A Framework for Security

e-IRG, Zürich, April 2008

SWITCH

Serving Swiss Universities

Christoph Graf
christoph.graf@switch.ch

Outline

What is “Security”?

or: Where’s the “Security Layer”?

Naming is always a problem

or: What is the plural form of “security”?

A framework for Security

or rather?: Frameworks for security

Quotes about “Computer Security”

- “Computer security imposes requirements on computers that [..] often take the form of constraints on what computers are not supposed to do.”
- “[..] negative requirements are deceptively complicated to satisfy and require exhaustive testing to verify.”
- “The designers and operators of systems should assume that security breaches are inevitable.”

Source: http://en.wikipedia.org/wiki/Computer_security

Quotes about “Security Architecture”

- “Security qualities are often considered as ‘non-functional’ requirements when systems are designed. In other words they are not required for the system to meet it's functional goals [..], but are needed for a given level of assurance that the system will perform to meet the functional requirements that have been defined.”

•http://en.wikipedia.org/wiki/Security_Architecture

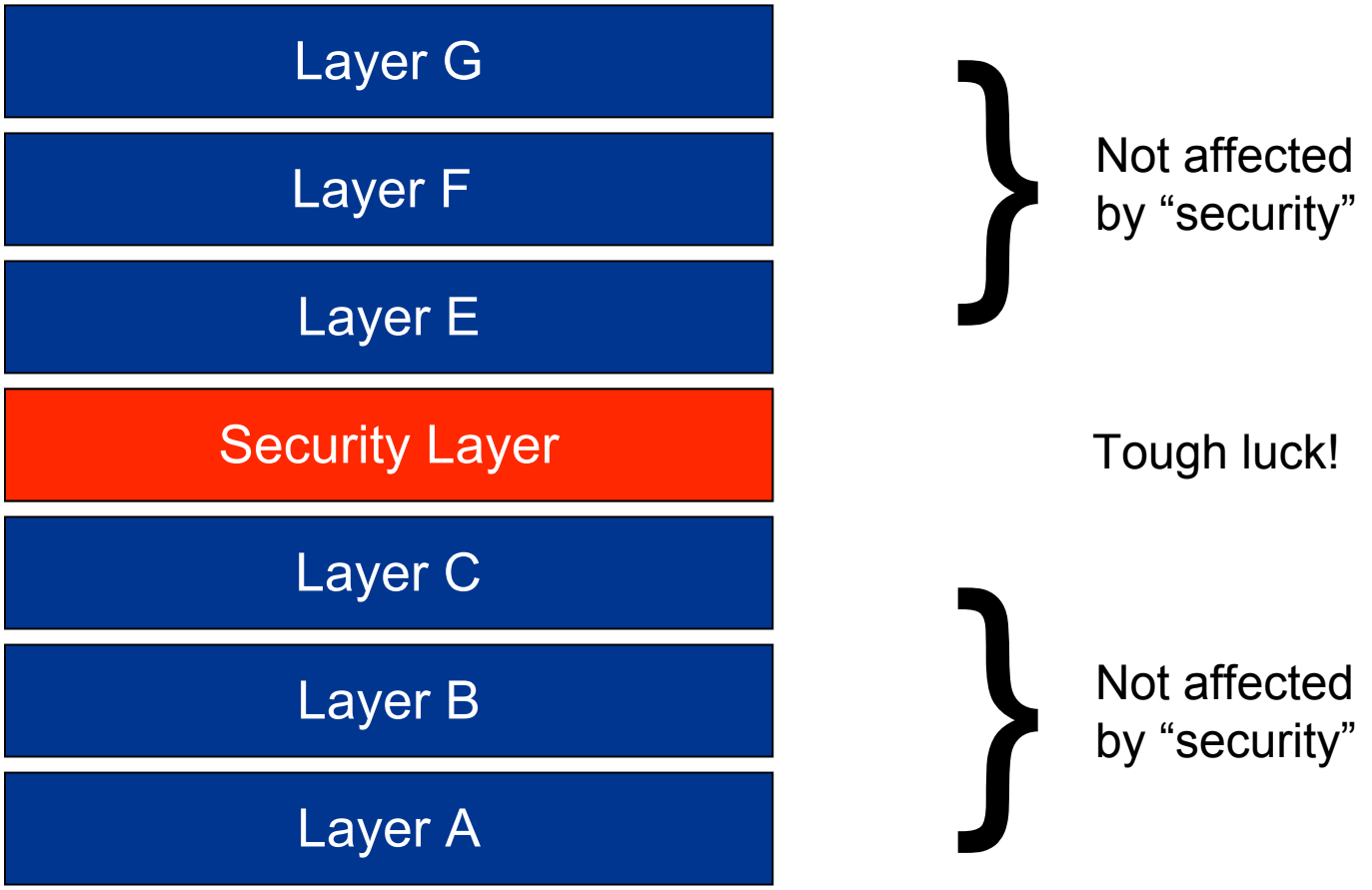
Properties of Security

- The one and only nice property of security:
  - Security creates assurance
  - ***> That's why we need it!***
- A pretty useless property of security:
  - Security doesn't add functionality
  - ***> That's why we are tempted to ignore it!***
- The many nasty properties of security:
  - Imposes limits, which often vary over time (often suddenly)
  - Creates dependencies on things beyond our control
  - Is utterly unimpressed by cool features, but forces us to think about very weird stuff happening in weird circumstances
  - In short: it's a pain!
  - ***> That's why we hate it!***

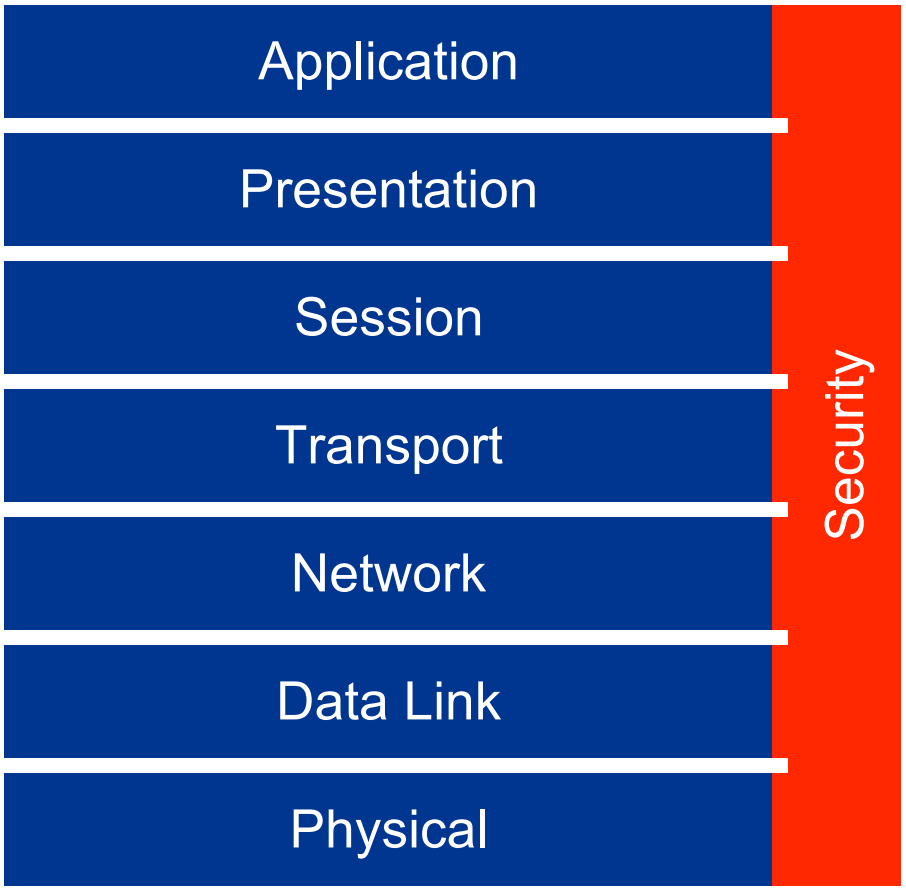
Where's the "Security Layer"?

- Since security is a pain:
  - can we confine security, where it does not hurt?
  - E.g. dump it into a "Security Layer"...
  - ... and make it someone else's problem?
- Start from something well structured: the OSI Reference Model
- Let's figure out how security fits the picture
- Can we identify the "Security Layer"?

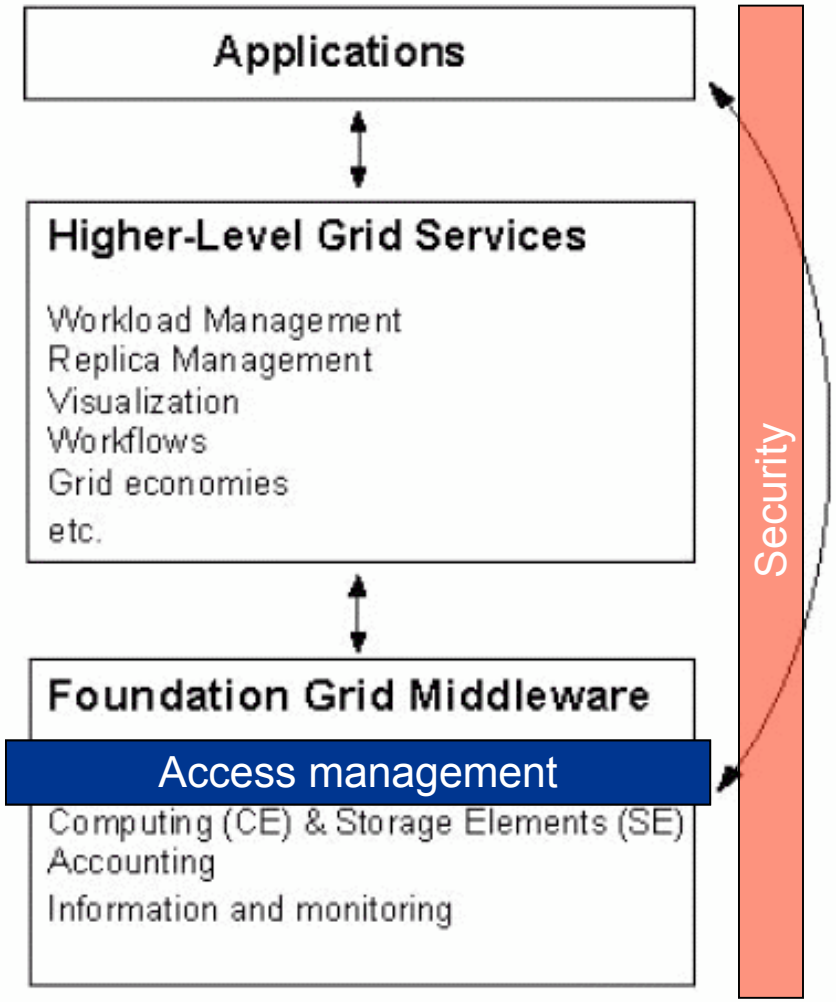
The ideal solution



The OSI Reference Model (enriched)



Security in the Grid Layer Model



Source: http://egee-jra1.web.cern.ch/egee%2Djra1/

- The term “security” is used in a different context here. This layer...
  - is a service element offering authentication and authorisation services (AA)
  - adds AA functionality to the Grid
  - is based on business needs (Grid without AA could perfectly make sense)
  - doesn’t impose anything (you may choose to ignore this service)

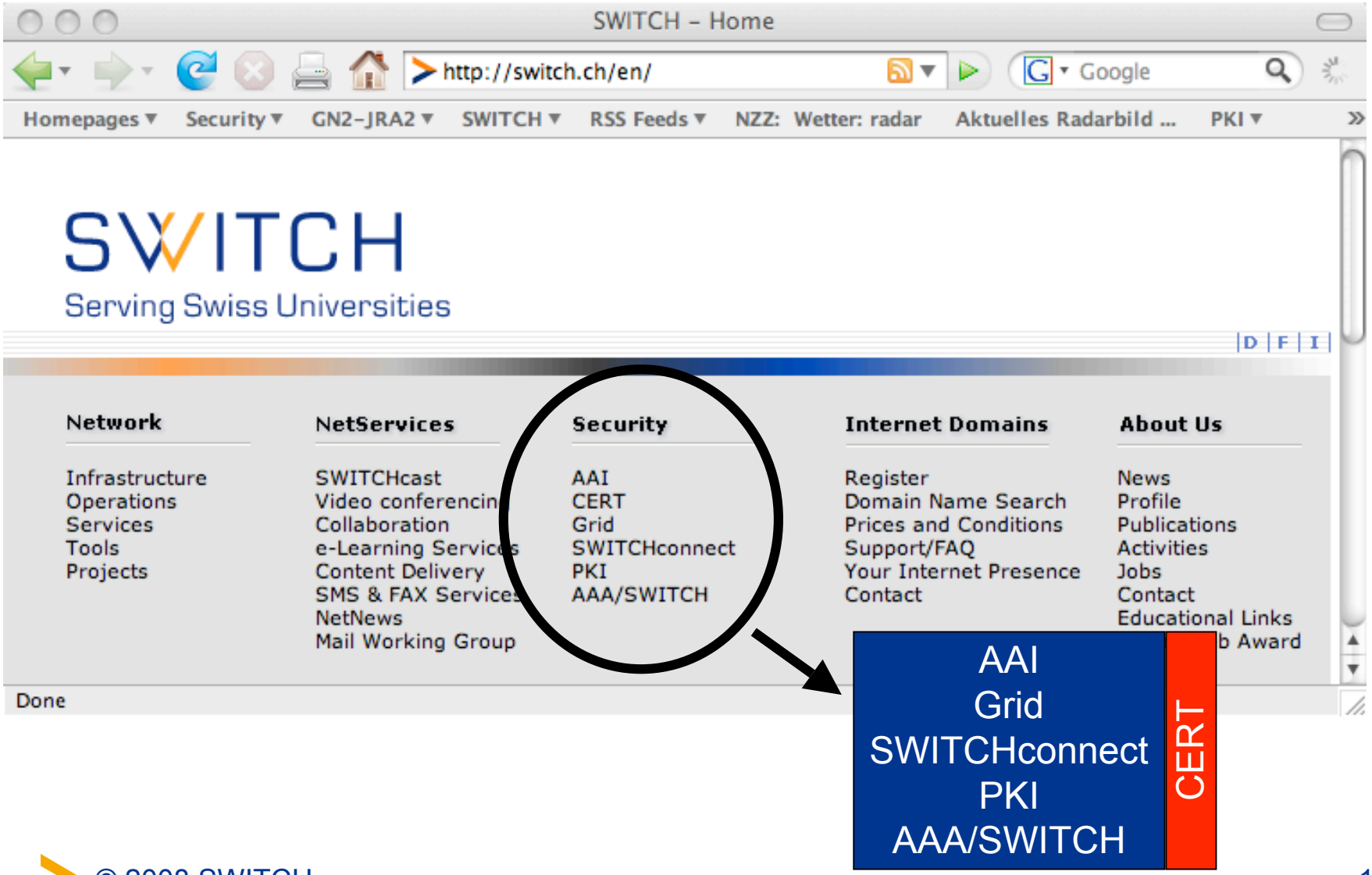
-> Wouldn’t it be a good idea to call this something else than “security”?

Proposed naming

- Access Management
  - A layered functional element
  - driven by business needs
  - Common understanding needed on relevant use cases, functionality and quality aspects (including the required level of assurance)

- Security
  - Guaranteeing the required level of assurance
  - Non-functional requirements
  - Cross-layer activity, imposing limits on any element in the whole supply chain

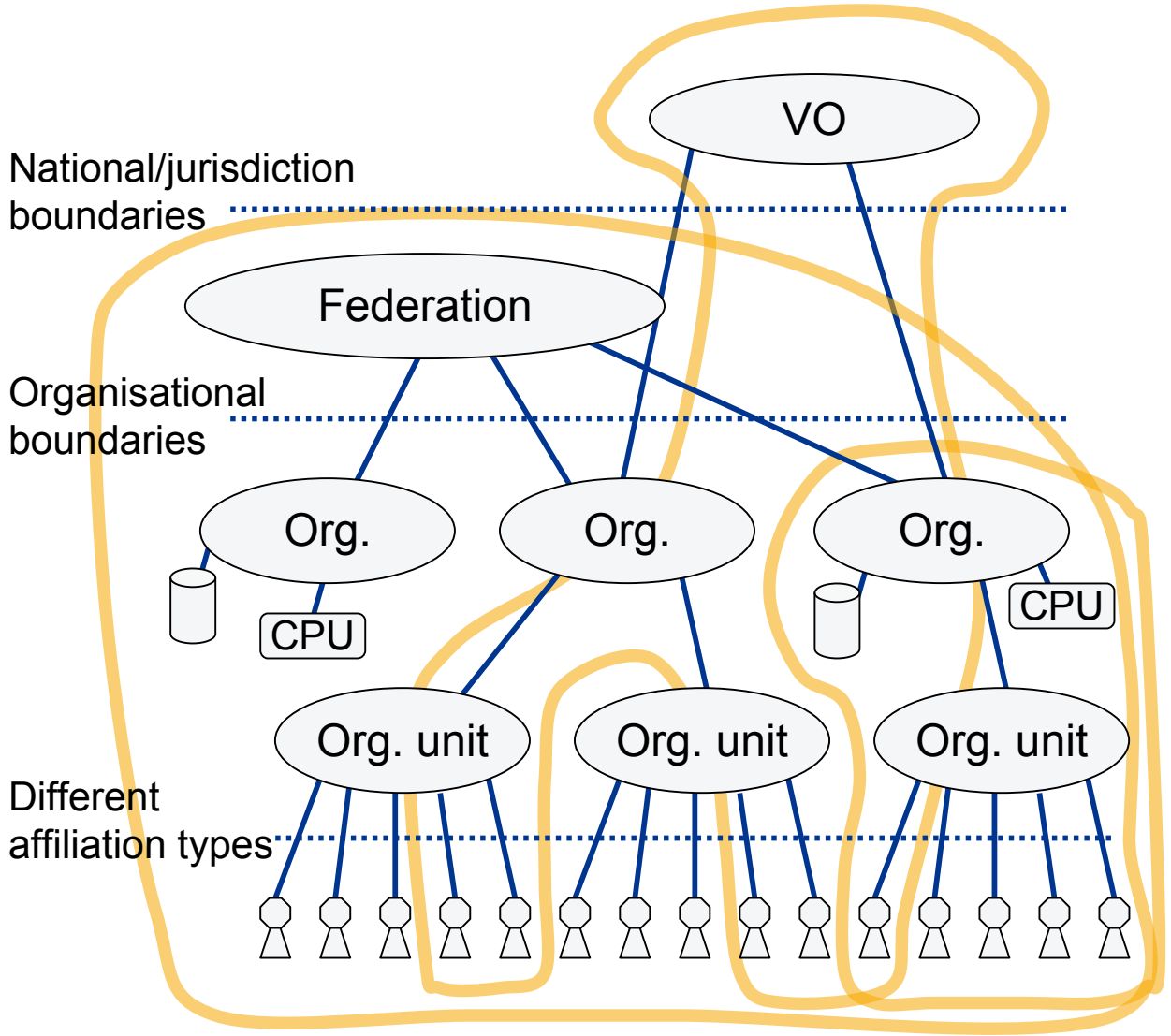
Putting things in context (1/2)



Putting things in context (2/2)

Relevant scopes

- Interfederation
- Inter-VO
- Virtual Organisation (VO)
- Federation
- Organisation



Framework for “Security” e-Infrastructures

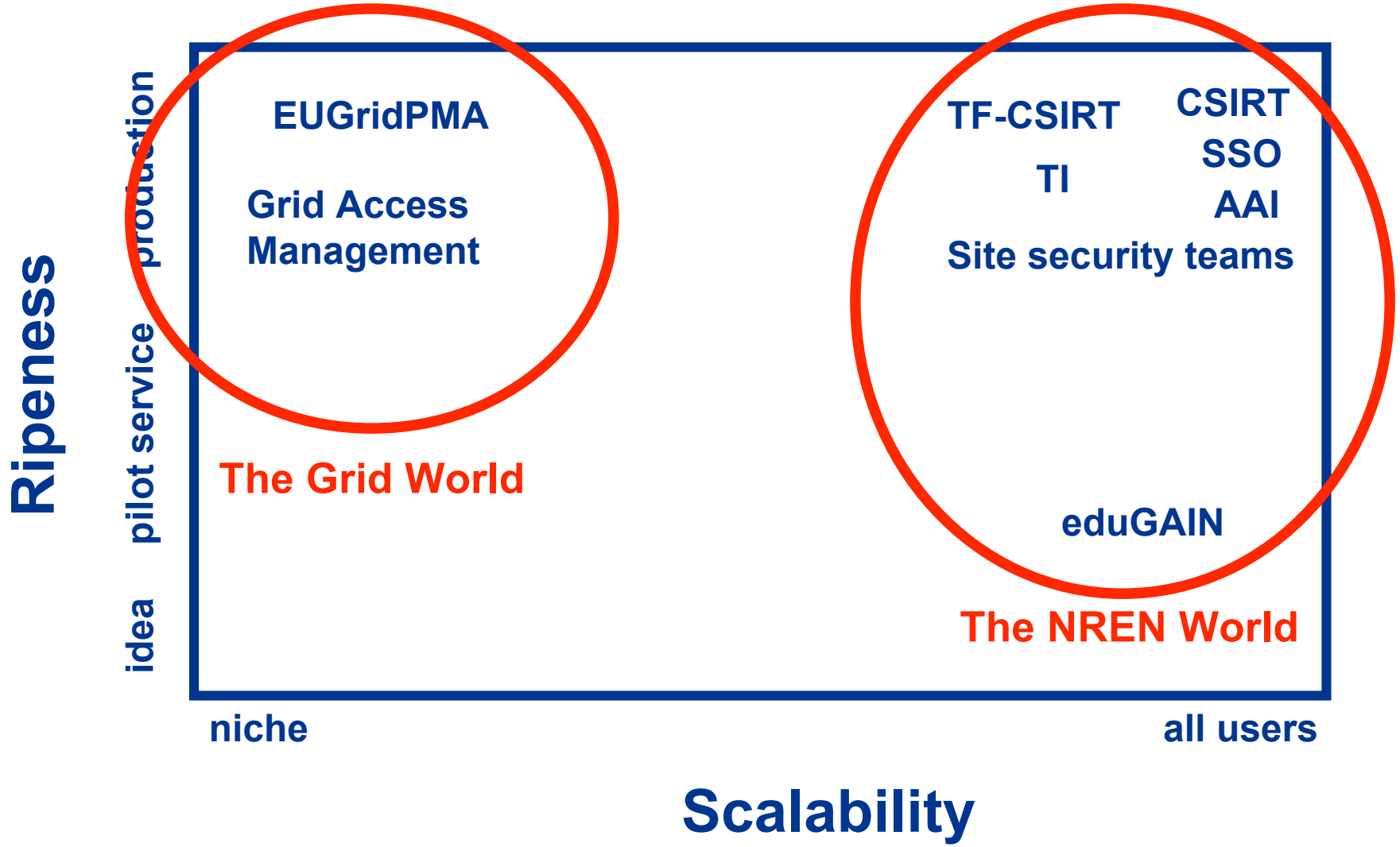
Access management:

- Organisation:
  - SSO: Single-Sign-On solution
- Federation:
  - AAI: Federated Authentication & Authorisation Service (AAI)
- VO:
  - Grid Access Management
- Interfederation:
  - eduGAIN: Interfederation AAI Pilot Service of GÉANT2
- Inter-VO:
  - EUGridPMA

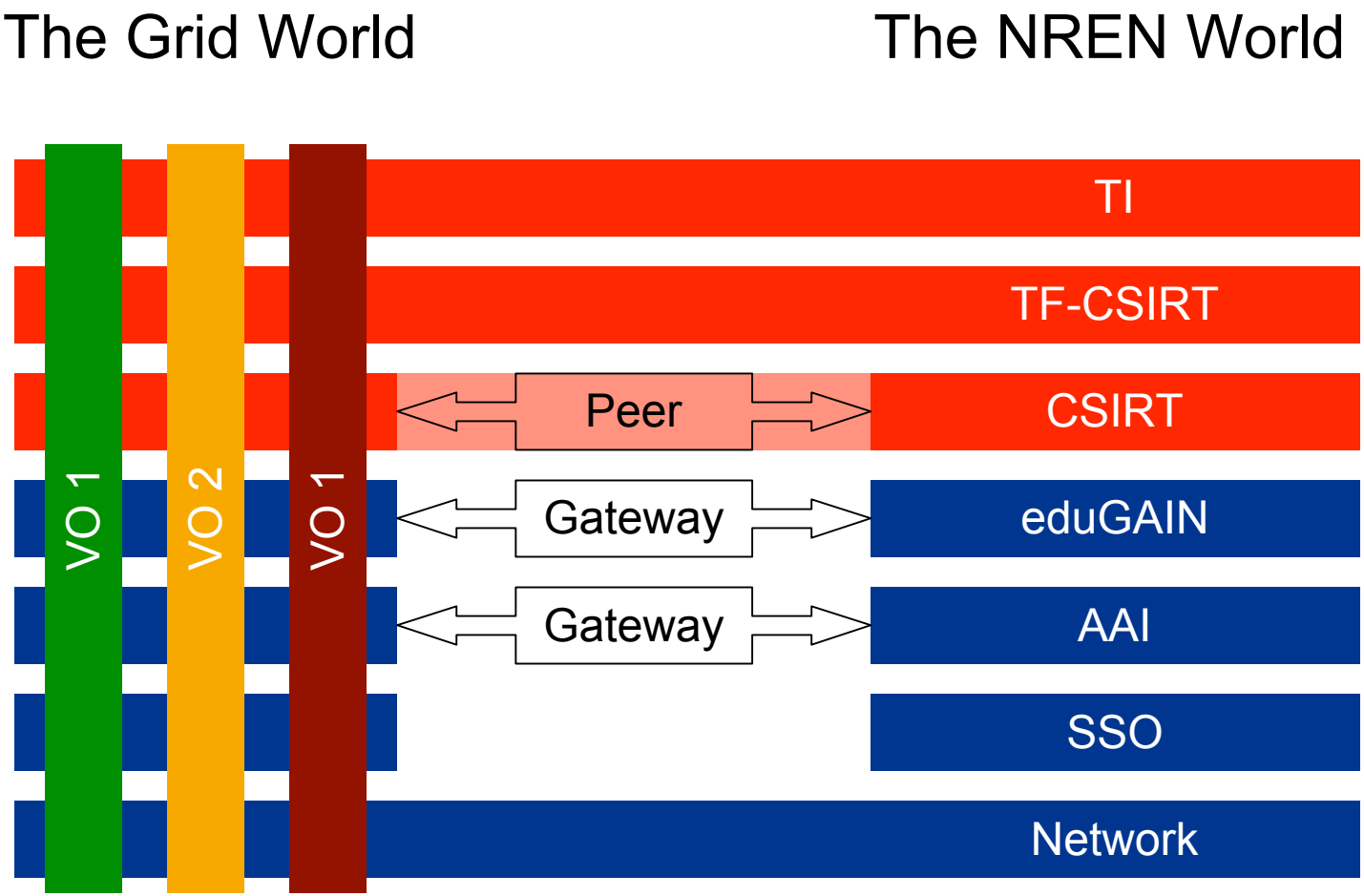
Security:

- Organisation:
  - Site security teams
- Federation:
  - CSIRT (Computer Security and Incident Response Team)
- VO:
  - Operational & product security groups
- Interfederation:
  - TF-CSIRT: TERENA’s security collaboration and networking platform
  - TI: Trusted Introducer, CSIRT Accreditation service of TERENA
- Inter-VO:
  - ---

Scalability vs. Ripeness



Merging the Worlds



Conclusions

- “Security” has different faces, let’s call things by name
  - Security: reasonably scalable services around for a decade (CSIRT collaboration)
  - Access management:
    - Federations: several national production AAIs exist, others emerging
    - Interfederation: eduGAIN in pilot stage, some more years needed
    - VO: solutions deployed, in production stage
- Parallel structures offer short-term solutions for smaller communities
- When “smaller” becomes “bigger”, think about migrating or gatewaying to (emerging) scalable solutions

SWITCH

Serving Swiss Universities

Christoph Graf
christoph.graf@switch.ch