



TESTA NG

Testa new generation

Pieter.wellens@ec.europa.eu

**2nd International Conference on Cyber Crisis
Cooperation and Exercises, 23-24 Sept 2013,
Athens, Greece**

Agenda



- *Mission*
- *Challenges*
- *Experiences and concerns*
- *Collaborative process*
- *TESTA NG*

Mission

- *Facilitate cooperation between public administrations in various policy areas*
- *Consolidate existing networks by providing a secure, reliable and flexible communication service layer*

Mission

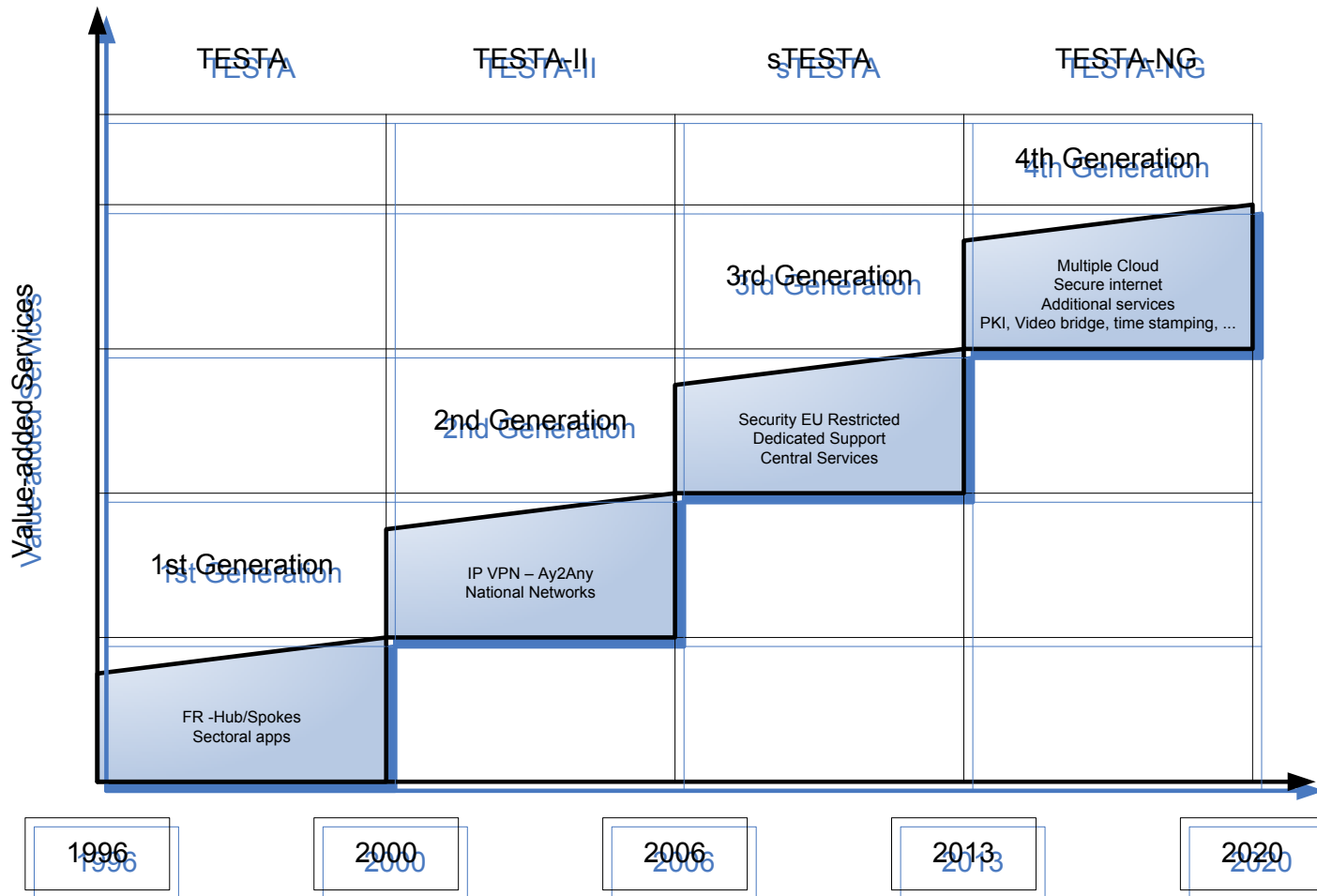
- *TESTA was born*

(Trans European Services for Telematics between Administrations) is a communication platform to exchange electronic data between European and Member States administrations in a secure, reliable and efficient way



European
Commission

Moving up the value chain



Challenges

- *EU is a mix of different cultures and a different country specific handling of information makes a common agreement on classification of information difficult*
- *Different security approaches in EU countries push at EU level to apply the most strict security measures*
- *Technical security implementations are often driven by political sensitivity and not by risk assessment and risk management*

Experiences and concerns

- *Security = End to end TRUST*
 - **By implementing measures and policies**
 - **By auditing**
 - **By having agreements**
 - Bilateral
 - Legal agreements
- *Concern of legal requirements with regard to the handling of EU Classified Information (EUCI) with Member States, Third countries and International organizations*

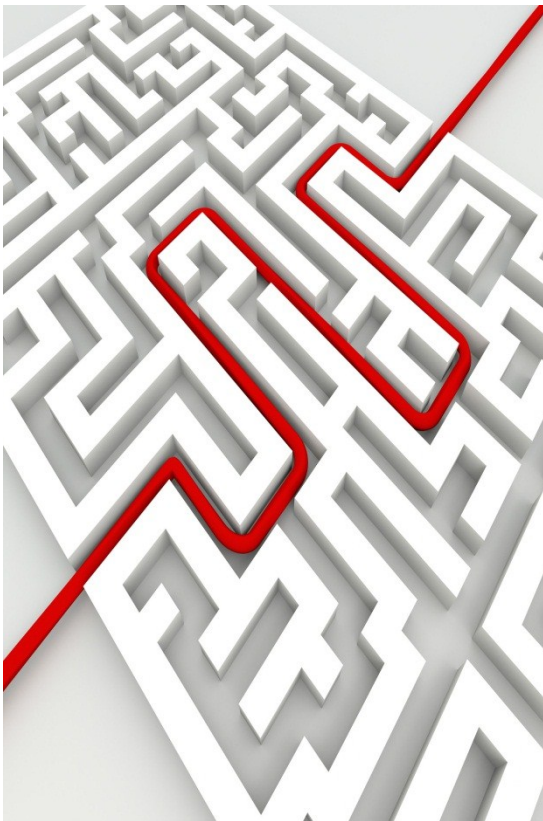
Experiences and concerns: Security accreditation

- **Step 1. Initial Demand**
 - TSO (Technical System Owner) sends a formal request to Commission SAA (Security Accreditation Authority)
 - Creation of SAP (Security Accreditation Panel)
- **Step 2. Pre-Certification**
 - TSO provides SSRS, SecOPs, Crypto documents (procedures) to SAP
 - Accreditation Panel approves SSRS
- **Step 3. Evaluation - Certification**
 - SAP assesses the conformity between deployed system and documents (SSRS, SecOPs, ...)
 - SAP produces statement of conformity (+ residual risks)
- **Step 4. Accreditation**
 - SAP takes decision on accreditation and informs Commission SAA
 - Commission SAA notifies the CSPAG (Commission security policy advisory Group)
- **Step 5. LDCP accreditation (statement of compliance by NSA)**



European
Commission

Experiences and concerns: Security accreditation



“Accrediting networks (or clouds) is neither necessary nor sufficient for the (obligatory) accreditation of the classified information system which uses such a network as transport layer”
(dixit HR/DS)

Experiences and concerns

- *Dedicated and/or public network?*
- *Availability*
 - **Today a public network like the Internet cannot give the contractual availability guarantee. Some applications like Schengen Information system require high availability. This results in commercial agreements and redundant infrastructure.**

Experiences and concerns

- *Dedicated and/or public network?*
- *Security*
 - **Although theoretically confidentiality and integrity can be achieved via the appropriate mechanisms over a public network, in practice application owners impose the implantation of private networks.**

TESTA NG: Collaborative process

- *TESTA is by concept based on a collaborative approach*
- *Consequences:*
 - **Agreements like MoU, Statement of compliance etc...**
 - **Setup of different working groups to prepare these documents (TESTA expert groups; Security Accreditation Panel)**
- *Difficulties:*
 - **Achieve common agreement on the content of the agreements**
 - **Signature at the same organisational level**
- *Lessons learned*
 - **To have clear policies and measures understood and accepted by everybody before proceeding**

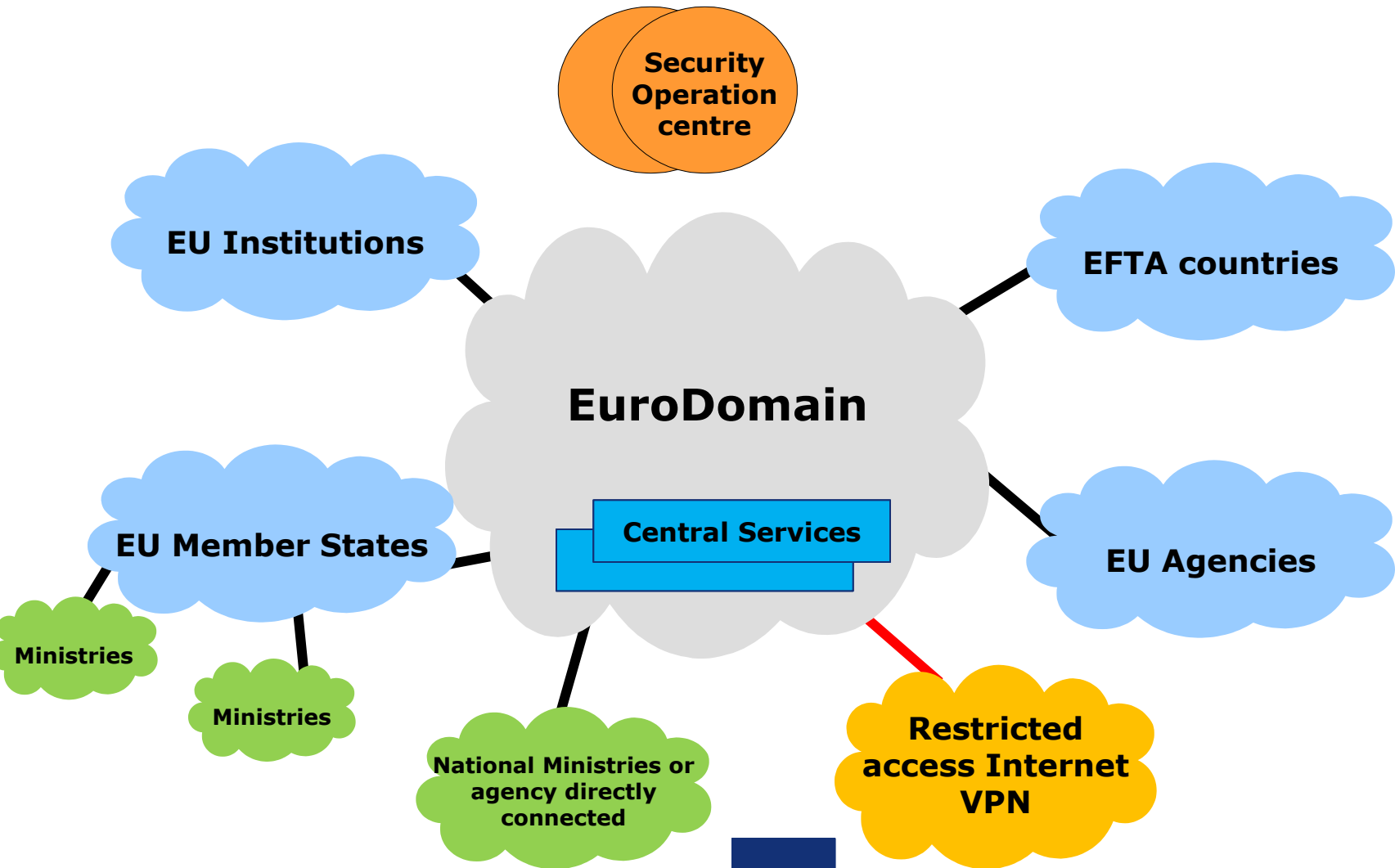
TESTA NG: Requirements survey

- *Information is requested to be protected from source to destination (End to End)*
- *From a security standpoint, the use of internet as an alternative transport network would be acceptable for a majority of the stakeholders.*
- *Data is often misclassified to be able to use sTESTA*
- *Additional security levels and services are highly desired. (security requirements in the future will be more stringent for some users).*
- *These additional security services should be on top of the current network security architecture.*
- *The usage of sTESTA is sometimes limited by the lack of common security policies and standards among countries.*

TESTA NG: Requirements survey

	Issues	%
Network	Bandwidth scalability to support network services	77
	Internet as transport	68
	Differentiated NW services	58
	Network consolidation	52
	Availability, bandwidth and latency	42
Security	Information protection E2E	71
	Additional security levels (Restricted, Confidential)	68
	Dedicated network security must be kept	55
	Additional security services (A2A)	52
	Encryption is sufficient to keep info confidential	32
Managment	Cost Sharing	39
	Cost reduction	19
	Vendor captivity	10
	Contract Clauses	3

TESTA NG: EuroDomain



TESTA NG: EuroDomain

- *Security based on risk assessment and management*
- *MPLS-based network*
- *Dedicated IP addressing*
- *IPSEC encryption*
- *Firewalling at all entry points*
- *IDS/IPS at all access points*
- *Dedicated security operations centre + Backup*
- *Dedicated central services domain + Backup*
 - **DNS, mail relay, PKI, collaboration tool, web server, ftp ...**
- *Tested BCP*



European
Commission

91 applications on EuroDomain

Criminal Records System

Prüm

CECIS

FIUnet

ECB

EURODAC

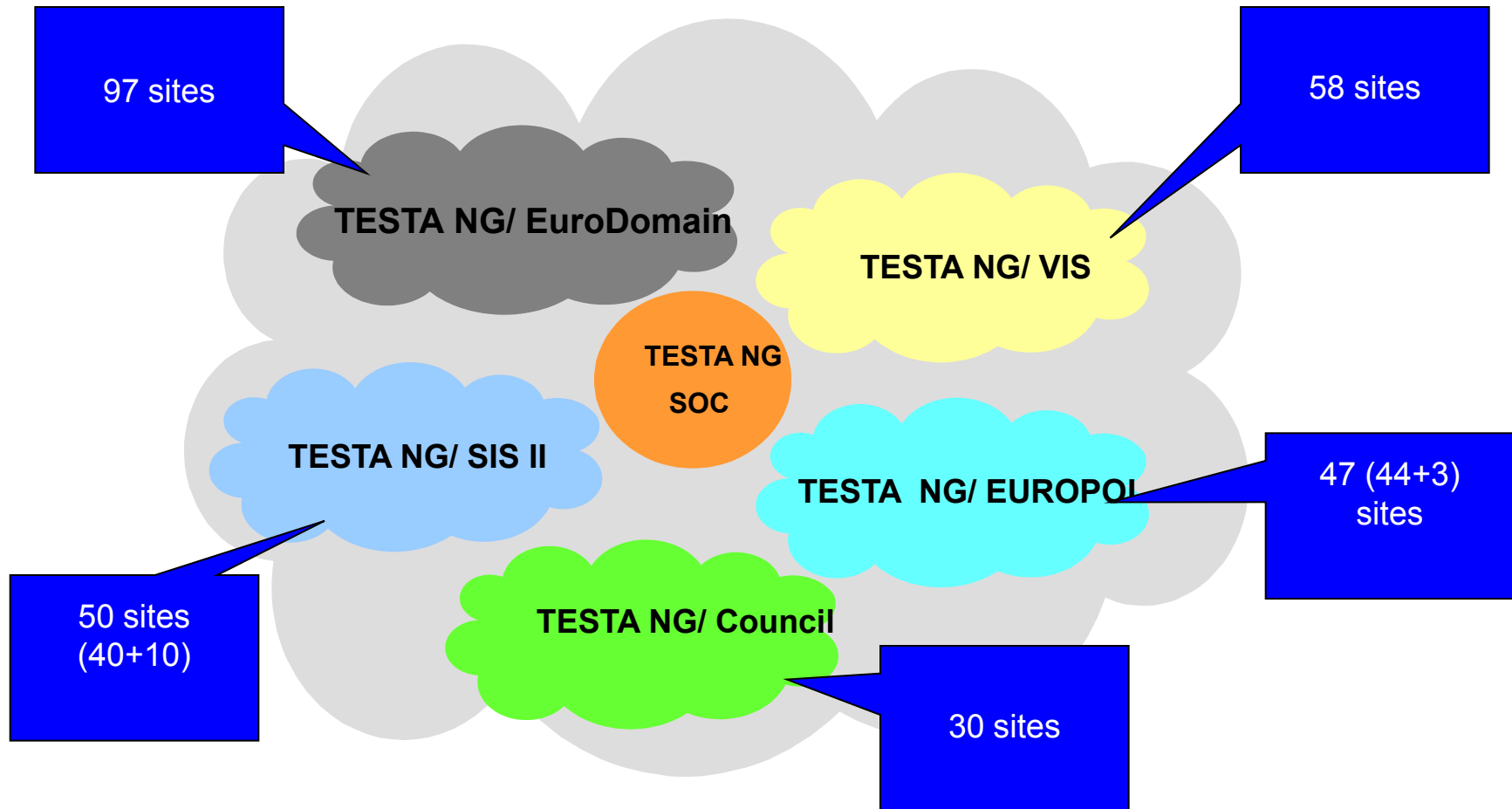
EESSI

SIGL

Tachonet

EURAMIS

TESTA NG: multiple clouds





European
Commission

Questions

Thank You!