30-11-2023

Milestone M8.3
Business Model for Joint Delivery of Security Services

Contractual Date:	30-11-2023
Actual Date:	30-11-2023
Grant Agreement No.:	101100680
Work Package:	WP8
Task Item:	Task 3
Nature of Milestone:	White Paper
Dissemination Level:	PU (Public)
Lead Partner:	GÉANT Association
Document ID:	GN5-1-23-1a6ae4
Authors:	Jochen Schönfelder (DFN-CERT); David Heed (SUNET)

Abstract

This white paper presents the business model options for a security service within the GÉANT NREN community. Three major options are detailed and existing security services matched to these options. The document is intended to be a first step towards a more defined business model selection for new and existing security services.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents

1 Introduction

A diverse array of offerings and capabilities are available in the landscape of security services. These offerings range from consultancy and training to the support of individual technical network elements. This report will focus on the delivery options for technical services in the NREN context. At a glance, these services can be broadly categorised into two distinct groups: those that are accessible to virtually anyone/anywhere and those that require specific network positioning. These services would usually need to be at least partially delivered by the controlling entity of the specific network part. However, while this limits delivery options for some security services, it does not apply to all of them.

The options for security service delivery via the GÉANT project fall within different business models which are mainly defined by the roles of the various stakeholders.

The three main business models defined respectively cover services that are:

1. Maintained and provided by GÉANT centrally ("GÉANT Central")
2. Run by one or more NRENs, provided by GÉANT ("GÉANT Resale")
3. Run by one or more NRENs, with GÉANT contractually supporting them ("GÉANT Community Support")

The report details the business model canvasses showcasing the different options and aspects of a hypothetical service falling under each model. For the security services within the GÉANT project which are currently being delivered, or close to delivery, a short overview of how they relate to those models is provided.

Finally, some considerations and recommendations are given towards the selection of the best business model for security services going forward.

2 Business Model Canvases

2.1 GÉANT Central Business Model

Having GÉANT create a central service offering that is accessible for participating NRENs involves the largest scale of cooperation of all the models examined. Centralising service delivery to a joint model requires community involvement, both in terms of establishing wants and needs and in formalising operations post-pilot. The benefits of this model include shared staff (and possibly reduced) overhead and other scale efficiencies compared to running multiple individual NREN services.

- **Key resources**
  - The key resources that are required by this model will depend on the individual service. However, for a central security-related business model these will likely include:
    - Staff to run the service, e.g. security analysts, operating, support
    - Servers or virtual machines
    - Licenses
    - Support infrastructure
    - Service management overhead to develop the service based on the NREN's needs as well as to keep it running
- **Key activities pre-service initialisation**
  - Initial requirements and demand pre-study
  - Review of technological architecture (scalability, security features, authentication mechanisms etc)
  - After successful Pilot-implementation, produce pre-service documentation and formalise initial operation
  - Service contract generation
  - Service communication material
  - Onboarding webinars and outreach to gain market
- **Key partners**
  - Stakeholders: GÉANT connected NRENs for network-related security services (e.g.: DDoS), other NRENs within the broader NREN community for non-network related services
  - External product or service provider (which might be the NREN that initially developed a specific service, or a commercial vendor)
  - Research community/end users, for services directly addressing research institutions/universities
- **Value propositions**
  - Network upstream protection for network-related services (e.g.: DDoS/FoD)
  - Central knowledge/capability creation for overarching or niche topics as in threat intelligence, open source information or vulnerability scanning capabilities
  - Lower shared licensing fees for seldom used services or cost-effective scaling solutions
  - Lower individual NREN staffing needs

- **Customer relationships**
    - Stakeholder meetings
    - Service coordinator gets input and feedback for service improvements
- **Channels**
    - NREN and NREN customer security teams/contacts – including SOCs and CSIRTs, ISOs
    - NREN and NREN customer #network teams/contacts – including NOCs and research computing/datacentre contacts
    - Engagement with national/regional cybersecurity centres/projects
    - GÉANT Project Task Forces (TFs) and Special Interest Groups (SIGs)
    - NREN engagement forums
    - Vendor forums
- **Customer segments**
    - NRENs
    - NREN customers within the terms of the NRENs (considering branding and outreach requirements)
    - GÉANT project and association
- **Cost structure**
    - Staff:
        - technical and operational staff
        - Service management
        - support
    - Hosting infrastructure/central service infrastructure costs
    - Vendor/product fees including licensing and support
    - Branding & multi-tenancy implementation costs
- **Revenue streams**
    - GÉANT project contributions for several aspects possible: service design & initial setup, service support
    - Service fees
    - GÉANT membership fees for mandatory security services:
        - these may be applicable for GÉANT network security protection services

2.2 GÉANT Resale Business Model

Creating effective frameworks and opportunities for vendors and prospective clients to meet can be a quick way to facilitate deployment and would not hinder delivery on an NREN's existing services. This model could often be used as an additional or complementary service.

- **Key resources**
    - The key resources that are required in this model will depend on the individual service. However, for a resale security-related business model these will most possibly include:
        - Staff for service management as well as possibly to support the service, e.g. project management, support
        - Service provided by an NREN ("NREN-SP")
        - Licence fees

- **Key activities pre-service initialisation**
  - Initial requirements and demand pre-study
  - Review of market and initial contacts with relevant vendors
  - Procurement and contract
  - PoC with contract winner to verify functionality
  - Service contract generation
  - Onboarding webinars and outreach to gain market
- **Key activities post-service initialisation**
  - Vendor management
  - Quantity and billing handling
- **Key partners**
  - Stakeholders: European NRENs
  - External product or service provider (which might be the NREN that initially developed a specific service, or a commercial vendor)
  - Research community/end users, for services directly addressing research institutions/universities
- **Value propositions**
  - Same as for the central business model except for those services which would need direct GÉANT network placement
- **Customer relationships**
  - Facilitate vendor information-sharing including webinars
  - Inform customers of changes and procurements
- **Channels**
  - While these should be mostly the same as for the central business model, the NREN providing the service can take a more active role within these channels
  - Service vendor management might be directly addressed by the NREN-SP
- **Customer segments**
  - NRENs
  - NREN customers within the terms of the NRENs (considering branding and outreach requirements)
  - GÉANT project and Association
- **Cost structure**
  - Staff: service management, support
  - NREN-SP contractual costs
  - Initial branding & multi-tenancy implementation costs
- **Revenue streams**
  - GÉANT project contributions for several aspects possible: service design & initial setup, service support
  - Service fees

2.3 GÉANT Community Support Business Model

The opportunity to collaboratively create services is one of the strengths of the community environment. A successful service offering from one NREN can serve as a reference or engender collaborative effort towards continual improvement. Joint engagement in projects such as GN5-1 can facilitate prioritised developments that can serve the community.

- **Key resources**
  - The key resources that are required will depend on the individual service. However, for a business model which depends on enabling members of the community to provide services to each other, these will likely include:
    - Staff for service contract management support
    - Small–scale funding either via the GÉANT project budget or collaboration between NRENs
- **Key activities pre-service initialisation**
  - Initial requirements and demand pre-study
  - Incubator or cooperation with existing service within NREN
  - Webinar and interest group/reference group meeting to seek 4 additional NRENs to support initiative
  - Create joint documentation
  - Establish community meetings (such as Campus Network as a Service)
  - Onboarding webinars and outreach to gain market.
- **Key activities post-service initialisation**
  - Service contract support
- **Key partners**
  - Stakeholders: service-providing NRENs
  - European NRENs for service/contractual feedback
- **Value propositions**
  - Better service structuring: scopes and contractual situations for different services can be better aligned
  - Outreach possibilities of the GÉANT project surpass those of some NRENs, so a wider user base is possible
  - Gap between an individual internal NREN service and a functional service for a wider audience can be bridged with project means
- **Customer relationships**
  - Facilitate working groups or special interest groups
- **Channels**
  - The GÉANT project can make its channels (see central business model) available for service outreach but does not need to play an active role in these apart from contract management
- **Customer segments**
  - NRENs
  - NREN customers within the terms of the NRENs (considering branding and outreach requirements)
  - GÉANT project and Association
- **Cost structure**
  - Contractual support
- **Revenue streams**
  - GÉANT project contributions
  - Supporting the NREN community is a core element of the GÉANT Association and GÉANT projects

3 Current Service Considerations

As detailed in the canvasses above, the three business models examined mostly differ in terms of affiliation and placement of the needed resources. While for some security services a choice might be set easily based on the requirements inherent to the type of service, for others more options are available. In particular staffing needs – and at which stakeholder staff is needed respectively – differ between the models and as such can help determine the best fitting choices. Other differentiation aspects include options for channel management, as well as for vendor management, which might also be relevant to business model selection, especially in those cases where one choice might be of greater financial benefit to the NREN community.

The business models above also cover existing security services which have already been deployed (or are in the process of being deployed) within the GÉANT project. The following services are considered:

DDoS - DDoS mitigation Service

- **Short description:** The GÉANT DDoS service is a GÉANT offering for NREN upstream protection via large-scale DDoS attacks
- **Applicable business model:** central business model
- **Remarks:** The GÉANT DDoS service has been developed in parallel to the creation of this document, so some of its elements have already been taken into account. While the central business model has been chosen for the DDoS service itself due to technical network positioning requirements, the underlying software (NeMo-DDoS) is co-developed and enhanced in collaboration with the NREN that originally developed it and still uses it internally. This means aspects of the community model also apply, as other NRENs are supported to also use the underlying software locally. Beyond this, the option of providing a DDoS service where part of the components are placed within different NRENs is also being considered. In this case, a different business model might be selected in future, or alternatively such an extension could be treated as an additional service with its own business model.

eduVPN

- **Short description:** Provides NREN- and/or institution-level access to a VPN-service
- **Applicable business model:** Community support business model. Self-service of components which can be hosted by NREN and provided as a service for institutions – variations exist.
- **Remarks:** Builds upon standardised components and cryptography.

FoD - Firewall on Demand

- **Short description:** FoD (Firewall on Demand) provides a self-service option for NRENs to filter unwanted traffic to their respective GÉANT uplinks via firewall-like rules.
- **Applicable business model:** central business model
- **Remarks:** None

TCS – Trusted Certificate Service

- **Short description:** TCS (Trusted Certificate Service) is a certificate service offering via GÉANT which enables NRENs and their end-users to obtain cryptographic certificates for different needs such as server, browser or email usage.
- **Applicable business model:** central business model
- **Remarks:** GÉANT is providing this service via a service vendor.

VAaaS – Vulnerability Assessment as a Service (Commercial)

- **Short description:** Provides a Vulnerability assessment scanning service.
- **Applicable business model:** Commercial procurement delivered as an MSSP-like central business model. Billable per asset/month.
- **Remarks:** NREN should deploy scanning nodes on national/local infrastructure for faster and more accurate results.

VAaaS – Vulnerability Assessment as a Service (Open-Source)

- **Short description:** Provides a Vulnerability Assessment scanning service with open source components.
- **Applicable business model:** community support business model: Free to use, free to copy. Hosted within GN5-1 as an ongoing pilot.
- **Remarks:** NREN could deploy scanning nodes on national/local infrastructure for faster and more accurate results. A docker image is maintained for ease of installation.

As can be seen, central and community support business models have mostly been used for the current services. However, it has to be considered that most of the underlying choices for this predate this document and it remains unclear whether these two models would be the best choice for upcoming new services, or if it would be more beneficial to provide better support for a GÉANT resale business model. Adopting such a model could potentially result in better time-to-market as it would likely require fewer key resources and have a more straightforward cost structure.

4 Conclusions and Next Steps

While the different business canvasses described showcase the options for the security services within the NREN community, it is neither easy nor obvious in all cases to identify which option should be selected for a specific service. Some services which require network access have to be run centrally within the GÉANT core network, and as such likely demand the use of a central business model, but the structure of other services may not directly imply which model is more applicable.

It might also not be trivial to identify the correct stakeholders for each service as, due to the nature of the security field, new threats arise which imply new service needs involving new competencies and leading to further NREN requirements. This can be seen for example in the broad trend towards SOC-related service offerings in the past years. Additionally, some security services within the NREN community may also be purposefully kept secret, so the development of unknown multiple solutions even for addressing very similar underlying security issues is a realistic possibility.

In view of the above, the creation of further guidelines and possibly selection matrixes by an expert panel or reference group in a future project phase is recommended to facilitate the creation and rollout of new security services.

Glossary

CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service (-attack)
FoD	Firewall on Demand
ISO	Information Security Officer
NeMo-DDos	Network Monitoring for DDoS attacks
NOC	Network Operation Centre
NREN	National Research and Education Network
NREN-SP	NREN as a service provider
PoC	Point of Contact
SIG	Special Interest Group
SOC	Security Operations Centre
TCS	Trusted Certificate Service
TF	Task Force
VAaaS	Vulnerability Assessment as a Service
VPN	Virtual private network