/loa

Assurance Profiles – declaration of consistency towards Relying Parties

1. Vetting and assurance – for identity and attributes
   - vetting rules and data quality
   - expiration and renewal
   - revocation and incident containment
2. Operational requirements for identity providers
   - operating environment and site security
   - staff qualification and control
3. Publication and audits
   - openness of policy, practices and meta-data
   - review and auditing
4. Privacy and confidentiality guarantees
5. Compromise, disaster recovery and business continuity

Engendering trust through transparent processes and procedures

- IGTF itself works on peer review process
- Supported by self-assessments shared with the peer group

- Depending on the RP risk assessment,
  for identified use cases this is actually sufficient LoA
- Especially when there are complementary
  sources of assurance: community attributes, 'reputation', …

Image: EUGridPMA Plenary Meeting, Amsterdam 2009

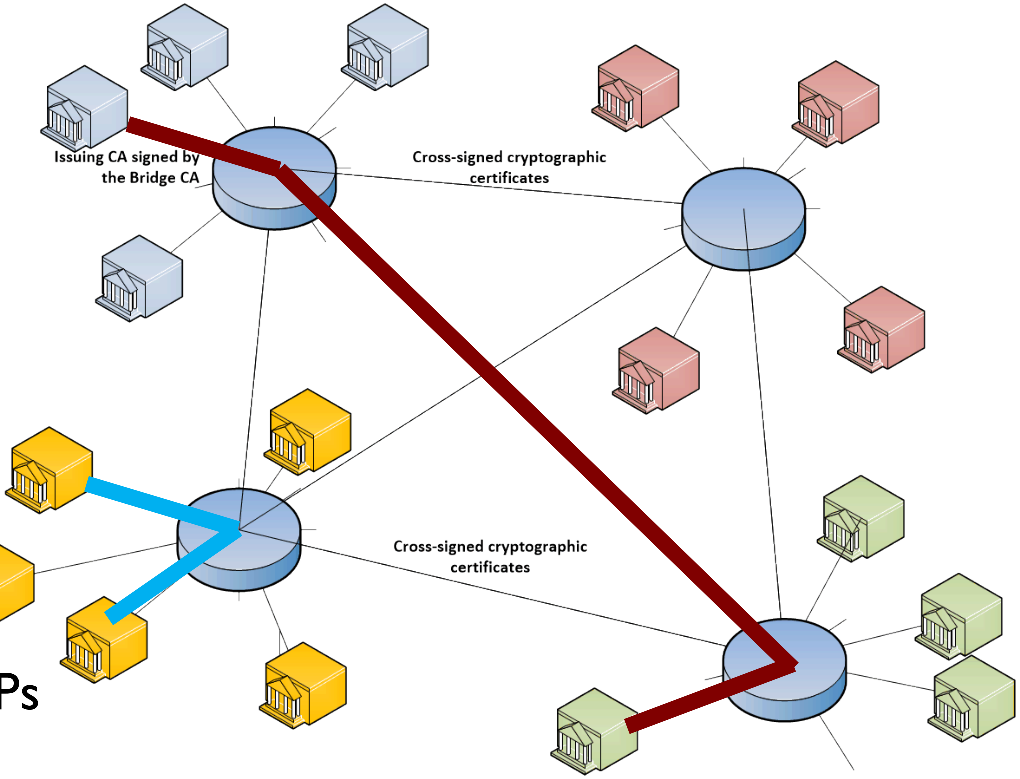
Cryptographic PKI bridging

Organisations typically act as *both* CA (IdP) *and* Relying Party

Technically

- path discovery support
- permissible ‘naming’ defined in the cross-signing certs
- policy mapping is done in the bridges only

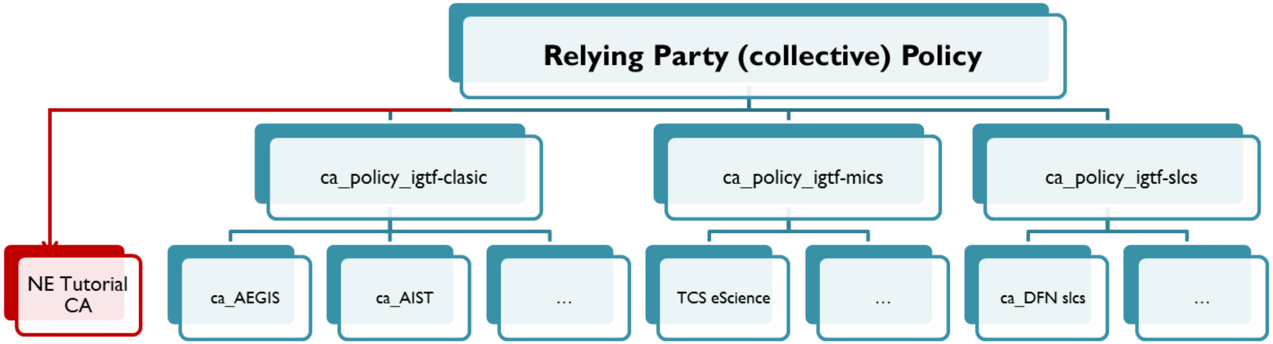
Bridges take care of policy responsibility for their trusting connected CAs *and* RPs


Issuing CA signed by the Bridge CA
Cross-signed cryptographic certificates
Cross-signed cryptographic certificates

Rendering a PKI federation as a Policy Bridge

Once role separation is recognised, federation is simple

1. **composable - and removable - assurance-tagged** trust anchor lists



2. mechanism to **distribute trust-anchor (meta) data** via the federation
3. provide controls that **permit the RP** – under its own policy – to trust only those elements that **match its risk profile**
   - based on **assurance profiles** expressed as accreditation trust marks
   - based on relying party defined **namespace constraints** to set trust **scope** and global uniqueness of identifiers in the federation
   - permit subject-based **policy decisions** (on name, issuer, attributes)

News as of 28 November, 2015

Release 1.69 available

Fetchcrl3: *CRL freshness for PKIs*

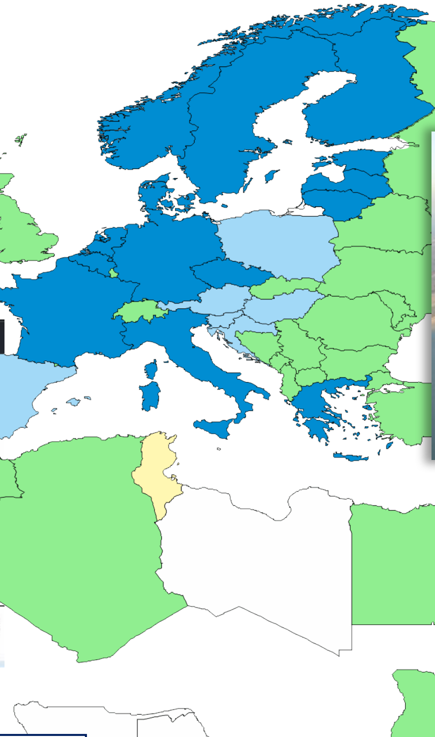
IGTF Authorities

https://dl.igtf.net/distribution/current, https://www.ogf.org/documents/GFD.189.pdf

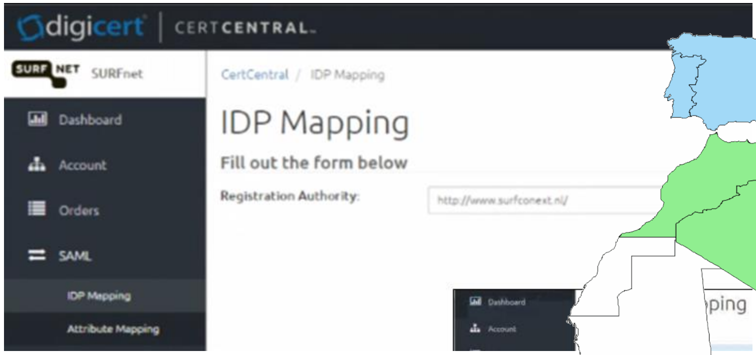
Collaboration is based on Bridging Trust!

Policy bridges are fairly common … in various technologies and scenarios …

GÉANT ASSOCIATION
QuoVadis
digicert



Bridging bridged trust fabrics



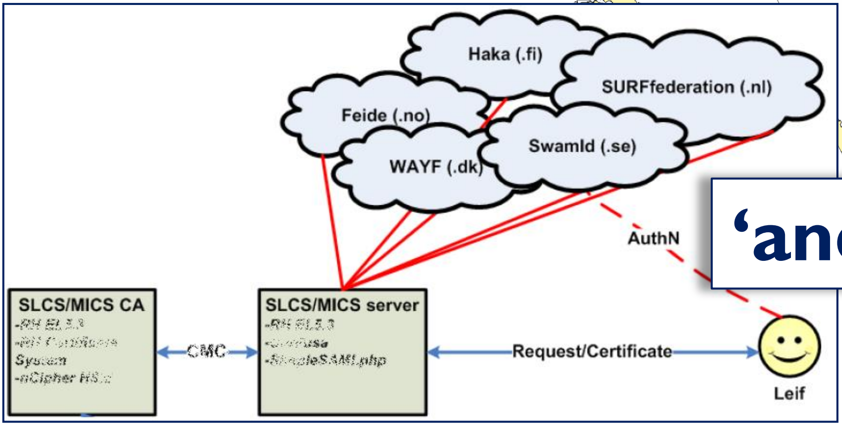
CertCentral / IDP Mapping

IDP Mapping

Fill out the form below

Registration Authority: http://www.surfconext.nl/

GEANT TCS
DFN AAI SLCS
CILogon Basic, Silver



‘and trust is technology agnostic’

SLCS/MICS graphic: Jan Meijer, UNINETT

Image: Bryan Tong Minh, CC-BY-SA
Oosterscheldekering, Rijkswaterstaat, NL

www.igtf.net

Interoperable Global Trust Federation

IGTF

AP | EU | TAG

davidg@nikhef.nl

Dutch National Institute for Subatomic Physics

David Groep
Nikhef
Amsterdam
PDP & Grid

Image: Bryan Tong Minh, CC-BY-SA
Oosterscheldekering, Rijkswaterstaat, NL