GÉANT

Email Security Project

Enterprise Security Architecture

TLP: AMBER

Fotis Gagadis

Security Officer

WISE – Krakow, Poland

Sept 27, 2016

Introduction – SABSA methodology usage

- This is a methodology that can be shaped
- Connecting link among Business and Security (Harmonising)
- Decision making upon:
  - Business-oriented
  - Human-oriented
  - Re-usable
  - Cost-effectiveness
- This methodology can be used for **compliance and technical architectures**
- We evaluate the methodology as part of normalising our environment in the future
- The methodology provides also guidance on security enhancing ITIL processes (aligned with Service Assurance). Therefore, better working environment and Services at end.
- In this case alignment with Service Assurance did not take place due to time constraints and resources. **BUT** it is only one step e.g. I want to have non-repudiation then registration process, authorisation process etc
- Helps understanding the environment and make better decisions

Gathering the Objectives from Stakeholders

Email Security Requirements																
Objectives (What)								What		Why			How		
Main stakeholder	Main stakeholder	Secondary Stakeholder	User		Secondary Stakeholder	User		Assets (Business Objectives, Goals, Business Assets,)	#BD	Motivation (Opportunities & Threats)	#BD	User	Process (Business Processes)	#BD	User
CITO		HR	PMO	Management (Valentino)	Finance + Compliance Officer	Operations									
									1	Not being able to communicate effectively inside and outside the company esnuring confidentility	21	HR,Finance, Operations, CITO		31	Operations, CITO
									2	Unlisensed products being used	22	Operations, CITO		32	Operations, CITO
									3	Due to unlicesced products fines might be pretty high	23	Operations, CITO		33	Operations, CITO
										Multiple cryptographic suites used across the company to ensure secret communication	24	Operations, CITO	CITO	34	Operations, CITO
x	x	x		x	x	x		To send secure emails internally		CERT team cannot communicate effectively	25	Operations, CITO		35	Operations, CITO
										CERT team using only					

Business Attributes Analysis

#BD	Security Drivers	Measurable Business Attributes
1	Communication to be kept confidential within the organization	Message Confidentiality
2	To ensure the integrity of the message within the organization	Message Integrity

Measurable Business Attributes	Security Drivers	Description of Attributes
Message Confidentiality	1,4, 8,11	The solution must ensure the confidentiality of the information contained within the message and specific people being able to view only the information as needed per their role and messages are not disclosed outside the chosen recipients. This means that the solution must prevent the unauthorised disclosure of information including personal assistants. Only Intended people can view this information
Message Integrity	2,5,9,12	The solution must be able to ensure the integrity of the message and of the information contained within the email body and the integrity of information in transit. This will prevent unauthorised modification of information being unnoticed. Only intended recipients and approved people can modify the message.

Assigning attributes to Stakeholders

Measurable Business Attributes	Security Drivers	Description of Attributes	Category	Main Stakeholder	Secondary Stakeholde		User		
				CITO	HR	Finance + Compliance Officer	PDO	PMO	Operations
Cost Effective	23, 44	The solution must be cost-effective to ensure that it does not affect the budgets within the company and cost effective on maintenance.	Financial Efficiency	M	-	-	-	-	M

Assigning Policy Authorities to Attributes and Set Enablers

Security Drivers	Description of Attributes	Measurable Business Attributes	Control Objective	Enablement Objective	Policy Domain	Policy Authority - ownership of assets and the risk to the assets which may be quite diferent
19	The solution must ensure that the information sent to various people is private and being treated in such a way that complies with laws and regulations that affect the organization	Privacy	Confidentiality	Treatment of information as stated across the regulations pertaining the operations of the organization	Information	CITO
22	The solution must be licensed with a third party to operate within the organization without fines being applied	Licensced	Protection against litigations	To ensure the reputation of the company across community by being able to protect its reputation	Finance	Finance

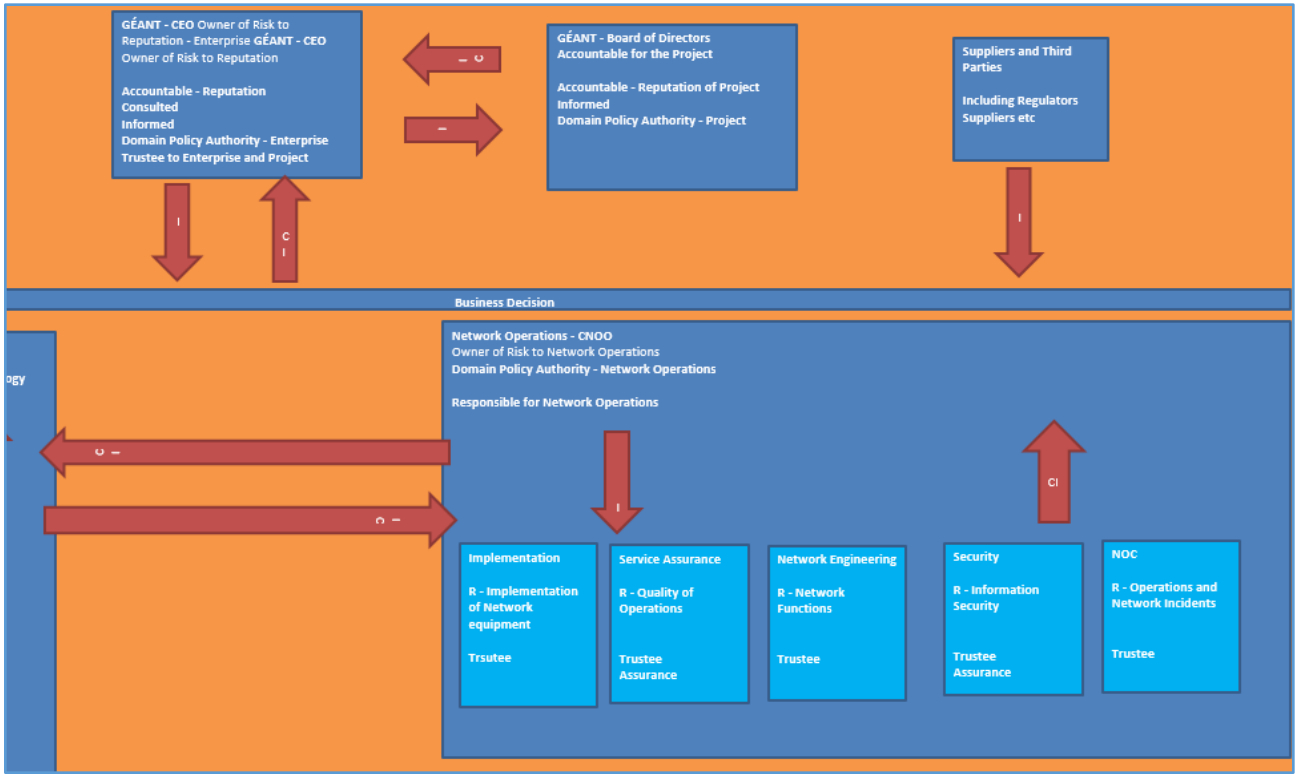
Risk Domains

		GÉANT - CEO	
	Risk Conflict Escalation Point	Owner of Risk to Reputation - Enterprise	

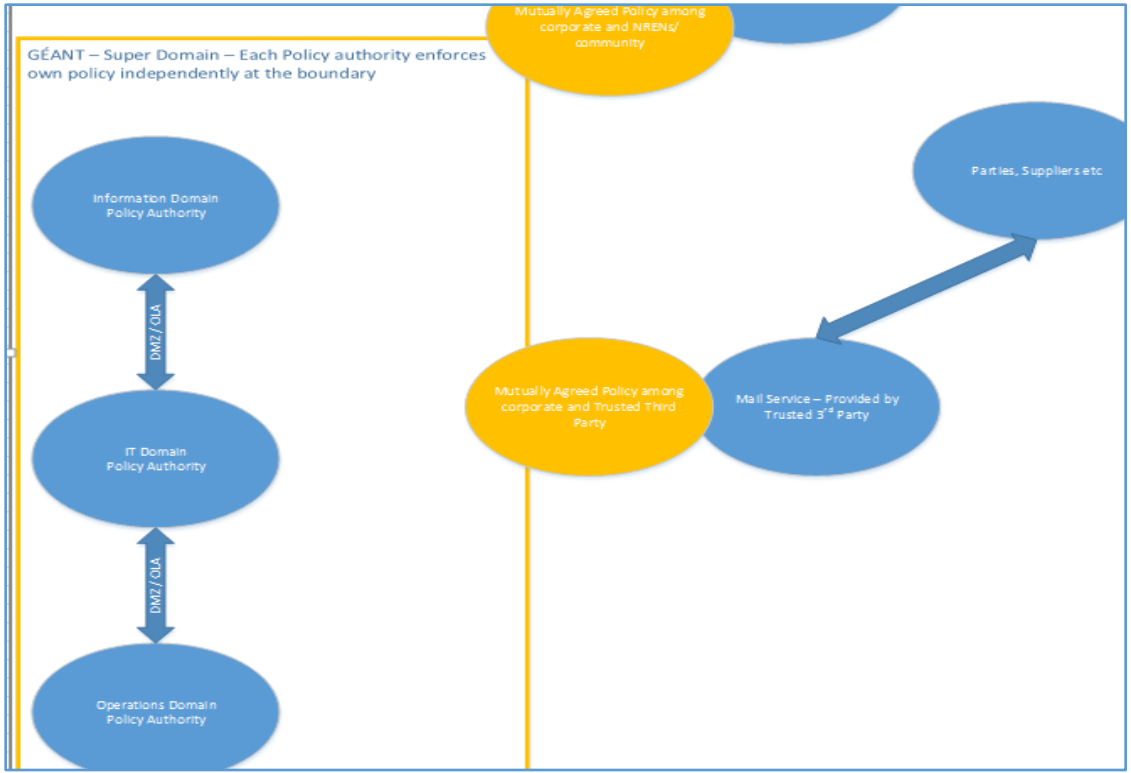
Main Stakeholder - Systems/IT/Information - CITO		Finance + Compliance Officer - CFO	Network Operations - CNOO
Owner of Risk to Information	Owner of Risk to Technology	Owner of Risk to Finance, Human Capital and Facilitie	Owner of Risk to Network Operation
		Conflict of Interest - Multiple Domain Policy Authority	
Sub departments responsible for		**Sub departments responsible for**	**Sub departments responsible for**
			Security
Systems		Finance	Networking/Implementation
		HR	NOC
		Facilities	Service Asssurance

- CNOO	**NRENS and Community**	**Suppliers and Third Parties**
k Operation	Board of Directors	Products, Services, Regulatory
	Owners of Project	
ble for		

RACI (responsible, accountable, consulted, informed)



Locations and high level interactions



Performance targets and primary KPIs

Security Drivers	Description of Attributes	Measurable Business Attributes	Policy Authority - Accountable Policy Owner	Recommended Measurement	Recommended Measurement Approach	Recommended Metric Type	Performance Target
23, 44	The solution must be cost-effective to ensure that it does not affect the budgets within the company and cost effective on maintenance.	Cost Effective	CFO	*Procurement method of 3 quotes * Benchmarking * Operational costs in 12 month period	* Procurement Method of 3 quotes *Within the range of acceptable budget Use *Operational Cost-effectivenes in the long run	Soft	Selection of most cost-effective solution that matches most of the bussiness attributes set
38	The solution should be uniformly used across the organization and its operations from all users.	Uniformed	CITO	All mail services using this solution	The solution to be working as inline technical control and being able to connect and cooperate with various mail services	Descriptive	Selection of the best value solution which can connect to various mail services and ensure efficiency of current and future requirements.

Identification of Assets

Information Assets	Office365
	Gmail
	sharepoint
	Internal SMTP servers for relay purposes

Services Layer

Security Drivers	Description of Attributes	Measurable Business Attributes	Logical Services	Physical Services	Component Services
18	The solution must have a mechanism to prevent sensitive information to be uncontrolled and it will not be easy for this information to leave the corporate environment except if special policies are set within the solution to permit this kind of communication	Containment	Security Policy Management	Data Content Monitoring and Filtering	DLP - Kaspersky (example)
				Realt-time system monitoring	DLP - Kaspersky (example)
			Audit Trails	Event Logs	Clearswift event log manager, Splunk (example)
				Event log integrity protection	
				Event log browsing tools	
				Event log analysis tools	
				Reporting tools	
			Security Service Management	Security service management sub-system	

Control Selection

Deparments Responsible to Mitigate Risk	CISO	CISO	CITO
Levels	**Policies Required**	**Policies Required**	**Policies Required**
Contextual	Enterprise Business Risk P	Enterprise Business Risk Policy	Enterprise Business Risk Policy
Conceptual	Information Security Polic	Information Security Policy	Information Risk
Logical	Continuity	Email Security Policy (Electonic	Information Classification Policy
Physical		Email Security Procedure	Information Handling Procedure
Component		Email Security Standards	Information Classification Standa
Operational		Email Security Guidelines	Information Classification Guidel
ISO 27001		PCI DSS	NIST 800-53
Too many control gaps			

KPI Measurements

Security Drivers	Description of Attributes	Measurable Business Attributes	Policy Authority - Accountable Policy Owner	Recommended Measurement	Recommended Measurement Approach	Recommended Metric Type	Performance Target	KPI	KPI Performance
26	The solution must be functional with all mail services used by the company and future services	Multi-functional Service	CITO	All mail services to be connected to the solution without issues	Mail services working with the solution	Soft	All mail services to be connected to the solution without restrictions	(#Mail services working with the solution/#of mail services of the company) * 100	green,amber,red
36	The solution must offer the capability for information to be retrieved and archived when needed to ensure business continuum and incident traceability. Information must be able to be recoverable by any future solution in place	Retrievable information	CITO	The solution to have the capabilities to archive any messages and back them up and be transferrable to any other solution selected in the future.	To ensure that the solution has backup/archiving/journaling capabilities that are common across industry and can be used across multiple solutions. Format of backup to be common across industry	Descriptive	Common backup/archiving/journaling format to be used across industry and journaling to be enforced	To ensure that the solution has backup/archiving/journaling capabilities that are common across industry and can be used across multiple solutions. Format of backup to be common across industry	green,amber,red

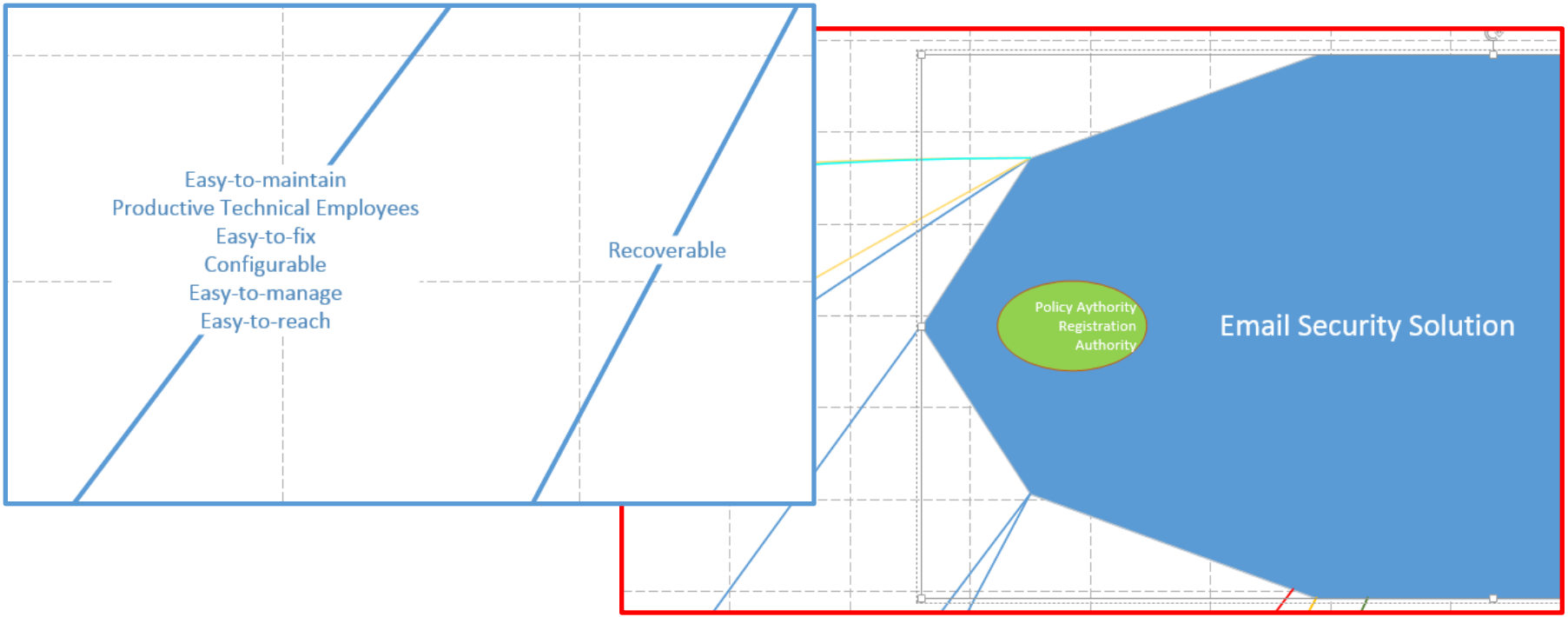
Attributes to Services

Security Drivers	Description of Attributes	Measurable Business Attributes	GÉANT Company Entity - Domain	Email Security Solution						
			GÉANT Company Domain - General controls	Applications	Middleware	Information	Data	Data Management	Platform	Network
39	The technology to be used by the organization must be widely adopted and proven solutions to be used for GÉANT purposes. This will ensure that are accepted by industry and governmental bodies and that is working to fit its purpose.	Reliable Technology	x	x	x			x	x	x
18	The solution must have a mechanism to prevent sensitive	Containment	x		x				x	x

Service Level Agreements and Operational Level Agreements

Party	CITO	CNOO	Trusted Parties	
SLA	-	-	GÉANT	
OLA	CNOO	CITO		

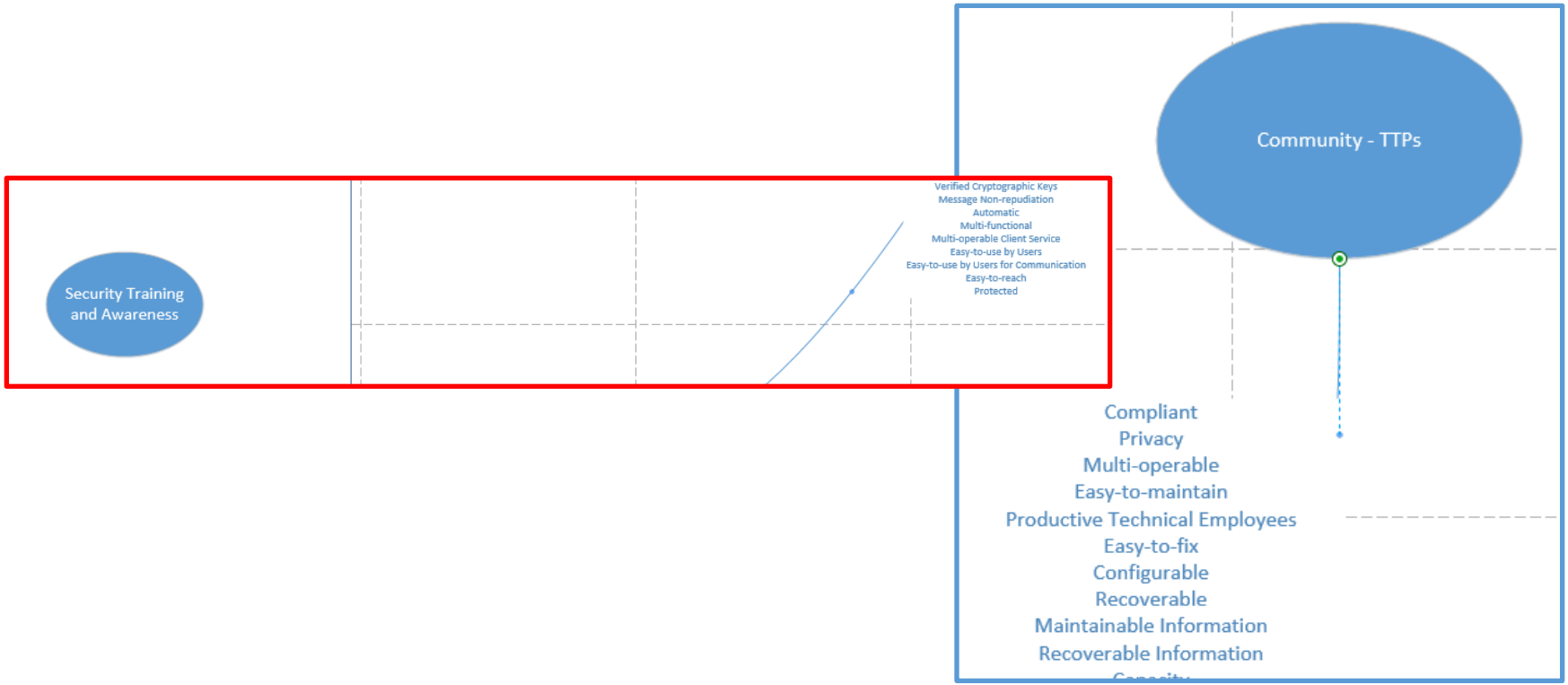
Trust Relationships



Inter and Intra Domain Relationships

			How the entity is passing through the logical services. End-to-end											
Security Drivers	Description of Attributes	Measurable Business Attributes	Logical Services	Physical Services	Component Services	GÉANT Company Entity - Domain			Email Security Solution					
						Entity e.g email client Note: not all controls easily applied to users and therefore the object is called Entitiy	Explicit Security Service for EMAIL CLIENT and Solution (Request from one domain to another e.g. API)	GÉANT Company Domain - General controls	Applications	Middleware	Implicit Security Service (Secure Domain from within. Usually use services from middleware)	Information	Data	Dat Mar
			Personnel Security	Disciplinary procedures				x						
			Environmental security	Air temperature and humidity controls				x						
				Electical power protection mechanisms				x						
17	The solution must be able to validate all keys held within the solution and protect them	Validation Cryptographic Keys	Key Management Process	Key management				x		x				
			Digital Management Process	Digital signatures management				x		x				
			data replication and backup	Regular backup copying				x		x		x	x	x
				Backup media management				x						

Service Sequencing – Modified

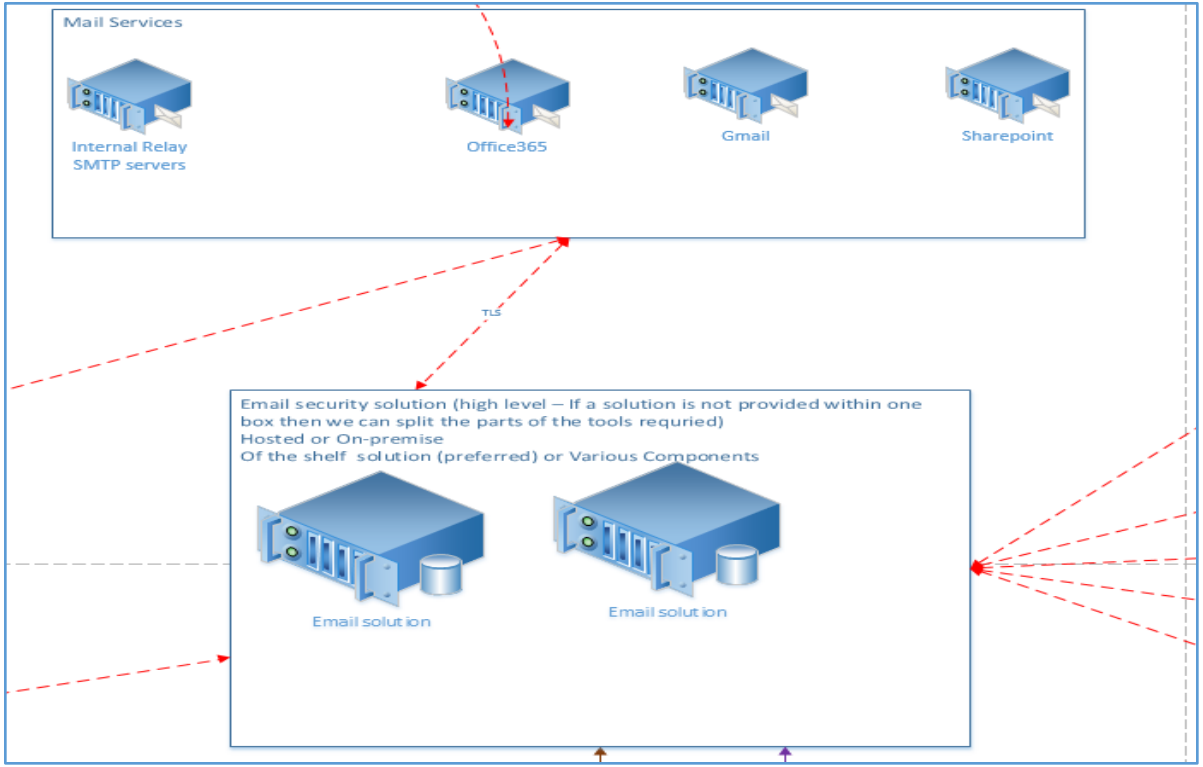


Evaluation and High level Diagrams

X where solution fits objective								COMBINED
Measurable Business Attributes	**Description of Attributes**	**Category**	**PGP Solution**	**RMS**	**EMAIL Security Gateway**			
Cost Effective	The solution must be cost-effective to ensure that it does not affect the budgets within the company and cost effective on maintenance.	Financial Efficiency	x	x	x			
Uniformed	The solution should be uniformly used across the organization and its operations from all users.	Financial Efficiency			x			

Evaluation and High level Diagrams (cont.)

We continue with this project so this is not the end of this exercise



Thank you

Questions

fotis.gagadis@geant.org

GÉANT

Networks · Services · People

www.geant.org