

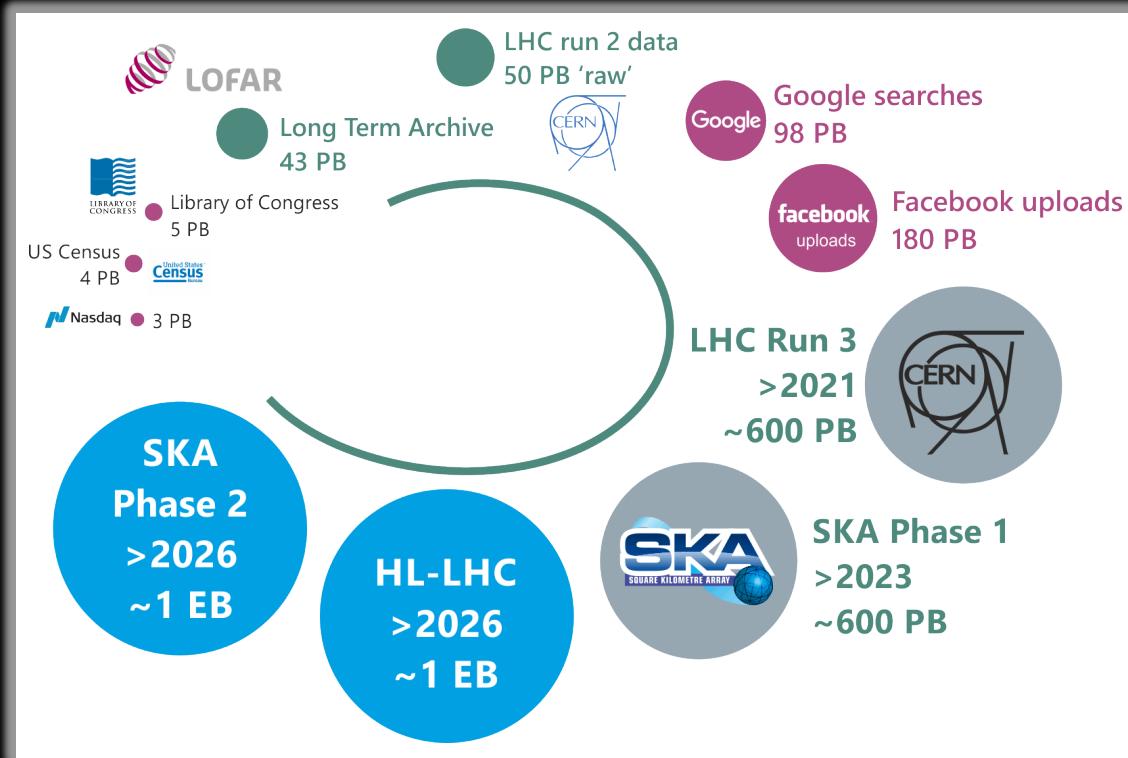
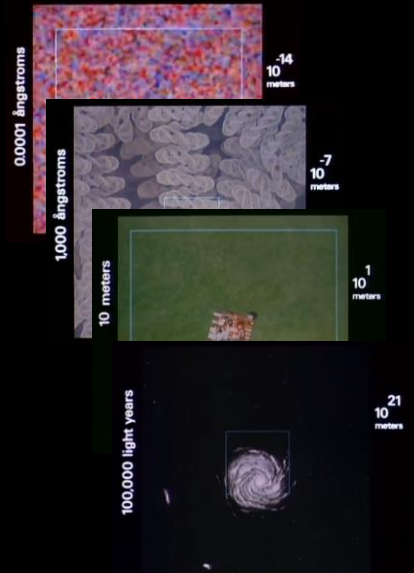


Making hardware, software, and people collaborate

Building scalable e-Infrastructures for research

David Groep, Nikhef
November 10, 2020
Physics-DKE colloquium

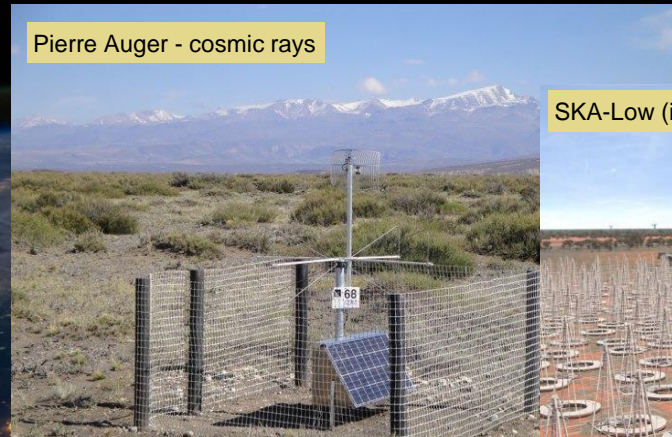
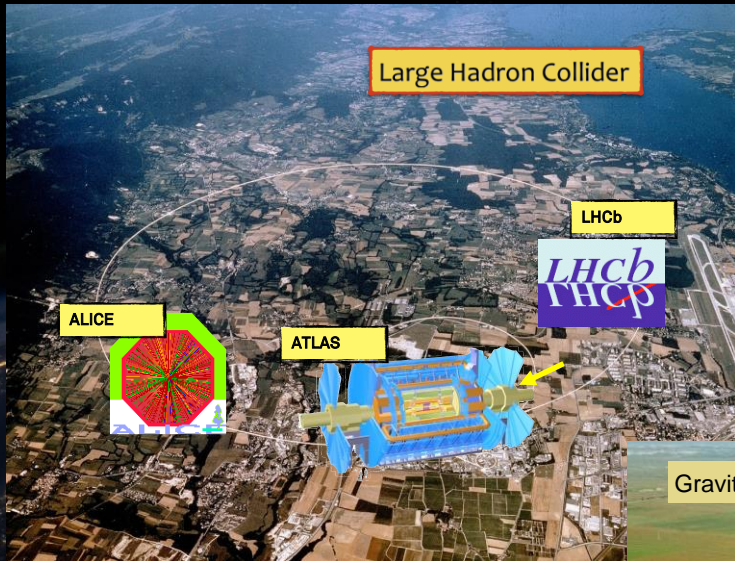
Scaling & the 'data deluge' ... with data comes processing



Data from various sources, for public entities: data ca. 2018, indicative, within ~ factor 2

LHC volumes: LCG Resource Scrutiny Group & CERN; 2020
SKA and LOFAR volumes: ASTRON/Michiel van Haarlem, 2020

Data is distributed – but collaboratively interpreted



>170 institutes in >42 countries
and economic regions

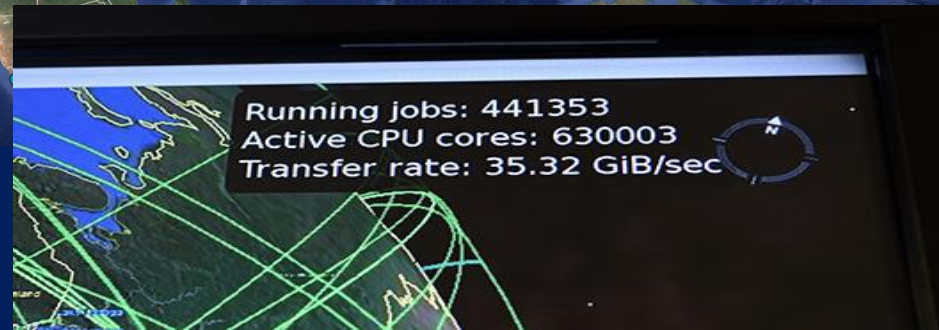


WLCG
Worldwide LHC Computing Grid



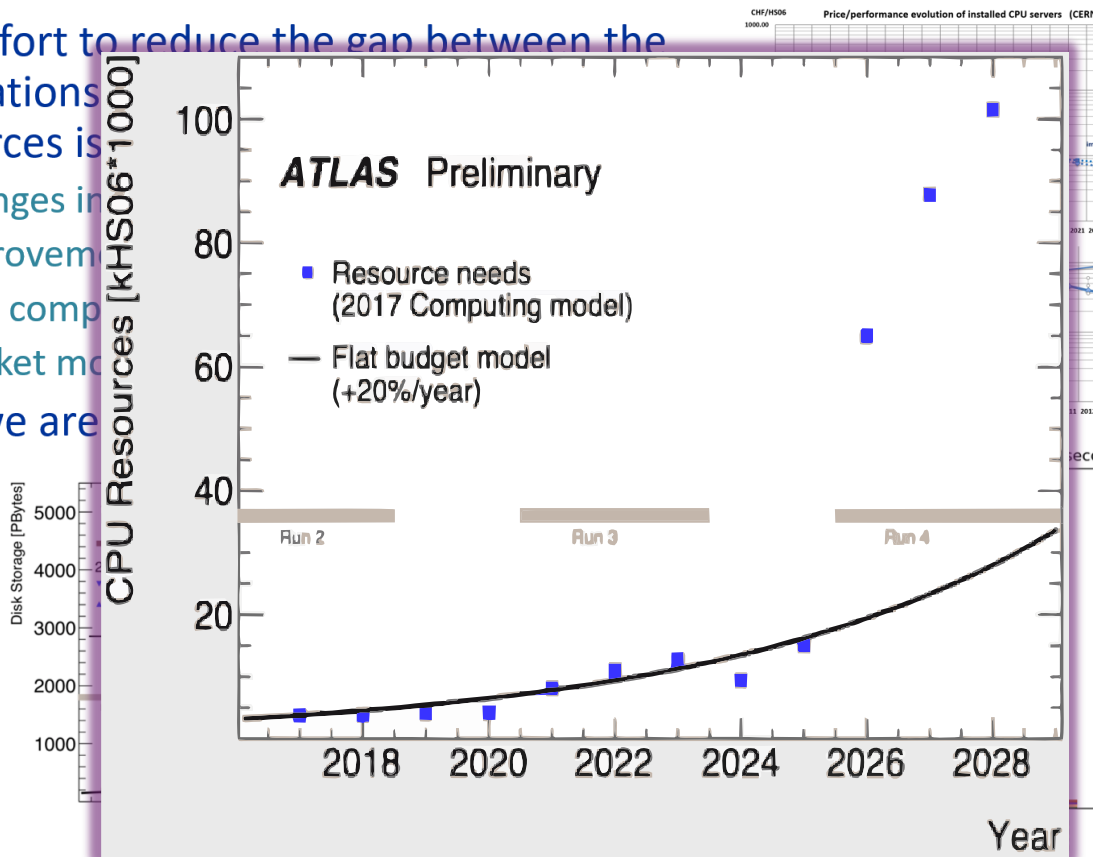
XSEDE
Extreme Science and Engineering
Discovery Environment

- *Computing* ~ 1,000,000 cores
- *On-line disks* > 310 PB
- *Archival* > 390 PB

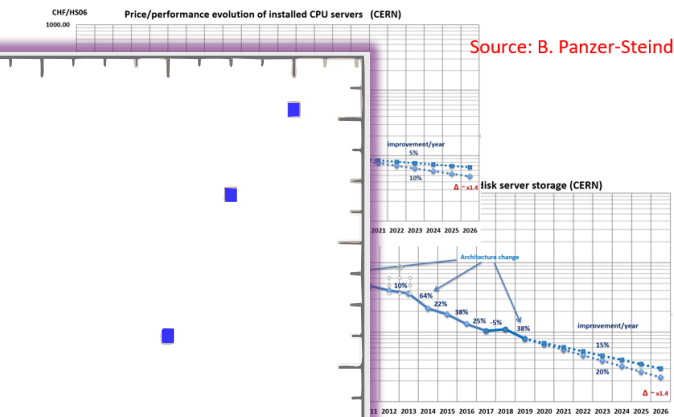


The High Luminosity Challenge

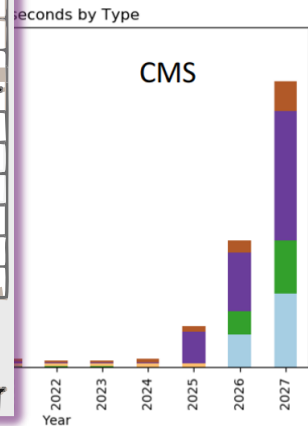
- The effort to reduce the gap between the estimations and resources is
 - Changes in
 - Improvement
 - GPU comp
 - Market mo
- Still, we are



Source: D. Costanzo



Source: B. Panzer-Steindel



Source: D. Lange

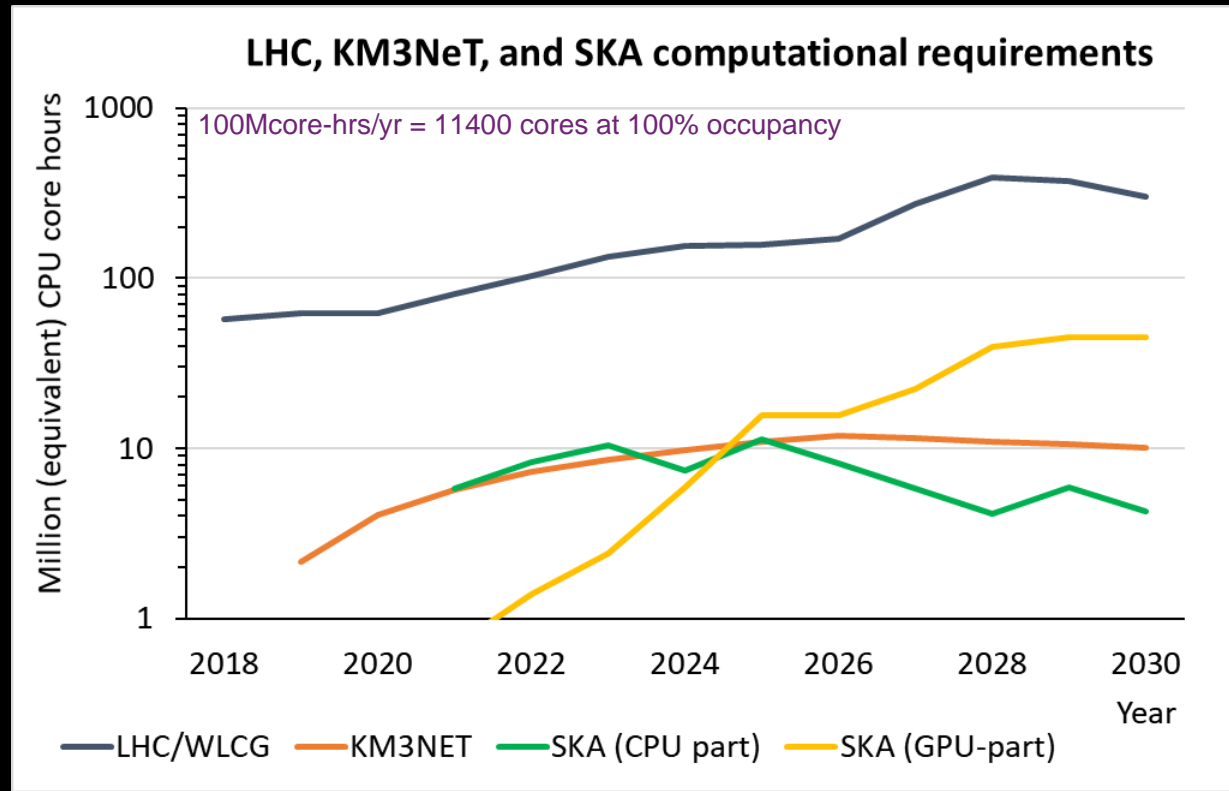
Scaling across all science domains

Dutch-only (!)

compute requirements for LHC, KM3NeT, and SKA, until 2030

Even then, it will be sufficient if and only if

- GPU and parallelism are fully exploited
- throughput per core continues to increase
- data access patterns will match system design



Infrastructure: dealing with data processing at scale

1: matching algorithms and systems design

- designing for high-performance processors
- rethinking design patterns for work & data orchestration



people - systems

2: collating compute, storage, and networks

- building 'facilities'
- peering and global networks
- stressing networks
- research 'cloud' services



systems - systems

3: accessing services, collaboratively & securely

- community building in a multi-national federation
- global trust and identity
- securing the infrastructure of an open science cloud
- our National e-Infrastructure



people - people

“It’s just hardware”

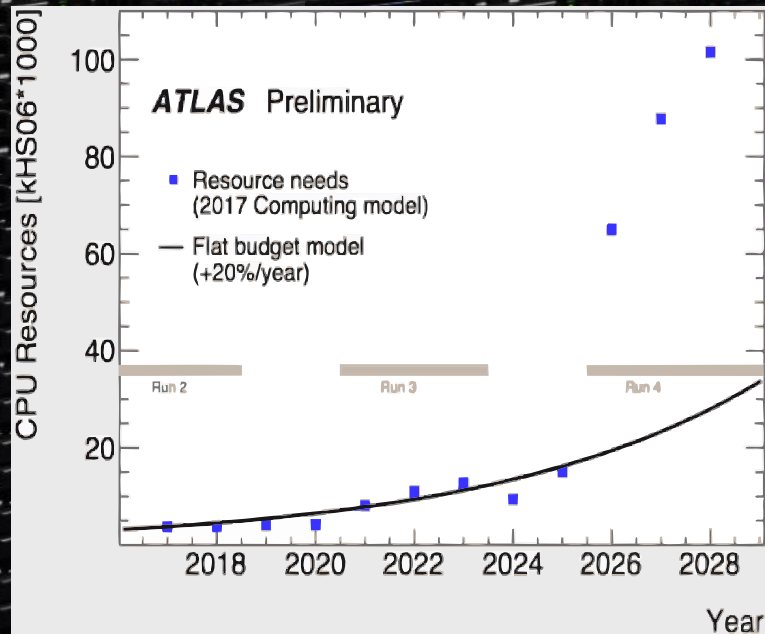
performance goes up, doesn't it?

- processor performance
- memory bandwidth and on-die caching
- accelerators (GPU, &c)



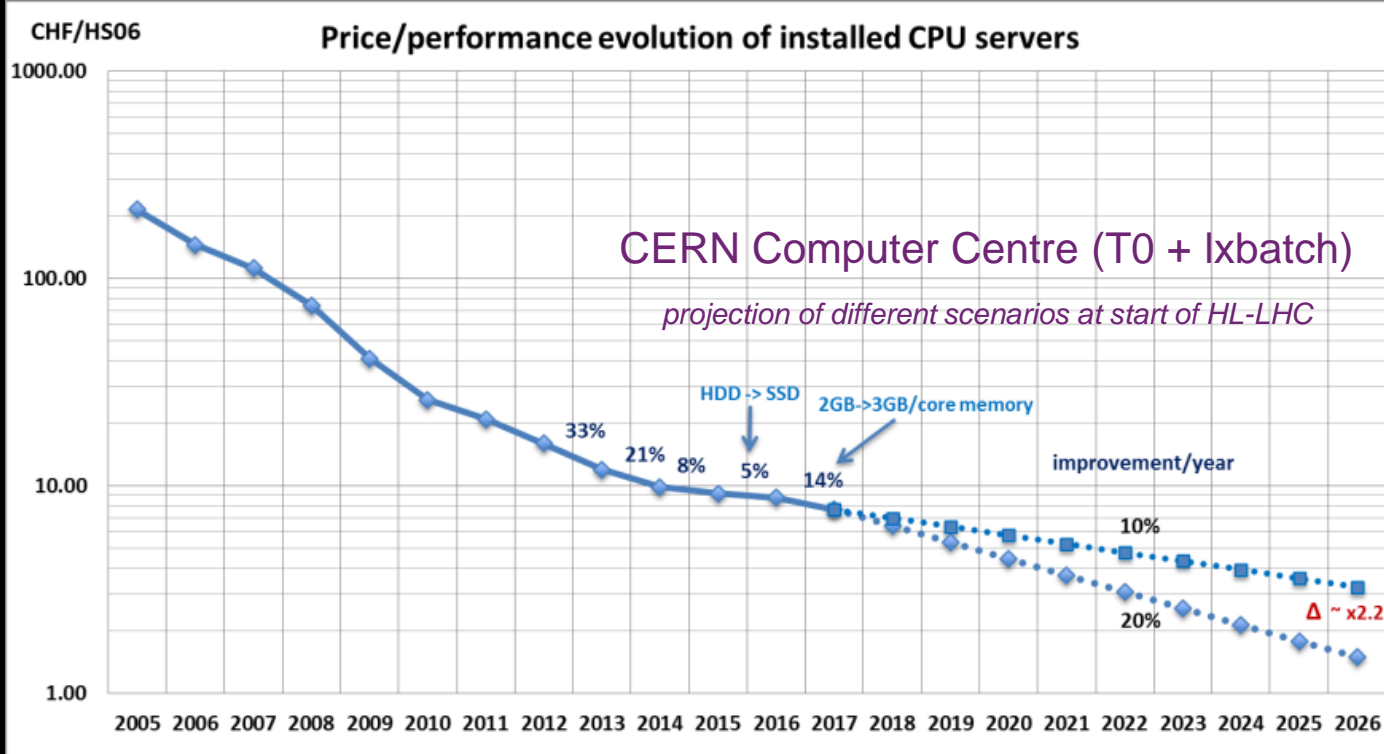
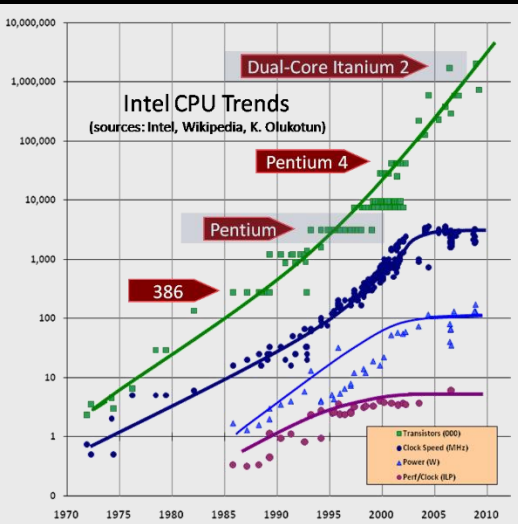
- wider and faster PCI bus throughput
- faster storage and global interconnects

... but ...



Atlas image source: Simone Campana for WLCG, 135th LHCC Meeting Open Session, September 2018

What we knew was coming ...



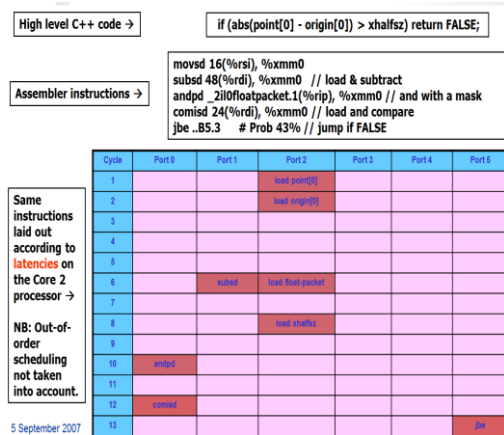
Helge Meinhard, Bernd Panzer-Steindel, Technology Evolution, <https://indico.cern.ch/event/555063/contributions/2285842/>

Figure left: Herb Sutter, Dr.Dobbs Journal 2004, updated 2009, see <http://www.gotw.ca/publications/concurrency-ddj.htm>

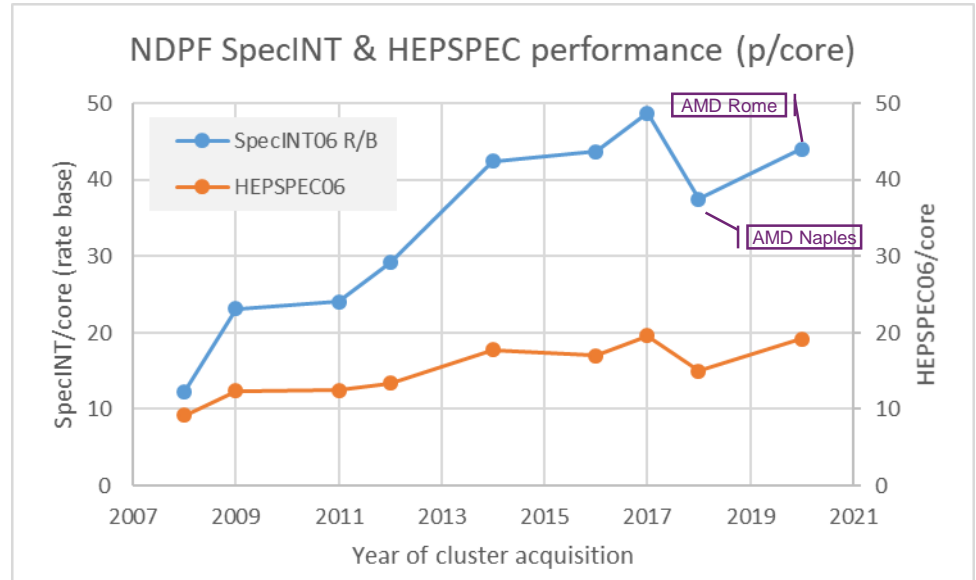
Yet exploiting even these improvements need people ...

... and implementations that take 'hardware' into account

Application performance ("HEPSPEC06")
diverging from system capability ("SpecINT")



2007 Core 2 efficiency: Sverre Jarp, CHEP 2007 (!)

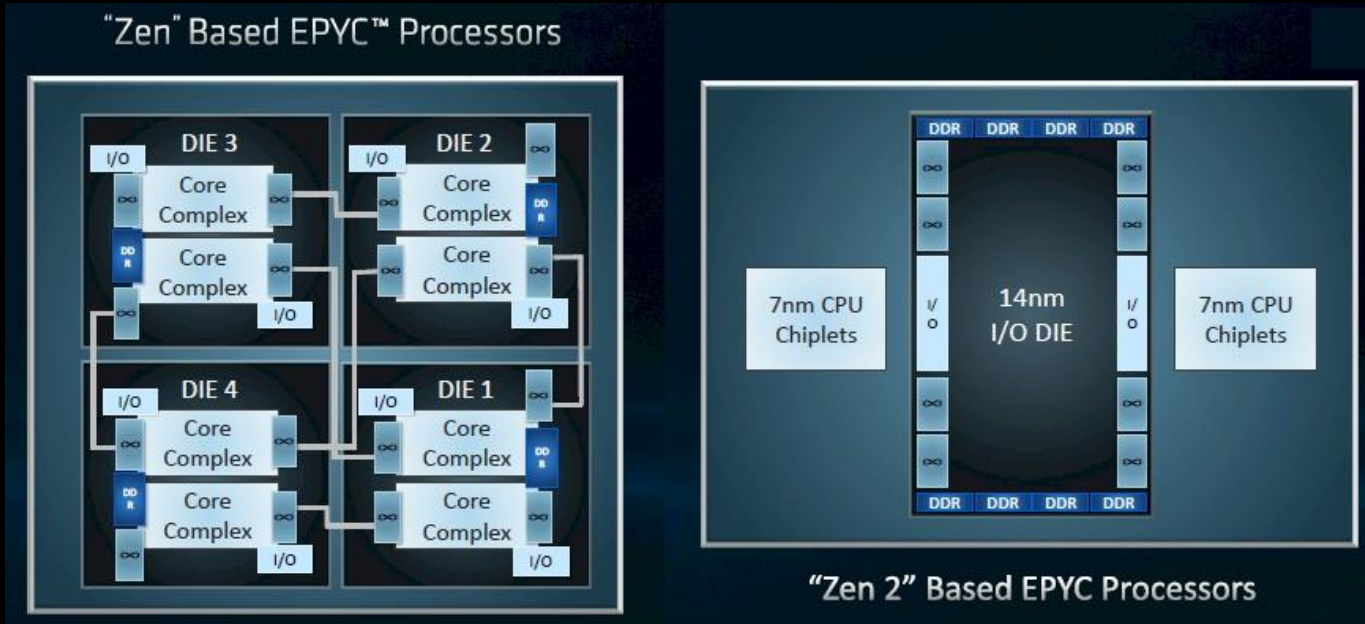


SPEC benchmark: spec.org, «Rate Base» (R/B) measures throughput under full load of all cores

Graph: measured HS06 and registered SpecINT06 Rate (base) performance per core, with SMT disabled, for the Nikhef Data Processing Facility NDPF (HTC compute) line is not monotonically increasing because of other design choices (power efficiency) and price-performance optimisation chosen

And of course depends on hardware & CPU architecture

AMD “Naples to Rome” – boost in application (“HS06”) performance due to new memory (I/O) architecture and direct access to all memory banks



And why some changes will not impact performance at all

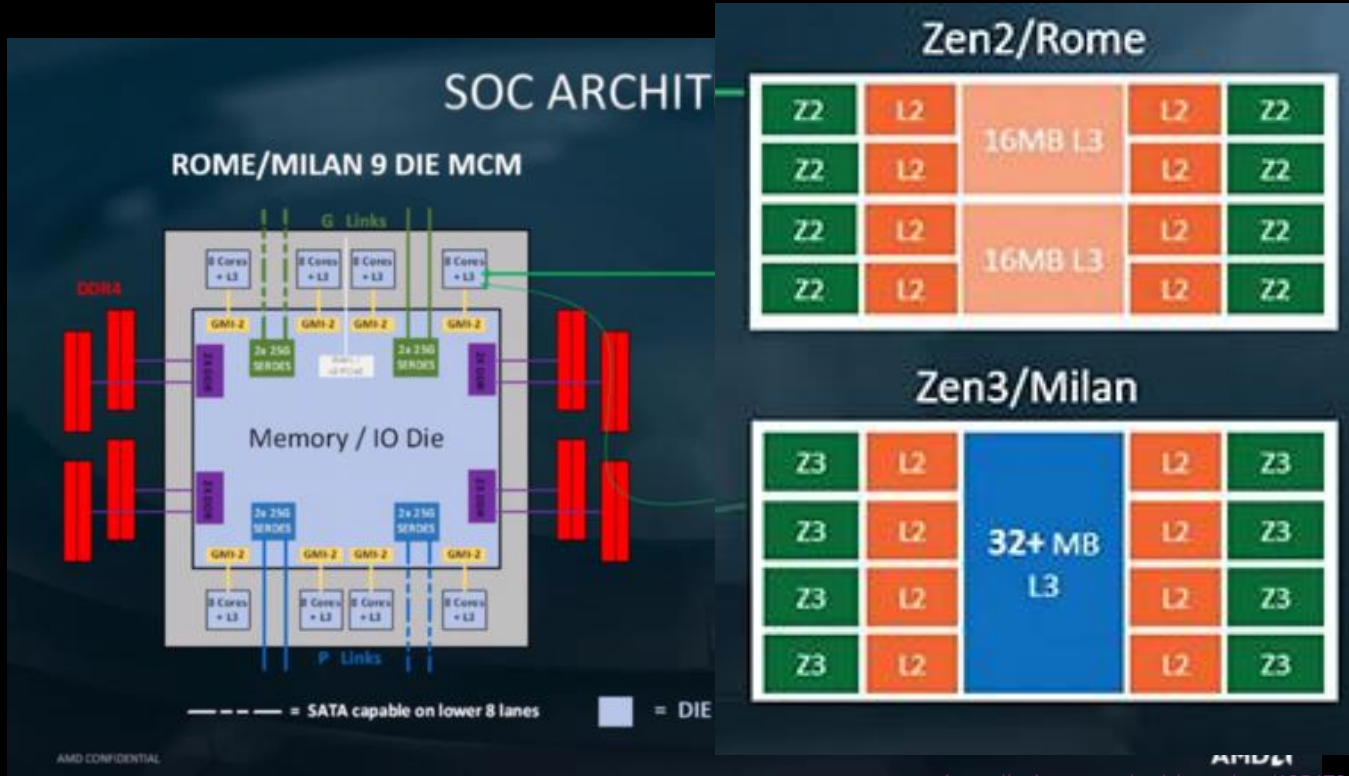


Image source: AMD, retrieved from <https://m.hexus.net/tech/news/cpu/135479-amd-shares-details-zen-3-zen-4-architectures/>

Bigger is Better - if you keep it together

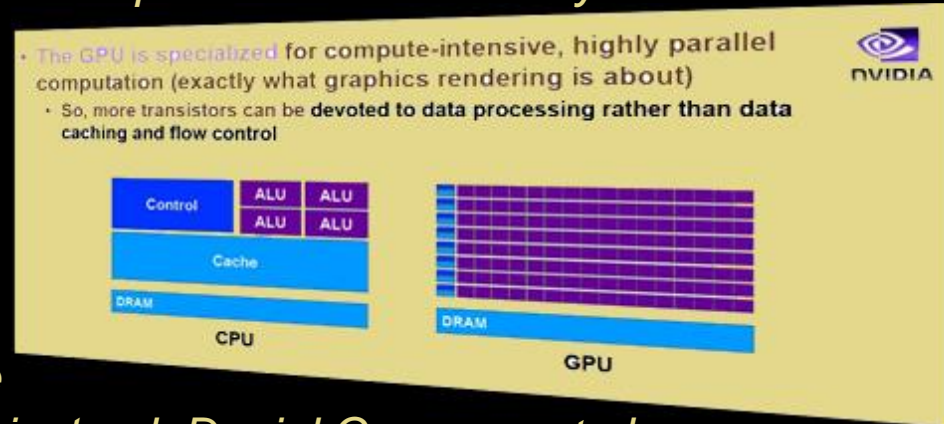
Common element: moving data is 'expensive', so
'keep on computing as long as you can, and don't move data around'

- e.g. AMD (and for others: single-socket systems), are better since there are *no (useless) cache coherency delays and improved direct memory access*
- similarly, keep your GPU busy ...
as data comes from (slow) RAM

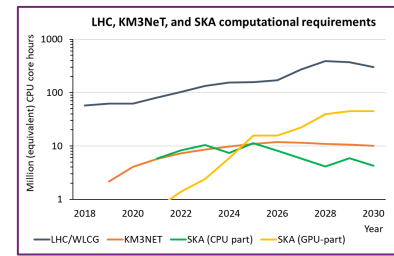


*Getting to be a quite specialised field
– use **frameworks** to implement key code*

... or just ask Daniel Campora et al.



and if it doesn't quite fit ...

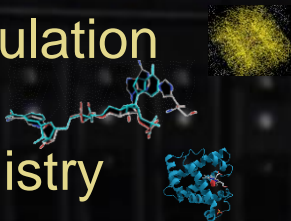


SuperMicro (branded as 'Lambda Blade')
4U chassis, supporting 10 consumer-grade GPUs ...
... with a bump

Beyond the single box

Luckily, many things in this world are *conveniently parallel*

- HEP events & simulation
- ligand matching
- structural biochemistry
- ...



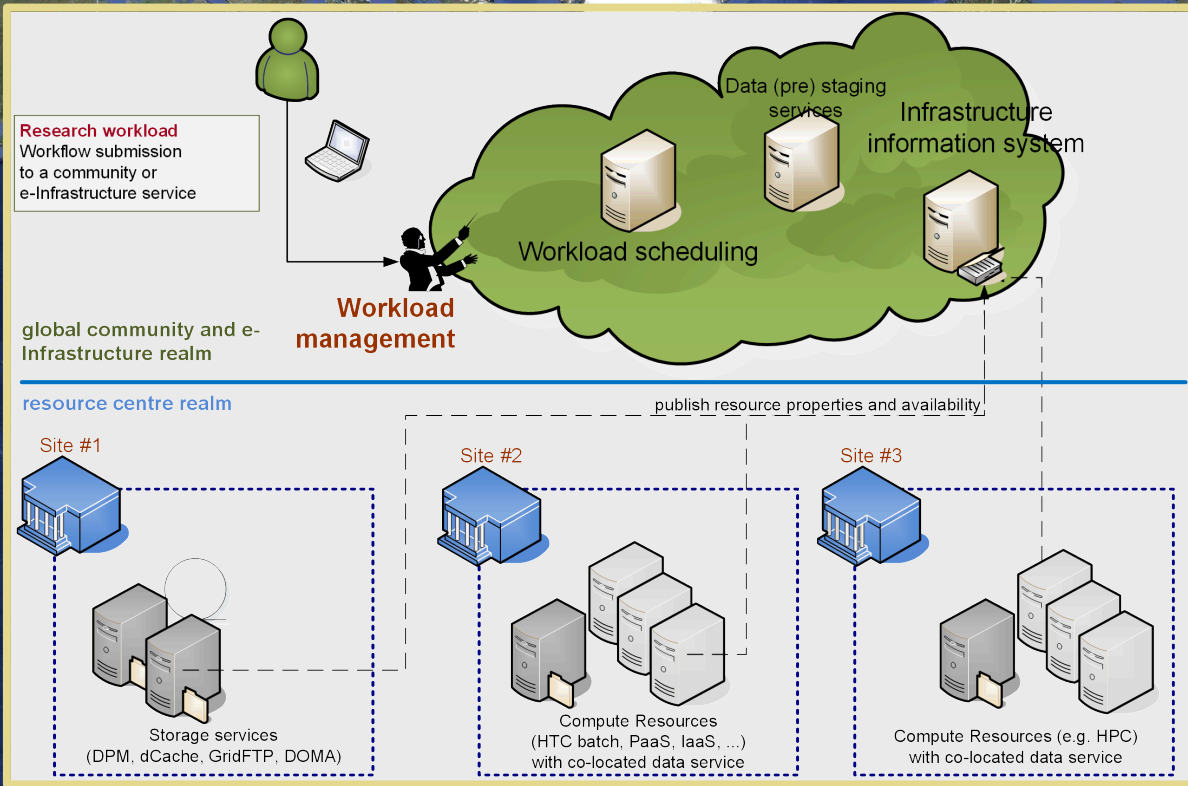
```
korf.nikhef.nl:
```

Job ID	Username	Queue	NDS	TSK	Req'd Memory	Req'd Time	S	Elap Time	
33134895.korf.nikhef.n	lhcbpi08	lhcb	1	1	5120m	41:59:57	R	37:46:21	wn-choc-023
33134901.korf.nikhef.n	lhcbpi08	lhcb	1	1	5120m	41:59:57	R	40:04:09	wn-smrt-128
33134908.korf.nikhef.n	lhcbpi08	lhcb	1	1	5120m	41:59:57	R	37:14:29	wn-choc-030
33134917.korf.nikhef.n	lhcbpi08	lhcb	1	1	5120m	41:59:57	R	14:23:42	wn-smrt-072
33135197.korf.nikhef.n	atlb019	atlasmc	1	4	16040	208:00:00	R	183:02:04	wn-mars-018+
wn-mars-018+wn-mars-018+wn-mars-018									
33135883.korf.nikhef.n	atlb019	atlasmc	1	4	16040	208:00:00	R	166:44:22	wn-mars-018+
wn-mars-018+wn-mars-018+wn-mars-018									
33142633.korf.nikhef.n	lhcbpi08	lhcb	1	1	5120m	41:59:57	R	37:30:47	wn-mars-043
33149106.korf.nikhef.n	lhcbpi08	lhcb	1	1	5120m	41:59:57	R	10:23:30	wn-car-027
33149132.korf.nikhef.n	lhcbpi08	lhcb	1	1	5120m	41:59:57	R	32:36:49	wn-mars-057
33149220.korf.nikhef.n	lhcbpi08	lhcb	1	1	5120m	41:59:57	R		4
33151669.korf.nikhef.n	lhcbpi08	lhcb	1	1	5120m	41:59:57	R		9
33152704.korf.nikhef.n	atlb019	atlasmc	1	4	16040	208:00:00	R		8+
wn-mars-018+wn-mars-018+wn-mars-018									



challenge is not in the parallelism itself,
but in **global compute with data**
just like difference between SI06 and HS06 showed data as the driving factor

Conveniently parallel: a global infrastructure for research



shared multi-community infrastructure

Already EGI e-infra has >250 communities just doing HTC

The screenshot shows the EGI operations portal interface. At the top, there is a "VO LIST" header. Below it, there is a "My VO(s)" section with a search bar and a table of Virtual Organizations (VOs). The table has columns for "VO", "Last update", "Last validation date", and "Last e".

VO	Last update	Last validation date	Last e
pvier	2017-04-28 16:31:53	2020-10-31 16:18:30	2015-1
xenon.biggrid.nl	2015-08-11 16:24:51	2020-10-31 14:19:26	2015-1

Below the table, there is a "Show 10 entries" option and a "Help" link. At the bottom, there is a table with columns for "Name", "Discipline(s)", and "Registry System".

Name	Discipline(s)	Registry System
acc-comp.egi.eu	• Support Activities	• VOMS

Showing 1 to 10 of 264 entries

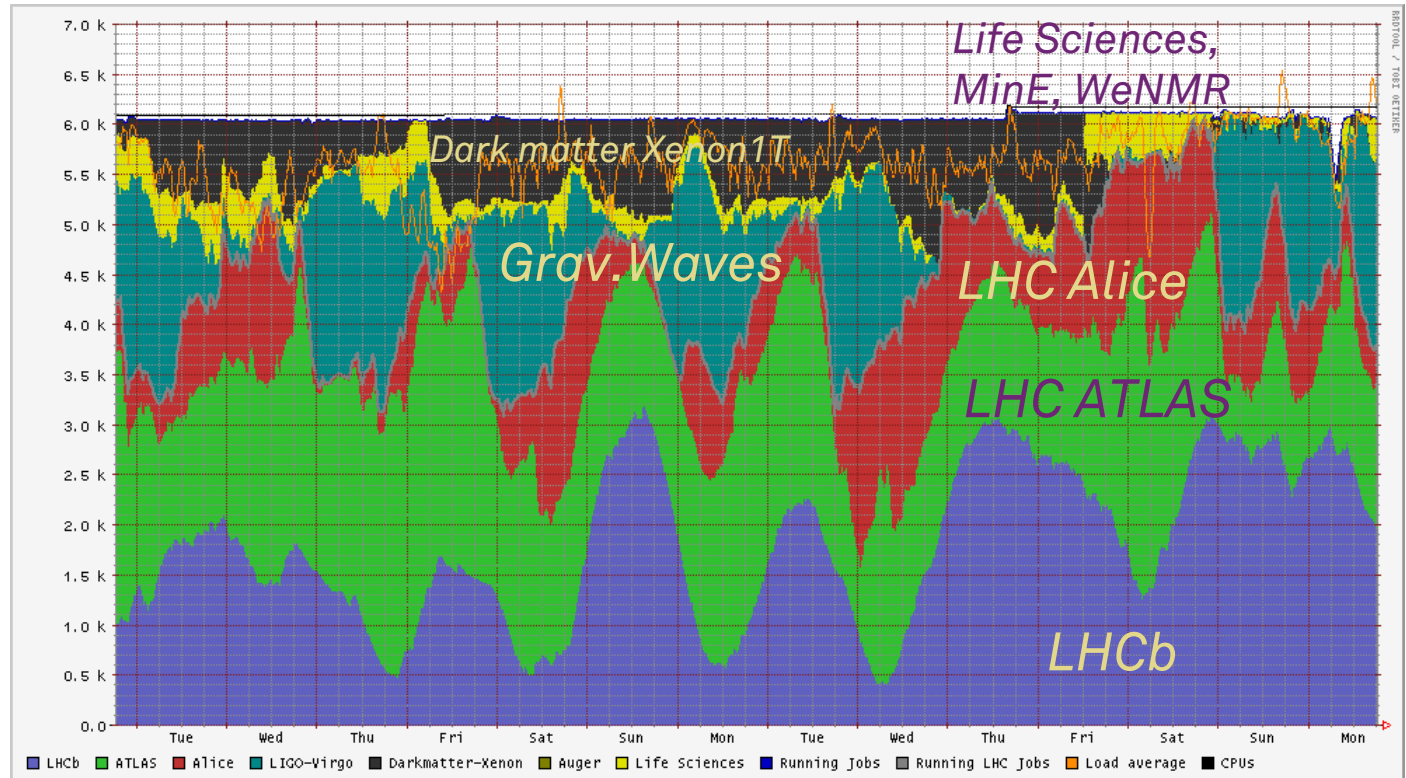
Nikhef Data Processing Facility – multi-community service

‘just one of these sites’

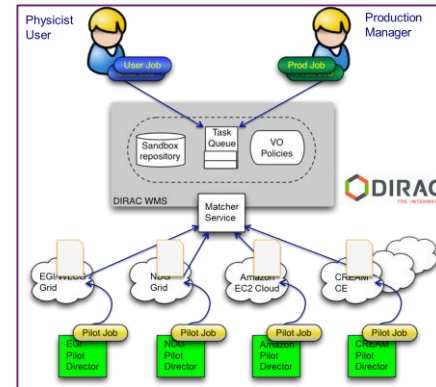
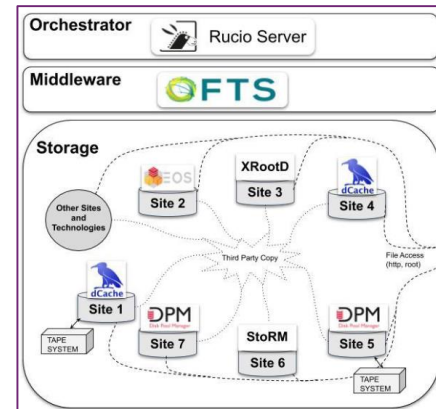
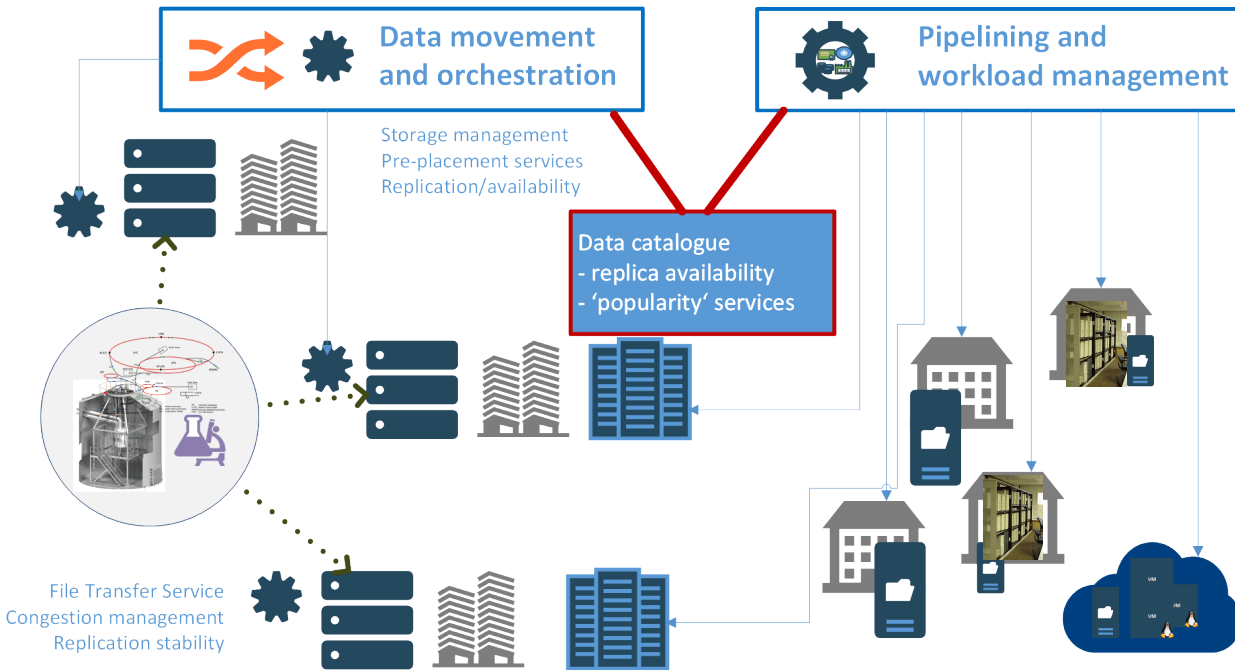


NDPF HTC platform

- member of a federated service with SURFsara, Nikhef, RUG-CIT
- high-throughput storage at SURFsara and Nikhef,
- long-term storage at SURFsara,
- interconnected by SURFnet, and authentication by TCS and IGTF



Getting the data to process ... in the right place



ESCAPE reference components: Rucio, FTS, and DIRAC

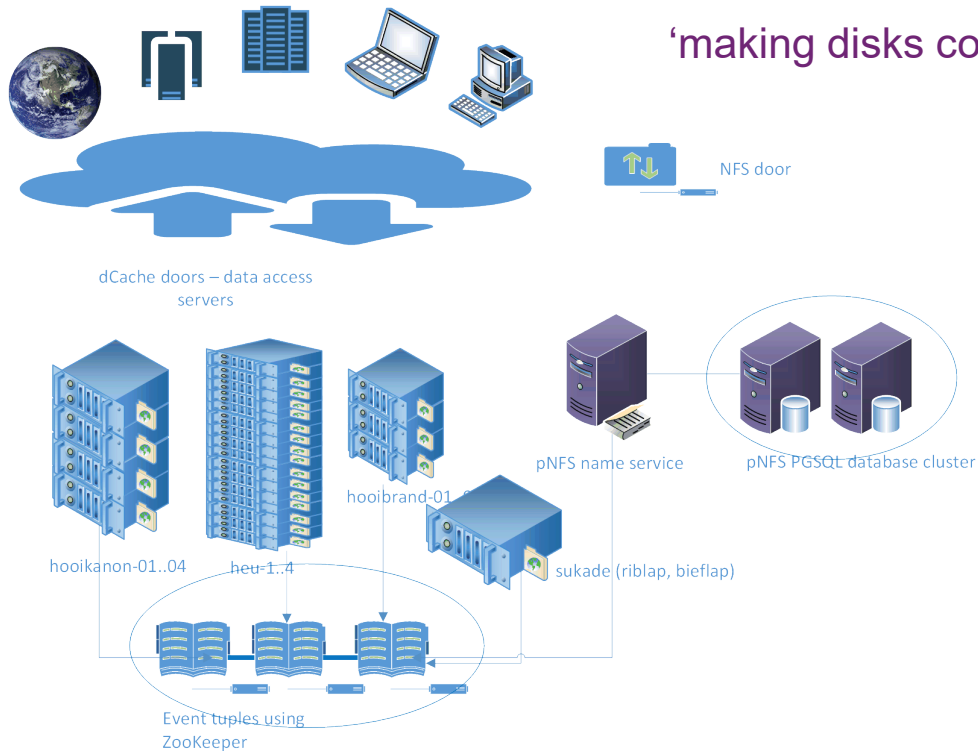
Rucio FTS image: "The ESCAPE Datalake" Aris Fkiaras, CERN, February 26th, 2020 ESCAPE WP2 eDIOS

<https://indico.in2p3.fr/event/20203/sessions/12778/#20200226>

DIRAC image from: A. Tsaregorodtsev, CPPM IN2P3

EGI Webinar, 7 June 2016 <https://indico.egi.eu/event/2973>

Nikhef storage infrastructure



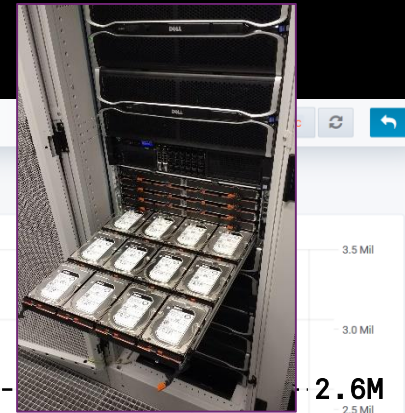
'making disks collaborate'



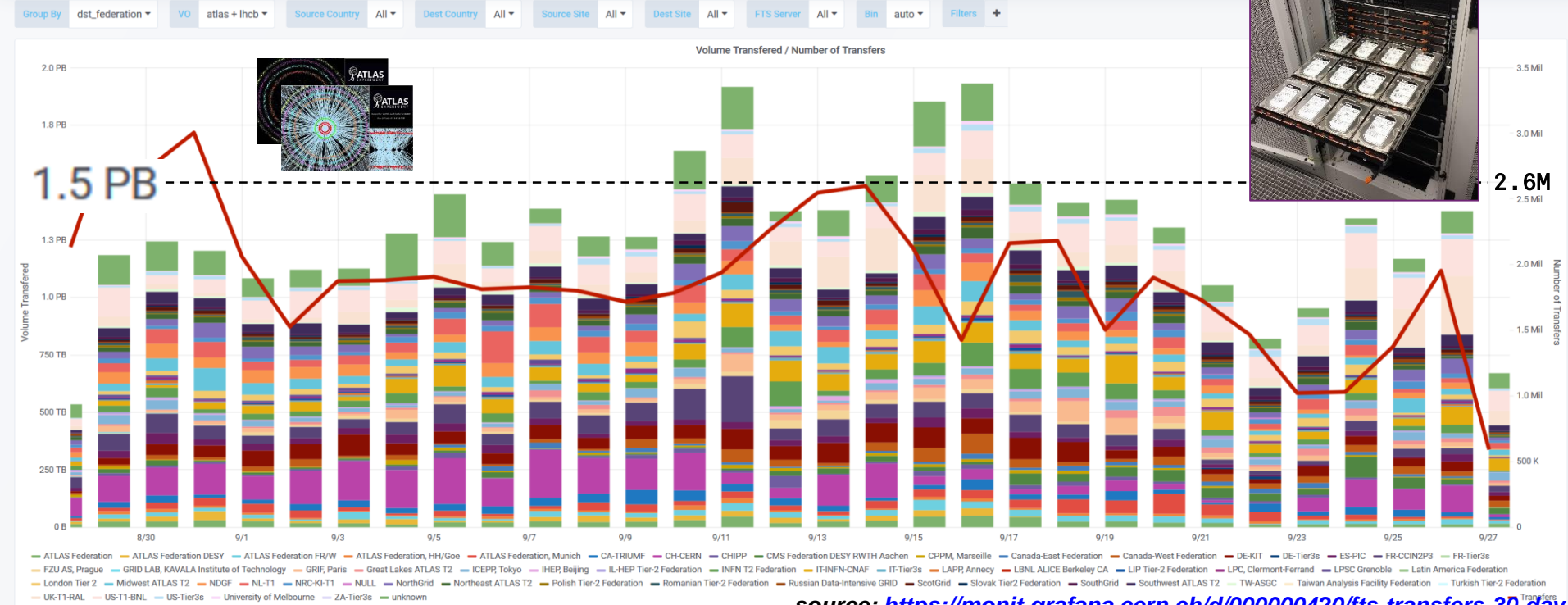
Storage as infrastructure – even a few PBytes requires some organization

- management challenge is **#files**, not capacity
- cost challenge is **throughput**, not capacity

Data distribution for WLCG



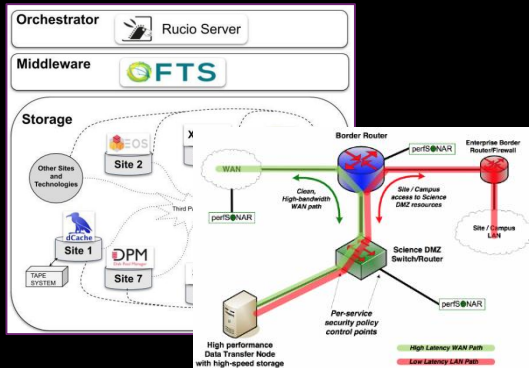
FTS Transfers (30 Days)



source: <https://monit-grafana.cern.ch/d/00000420/fts-transfers-30-day>

Structuring of frameworks impacts systems design

pre-staging all data locally supports
latency hiding, posix-style access with lseek(2), '\$TMPDIR'
e.g. why there are Data Transfer Nodes (DTNs) in the 'Science DMZ' concept



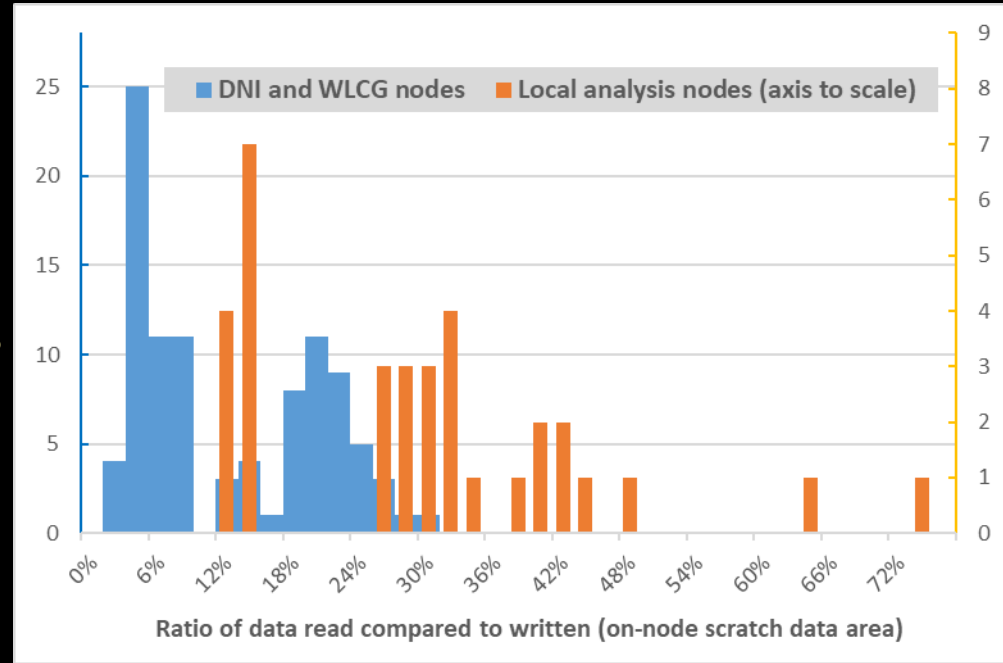
but, recently, pre-staging starts coming at a cost, when using SSDs as local data 'scratch' area ... because of their unique element: 'endurance'

WORN storage – Write Once Read Never

Frequency distribution observed on the NDPF execution nodes for outside ('grid') access (blue) and local access (orange)

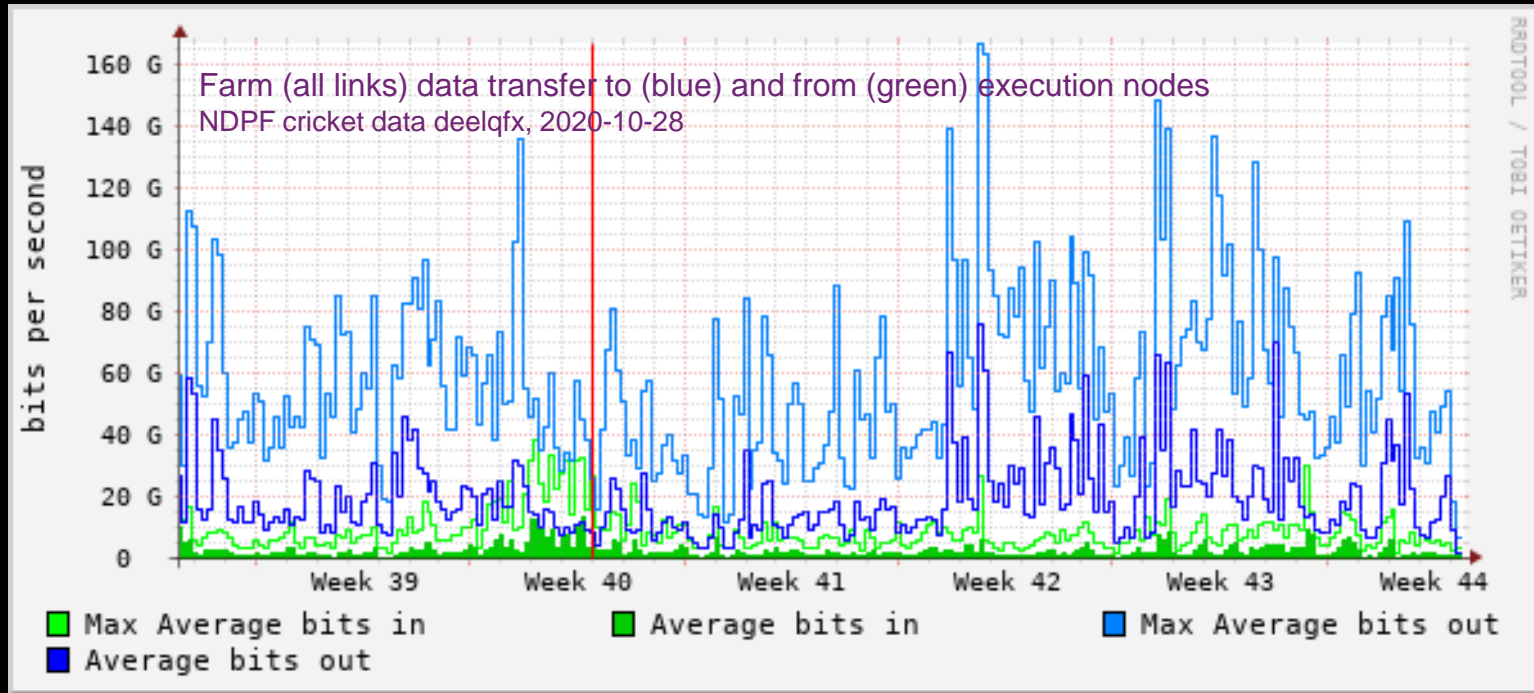
Access pattern is rather different. But why?

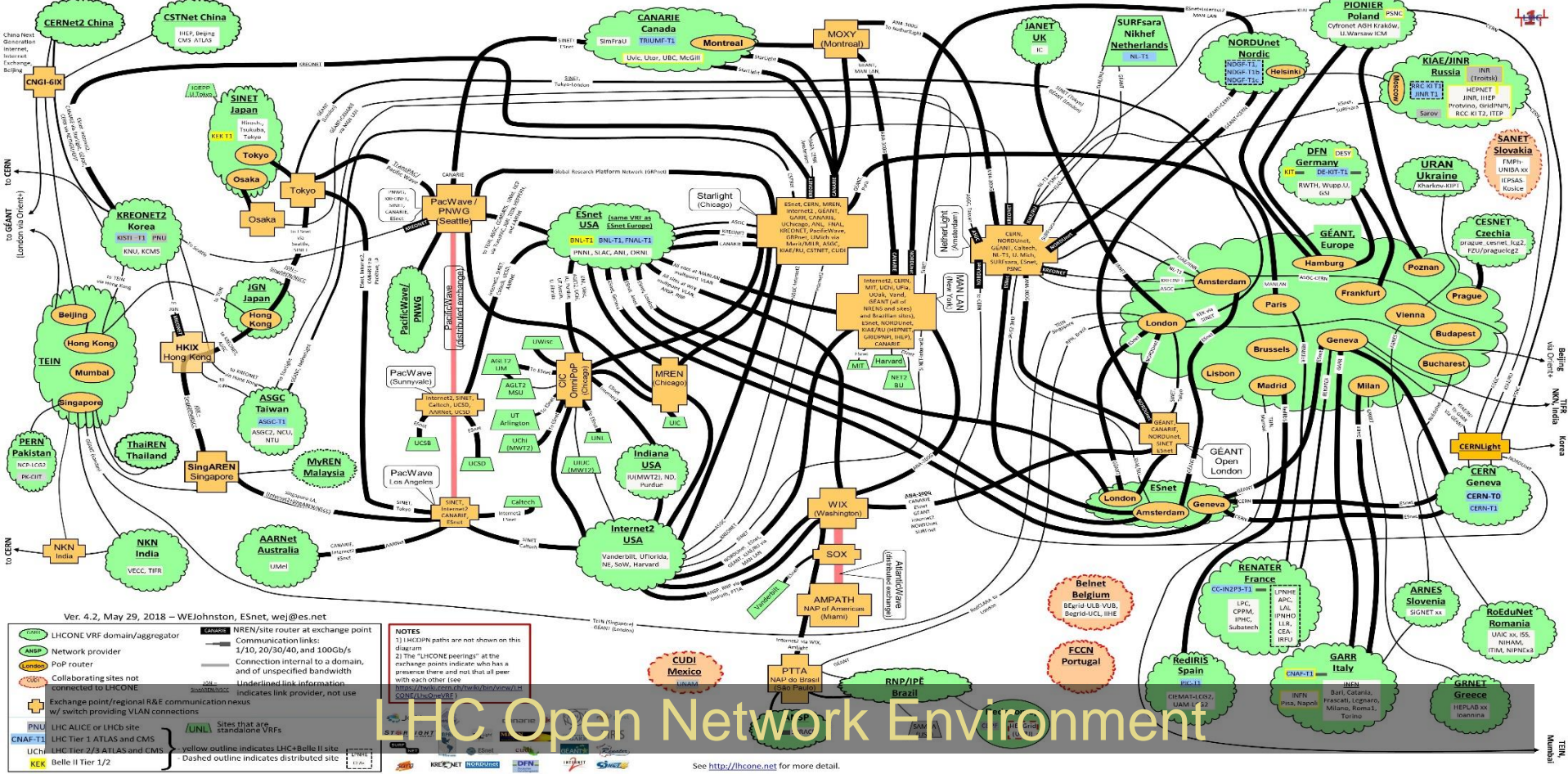
- external users pre-stage, because that is built into the frameworks (like DIRAC, Athena), where local users can use streaming access ('dCache NFSv4') *yet there are changes in pre-stage streaming behaviour over time*
- different types of workload: ntuple-data analysis vs (re)processing
- ...



Data: NDPF execution nodes, based on SSD SMART data, integrated over total device lifetime plot shows number of local analysis nodes scaled to DNI-WLCG count; collected using smartctl on 2020-10-28

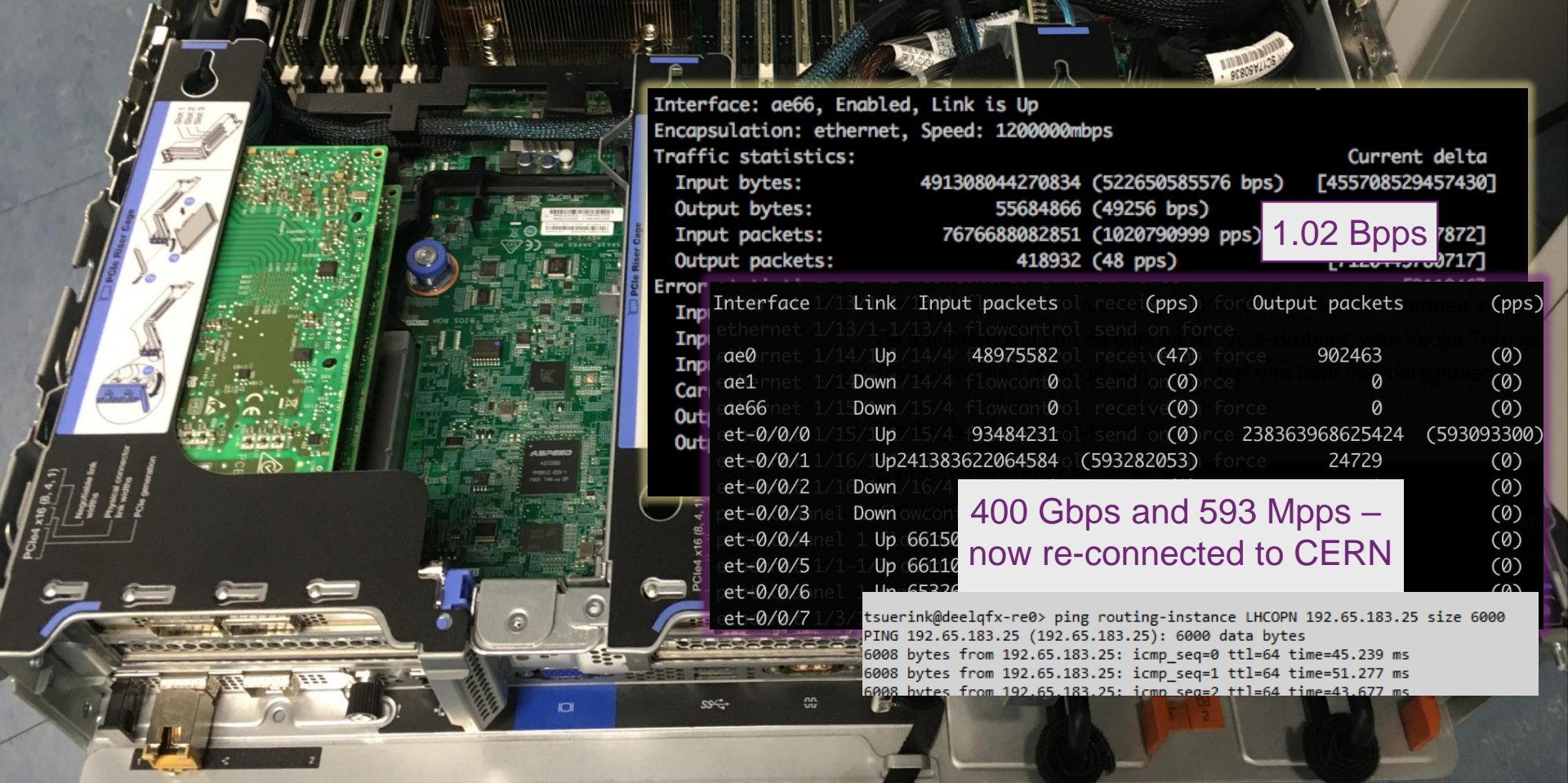
Data comes from somewhere, and has to go somewhere ...





LHC Open Network Environment

See <http://lhcone.net> for more detail.



```
Interface: ae66, Enabled, Link is Up  
Encapsulation: ethernet, Speed: 1200000mbps
```

```
Traffic statistics:                               Current delta  
Input bytes:           491308044270834 (522650585576 bps) [455708529457430]  
Output bytes:         55684866 (49256 bps)  
Input packets:       7676688082851 (1020790999 pps) [7872]  
Output packets:      418932 (48 pps) [712045700717]
```

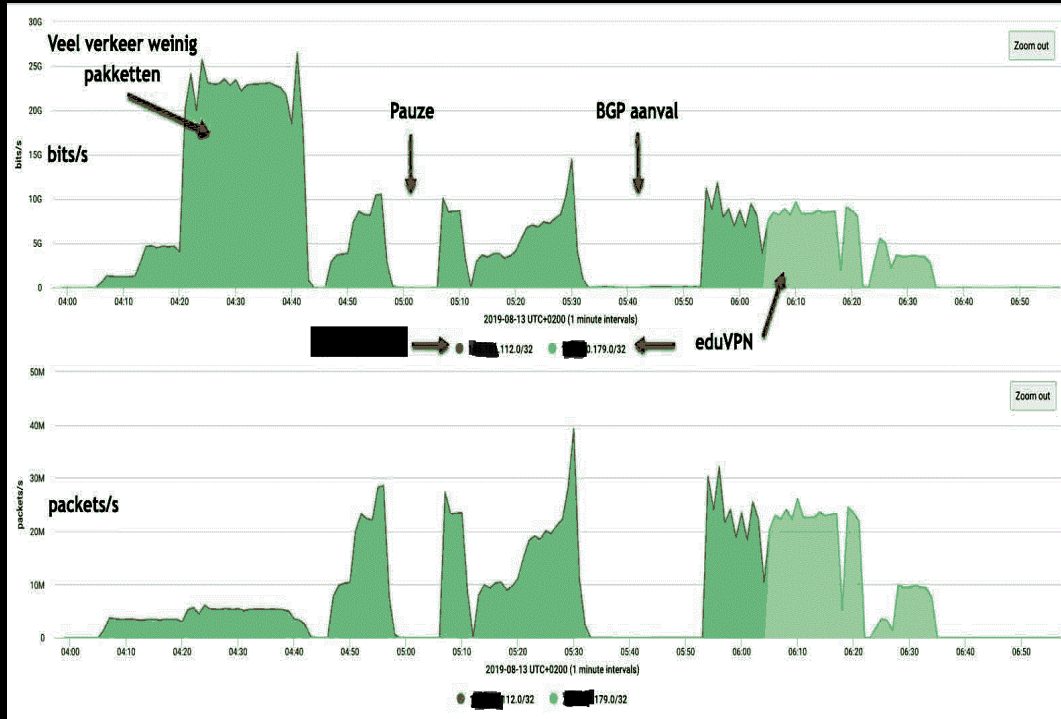
1.02 Bpps

```
Error  
Interface 1/1 Link / Input packets ol receive (pps) for Output packets (pps)  
Input ethernet 1/13/1-1/13/4 Flowcontrol send on force  
Input ae0 rnet 1/14/Up /14/4 48975582 ol receive (47) force 902463 (0)  
Input ae1 rnet 1/1/Down /14/4 Flowcontrol send on (0) receive 0 (0)  
Card ae66 net 1/1/Down /15/4 Flowcontrol receive (0) force 0 (0)  
Output et-0/0/0 1/15/Up /15/4 93484231 ol send on (0) receive 238363968625424 (593093300)  
Output et-0/0/1 1/16/Up 241383622064584 ol (593282053) force 24729 (0)  
Output et-0/0/2 1/1/Down /16/4  
Output et-0/0/3 net 1 Down owcon  
Output et-0/0/4 net 1 Up 66150  
Output et-0/0/5 1/1-1/Up 66110  
Output et-0/0/6 net 1 Up 65320  
Output et-0/0/7 1/3/
```

400 Gbps and 593 Mpps –
now re-connected to CERN

```
tsuerink@deeljfx-re0> ping routing-instance LHCOPI 192.65.183.25 size 6000  
PING 192.65.183.25 (192.65.183.25): 6000 data bytes  
6008 bytes from 192.65.183.25: icmp_seq=0 ttl=64 time=45.239 ms  
6008 bytes from 192.65.183.25: icmp_seq=1 ttl=64 time=51.277 ms  
6008 bytes from 192.65.183.25: icmp_seq=2 ttl=64 time=43.677 ms
```

Our science data looks akin to a DoS



evaluating resilience to cyberattack – *in a cooperative way*

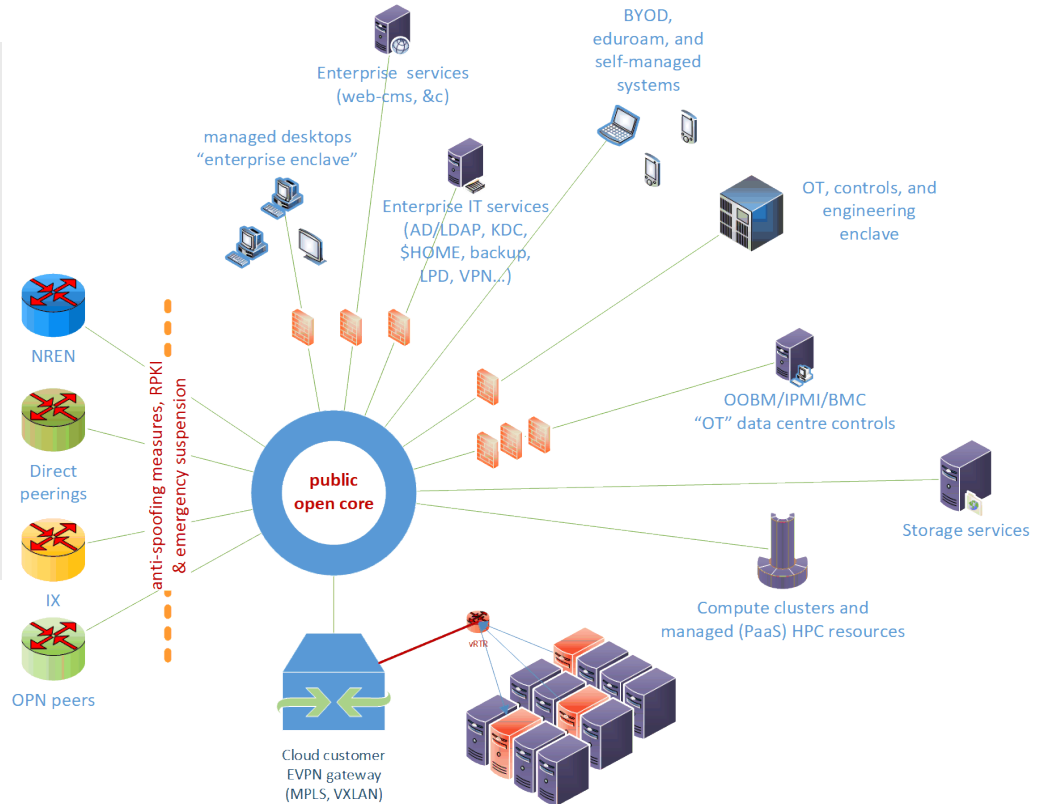
Segmentation: a network of 'private domain' clouds within

open-core research network model implements the enclave structure

protects against overload by *no stateful components in the network path*

and allows open research federated cloud using eVPN overlays

although you'll always have some (reputational) risks even if you advertise the block as 'customer network devices'



Nikhef cloud – targeting high-throughput use cases

openstack. NDPFcloud davidg

Instances

Instance ID =

Displaying 5 items

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
testje	-	145.110.24.17	basic	dennisvd	Active	nova	None	Running	4 days, 17 hours	Create Snapshot
c8local	c8	145.110.24.4	basic	dennisvd	Active	nova	None	Running	1 week, 2 days	Create Snapshot
newcentos-centos8-clou						nova	None	Running	2 weeks, 1 day	Create Snapshot
						nova	None	Shut Down	3 weeks, 3 days	Start Instance
						nova	None	Shut Down	3 weeks, 3 days	Start Instance

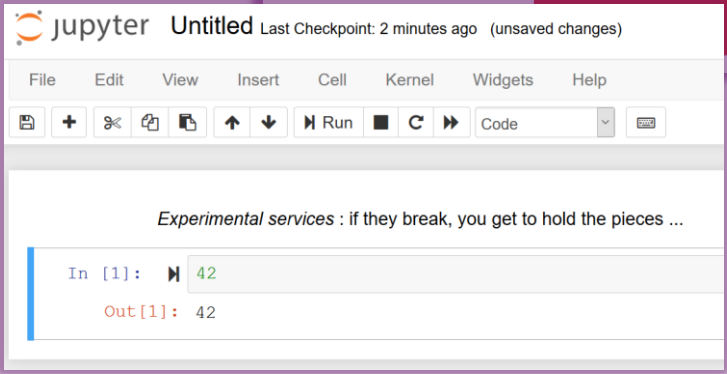
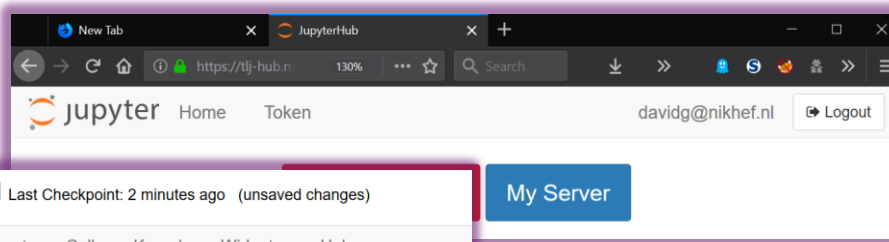
- ‘MPLSoUDP-eVPN’ using Tungsten Fabric
- no NAT overhead – use public IP for external traffic
- same 40/100G substrate network
- direct access to storage network



There is NO CLOUD, just other people's computers

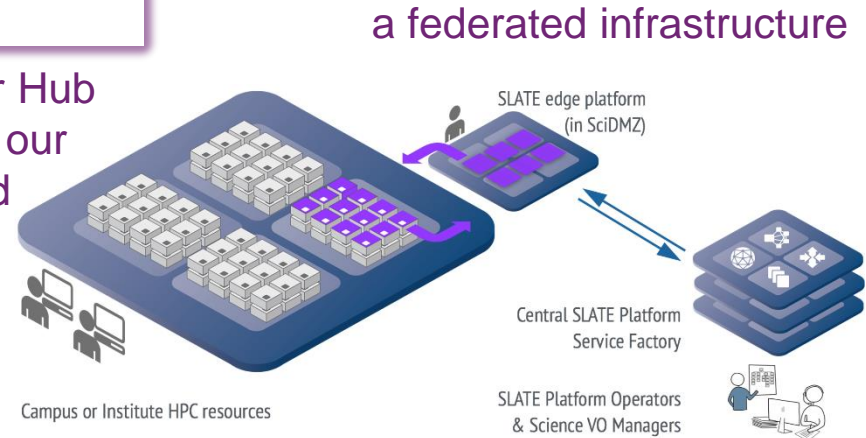
Image source: Free Software Foundation Europe - <https://fsfe.org/>

Nobody wants a cloud ... you want a solution! *research community overlays and 'virtual clusters'*



My Server

NDPF Jupyter Hub
experiment in our
on-prem cloud



at scale: container computing, yet with curated application images – slateci.io

Cross-organisation infrastructure *we need an 'ecosystem' more than a cloud*

on-prem cloud, or research cloud, is oft better

- very cost-efficient if utilised at capacity
- effective as it can provide more than 'IaaS'
- can leverage our own R&E federated access

and not all 'cloud' is what you think it is ...

EOSC – the European Open Science Cloud *more an ecosystem (or 'web of data') than a 'cloud'*

Photo by Pop & Zebra on Unsplash



PROMPTING AN EOSC IN PRACTICE

"We are creating a European Open Science Cloud now. It is a trusted space for researchers to store their data and to access data from researchers from all other disciplines. We will create a pool of interlinked information, a 'web of research data'. Every researcher will be able to better use not only their own data, but also those of others. They will thus come to new insights, new findings and new solutions."



Ursula von der Leyen,
European Commission President
World Economic Forum in Davos,
January 2020



sources: <https://www.eoscsecretariat.eu/eosc-symposium-programme>

An ecosystem built on federated infrastructures

The image displays two overlapping screenshots of the European Open Science Cloud (EOSC) Portal. The top screenshot shows the main navigation menu with options like 'About', 'Services & Resources', 'Policy', 'Use Cases', 'Media', 'For providers', 'Subscribe', and 'Using the Portal'. A dropdown menu is open under 'Services & Resources', listing categories such as 'Sharing & Discovery', 'Processing & Analysis', 'Data Management', 'Compute', 'Storage', 'Networking', 'Training & Support', 'Security & Operations', and 'Help Desk'. The bottom screenshot shows a search results page for 'Data' (50 results), listing services like 'AMNESIA' (Anonymize your datasets) and 'French Tuna Atlas Spatial Data Catalog'. The AMNESIA entry includes a star rating of 0/5, a heart icon, and an 'ADD TO COMPARE' button. The French Tuna Atlas entry also includes a star rating of 0/5 and an 'ADD TO COMPARE' button. The background of the top screenshot features a large illustration of a globe with a ladder, representing the 'Open Cloud Strategic Innovation' theme.

Whence we came: the long road to federated access

From disparate systems in ~2000

separated authentication and authorisation, splitting *identity sources, community membership, and services*

NIKHEF
NATIONAAL INSTITUUT VOOR KERNFYSICA EN HOGE-ENERGIEFYSICA

Guest / students form (please with a copy of your identity card)

CERN/User Registration Date: 01.03.2004
CERN COMPUTER CENTRE - USER REGISTRATION FORM
<http://cern.ch/it/documents/ComputerUsage/CompAccountRegistrationForm-English.pdf>

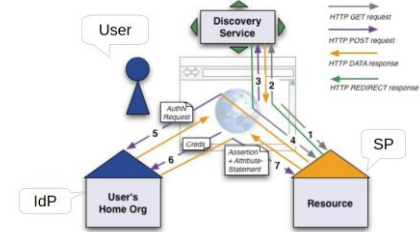
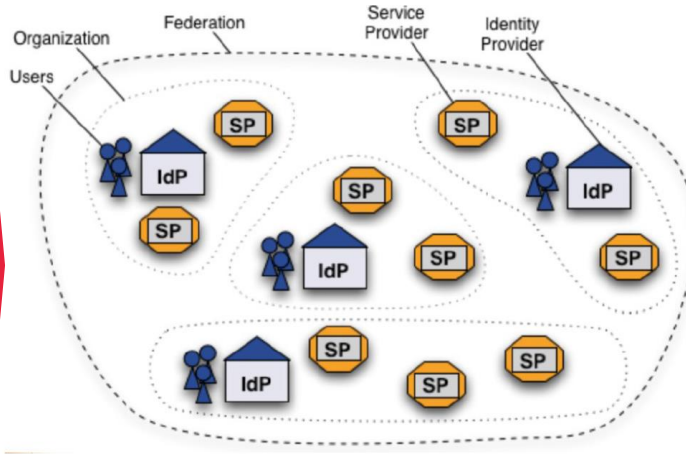
To be returned to the User Registration box at the entrance of Building 513, after being completed by a user who requires a computer account in a Central Service provided by IT Department, and is not yet registered in another group or system or has already signed it before.

To be completed by the User:
It is **MANDATORY** to provide the following information (except those with an *). It will be treated confidentially and only be used for ensuring correct identification.
Supply name as registered by the Users' Office or HR Division.
FAMILY NAME(S):
FIRST NAME(S):
SEX [M] [F] BIRTHDATE: Day Month Year
HOME INSTITUTE/FIRM:
NATIONALITY: *CERN SUPERVISOR.....
*CERN DEPARTMENT: *CERN ID NUMBER (as on CERN card).....

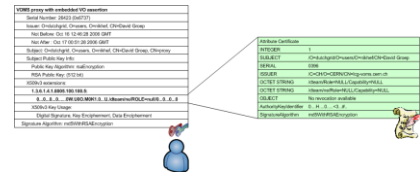
To be completed by the Group Administrator:
University or Institution Name: **FLORIDA STATE UNIVERSITY** Phone Number: **850 644-XXXX**

Exp. / Dept.	Spokesperson	Home Institution Contact	Contact Telephone
D0	WOMERSLEY WEERTS	SHARON HAGOPLAN	850 644 4777

CERN User Registration
Date: 01.03.2004
CERN COMPUTER CENTRE - USER REGISTRATION FORM
FAMILY NAME(S):
FIRST NAME(S):
SEX [M] [F] BIRTHDATE: Day Month Year
HOME INSTITUTE/FIRM:
NATIONALITY: *CERN SUPERVISOR.....
*CERN DEPARTMENT: *CERN ID NUMBER (as on CERN card).....



SAML2.0 auth flow



Federated (R&E) AAI, the global IGTF PKI, VOMS, and 'AARC BPA' AAI architecture all have this as fundamental property

VO Management System
VOMS attributes certificates

Shibboleth IdP image: SWITCH (CH)

Federated Access

Login via the Nikhef service proxy to *gitlab*, *ifosim.org*, ...

“Where are you from”

discovery screen showing entities from the eduGAIN global interederation

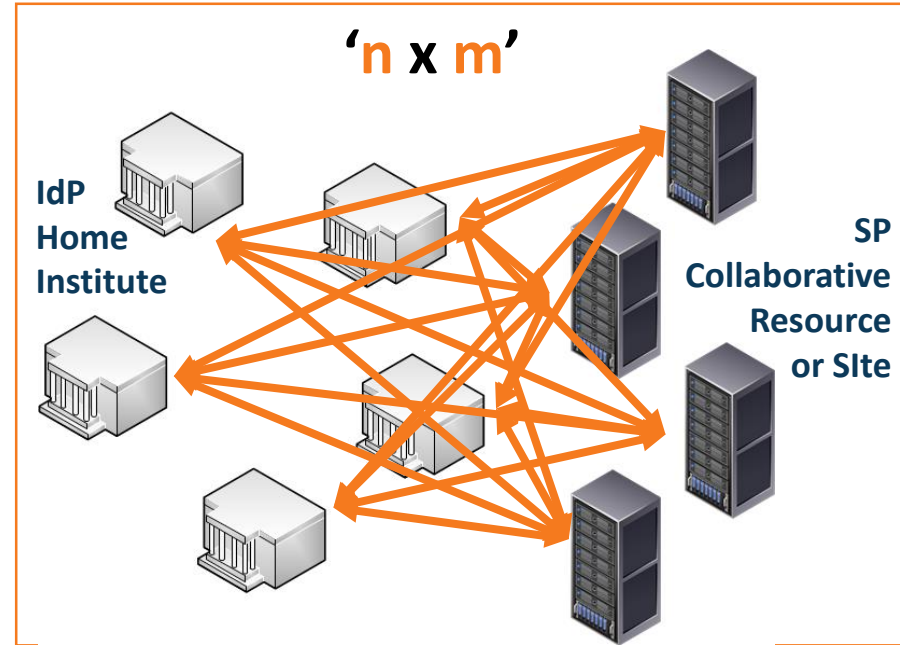


Challenges of scaling federation

Beyond 'enterprise' services, it becomes challenging!

Collaborations - by design - have their services distributed *and*

- not that many collaborations are a legal entity
- or not 'legally authoritative' for constituent services
- or run into risk-averse, or slow, 'home organisations'



Scaling community and institutional trust

eduGAIN (global R&E) Entity Categories

Curated grouping of entities
‘REFEDS R&S’
this is a research service

‘DP CoCo’
abides by GDPR

‘Sirtfi’
cares for security response



slower adoption process
adding identity assurance needs
action at all 60+ Feds & 4k+ IdPs

e-Infrastructure IGTF Authentication Profiles

Common baseline and profiles
co-defined by relying parties

user-centric ID harmonisation
with unique global naming
‘BIRCH’

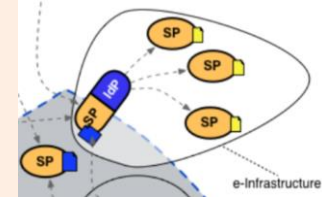
real person with real name

‘DOGWOOD’
persistent linkable identifier



research-specific user base

Use of proxy bridging components




Identity and access ‘proxy’
harmonised eduGAIN IdPs

based on entity categories
leverage Sirtfi and ‘R&S’
proxying is bi-directional

responsibility on the proxy operator

Research-friendly federation: REFEDS R&S ... or SRAM



REFEDS Spaces Search Log in

Entity-Categories

Pages / Entity-Categories Home

Research and Scholarship

Created by Nicole Harris, last modified on Apr 30, 2020

Pages

Blog

CHILD PAGES

- Entity-Categories Home
- Research and Scholarship
- Research and Scholarship FAQ

For IdP Operators

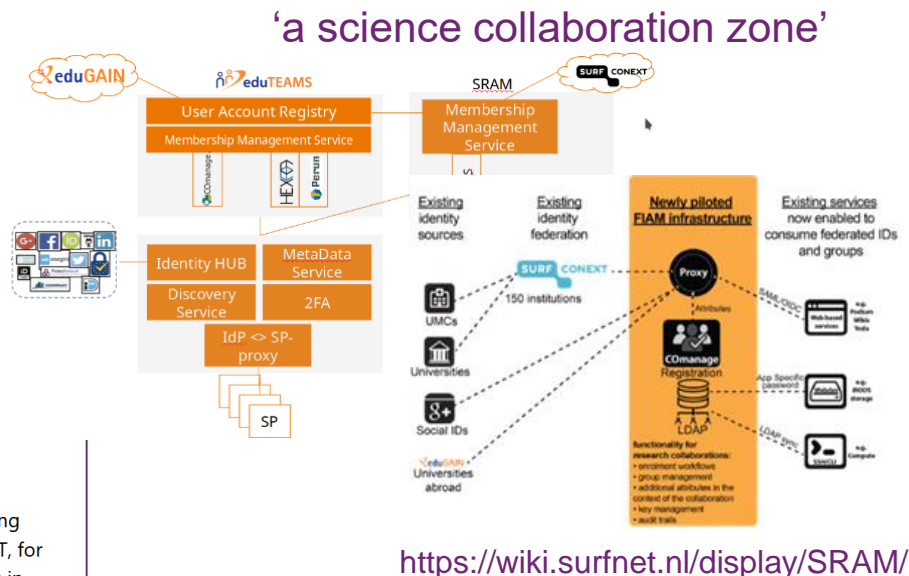
What attributes should be released by an R&S IdP?

The Research & Scholarship specification defines a bundles of attributes the Providers are encouraged to release to R&S services:

- personal identifiers: email address, person name, eduPersonPrincipaln
- pseudonymous identifier: eduPersonTargetedID
- affiliation: eduPersonScopedAffiliation

Category support is defined as follows:

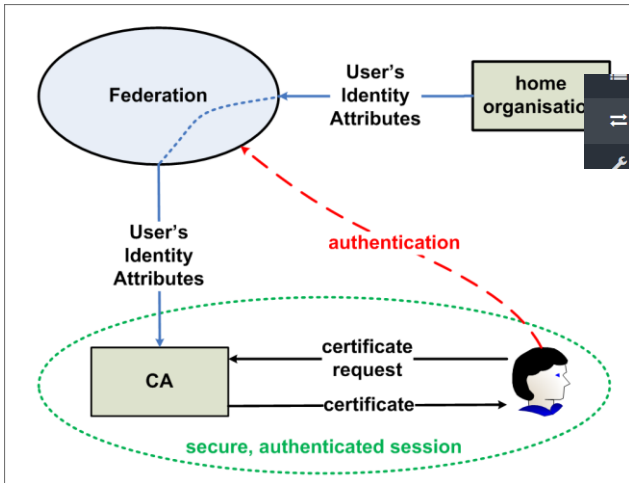
An Identity Provider indicates support for the R&S Category by exhibiting the R&S entity attribute in its metadata. Such an Identity Provider MUST, for a significant subset of its user population, release all required attributes in



<https://refeds.org/SIRTFI>
<https://refeds.org/assurance>
<https://refeds.org/category/research-and-scholarship>

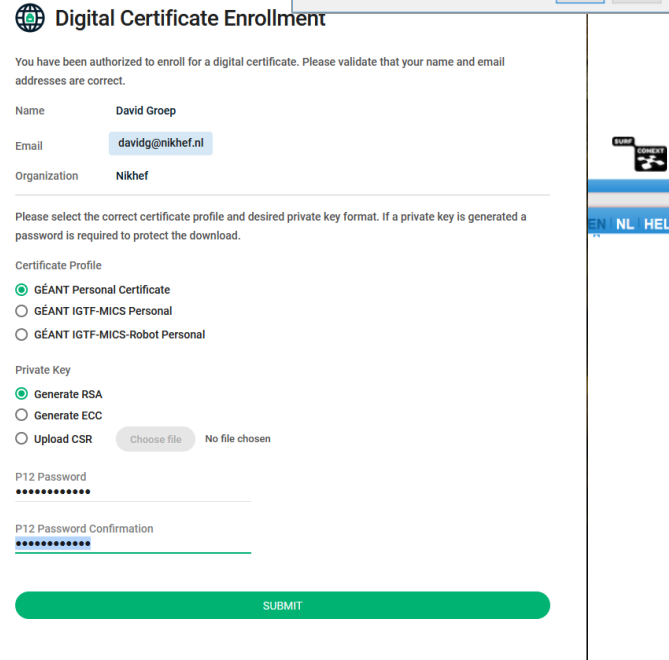
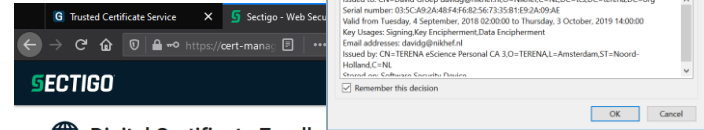
Bridges and Token Translation Services

GEANT Trusted Certificate Service



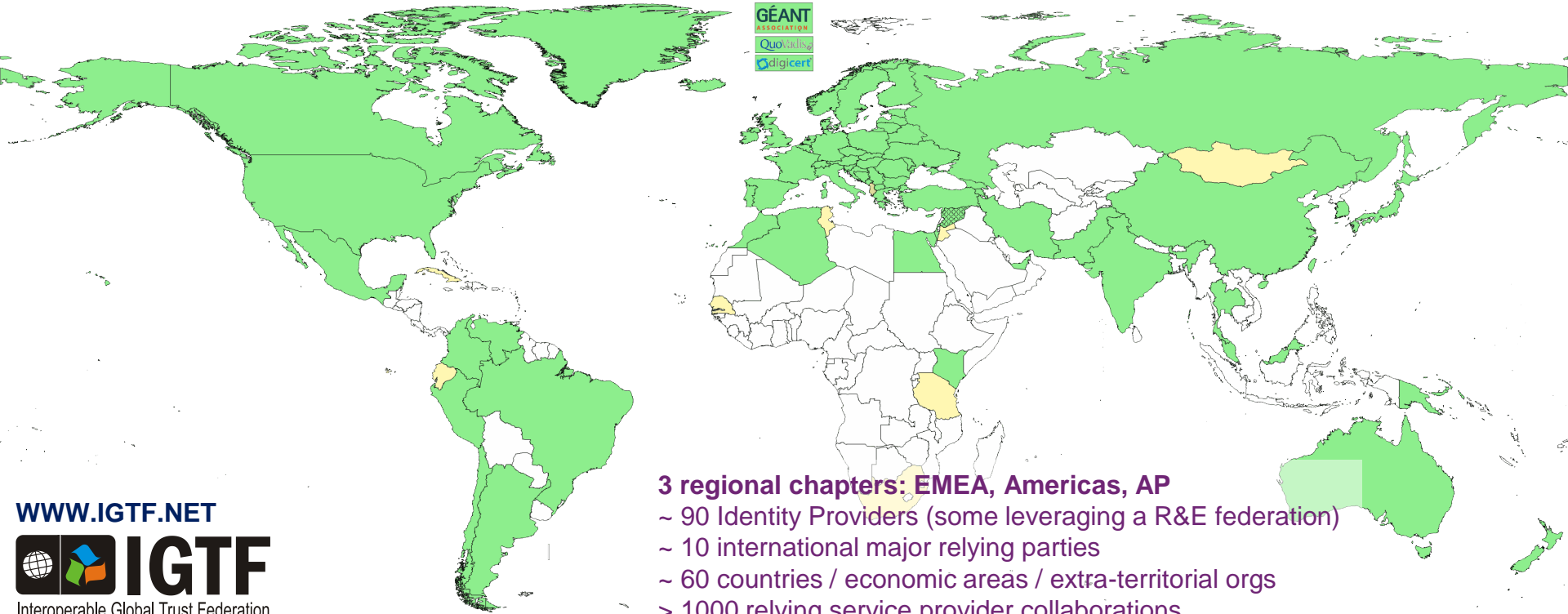
Organization Mapping

Organization	Attributes
Nikhef	nikhef
FORM INSTITUTE AMOLF	



TCS (today: Sectigo) acts as SAML Service provider to eduGAIN: eligible authenticated users can obtain client certificate for access and delegation to services

Interoperable Global Trust Federation IGTF



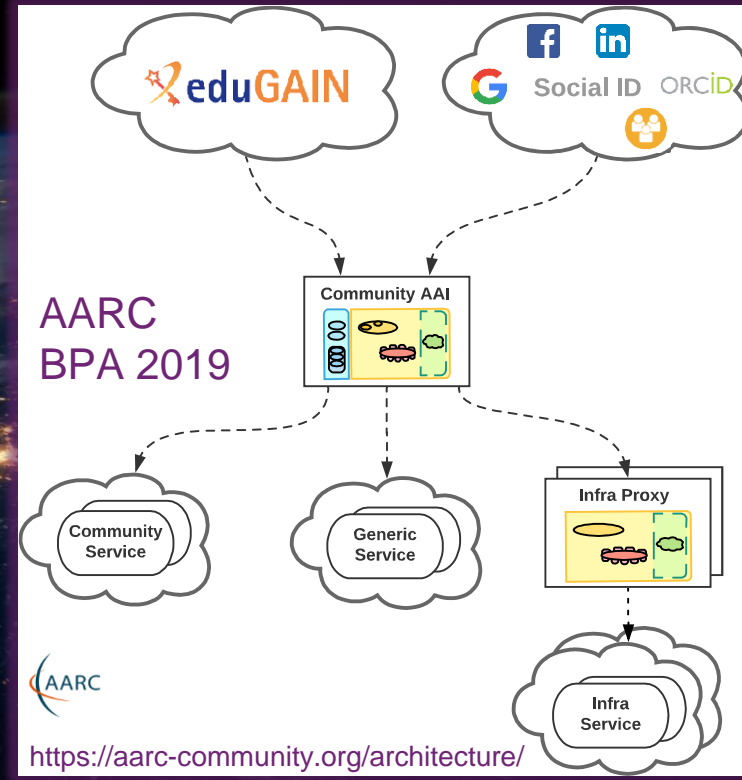
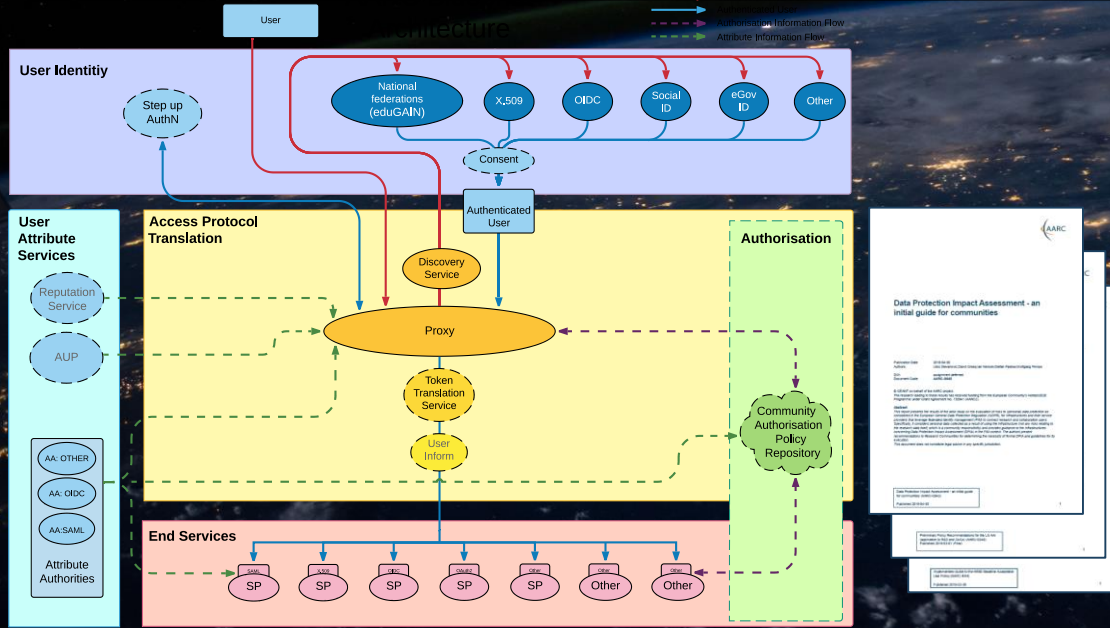
- 3 regional chapters: EMEA, Americas, AP**
- ~ 90 Identity Providers (some leveraging a R&E federation)
- ~ 10 international major relying parties
- ~ 60 countries / economic areas / extra-territorial orgs
- > 1000 relying service provider collaborations

WWW.IGTF.NET



'Community First' AARC Blueprint Architecture: the Proxy

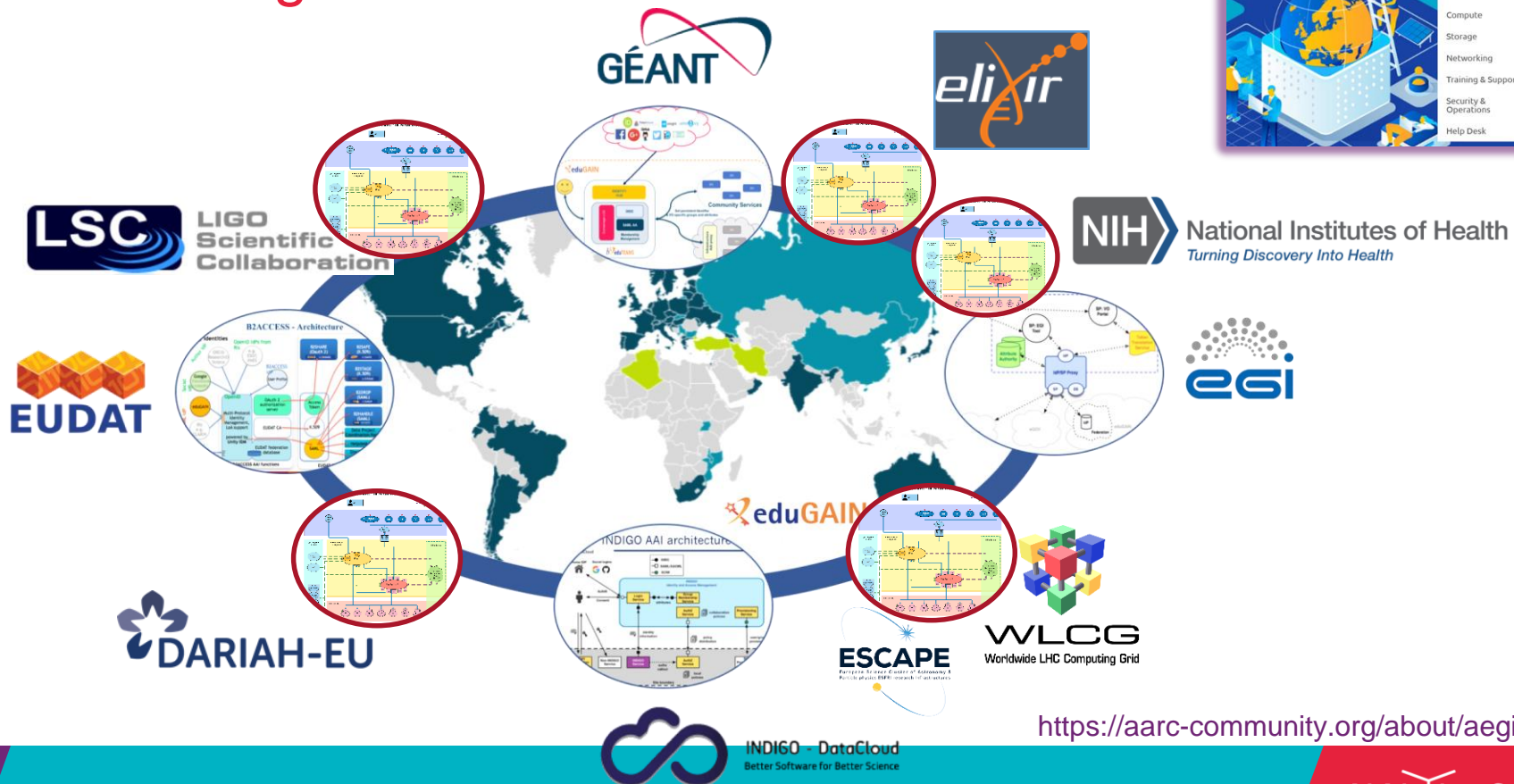
... user and group ID same across services
 ... minimize discovery 'wayf' & info screens



Interconnecting communities and infrastructures

EUROPEAN OPEN SCIENCE CLOUD

- About
- Services & Resources
- Sharing & Discovery
- Processing & Analysis
- Data Management
- Compute
- Storage
- Networking
- Training & Support
- Security & Operations
- Help Desk

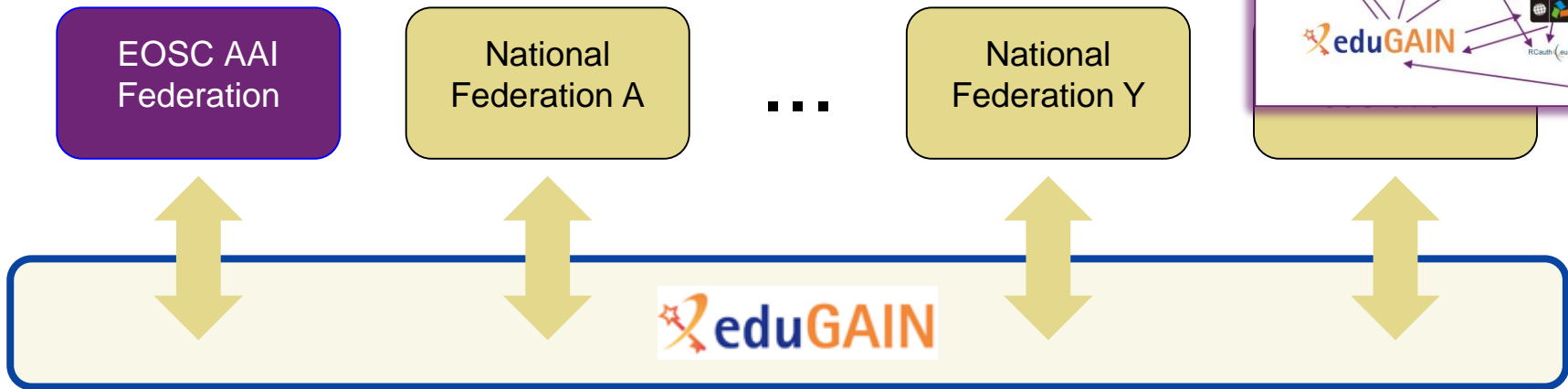


<https://aarc-community.org/about/aegis/>

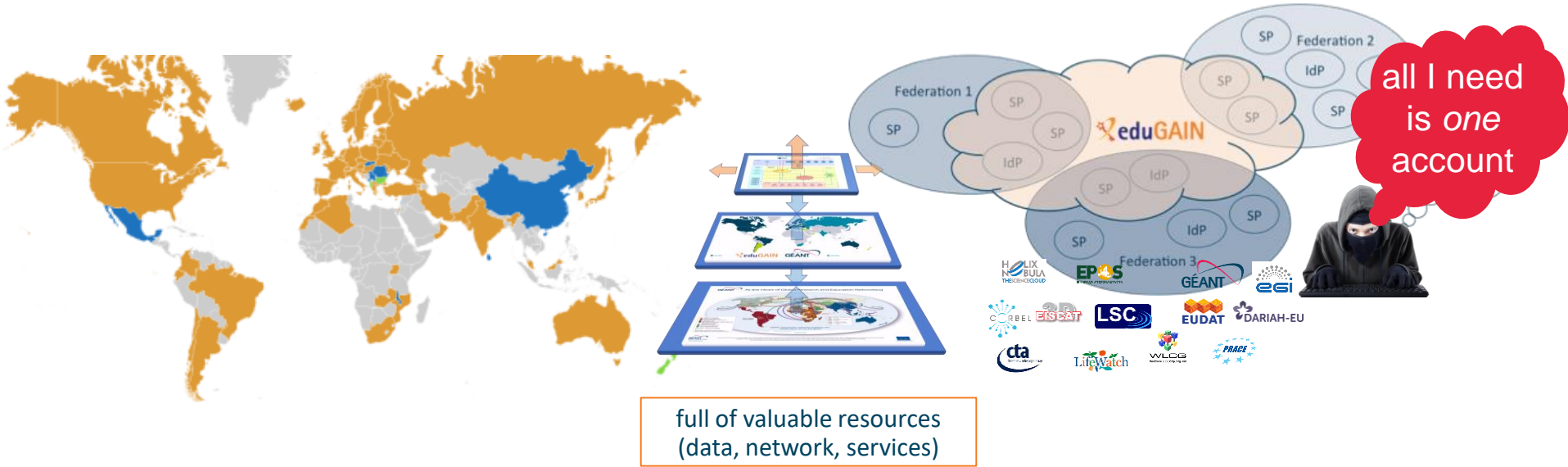
Linking the providers and users together - AAI

AARC BPA's 'community-first' model does not cover all EOSC cases, e.g. *infrastructures acting as providers **and** suppliers **and** as attribute authority*

turn EOSC entities into a federation itself, linked to eduGAIN, preventing 'user loops' & meeting common (security) baseline



Now *what* have we built?!



We have federation and single sign-on ...
... but can we share security information when needed?
... timely and confidentially, protecting everyone's reputation?

Assessing risk ... in a collaborative infra



L Florio¹, S Gabriele², F Gagadis³, D Groep⁴, W de Jong⁵, U Kaila⁶, D Kelsey⁷, A Moens⁸, I Neilson⁹, R Niederberger¹⁰, R Quisq¹¹, W Raquel¹², V Rbailier¹³, M Salie¹⁴, A Scicchitano¹⁵, H Short¹⁶, A Stiegel¹⁷, U Stevanovic¹⁸, G Venekamp¹⁹ and R Warter²⁰

The WISE SCIv2 Working Group - e-mail: david.kelsey@feri.ac.uk, sci@wise-community.org

¹GEANT Association, Amsterdam, The Netherlands; ²Nikhef, Amsterdam, The Netherlands; ³GEANT Ltd., Cambridge, United Kingdom; ⁴SRF/Fara, Amsterdam, The Netherlands; ⁵SCS, IT Center for Science Ltd., Espoo, Finland; ⁶STFC, Rutherford Appleton Laboratory, Didcot, United Kingdom; ⁷SRF-FET, Utrecht, The Netherlands; ⁸Forschungszentrum Jülich GmbH (FZJ), Jülich, Germany; ⁹Indiana University, Indianapolis, USA; ¹⁰National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign, USA; ¹¹Centre for Data Science, University of Cambridge, UK; ¹²Centre for Data Science, University of Cambridge, UK; ¹³Centre for Data Science, University of Cambridge, UK; ¹⁴Centre for Data Science, University of Cambridge, UK; ¹⁵Centre for Data Science, University of Cambridge, UK; ¹⁶Centre for Data Science, University of Cambridge, UK; ¹⁷Centre for Data Science, University of Cambridge, UK; ¹⁸Centre for Data Science, University of Cambridge, UK; ¹⁹Centre for Data Science, University of Cambridge, UK; ²⁰Centre for Data Science, University of Cambridge, UK

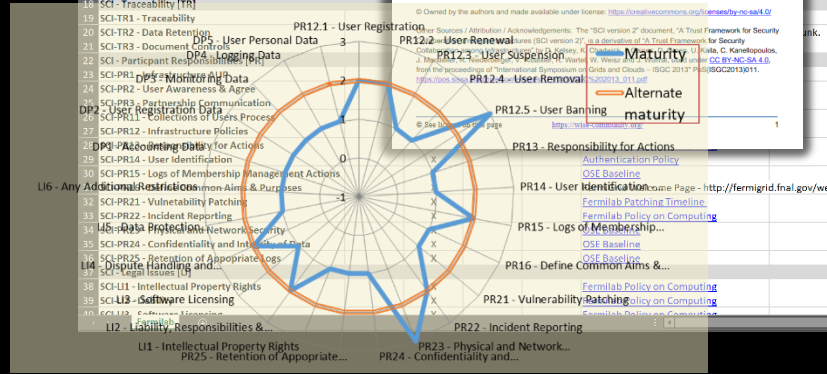
	A	B
1 Infrastructure Name:	Fermilab	Fermilab
2 Prepared By:	Keith Ch...	Keith Ch...
3 Reviewed By:		
4		
5 SCI - Operati...		
6 SCI-OS1 - Sec...		
7 SCI-OS2 - Sec...		
8 SCI-OS3 - Vul...		
9 SCI-OS4 - Int...		
10 SCI-OS5 - Regu...		X
11 SCI-OS6 - Cont...		X
12 SCI-OS7 - Poli...		
13 SCI - Incident Response [R]		
14 SCI-IR1 - Cont...		
15 SCI-IR2 - Respo...		
16 SCI-IR3 - Coll...		X
17 SCI-IR4 - Assu...		X
18 SCI - Traceability [TR]		
19 SCI-TR1 - Trac...		
20 SCI-TR2 - Data...		
21 SCI-TR3 - Docu...		
22 SCI - Particip...		
23 SCI-PR1 - Part...		
24 SCI-PR2 - Use...		
25 SCI-PR3 - Part...		
26 SCI-PR4 - Ass...		
27 SCI-PR5 - Log...		
28 SCI-PR6 - Vul...		
29 SCI-PR7 - Inc...		
30 SCI-PR8 - Con...		
31 SCI-PR9 - Con...		
32 SCI-PR10 - Ret...		
33 SCI-PR11 - Int...		
34 SCI-PR12 - S...		
35 SCI-PR13 - Li...		
36 SCI-PR14 - Int...		
37 SCI-PR15 - S...		
38 SCI-PR16 - S...		
39 SCI-PR17 - S...		
40 SCI-PR18 - S...		
41 SCI-PR19 - S...		
42 SCI-PR20 - S...		
43 SCI-PR21 - S...		
44 SCI-PR22 - S...		
45 SCI-PR23 - S...		
46 SCI-PR24 - S...		
47 SCI-PR25 - S...		
48 SCI-PR26 - S...		
49 SCI-PR27 - S...		
50 SCI-PR28 - S...		
51 SCI-PR29 - S...		
52 SCI-PR30 - S...		
53 SCI-PR31 - S...		
54 SCI-PR32 - S...		
55 SCI-PR33 - S...		
56 SCI-PR34 - S...		
57 SCI-PR35 - S...		
58 SCI-PR36 - S...		
59 SCI-PR37 - S...		
60 SCI-PR38 - S...		
61 SCI-PR39 - S...		
62 SCI-PR40 - S...		
63 SCI-PR41 - S...		
64 SCI-PR42 - S...		
65 SCI-PR43 - S...		
66 SCI-PR44 - S...		
67 SCI-PR45 - S...		
68 SCI-PR46 - S...		
69 SCI-PR47 - S...		
70 SCI-PR48 - S...		
71 SCI-PR49 - S...		
72 SCI-PR50 - S...		
73 SCI-PR51 - S...		
74 SCI-PR52 - S...		
75 SCI-PR53 - S...		
76 SCI-PR54 - S...		
77 SCI-PR55 - S...		
78 SCI-PR56 - S...		
79 SCI-PR57 - S...		
80 SCI-PR58 - S...		
81 SCI-PR59 - S...		
82 SCI-PR60 - S...		
83 SCI-PR61 - S...		
84 SCI-PR62 - S...		
85 SCI-PR63 - S...		
86 SCI-PR64 - S...		
87 SCI-PR65 - S...		
88 SCI-PR66 - S...		
89 SCI-PR67 - S...		
90 SCI-PR68 - S...		
91 SCI-PR69 - S...		
92 SCI-PR70 - S...		
93 SCI-PR71 - S...		
94 SCI-PR72 - S...		
95 SCI-PR73 - S...		
96 SCI-PR74 - S...		
97 SCI-PR75 - S...		
98 SCI-PR76 - S...		
99 SCI-PR77 - S...		
100 SCI-PR78 - S...		

<https://wise-community.org/>

InfoSec risk assessment framework for (EOSC) services based on WISE SCI



e.g. ISO27001 can help structure or identify gaps in your knowledge, but ISO27002 should not be blindly applied without considering the federated interactions



this spider diagram is fictional – based on a idea by Urpo Kaila, CSC



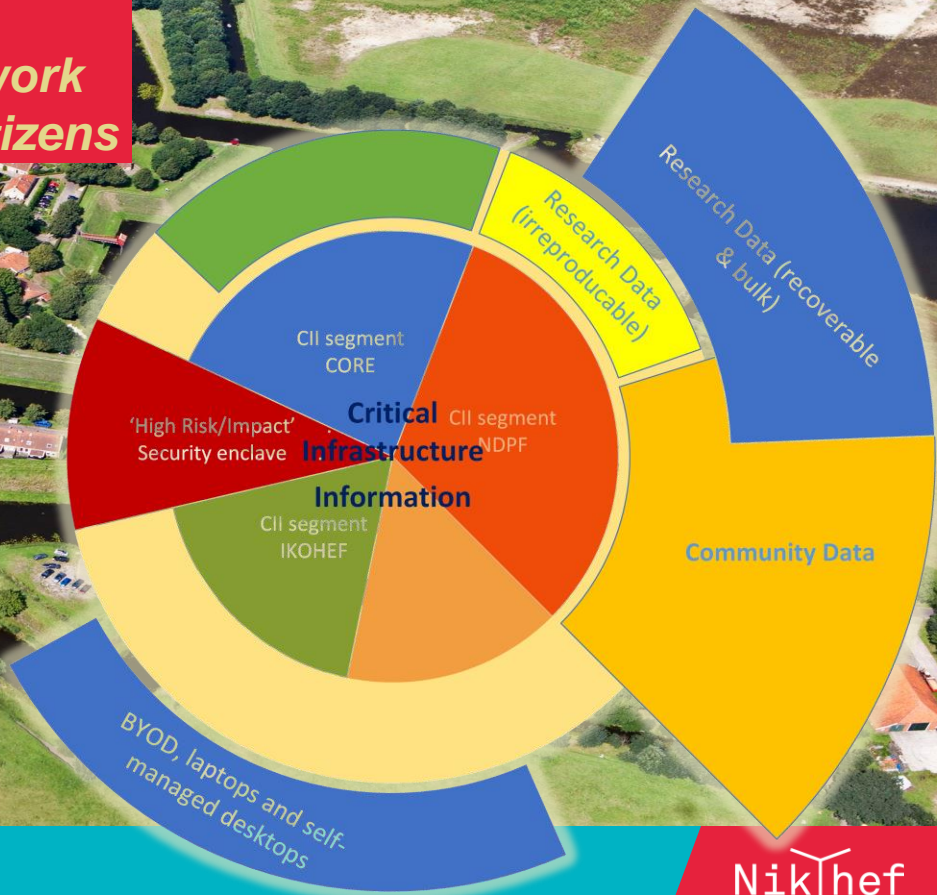
Containment & segmentation

matching the 'open core' research network
community data & systems 1st class citizens

BC/DR
Haarlem

impression Nikhef network-level segmentation

beeld: stichting vesting Bourtange



A question of *when*, not *if*

Communication:

- Endpoints valid?
- Form/Content OK ?

Containment

- Ban "malicious"
- Find/Stop malware
- Find submission

Forensics

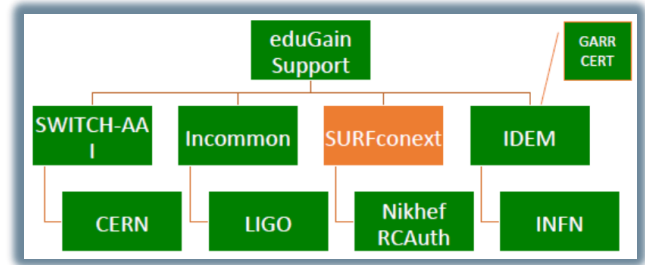
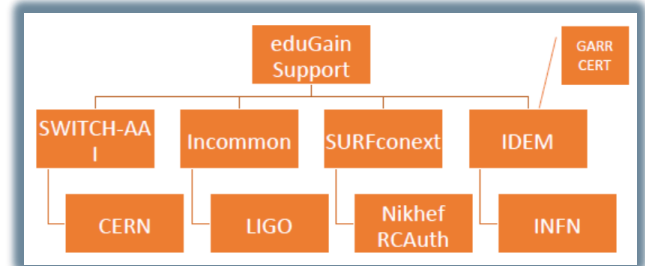
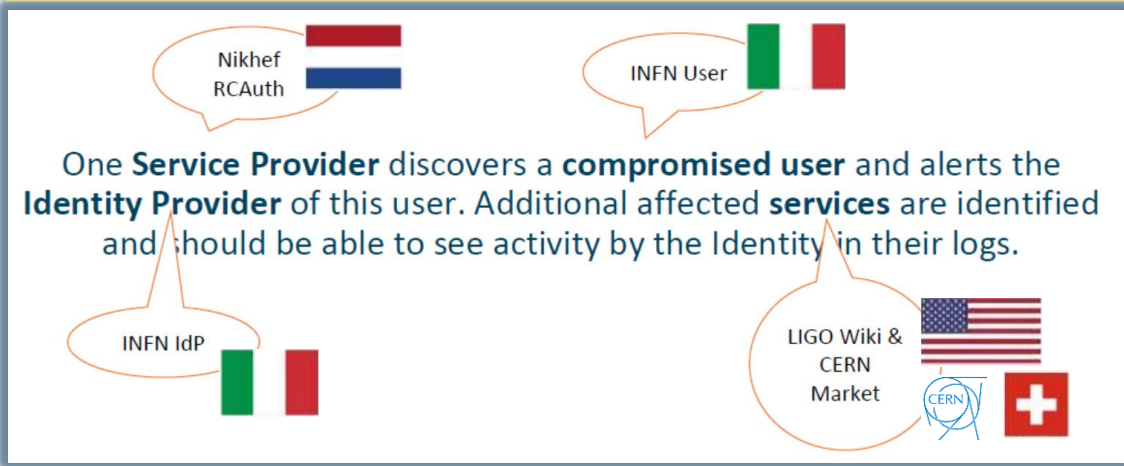
- Basic Forensic
- Network traffic



A federated community security challenge

Can we coordinate our collective R&E response?
'challenges' based on the *Sirtfi* contact model

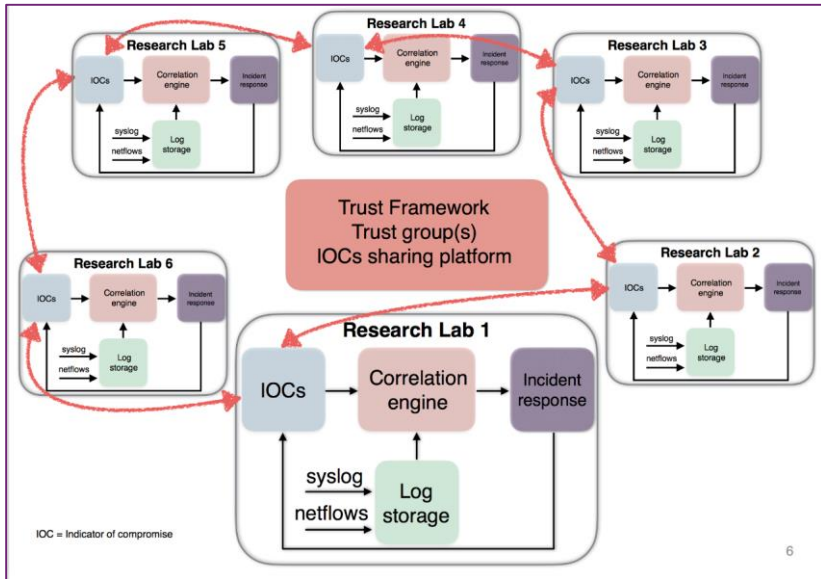
Security Incident Response Trust Framework for Federated Identity



PARTIES INVOLVED IN RESPONSE CHALLENGE

REPORT-OUTS SEE [HTTPS://WIKI.GEANT.ORG/DISPLAY/AARC/SIRTFI+COMMUNICATIONS+CHALLENGES%2C+AARC2-TNA3.1](https://wiki.geant.org/display/AARC/SIRTFI+COMMUNICATIONS+CHALLENGES%2C+AARC2-TNA3.1)

Sharing threat intel – working with our community

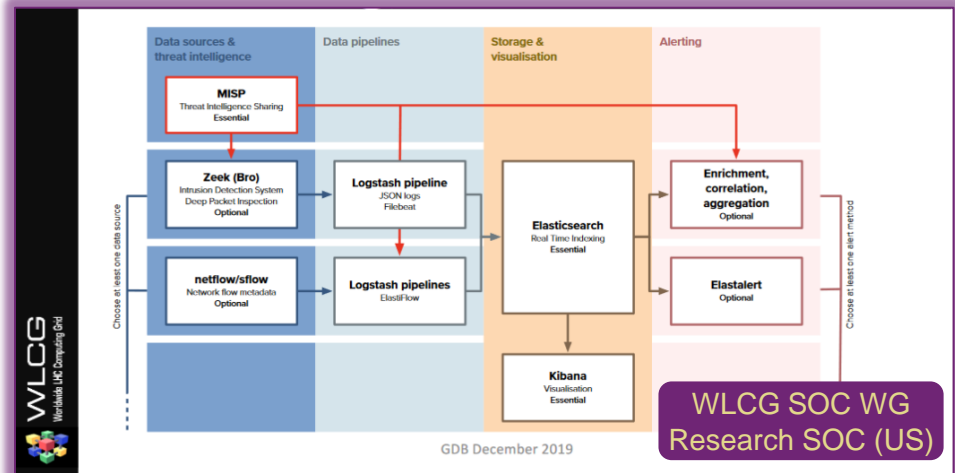


OSINT - CVE-2015-2545: overview of current threats

Event ID	3865	Related Events	Org: CIRCL
Justs	57460963-76ds-4272-8116-4ea302a0b61	2016-05-27 (3863)	Date: 2016-05-25
Org	CIRCL	2016-05-23 (3844)	Info: OSINT - Operation Kac'hang
Owner org	CIRCL	2016-05-06 (2825)	Resurfaces With New TidePool Malware
Contributors			
Email	alexandre.dulauoy@circl.lu		
Tags	tip:white x #cve:2015-2545 x Type:OSINT x estimative-language:likelihood-probability="very-likely" x		
Date	2016-05-25		
Threat Level	Medium		
Analysis	Completed		
Distribution	All communities		
Info	OSINT - CVE-2015-2545: overview of current threats		
Published	Yes		
Lightings	0 (0)		

MISP Threat Sharing

The network graph shows connections between several IP addresses and domains, including 212.7.217.10, www.oncheck.myfw.us, bc35b7882449e4d50c231f7567b6f211f6c2c878694479a3e5872e4e78542, and reg.fmt.org.



AARC AARC I-051 Guide to federated incident response
<https://aarc-community.org/guidelines/aarc-i051/>

Nikhef SOC – NDPF traffic analysis

many 'false warnings': needs tuning

The screenshot shows the Elasticsearch (Suricata/Fast) interface. At the top, there's a search bar with 'Lucene query' and an 'Alias' dropdown set to 'alias patterns'. Below that, a 'Metric' section shows 'Count' and a 'Group by' section with 'Date Histogram' and '@timestamp'. A date histogram shows a bar chart of counts over time from 07:54:00 to 07:59:30. Below the histogram, there are toggle switches for 'Time', 'Unique labels', 'Wrap lines', and 'Dedup' (set to 'none'). A log entry is displayed for '2020-08-25 07:59:50 1' with the following fields:

```
Parsed Fields:
  .@timestamp      2020-08-25T05:59:50.000Z
  ._id            SRA2JHQBg1VRchyIYZ
  ._index        suricata-fast-2020.08.25
  ._source       [object Object]
  ._type         _doc
  .facility       21
  .facility_label local15
  .logsource     bron
  .message       [1:2000418:16] ET POLICY Executable and linking for
  .pid          520408
  .priority      169
```

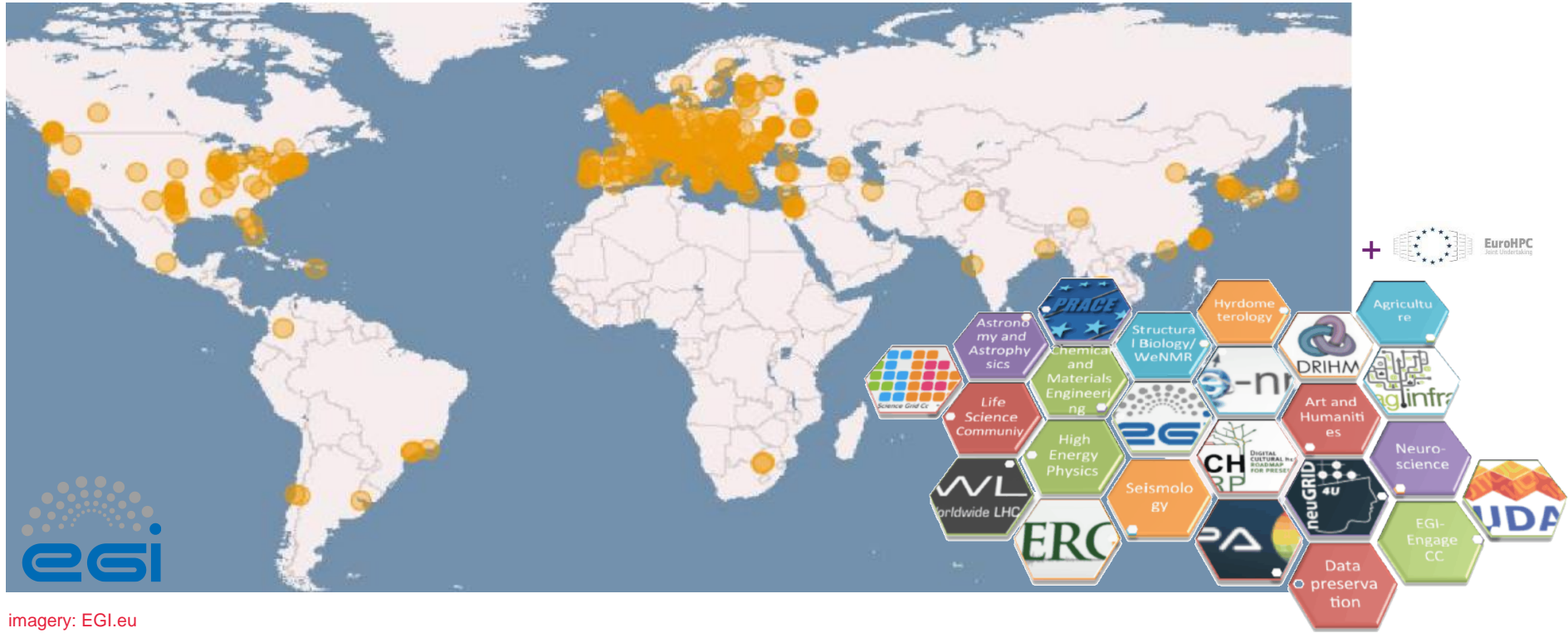
```
inetnum:      141.85.0.0 - 141.85.255.255
netname:      PUB-NET
country:      RO
tech-c:       GB6367-RIPE
status:       LEGACY
mnt-by:       RIPE-NCC-LEGACY-MNT
```

bron

```
[1:2000418:16] ET POLICY Executable and linking format (EL
F) file download [Classification: Potential Corporate Priv
acy Violation] [Priority: 1] {TCP} 141.85.240.238 1095 ->
194.171.102.47:33084
```

NikhefSOC/NDPF ELK setup: Jouke Roorda

e-Infrastructures: EGI, EUDAT, GEANT, PRACE, ... and DNI!



imagery: EGI.eu

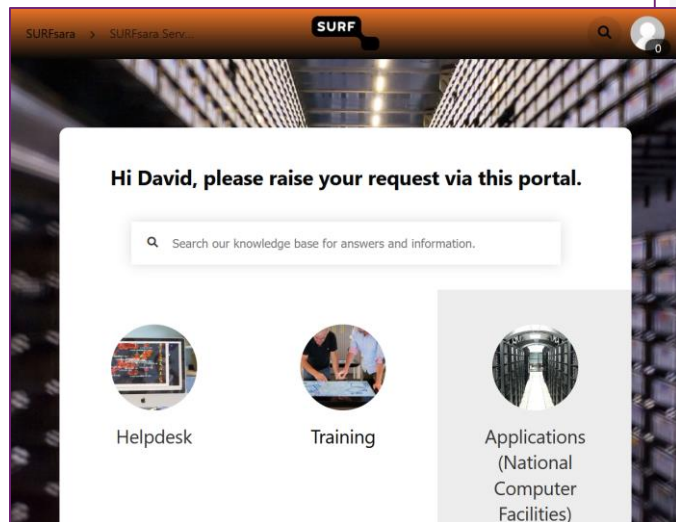
'DNI coordinated by SURF'

Coordinated Dutch National e-Infrastructure

- Single application portal (at SURF and NWO)
- Resources allocated at most-suitable partners
- Federated management and common innovation



BiG Grid
the dutch e-science grid



Home

Systems ▾

About this site

System status

Status update SURFsara systems:

System	Status	Remarks
Cartesius	Up and running	21-10-2020: The scratch file system was I/O on scratch at that time.
Lisa CPU	Up and running	
Lisa GPU	Up and running	
Data Archive	Up and running	Maintenance 2020-11-10 08:00 till 14:00
EPIC PID	Up and running	
ResearchDrive	Up and running	
B2SAFE	Up and running	
Grid	Up and running	National e-Infrastructure Grid Downtimes
HPC Cloud	Up and running	See Maintenance Calendar
Hathi Hadoop	Discontinued	
Lucy	Discontinued	
Elasticsearch	Discontinued	
SURFdrive	Up and running	

<https://servicedesk.surfsara.nl/jira/plugins/servlet/desk/portal/1>

Connecting resources – people – organisations – data

Programma Rekentijd Nationale Computersystemen

< Naar de lijst van programma's

> **Rekentijd nationale computersystemen**
Achtergrond
Organisatie
Projecten
Contact

Geavanceerde (super)computersystemen worden gebruikt voor technisch-wetenschappelijk onderzoek waarbij grote rekenproblemen moeten worden opgelost. Door tijd beschikbaar te stellen via het programma 'Rekentijd nationale computersystemen' maakt NWO geavanceerde nationale computerfaciliteiten beschikbaar voor wetenschappelijk onderzoek. Hierdoor is hoogwaardig en competitief onderzoek mogelijk in Nederland.

Geavanceerde computersystemen worden bijvoorbeeld gebruikt voor berekeningen voor de weerverwachting, waarbij grote hoeveelheden data van satellieten en weerstations verwerkt moeten worden. Andere voorbeelden zijn de verwerking van grote hoeveelheden data in de radioastronomie, klimaatonderzoek, onderzoek naar grote historische archieven en tekstcorpora, of genom- en eiwitanalyse.

Voorlezen
Print
Mail
Delen

Nieuws

8 oktober 2020
> NWO honoreert drie aanvragen voor
Rekentijd op de Nationale
Computersystemen

9 juli 2020
> NWO honoreert 10 aanvragen voor
Rekentijd op de Nationale
Computersystemen

20 mei 2020
> NWO honoreert 24 aanvragen voor
Rekentijd op de Nationale
Computersystemen

> **Al het nieuws voor Rekentijd nationale computersystemen**

Kalender

31 Rekentijd Nationale



Staatscourant van het Koninkrijk der Nederlanden

Datum publicatie
07-06-2018 09:00

Organisatie
Nederlandse Organisatie voor Wetenschappelijk Onderzoek

Jaargang en nummer
Staatscourant 2018, 31287

Rubriek
Overig

The Dutch National e-Infrastructure

In this call, all applicants are asked to indicate the project's e-Infrastructure needs, in terms of compute hours, data storage capacity, lightpath connectivity, or otherwise. A 'use-or-explain' policy will be applied, meaning that

- projects *without* e-Infrastructure needs are asked to give a brief explanation;
- projects with clear e-Infrastructure needs are expected to select the hardware resources and services as part of the Dutch National e-Infrastructure as first option, and to indicate the expected extent of use;
- projects with clear e-Infrastructure needs that aim to use international (e.g. PRACE, XSEDE, etcetera) or commercial (e.g. web, cloud, etcetera) hardware and services instead are required to give a brief explanation.

The use of the Dutch National e-Infrastructure is not a requirement, nor is it a formal review criterion. However, in all cases in which the Dutch National e-Infrastructure is not used, a justification should be provided.

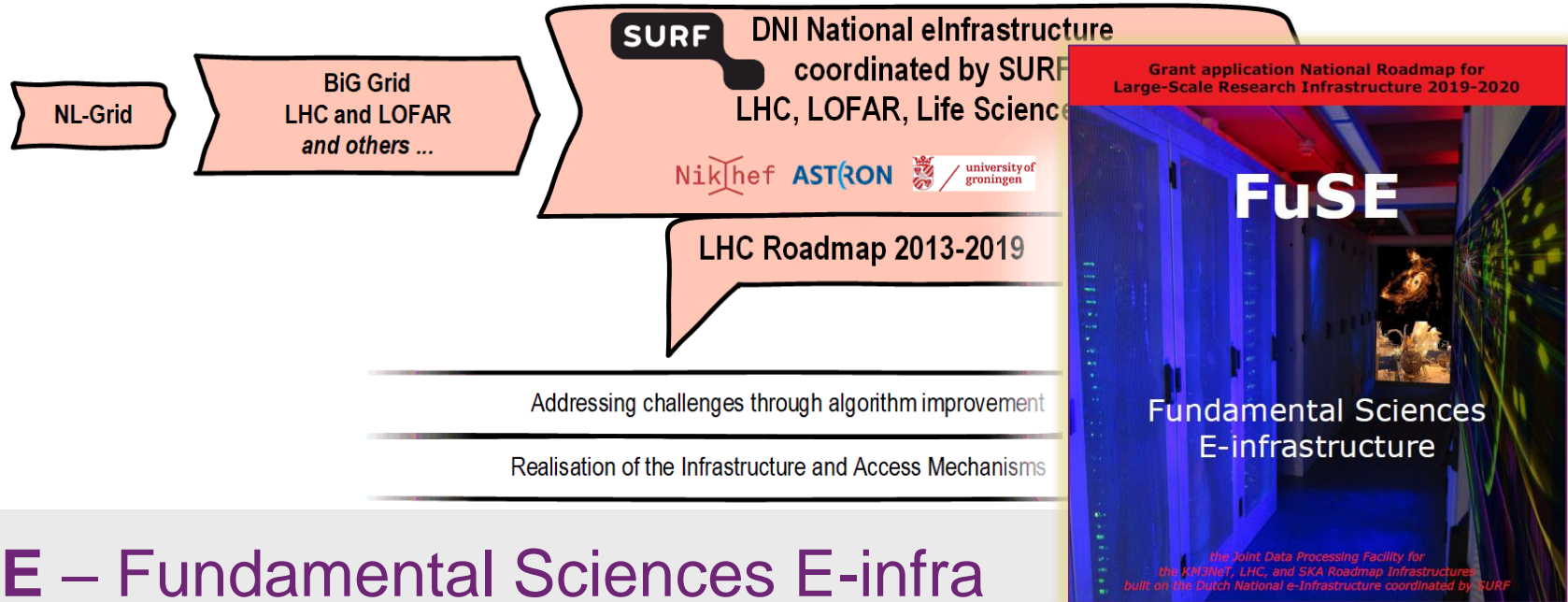
In this call, the Dutch National e-Infrastructure is defined as follows:

The definition distinguishes between hardware resources and services available to all researchers in the Netherlands (Category I), and those made available to a selected subset (Category II). The Category I e-Infrastructure, outlined below, is formed by the hardware resources and services provided and maintained by SURFsara, SURFnet, DANS, and – in part – also by Nikhef and RUG-CIT.

accession to a selected group of researchers following thematic or geographic criteria. Examples of















<https://www.nwo.nl/onderzoek-en-resultaten/programmas/Rekentijd+nationale+computersystemen>

Balanced infrastructure - based on our joint science cases



FuSE – Fundamental Sciences E-infra
*an integrated infrastructure
for algorithms, hardware, networking, and collaboration*

Liquid CO₂ cooling test bench,
24.33% overclocked
using CineBench R20
best sustained, i.e. without LN2...
In a Nikhef-AMD collaboration

	SCORE	USER	FREQUENCY	HARDWARE	COOLING	HW	
1.	23323 pts	 Splave	5400.2 MHz	AMD Ryzen Threadripper 3970X	LN2	0pts	0 
2.	23081 pts	 Alex@ro	5375 MHz	AMD Ryzen Threadripper 3970X	LN2	0pts	 1 
3.	22064 pts	 Hiwa	5050.6 MHz	AMD Ryzen Threadripper 3970X	LN2	0pts	 0 
4.	21601 pts	 keep8n	5000.4 MHz	AMD Ryzen Threadripper 3970X	LN2	0pts	 0 
5.	20022 pts	 Nikhef	4600.1 MHz	AMD Ryzen Threadripper 3970X	SS	0pts	 0 

Let It All Collaborate!



Nikhef

David Groep

davidg@nikhef.nl

<https://www.nikhef.nl/~davidg/presentations/>

 <https://orcid.org/0000-0003-1026-6606>