Security in the academic networks: current advances within the GEANT project

business continuity, security baseline and products and services offered to the national academic and research networks

Anastas Mishev
FINKI-CIRT/GEANT

To support collaboration and development amongst researchers, the dissemination of information & knowledge, and provide access to a portfolio of services and infrastructure resources:

Runs a membership association for Europe's National Research & Education Networks (NRENs)
GÉANT Association

Coordinates and participates in EC-funded projects
Under Horizon 2020 the financial instrument for implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness

Operates a pan-European e-infrastructure
GÉANT network

Manages a portfolio of services for research & education
EduX

Organises and runs community events & working groups
TNC, task forces & special interest groups

Membership Association

GÉANT Association supports and represents over 40 NRENs across Europe.

Together they support over 10,000 institutions and 50 million academic users.

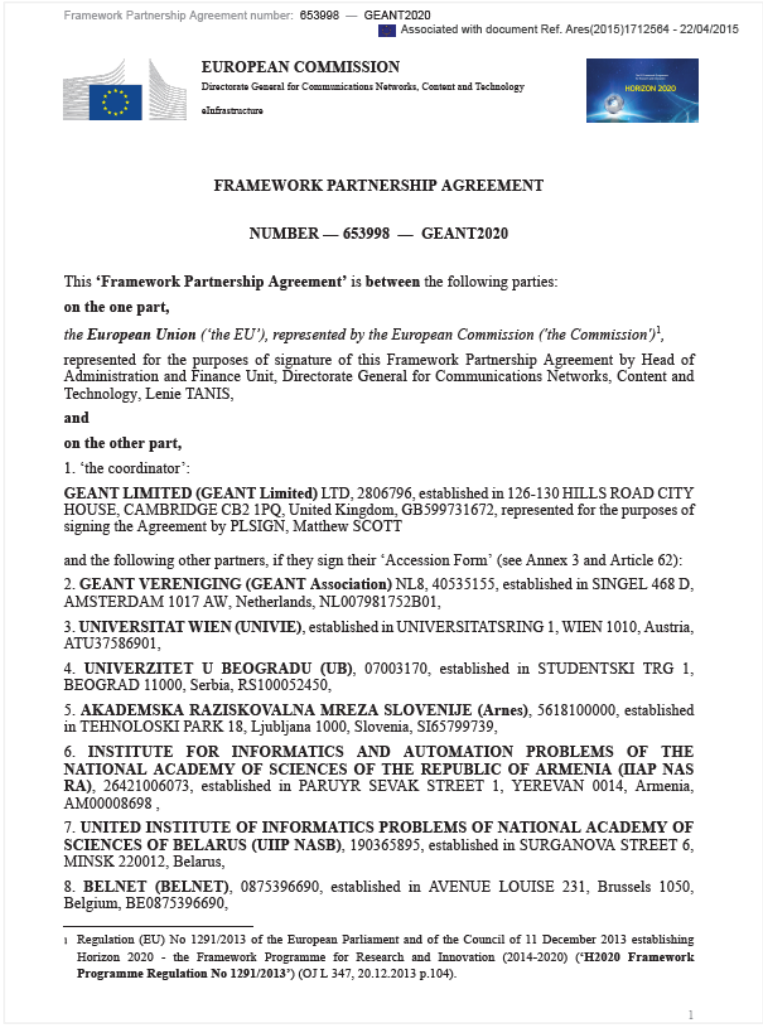
Membership Association

GÉANT Association supports and represents over 40 NRENs across Europe.

Together they support over 10,000 institutions and 50 million academic users.

GÉANT Project

- GN4-1: 1 May 2015 to 30 April 2016
- GN4-2: 1 May 2016 to 31 December 2018
- GN4-3: 1 January 2019 to 31 December 2022



Framework Partnership Agreement number: 653998 — GEANT2020
Associated with document Ref. Ares(2015)1712564 - 22/04/2015

EUROPEAN COMMISSION
Directorate General for Communications Networks, Content and Technology
eInfrastructure

FRAMEWORK PARTNERSHIP AGREEMENT

NUMBER — 653998 — GEANT2020

This **'Framework Partnership Agreement'** is **between** the following parties:

on the one part,

the ***European Union*** *('the EU'), represented by the European Commission ('the Commission')*[1],

represented for the purposes of signature of this Framework Partnership Agreement by Head of Administration and Finance Unit, Directorate General for Communications Networks, Content and Technology, Lenie TANIS,

and

on the other part,

1. 'the coordinator':

GEANT LIMITED (GEANT Limited) LTD, 2806796, established in 126-130 HILLS ROAD CITY HOUSE, CAMBRIDGE CB2 1PQ, United Kingdom, GB599731672, represented for the purposes of signing the Agreement by PLSIGN, Matthew SCOTT

and the following other partners, if they sign their 'Accession Form' (see Annex 3 and Article 62):

2. **GEANT VERENIGING (GEANT Association)** NL8, 40535155, established in SINGEL 468 D, AMSTERDAM 1017 AW, Netherlands, NL007981752B01,

3. **UNIVERSITAT WIEN (UNIVIE)**, established in UNIVERSITATSRING 1, WIEN 1010, Austria, ATU37586901,

4. **UNIVERZITET U BEOGRADU (UB)**, 07003170, established in STUDENTSKI TRG 1, BEOGRAD 11000, Serbia, RS100052450,

5. **AKADEMSKA RAZISKOVALNA MREZA SLOVENIJE (Arnes)**, 5618100000, established in TEHNOLOSKI PARK 18, Ljubljana 1000, Slovenia, SI65799739,

6. **INSTITUTE FOR INFORMATICS AND AUTOMATION PROBLEMS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF ARMENIA (IIAP NAS RA)**, 26421006073, established in PARUYR SEVAK STREET 1, YEREVAN 0014, Armenia, AM00008698 ,

7. **UNITED INSTITUTE OF INFORMATICS PROBLEMS OF NATIONAL ACADEMY OF SCIENCES OF BELARUS (UIIP NASB)**, 190365895, established in SURGANOVA STREET 6, MINSK 220012, Belarus,

8. **BELNET (BELNET)**, 0875396690, established in AVENUE LOUISE 231, Brussels 1050, Belgium, BE0875396690,

1 Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) (**'H2020 Framework Programme Regulation No 1291/2013'**) (OJ L 347, 20.12.2013 p.104).

1

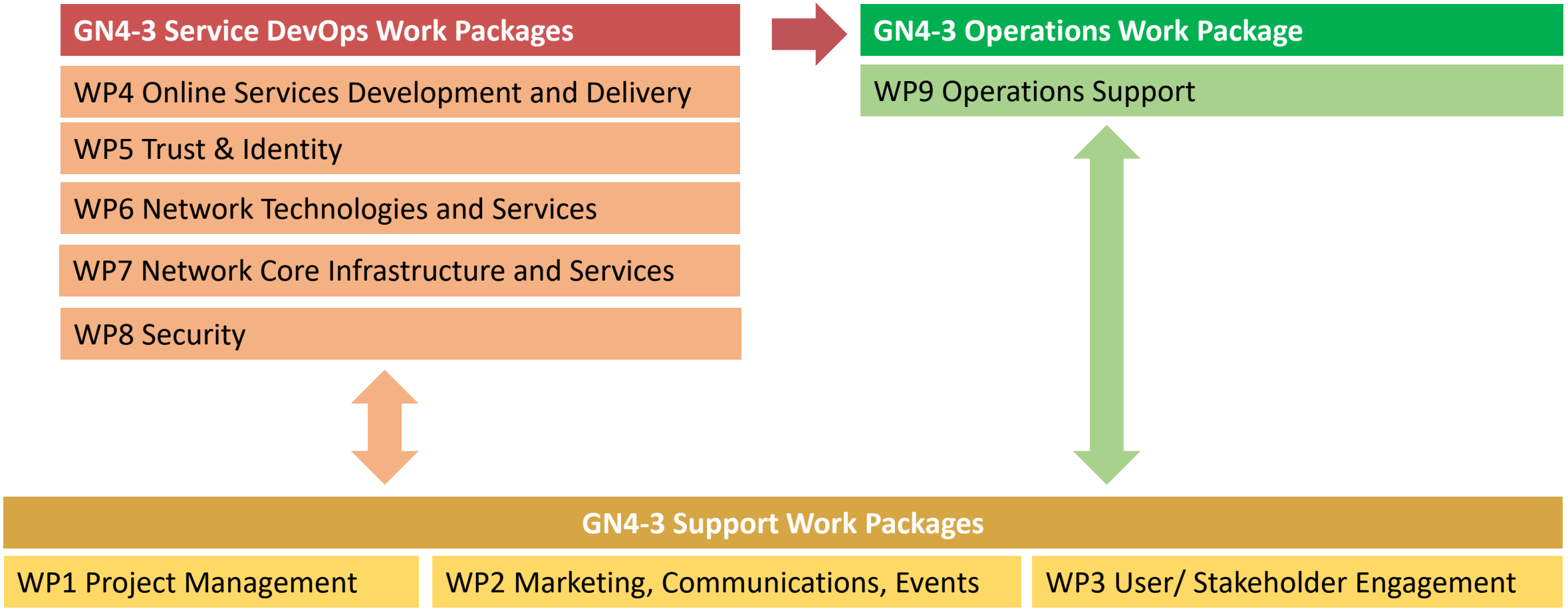
GÉANT Project in numbers

39 Partners, 42 Countries
157 FTEs (average per year over project duration)
500+ registered contributors

EC funding: €128M

9 Activities, 34 Tasks
124 Deliverables
32 Milestones

GÉANT Project Structure



Security Work Package Objective

Keeping the R&E network safe and secure at the backbone level and supporting the GÉANT Partners with up-to-date tools to keep their networks and connections to the GÉANT network safe and secure in an environment of increasing levels of cyber-security threats.

Security WP – Facts and Figures

- 43 participants, 19 organizations, 14 countries, 4,3M euro budget

Task	Topics
Business Continuity	Crisis Management, Training and Awareness, Business Continuity Recommendations
Security Baselining	Risk Management, Security Baselining
Products & Services	**SUBTASKS:**
	SOC
	Vulnerability assessment as a service
	DDoS
	Firewall on Demand
	eduVPN

Task 1 – Business Continuity

- Business Continuity, Crisis Management, Security Training and Awareness
- Purpose: The task will aim at creating (cyber security) resilient NRENs with a cyber security awareness culture within our partner organisations and community as a whole.
- Year 1:

  Status analysis and requirements analyses

  CLAW 3 – crisis management event

  Summary of security training and awareness campaign materials

Task 2 – Security Baselining

- Security Baseline, Benchmarking, Risk Management
- Purpose: Agree upon security frameworks and set up and test a benchmarking system based upon the agreed security baselines, encourage a risk based approach
- Year 1:

  Security Baseline for NRENs based on international standards and security best practices

  Annual Top 10

Task 3.1 – SOC

- Security Operations Center
- Purpose: Develop a comprehensive set of SOC tools, some of which will require training and documentation to adopt the available solutions in different operational infrastructures, share good practices.
- Year 1:
    - Description of high level SOC architecture
    - Release of the first, limited toolset

Task 3.2 – Vulnerability Assessment as a Service

- Vulnerability Assessment as a Service
- Purpose: investigate feasible and scalable solutions for identification of security vulnerabilities and the tools that are best suited for this purpose, building on experiences from the NRENs
- Year 1:
    - Collect legal requirements from participating countries
    - Collect and share good practices
    - Collect and compare requirements to existing tools, both open source and commercial

Task 3.3 – DDoS

- Defend against (distributed) Denial of Service attacks
- Purpose:
  - Build and maintain a fit-for-purpose modular flow-analysis suite.
  - Deliver best practice guides for detecting and mitigating DDoS solutions, both technological and organisational (tools, processes and procedures)
  - Design and implement one or more central or regional DDoS mitigation facilities
- Year 1:
  - DDoS workshop, identifying interested parties + showcasing existing solutions
  - Collect and share good practices
  - Make the (DFN) NeMo-Software more open

Task 3.4 – Firewall on Demand

- Firewall on Demand
- Purpose:

  Development of a generalised, multi-domain Firewall on Demand interface supporting FlowSpec and, if necessary, additional protocols.

  Establishing Firewall on Demand as a multi-domain interface to allow integration into the coordinated DDoS mitigation across multiple domains (GÉANT, NRENs, institutions).

  Delivery of attack and monitoring data to improve and analysis
- Year 1:

  FoD future development requirements analysis

  New release

Task 3.5 – eduVPN

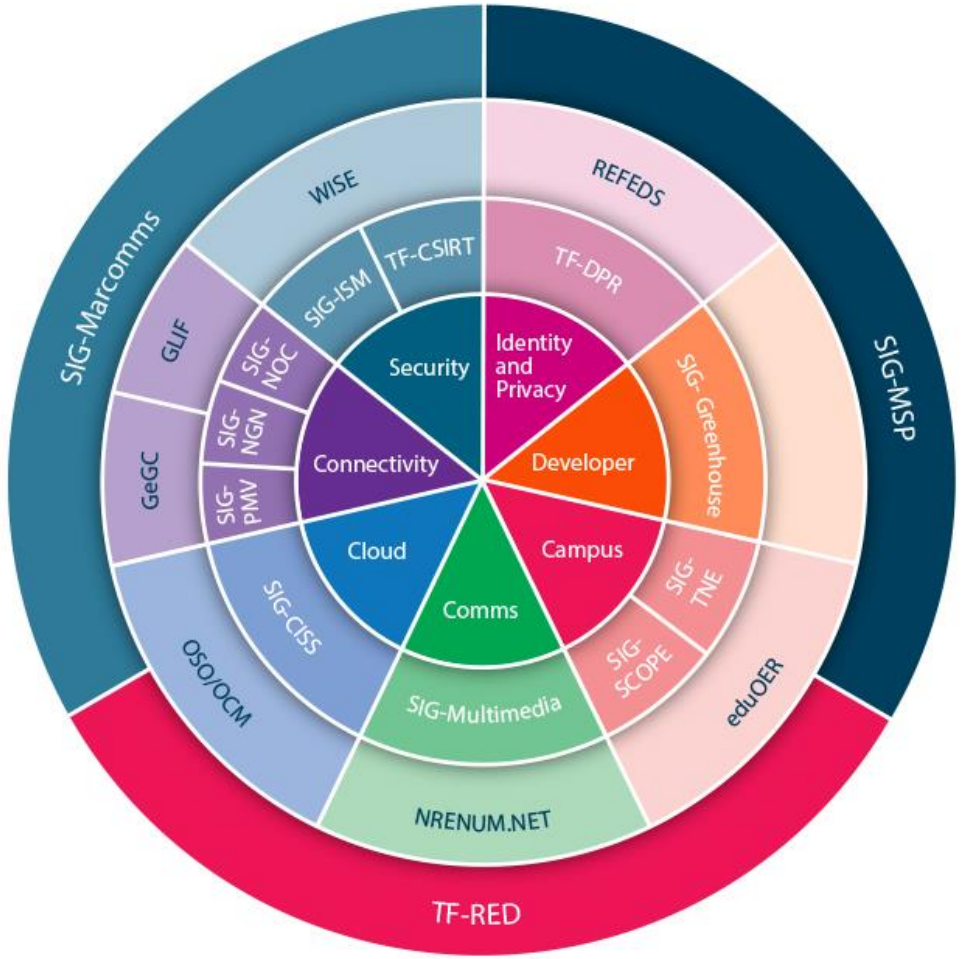
- Virtual Private Networking
- Purpose: Continue development of eduVPN and increase adoption for both ‘business’ and students.
- Year 1:
  - Community workshop to promote the service and gather requirements
  - New release, new apps
  - International outreach

Security WP - YEAR 1

- Gathering requirements, contacts, examples - what is already available?
- Defining the scope of work - what are we trying to achieve?
- Importance of collaboration
- Why can’t we just buy something?
- What is important to us?

Common problems - common solutions!

SIGs and TFs

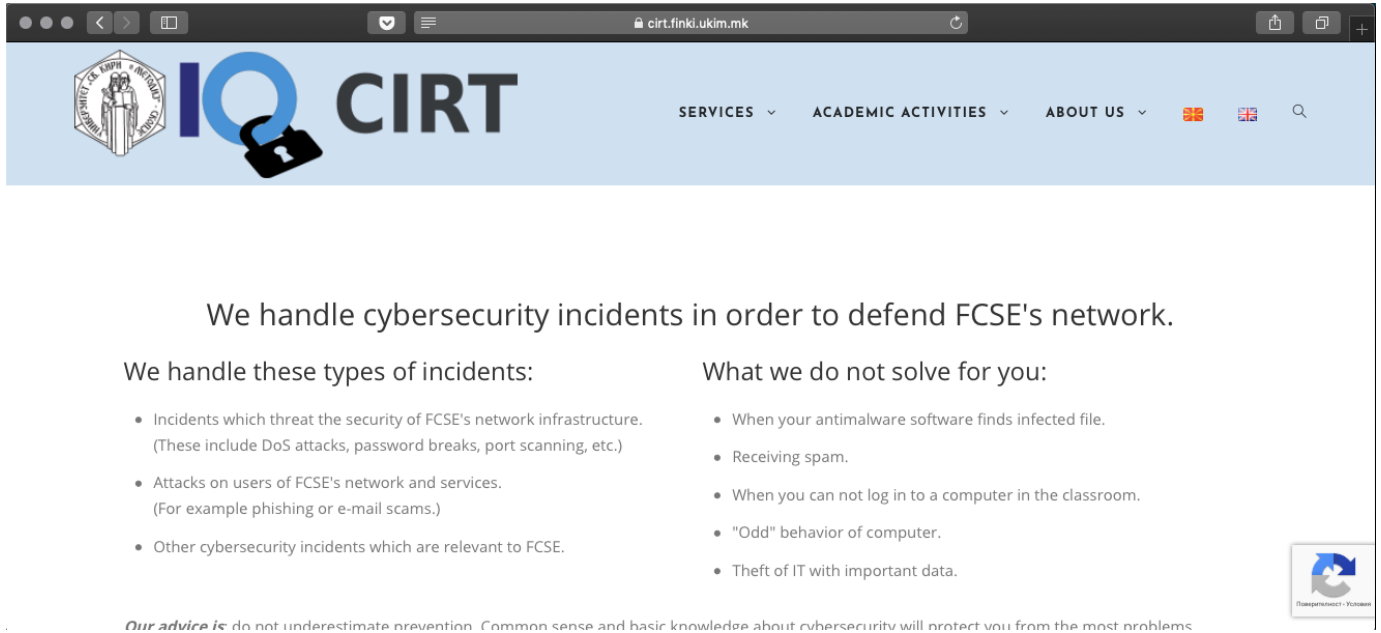

SIG-Marcomms
WISE
REFEDS
SIG-MSP
GLIF
TF-CSIRT
TF-DPR
SIG-ISM
SIG-NOC
SIG-NGN
SIG-PMV
GeGC
Security
Identity and Privacy
Developer
SIG-Greenhouse
Connectivity
Cloud
Campus
Comms
SIG-TNE
SIG-SCOPE
SIG-CISS
OSO/OCM
SIG-Multimedia
eduOER
NRENUM.NET
TF-RED

TF-CSIRT

- Facilitate and improve the collaboration between the European CSIRT community to make cyber space a better place, supported by GEANT
- TRANSITS provides state of the art, high-quality training to Computer Security and Incident Response Team (CSIRT) personnel, co-ordinated by GÉANT
- The Trusted Introducer Service forms the trusted backbone of infrastructure services and serves as clearinghouse for all security and incident response teams.

FINKI-CIRT

- Established in 2017 as an organizational unit of the Faculty of computer science and engineering, UKIM, as the first (and probably still the only academic CIRT in the country)
- Main working groups
  - Incident handling
  - Proactive security
  - Quality management
- Services
  - Incident reporting and handling
  - Information dissemination
  - Security advices to the students
  - Security education
  - Pen-testing
- Volunteer organization
  - Academic staff
  - Technical staff from the faculty computing center
  - Students interested in security, organized as a student CIRT club
- Close collaboration with MKD-CIRT



Thank you

Any questions?