



# **Security activities within GN2**

**Christoph Graf**  
**<christoph.graf@switch.ch>**

## Sixth Framework Project:

- Title: Multi-Gigabit European Academic Network
- Project acronym: GN2, it is spelt “GN2” but often pronounced “GÉANT2”
- Successor of project GN1, which produced the GÉANT network

## Partners:

- DANTE, co-ordinating partner
- Consortium of NRENs (29)
- TERENA

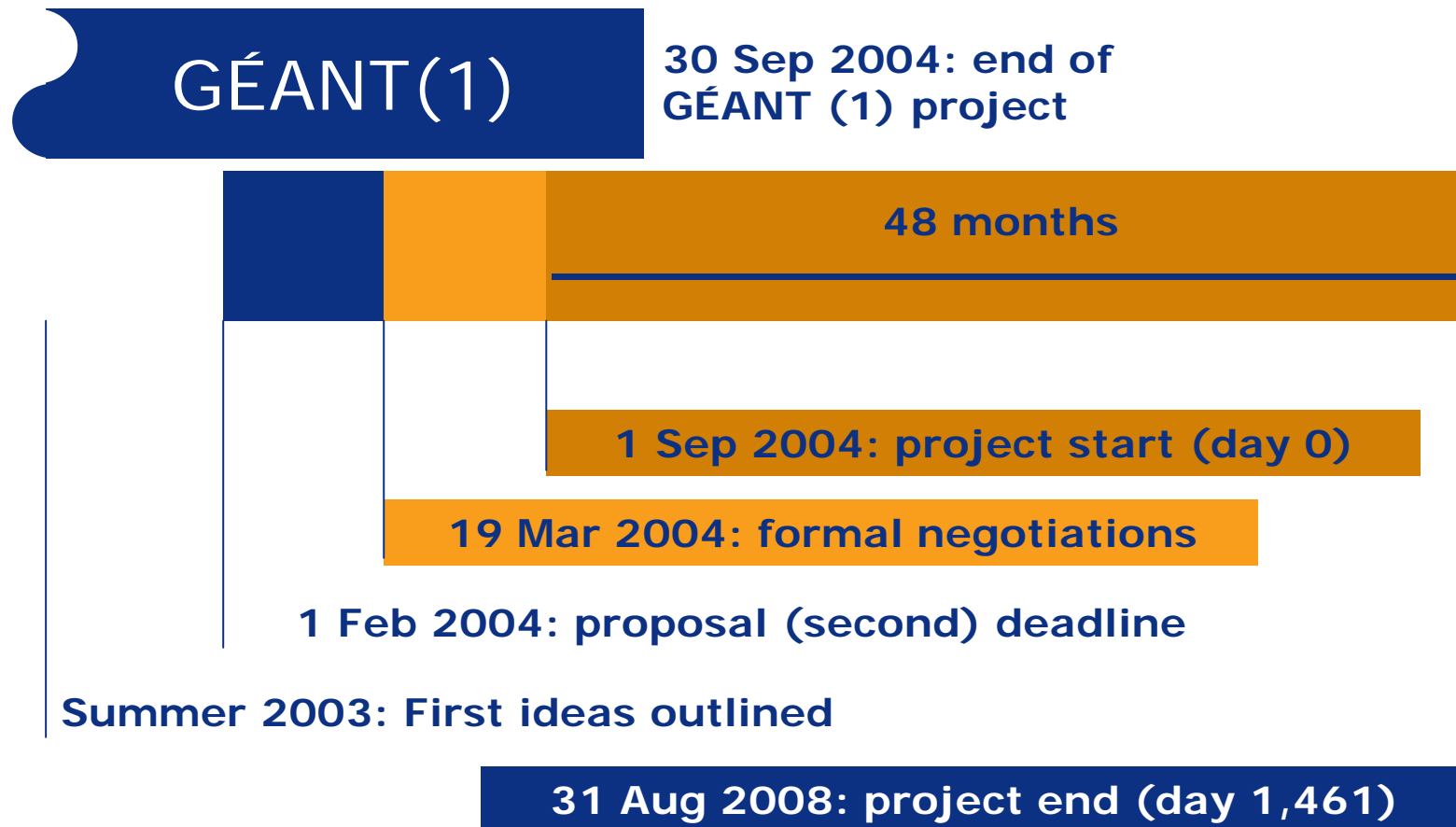
## Project structure, work packages

- 7 Network activities
- 4 Service activities
- 5 Joint research activities

## Timelines

- Project start: Sept. 04
- Duration: 4 years
- Reporting period: 1 year
- Detailed planning to date: first 18months

# GN2 time line



# Context of security activities

## GN2 (in terms of cost)

- Total projected cost: about 180M€
- Co-financing request: 93M€

## GN2 (in terms of manpower investment)

- Network Activities 25%
- Service Activities 27%
- Joint Research Activities 48% = 100%
  - » JRA1: Measurement & Mgmt 25%
  - » **JRA2: Security 25%**
  - » JRA3: New Services Development 25%
  - » JRA4: Technology & Service Testing 8%
  - » JRA5: Ubiquity and Roaming Access 17%

**JRA2 will help security teams  
within GN2 in their daily work**

# Security: why and what?

## Networking is the goal, not security per se

- We're making security not because it's cool ...
- ... but because it's needed to do networking
- We go for stuff we consider helpful to do our own job

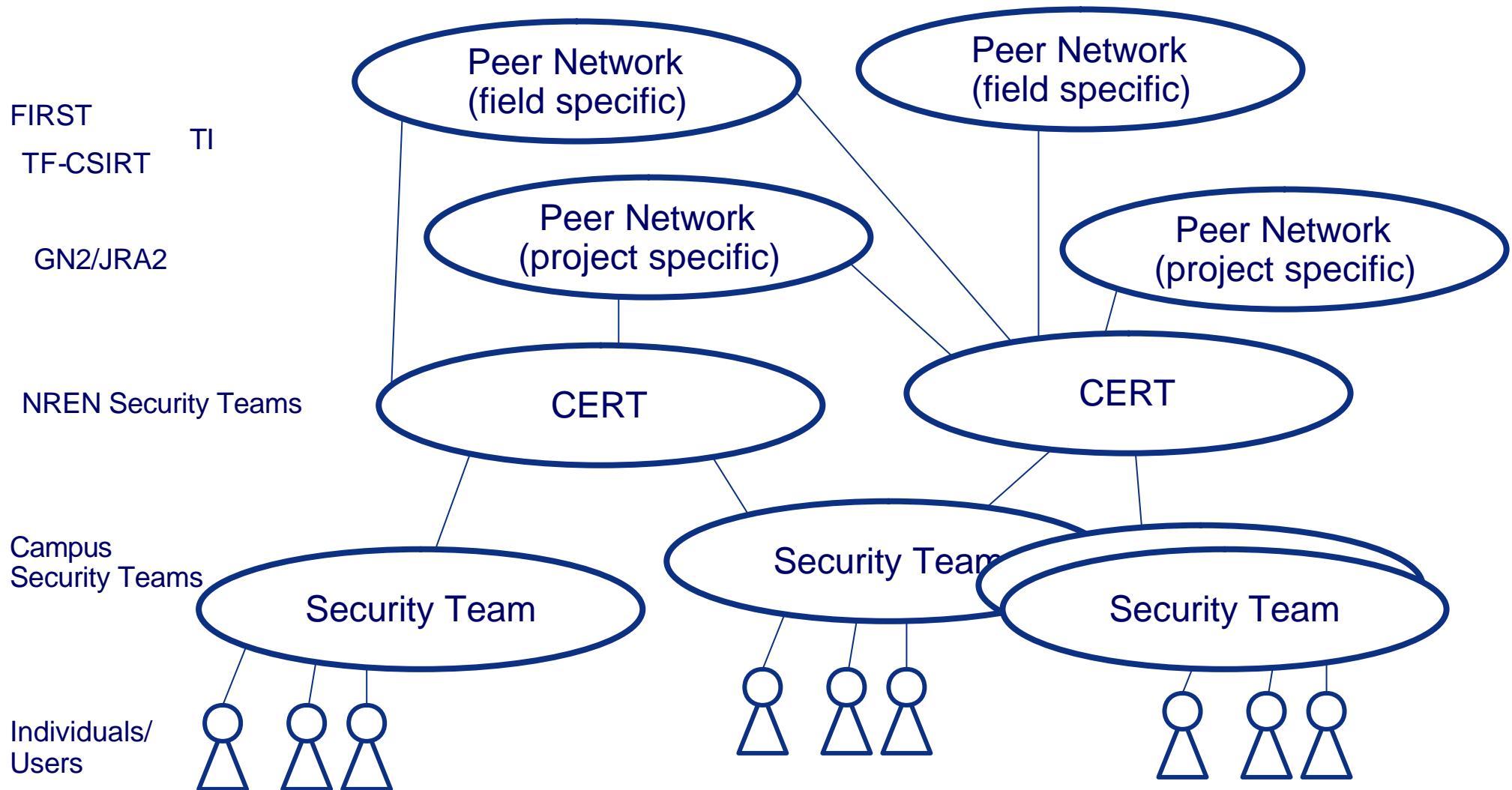
## Cool tools are:

- Maybe useful operationally, maybe not
- We have to find out by involving security stakeholders in early stages  
-> *That means us, the security teams within GN2 and friends!*

## Size does matter! As do common projects...

- Where does co-operation and sharing of information (1-to-many) in semi real-time *really* work?
- Not within FIRST, not within TF-CSIRT, not within TI ...
- ... maybe within GN2? Let's see: ./.

# Some thoughts on: Collaboration



# Which type of collaboration?

Peer Network  
(field specific)

## Which is the correct level?

- Lobbying activities
- Establish best practices
- Discuss collaboration models
- Discuss, develop new services
- Discuss new findings - anonymised
- Discuss new findings - including raw format
- Incident handling - information exchange
- Incident handling - hands on
- Incident handling - on site intervention
- ... etc.

Individuals/Users

## When are you willing to exchange potentially sensitive information?

### Group size is one important aspect:

- Without strict rules, based on personal trust: up to 20 partners (individuals/organisations)
  - » aka: Pub trust model
- Supported by rules with a trusted maintainer: maybe up to 60 partners
  - » aka: Mentor trust model
- Anything beyond 60?
  - » It wont work, let the group do something else!

### Other important aspects:

- Why? What do I gain? What are the risks?

# Apply this to JRA2...

## Size?

- Between 30 and 40 partner organisations

## Something precious in common?

- Absolutely! Smooth operation of GÉANT2

## Why collaboration?

- We have to: GN2 spans multiple management domains: GÉANT2 and NRENs
- Not to collaborate may hurt: If something breaks somewhere, everybody is affected (to some extent)
- Collaboration pays: We are all doing basically the same things
- We want to: Why GN2 after all?

## Level of collaboration?

- Semi real time information exchange with potentially sensitive information looks like the thing to go for and it looks perfectly doable

# And now: The GN2/JRA2 work items

## Based on draft GN2 “Description of Work” dated: 20040504

- Still under review
- Currently only available within GN2
- Contents of subsequent slides therefore subject to change

## **WP1: Securing GN2 network elements and services**

- recommendations and policies for GN2 & NRENs
- implementation on backbone and access links

## **WP2: Building of security services**

- Introducing “The Toolset”©
- deployment of eCSIRT.net results

## **WP3: Designing and establishing an infrastructure for co-ordinated security incident handling**

- Making use of “The Toolset”© and provide operational feedback to WP2
- Several partners to trial each new service

## **WP4: Relationship with TF-CSIRT**

- Acknowledge the overlap in membership and interests
- Ad-hoc groups of TF-CSIRT experts for advice to GN2

## **WP5: Establishment of advisory panel**

- Clearly defined role of TF-CSIRT

## Issues

- recommendations and policies for GN2 & NRENs
- implementation on backbone and access links

## When, what

- M 4 (month 4 of GN2), Deliverable: Initial security recommendations and policy for GN2 and partner NREN, implemented by M 12
- M 14, Deliverable: Revised recommendations and policies, implemented by M18

## Who

- Lead: DANTE
- Participation (co-funded): FCCN, GRNET, HUNGARNET, REDIRIS, RENATER
- Implementation (unfunded): Everybody

# WP2: Building of security services

## Issues

- Introducing “The Toolset”©
- Deployment of eCSIRT.net results
- NetFlow v9 exporter for line rates beyond 1Gbps (CESNET contribution)

## When, what

- M 5, Deliverable: User report, status of “The Toolset”©
- M 11, Deliverable: Updated user report (version 2)
- M 13, Deliverable: User and test report of the NetFlow v9 exporter
- M 17, Deliverable: Updated user report (version 3)

## Who

- Lead: SURFNET
- Participation (co-funded): DANTE, CARNET, CESNET, FCCN, GARR, GRNET, HUNGARNET, ISTF, IUCC, REDIRIS, SURFnet, SWITCH
- Implementation (unfunded): The more the merrier!

## Issues

- Policy and procedures describing the collaboration between security teams (classification, timelines, communication inside/outside GN2)
- Set up communication channels (re-use of eCSIRT.net results envisaged)
- Making use of “The Toolset”© and provide operational feedback to WP2

## When, what

- M 15, Deliverable: Report on pilot and recommendations

## Who

- Lead: GARR
- Participation (co-funded): not specified, all are directly concerned
- Implementation (unfunded): expected to cover all GN2 partners

## Issues

- Acknowledge the overlap and area of common interest in GN2/JRA2 and TF-CSIRT
- Ad-hoc groups of TF-CSIRT experts for specific advice to GN2

## When, what

- M 12, Deliverable: Report on ad-hoc advisory groups creation and activities
- M 18, Deliverable: Updated report

## Who

- Lead: SWITCH
- Participation (co-funded): SURFnet
- Implementation (unfunded): Volunteering TF-CSIRT members

# WP5: Establishment of advisory panel

## Issues

- Discussing and shaping the strategic direction of JRA2
- Advisory panel recruited from TF-CSIRT
- Panel meetings adjacent to TF-CSIRT

## When, what

- M 12, Deliverable: Report on activities and recommendations of advisory panel (updated yearly)

## Who

- Lead: SWITCH
- Participation (co-funded): JRA2 activity leader
- Implementation (unfunded): volunteers from within TF-CSIRT