Setting up a Grid-CERT

Experiences of an academic CSIRT

19th Annual FIRST Conference 2007
June 18 - 22, Seville, Spain

Klaus Möller
DFN-CERT Services GmbH

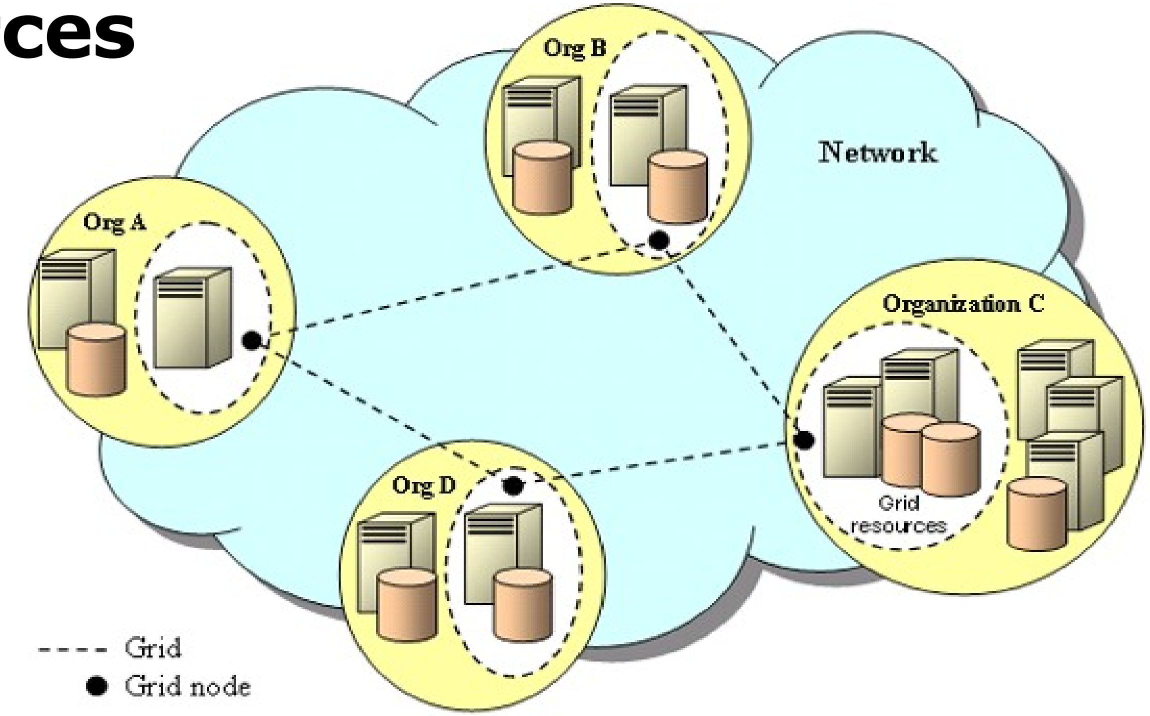
Agenda

- Introduction
- Organisational Challenges
  - Making yourself known
  - Incident reporting
  - International cooperation
- Technical Challenges
  - Grid software expertise
  - Software vulnerabilities

Introduction

What is Grid computing ?

- A form of distributed computing
- Different organisations cooperate in a **virtual organisation (VO)** to **share resources**



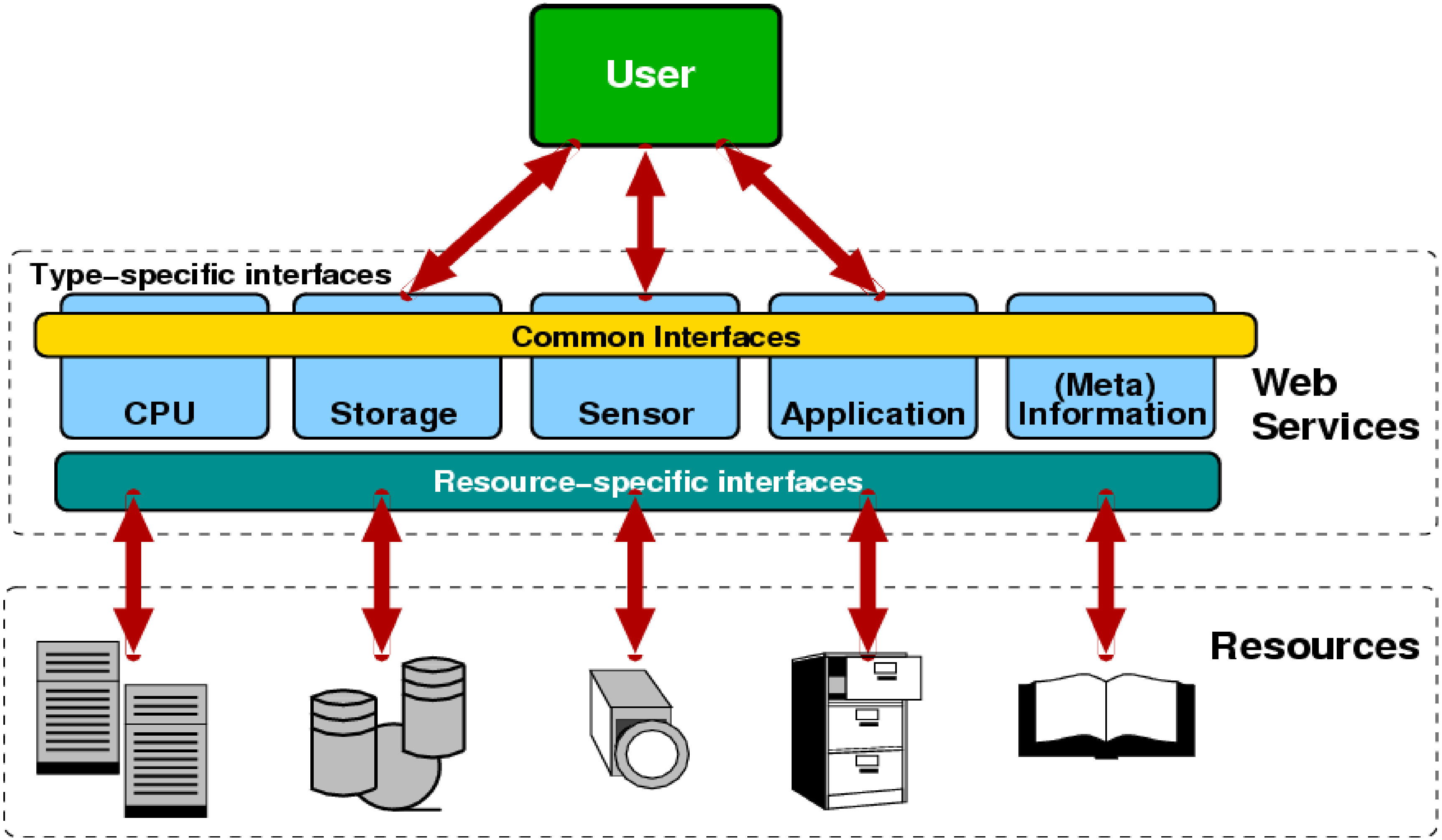
Introduction

What is Grid-computing ?

- Resources can be CPU, storage, sensors, applications, etc.
- Organisations decide themself how their resources are shared
  - I.e. what a user is allowed to do at their site
- Users of a Grid have a single sign-on to use all resources of the Grid
  - Based on X.509 certificates and/or federated authentication schemes (Shibboleth)

Introduction

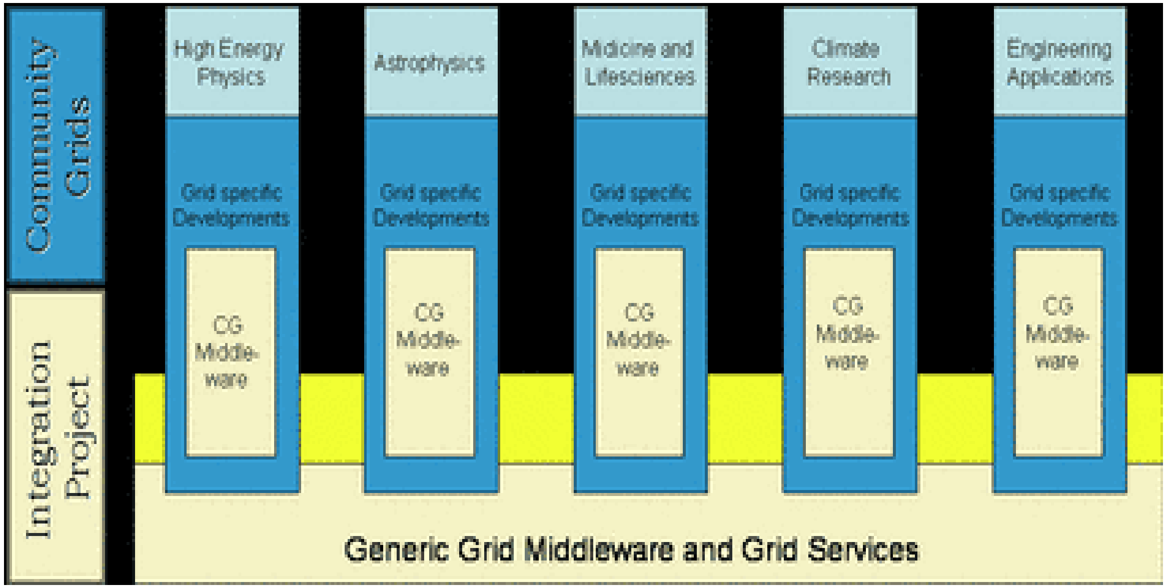
Accessing Grid Resources



Introduction

D-Grid Initiative

- Six (initially five) community projects furthering Grid computing in specific areas
- One integration project
  - Among other tasks: Set-up of Grid-specific CSIRT Services


Community Grids
Integration Project
High Energy Physics
Astrophysics
Midicine and Lifesciences
Climate Research
Engineering Applications
Grid specific Developments
Grid specific Developments
Grid specific Developments
Grid specific Developments
Grid specific Developments
CG Middle-ware
CG Middle-ware
CG Middle-ware
CG Middle-ware
CG Middle-ware
Generic Grid Middleware and Grid Services

Introduction

CSIRT Services

Reactive	Proactive
Alerts and Warnings	Technology Watch
Incident Handling	Security Audits or Assessments
- Incident analysis	
- Incident response on site	Configuration and Maintenance of Security Tools, Applications, and Infrastructures
- Incident response support	
- Incident response coordination	Development of Security Tools
Vulnerability Handling	Intrusion Detection Services
Artifact Handling	**Security-Related Information Disemination**

Introduction

Adapting services for Grid needs

- Alerts and warnings
- Incident handling
  - How to detect and analyze Grid incidents
- Vulnerability Handling
  - Promote security best practices with writers/vendors of Grid software
- Security-related information dissemination
  - Develop and distribute security best practices for Grid administrators

Organizational Challenges

Making yourself known

- First task when establishing a CSIRT: Make yourself known to the constituency
  - DFN-CERT is already well known
  - However: This does not extend into Grid-communities
- Easy to solve through the D-Grid Initiative
  - Platform for exchange, simply go there and discuss matters with the community partners
  - Otherwise, it would have been difficult just to find out which Grid-communities exist
  - But does not cover Grids outside the initiative

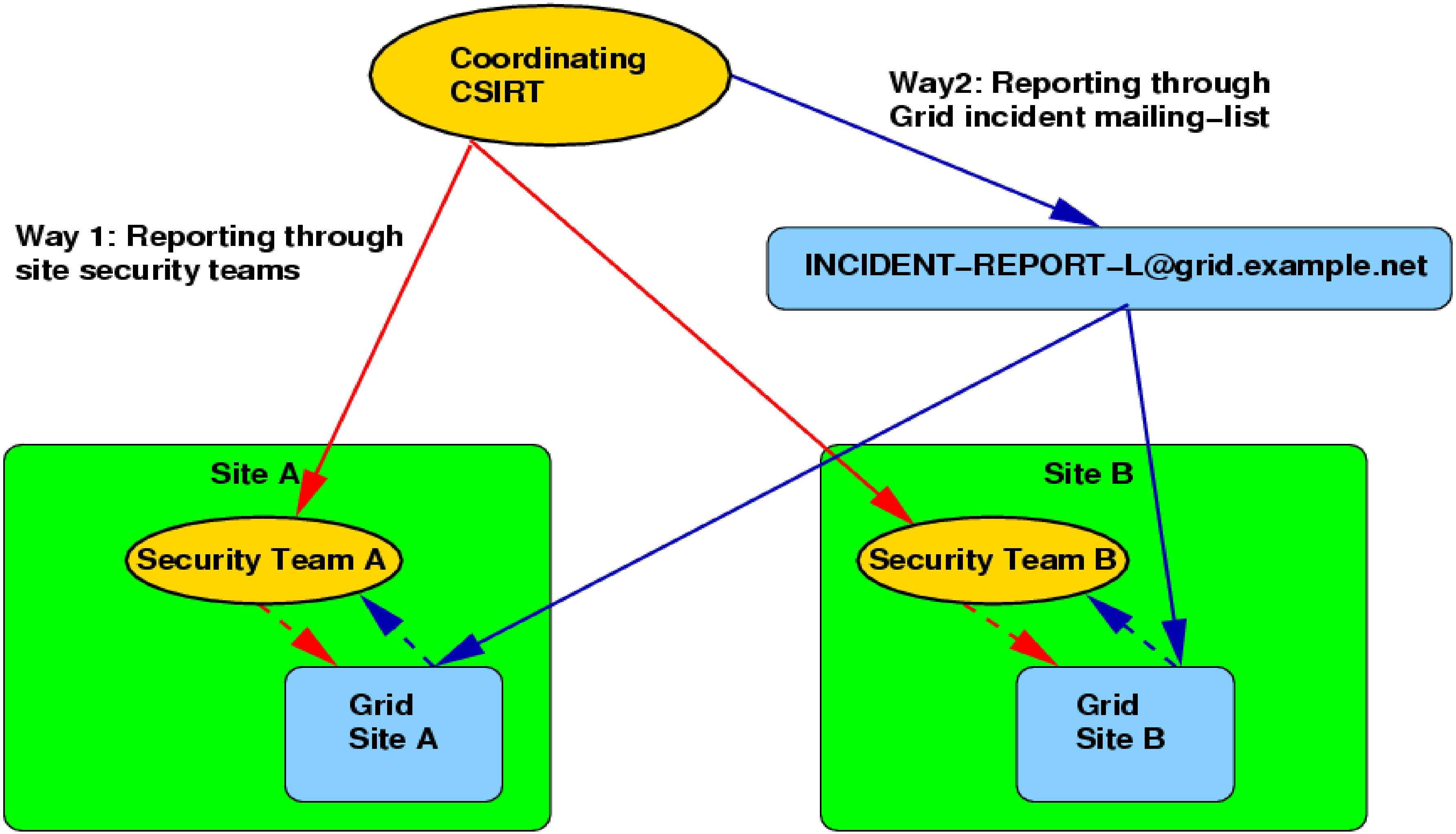
Organizational Challenges

Finding Security Contacts

- With an incident, you typically have an event (like portscans or SPAM) and an IP-address
- Find the responsible person for the IP-address
  - Traditionally: Use the WHOIS service
  - There is no database about which IP-addresses belong to which Grid
  - Grid and local site security team may not be identical
- New ways of reporting incidents needed
  - Mailing list proposal by Open Science Grid

Organizational Challenges

Incident reporting


Coordinating CSIRT
Way2: Reporting through Grid incident mailing–list
Way 1: Reporting through site security teams
INCIDENT–REPORT–L@grid.example.net
Site A
Security Team A
Grid Site A
Site B
Security Team B
Grid Site B

Organizational Challenges

Incident reporting

- Reporting through site security team:
  - Directly involves local site security team
  - Data often incomplete a coordinating CSIRT level
  - Registration with CSIRT is a bottleneck
- Reporting through Grid incident mailing list:
  - Fast, automatic information of **all** Grid members
  - Only as good as Grid mailing list database
  - Local site security team may not be involved automatically
  - Message content **must not** make a site, job or user identifiable :(

Organizational Challenges

International cooperation

- Try to pool CSIRTs experience together
  - Terenas TF-CSIRT: European CSIRT forum
  - FIRST: International CSIRT forum
- BoF at joint FIRST - TF-CSIRT meeting in January 2006
  - Pre working group stage
- Grid security since September 2006 part of the TF-CSIRT terms of reference
- A lot of initial interest, but little active cooperation so far

Technical Challenges

- To help securing their infrastructure CSIRTs have to develop an understanding about the software used in Grids, especially
  - How to securely configure Grid software
  - How Grid software interacts with other software
  - How to detect break-ins
  - How to estimate the damage from a break-in
- No or very little experience at other CSIRTs
  - So no opportunity of learning from them
  - Even in the Grid-communities, few people truly understand Grid software

Technical Challenges

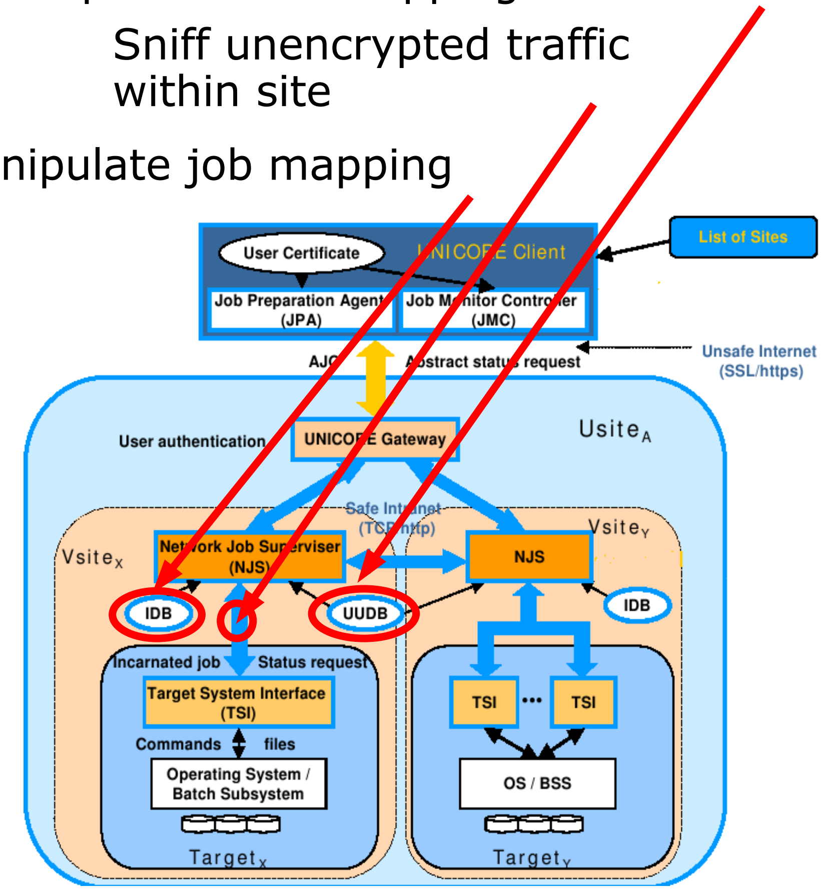
Software Audit

- Extrapolate from known attacks on other systems
- Works only with smaller software packages (UNICORE)
- Beyond the resources of academic CSIRTs for larger packages (gLite, Globus)
- Also: Test setup chosen by CSIRT may not be representative

Manipulate User Mapping Database

Sniff unencrypted traffic within site

Manipulate job mapping



Technical Challenges

Penetration testing of existing Grid sites

- Black box test (no prior knowledge)
    - Basic standard tools: nmap, netcat, OpenSSL
    - Attackers can locate Grid sites and identify to which Grid they belong (server gives list of acceptable X.509 client Cas during SSL handshake)
    - Grid services can be identified, even if running on non-standard port numbers (nmap signatures)
    - Even with custom Linux distributions, services remain open that are not needed (finger) or are configured in an insecure way (SSH protocol version 1)

Technical Challenges

Leveraging penetration test results

- Use CSIRT infrastructures for network monitoring
  - Directly observe attackers or suspicious traffic
  - Automatic alerts to constituency
  - Network telescopes
    - Observe traffic flows to ports used by Grid software
    - So far, very little traffic has been seen
  - Honeypots (in planing)
    - Directly observe attacks
    - Start with low interaction honeypots
    - Has to be SSL-capable

Technical Challenges

Software vulnerabilities

- Grid software vulnerabilities in the CVE database
  - 2005: 1 (Sun Grid Engine)
  - 2006: 7 (Globus Toolkit, Sun Grid Engine, OpenPBS/Torque)
  - Grid software per se not more secure than anything else
- This does not count vulnerabilities in software the Grid software is build upon
  - OpenSSL, Apache, etc.

Technical Challenges

Software vulnerabilities

- Grid software vendors don't follow standard practices
  - No published point of contact for reporting security problems
  - No open way of disseminating security information, i. e. open security announcement mailing list
  - Unsigned advisories
  - Unsigned software packages: MD5/SHA-1 checksums are not good enough
- Initial contact with some vendors has been made

Conclusions

- DFN-CERTs “Grid-CERT” operational since December 2006
- So far, only a few incidents could be classified as Grid-related
  - Most involve stolen X.509 certificates
  - One false alarm at a cluster site
  - However: Many community projects are not yet operational
- Some solutions are not optimal but will have to do for the beginning
- New developments may change the picture

Thank you !

Questions ?