EUROPEAN COMMISSION
DIRECTORATE-GENERAL INFORMATICS

Directorate DIGIT.D - Digital Services
DIGIT D3 – Trans-European Services

TESTA Overview & Service Catalogue

Doc. Ref. : TESTA Overview.doc
Owner : DIGIT Stakeholder Manager
Release Date : July 2018

Table of Contents

1. Intended Audience

This Service Catalogue describes the main aspects of the TESTA network.

It is intended for people already involved, and for people interested in TESTA. The audience is therefore:

- Application Developers
- Application Project Officers
- Network Coordinators
- Application Help Desks.

2. TESTA Environment

The objective of TESTA1 is to offer a managed, reliable and secure pan-European communication platform on top of which European and National administrations can build pan-European eGovernment services irrespective of the policy area in which they are involved. TESTA users can achieve great synergies, compared to the situation where each sector would have to set up and manage its own communication network infrastructure. One single network control and operation centre can manage the (virtual) networks used by the sectors and, where possible, physical network connections can be shared.

Because of the nature of some of these pan-European eGovernment services, this infrastructure must be able to transport classified information (up to the "RESTREINT UE" level).

The TESTA approach is collaborative. It builds on national efforts within the Member States to establish national networks interconnecting regional and local administrations. TESTA connects these national networks and allows administrations to exchange information with the European Institutions and/or with their peers in other Member States.

TESTA is the natural successor to the initial TESTA, TESTA II and sTESTA networks developed respectively under the IDA, IDABC, ISA and now ISA^2 Community programmes. The TESTA project is funded by the ISA^2 Community Programme managed by the European Commission Directorate-General for Informatics (DG DIGIT). The TESTA network infrastructure interconnects all EU Institutions, EU Agencies, Member States' Administrations and European Economic Area (EEA) countries.

ISA^2 stands for Interoperability Solutions for European Public Administration. ISA aims to foster interoperability between public administrations by helping to establish common approaches that will make collaboration a lot easier. Sharing and reusing tools such as common platforms and common components, along with the sharing of services like common infrastructures, will also play a part by keeping costs down and reducing time to market.

[1] TESTA: Trans-European Services for Telematics between Administrations.

2.1 When to use TESTA

TESTA is the preferred solution for pan-European information exchange between administrations requiring guaranteed service levels for network availability, performance and/or security. The TESTA infrastructure has been built to be subject to a security accreditation process to allow the exchange of EU classified information up to the "RESTREINT UE" level.

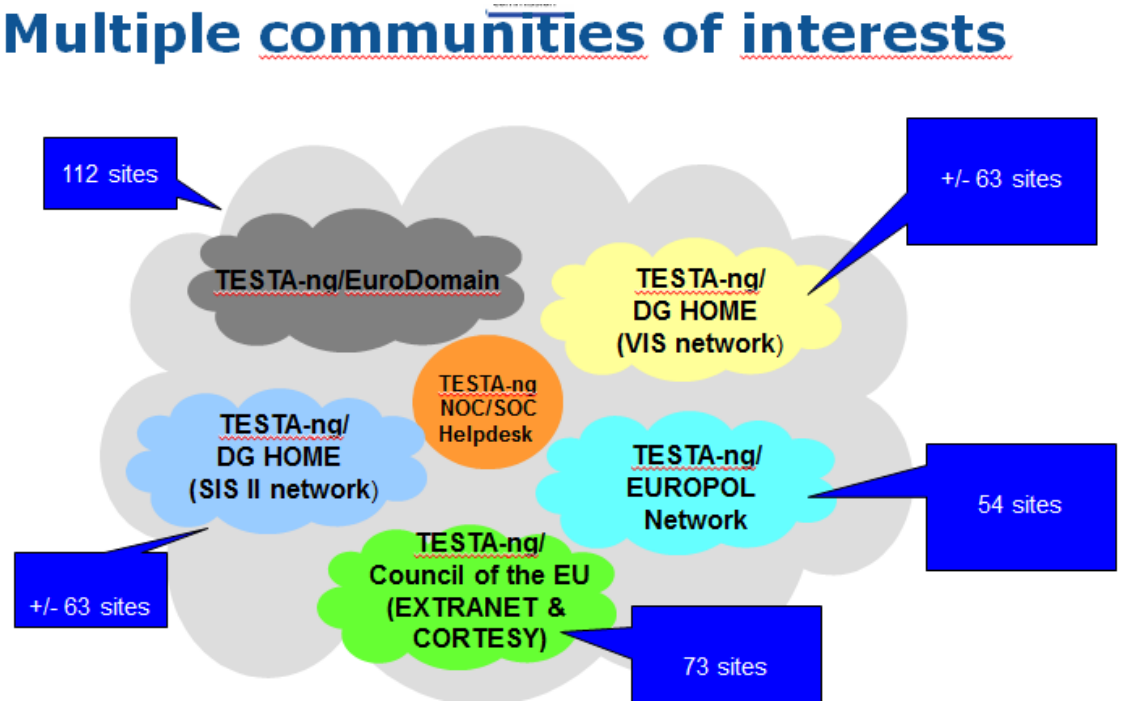
Information systems requiring less stringent service or security levels should consider other communications solutions such as the Internet. The technical and security requirements inherent in a highly secured infrastructure like TESTA might prove too heavy and ultimately be counterproductive for less demanding information systems.

It is up to each policy sector to analyse in advance the requirements of its information system and the required level of security of the data to be exchanged. Therefore, a risk analysis should be made. Policy sectors are invited to involve the TESTA Project Officer in the early stages of such a process.

2.2 Who is connected today?

Currently TESTA allows interconnection and provides services to a wide number of registered applications and stakeholders including Member States' Administrations, European Institutions and European Agencies. Some European countries not currently part of the European Union are also connected. TESTA is also used in the context of non-Community projects by Member State Administrations or bodies/organisations acting on their behalf.

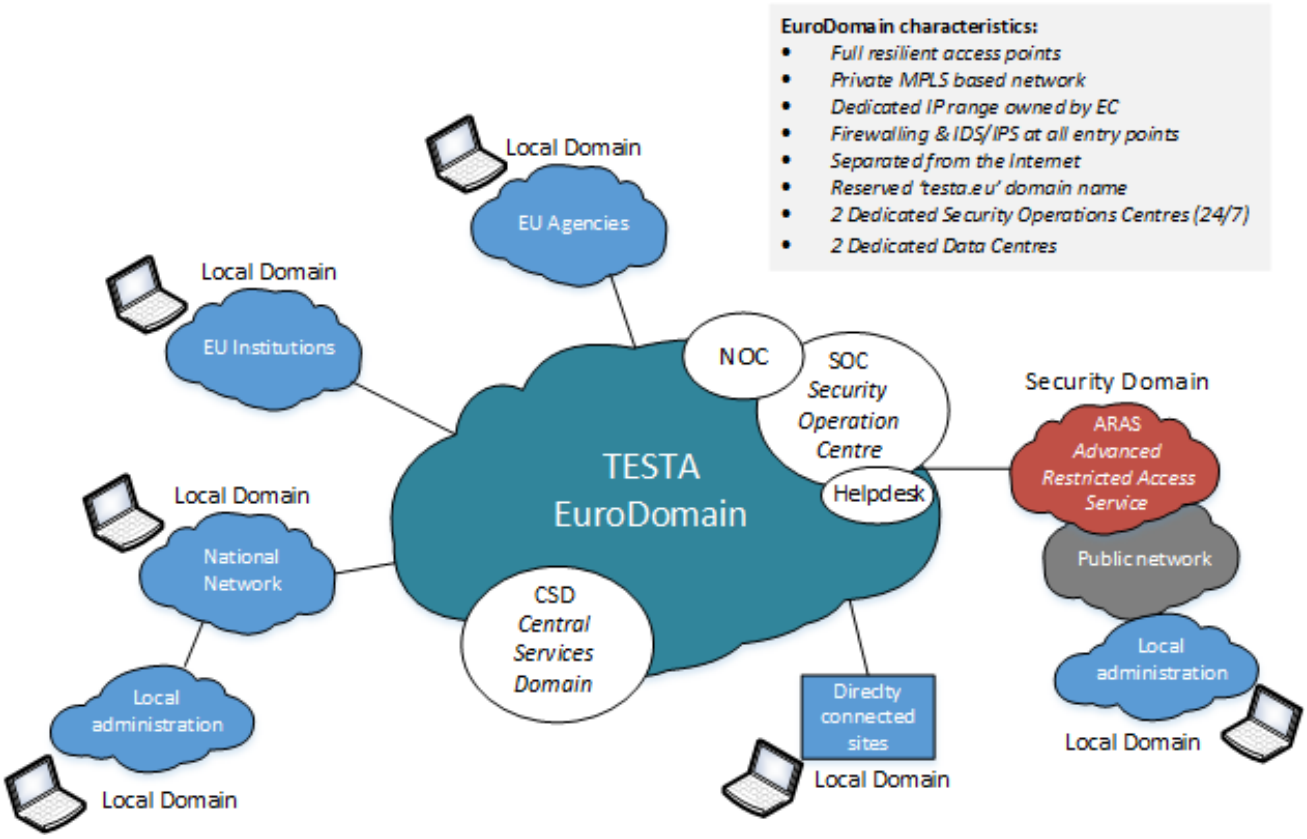
Moreover, the TESTA Framework is extensively used by the EU Commission DG HOME for the implementation of the VIS and SIS II networks, the Council of the European Union and by EUROPOL for the implementation of their own dedicated EUROPOL network.



3. TESTA Services

3.1 Architecture of TESTA

TESTA building blocks are shown in the figure below and are described in more detail in the following sections.



3.1.1 EuroDomain

The EuroDomain is central TESTA building block that allows data transfer and services between TESTA stakeholders such as the European Commission, various European Agencies, other European Institutions, Member States' administrations, the Security Operation Centre (SOC) and the Central Services Domain (CSD). All connections to the EuroDomain are encrypted using certified IPSec technology.

3.1.2 Local Domain

The Local Domains are the domains related to the end-user. They are all specific and are typically based on various LAN architectures and vary from one Local Domain to another. The EuroDomain interconnects various Local Domains and provides them with central services via the Central Service Domain.

A Local Domain can either be directly connected to the EuroDomain via a TAP (Turnkey Access Point) located in its LDCP (Local Domain Connection Point) or be interconnected via another network (e.g. a national network) which eventually hosts the TAP in its LDCP.

3.1.3 Central Service Domain (CSD)

The Central Service Domain (CSD) provides facilities for EU users to exchange data. It contains dedicated services such as DNS, (secured) Mail, (secured) FTP, NTP, Time stamping and Web services (web portal, web cooperation services).

The portal provides access to

- the end-users and administrations by offering a view of the set of services that are accessible over TESTA and give information on how to obtain these services;
- the sectoral managers, so they can disseminate information on the sectorial applications for which they are responsible;
- the network managers and administrators by providing a place where all technical and administrative information concerning the configuration and the performance of the network can be retrieved and managed.

3.1.4 Network Operation Centre (NOC)

The Network Operation Centre will operate the provision of network transport (Backbone services, local loop services and the monitoring thereof).

The NOC is available on a 24/7 basis, 365 days a year.

3.1.5 Security Operation Centre (SOC)

The SOC manages the services that are dedicated to TESTA. These include: crypto management, firewall management, management of all the services that are protected by the TESTA security environment e.g. Mail relay, secured mail, secured FTP, NTP, DNS, web portal, web cooperation tool, Advanced Restricted Access VPN management.

The management infrastructure of the SOC is dedicated to TESTA and is responsible for ensuring quality and operational support for the TESTA EuroDomain Services.

The personnel assigned to operate these dedicated services have a minimum security clearance of National Confidential.

3.1.6 Helpdesk services

The helpdesk is acting as a single point of access that registers and coordinates all incidents problems and requests coming from authorised users (helpdesk, support teams of the connected local domains or helpdesks of application owners).

The Helpdesk is available on a 24/7 basis, 365 days a year and registers requests via telephone, mail and web portal.

The personnel assigned to operate the helpdesk have a minimum security clearance of National Confidential.

3.2 Quality

The quality of the TESTA services is guaranteed via Service Level Agreements. The quality indicators defined in the service level agreement (SLA) are measured and computed periodically.

Service levels are contractually guaranteed and backed up by liquidated damages. The following is an excerpt from the guarantees applied to TESTA services.

a. "Adherence to Requirements" (SQI_ATR) = shows the TESTA requirements implementation rate and it measures how close the accepted TESTA is from the initial TESTA.

b. "Adherence to the planning SLA" (SQI_ATP) = measure the slippage of the duration of a Work Package compared with the duration initially planned and agreed.

c. Service Support Indicators

   i. SQI_RTSx (with x = 1, 2, 3 and 5) = to measure the average of the delay in the response time for Px incidents.

   ii. SQI_SRT - to calculate the average slippage by the SOC staff when it has to disseminate security patches / releases into TESTA production environment.

   iii. SQI_SCU = to measures the average slippage in installing new security configurations.

   iv. SQI_RCTx (with x = 1, 2, 3 and 5) = to measure the average time to close Priority x Problems.

   v. SQI_CITx (with x = 1, 2, 3 and 5) = to measure the average time to implement Priority x RfCs (once approved by the authorized parties).

d. "Availability of the services SLA" (SQI_xxxA)

   o SQI_xxxA where xxx is the Acronym of the Service (FTP, NTP, SMTP, DNS, WP, etc) = to measure the availability of the Services to the user. Whereas the limit is 99.85% (= more or less one hour per month).

e. "Network Performance Indicator (NPI)" (SQI_NPI).

f. "Quality of Classes of Services".

   o SQI_QoS_RTDx,SQI_QoS_PLx, SQI_QoS_JitRT Where x maybe „1", "2", "RT" or „APP" (proposed Classes of Service) to measure the TESTA End to End traffic quality of the related Class of Service based on IPSLA/RPM.

Full information regarding the SLAs can be made available upon request by the TESTA Project Officer.

3.3 Security

The security of TESTA is ensured at multiple levels in order to prevent unauthorized people or applications from accessing specific or sensitive applications or services, and from reading, modifying and/or deleting critical and/or sensitive data.

TESTA security is based on the End to end TRUST by

- implementing measures and policies;
- auditing;
- having agreements (Bilateral & Legal agreements).

It also follows the following principles:

- Integrity of data and IT systems;
- Confidentiality of data;
- Authentication of people, IT systems and applications;
- Availability of data and IT systems.

In addition to firewalls and encryption devices, IT applications using TESTA services may have their own security requirements covering access control and data sensitivity levels. Each administration will seek accreditation for its LDCP.

If so needed, it can ask the representative of the National Security Agency (NSA) concerned, or the TESTA Security Officer, about the procedure to be followed.

It is to be noted that the Commission implemented the TESTA-ng secured infrastructure for the exchange of non-classified information. The implementation of the classified network to exchange classified information “RESTREINT UE” according to article 2 of the Council Decision 2001/264/EC of 19 March 2001 adopting the Council’s security regulations as last amended by Commission Decision 2005/952/EC is not covered by the current TESTA-ng implementation.

3.4 Reliability

The reliability of the TESTA network is achieved through the use of reliable, state of the art system components with certified encryption. In addition, single points of failure are avoided:

- At the TAP, by using redundant network components at all levels. Well known redundancy protocols allow a resilient interconnection with the local domain network.
- In the local loop, by allowing the use of a standby local loop from a different provider.
- In the EuroDomain through the use of a reliable and redundant MPLS network from a single, well known provider.
- In the Central Service Domain through load balancing technology and well known resiliency protocols for mail and domain name services.
- At the EC main application sites in Brussels and Luxembourg by taking advantage of the internal EC network as an additional resilient interconnection.

3.5 Assistance services

Upon request, the European Commission may provide the following assistance though its Assistance Services contractor to the Local Domain Administrations and/or the providers of IT applications using the TESTA network in order to facilitate the integration of networks or IT applications in the TESTA environment. Assistance services may consists of :

- Quality audits,
- Security risk analysis and security audits,
- Technical consultancy and assistance such as e.g.:
    - Drafting of documents on operational procedures and guidelines in the field of security, quality assurance or support for Local Domain Administrations and IT application provider;
    - Drafting of documents on network and security requirements for the integration of IT applications in TESTA;
    - Assistance in the planning and follow-up of Local Domain network implementations and the integration in the TESTA network;
    - Etc.

4. Practical information about TESTA

4.1 Roles and responsibilities

4.1.1 The European Commission

DG DIGIT is the technical system owner for TESTA. It is responsible for the EuroDomain, including its Central Services and the Security Operation Centre (SOC).

4.1.2 Member States – National Coordinators

The National TESTA coordinators are nominated by the Member States. Their responsibility is to coordinate all activities with regard to the connection and the integration of TESTA in their network. This also includes coordination with directly connected national administrations within their Member State.

4.1.3 European Agencies and other European Institutions

European Agencies and Institutions are part of the TESTA community.

4.1.4 Sector Project Officer

The Sector Project Officer has specific responsibility for the management of the one or more application(s) running over TESTA.

4.1.5 Sector Application User

The Sector Application User is the end-user of an application running over TESTA.

4.1.6 TESTA Network Services Contractor

The TESTA Service Contractor is currently T-Systems GmBH and is responsible for the provision of the TESTA network communication platform and services.

4.1.7 TESTA Assistance Service Contractor

The TESTA Assistance Service Contractor is contracted via the DESIS Framework Contract awarded by the European Commission. It provides quality auditing covering security and service to the other TESTA stakeholders. It also assists the EC with quality levels, and security measures are provided.

4.2 Who can apply for TESTA services?

TESTA is an efficient, secure and reliable trans-European communication platform for the interchange of data between public administrations. TESTA is based on a dedicated and private infrastructure, available to all National and European administrations in order to exchange up to sensitive information and requiring guaranteed availability and performance service levels.

TESTA is a generic service provided under the ISA^2 Programme. Eligibility for TESTA services is governed by the ISA^2 Decisions outlining Community activities in the field of trans-European telematic networks for administrations.

Potential beneficiaries are:

- European Institutions;
- European Agencies;
- Member States and candidate countries, EEA countries;
- national or European public administrations (including European Union institutions and agencies);
- any other national, regional or local public body or office and;
- any international organization;
- any other institution, agency or body that will be created on the basis of the Treaties or secondary Union law within the duration of the contract.

The procedure for getting TESTA services is the following:

- Clarification of requirements
- Application for TESTA services
- Agreement on implementation proposal
- Implementation proposal
- Installation
- Quality review.

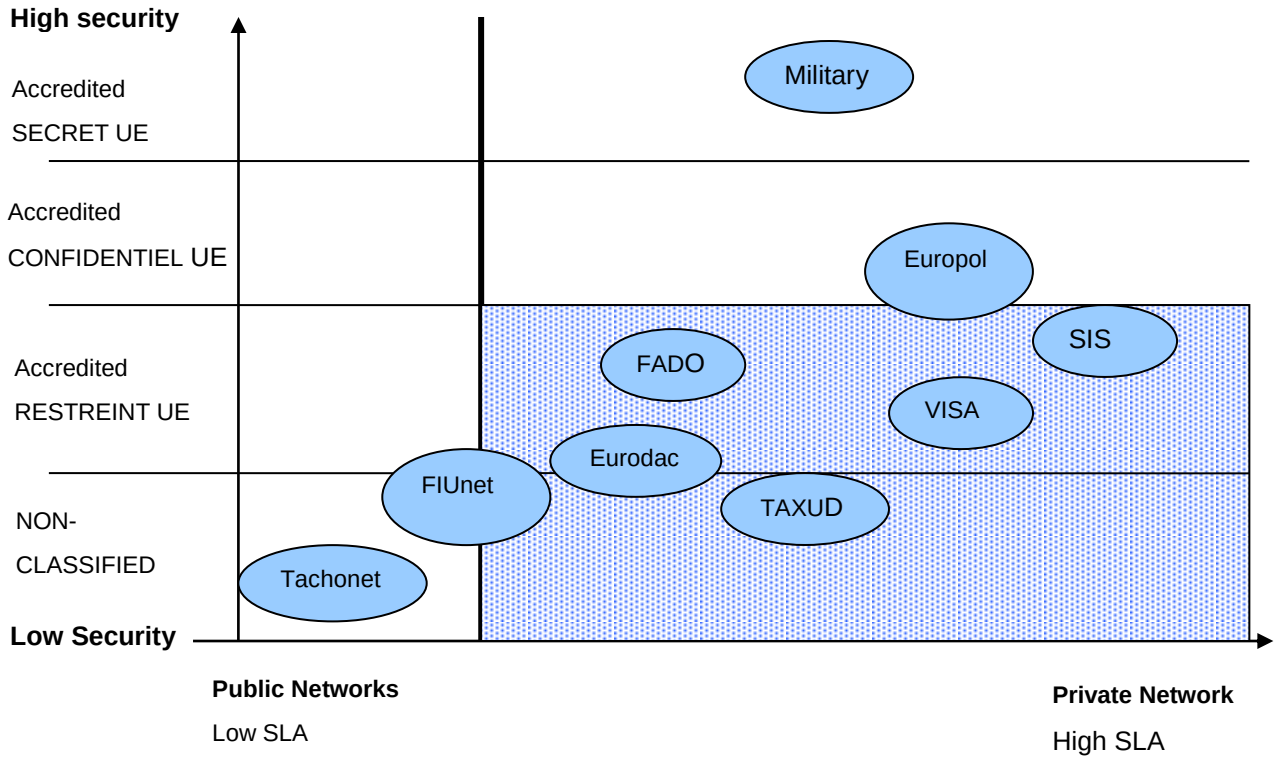
The following chapters provide some details of each these steps. If needed the TESTA Project Officer can be contacted for further information.

4.3 How to use TESTA Services?

4.3.1 Clarification of requirements

Administrations should start by clearly defining their needs for TESTA Services, basically why and what services are needed. TESTA is focusing on users that have high security and/or availability requirements. Information systems requiring less stringent service or security levels should consider other communication solutions such as the Internet.

Based on the picture below, administrations or policy sector manager should determine where to position their own application:



It is up to each policy sector to analyse the requirements of its information system and the required level of security of the data to be exchanged. The analyses should be supplemented by a risk analysis in order to make the best decision with regard to the communication solution to be deployed. Policy sectors are invited to involve the TESTA project officer for advice in the early stages of such process.

A pre-requisite for using TESTA Services for all the administrations joining the TESTA network is to agree on a Memorandum of Understanding (MoU) regarding the quality of services and security. This is necessary in order to guarantee the same overall service level between the administrations.

If the minimum quality and security requirements for TESTA are not reached, the administration cannot join the network.

ISA[2], after consulting all relevant Community services, may also refuse the use of TESTA to projects that are not in line with TESTA scope.

4.3.2 Applying for TESTA Services

After clarifying their requirements, interested parties should inform the TESTA Project Officer of their interest.

Applications will typically come from a user community engaged in a particular policy area. Demands for connections from individual administrations should be justified in terms of these administrations' business requirements.

The applicant should provide the following information:

- Information on the site/administration that wishes to be connected (name, location, coordinates of local contacts, Information about the legal basis of their communication requirements);
- Type of TESTA access requested:
    - available TESTA services
    - existing application running on TESTA
    - new application
    - sectoral or non-Community project
    - client location and access (via national TESTA connection or a direct link);
- Description of the services requested and SLA requirements;
- Brief description of their communication requirements: with what sites they need to communicate with expected traffic load;
- Information security classification;
- Where a request is submitted on behalf of others, proof of the other administrations' interest (for example minutes of a meeting where this was decided);
- Contact information for the Project Coordinator.

On the basis of this information, the Commission Project Officer (and potentially ISA[2] if so needed) will check eligibility and then consult national network coordinators on implementation options. In most cases, access can be configured via the National Network. In cooperation with the Commission Project Officer, the National TESTA coordinator will decide whether or not a direct connection is required.

Preference will be given to establishing connections through national administrative networks. Direct links to TESTA need to be funded by the concerned administration.

4.3.3 Implementation proposal

Once the application has been approved, the project coordinator is requested to provide some further information necessary for implementation, such as technical details. Applicants will also be requested to fill in a site survey and sign the MoU if they have not already done so.

The project coordinator will receive an implementation proposal after all the required information has been submitted.

4.3.4 Installation

At the same time that the implementation proposal is sent, the installation request is sent to the TESTA Services Contractor. The implementation proposal is reviewed by the contractor and the installation (implementation) of applied TESTA access is started in close cooperation with the site.

4.3.5 Quality review

After a pre-defined period a post-installation review will be done with the site and the project coordinator from the TESTA Services Contractor to ensure that all the requirements have been fulfilled.

4.4 Which applications can use TESTA

The TESTA infrastructure is built for communication between public administrations. Connections for businesses and citizens are not envisaged.

TESTA has been designed to support the needs for a whole range of application architectures relying on protocols such as HTTP, HTTPS, FTP and SMTP.

Applications may require interaction with web sites, involve the transfer of information between servers and clients or the exchange of messages in real time.

Member States' stakeholders actively sponsor the TESTA network amongst their national administrations, which allows TESTA to rely on an increasing number of new sectoral applications – we count more than 90 applications using TESTA today.

To illustrate these capabilities, some examples of information systems supporting the implementation of Community policies are presented below:

EUCARIS: *"EUCARIS, the EUropean CAR and driving license Information System, is a system that connects countries to enable them to share vehicle and driving license information and other transport related data. EUCARIS is merely an exchange mechanism that connects the Vehicle and Driving License Registration Authorities in Europe and has no database of its own. It is developed by and for governmental authorities and supports:*

- *the exchange of vehicle data and the fight against car theft and registration fraud at re-registration of cars after import;*
- *the fight against crime and terrorism based on Council Decisions 2008/615/JHA and 2008/616/JHA;*
- *the exchange of driving license Information within the EU system RESPER;*
- *the exchange of owner/holder data for the enforcement of road-safety related traffic offences (CBE).*

Currently all EU and EFTA Member States are connected to EUCARIS and exchange an estimated 50 million messages per year. As from 2007, all data exchange is over the closed TESTA network, guaranteeing a high level of security on top of the XML-signing offered by the EUCARIS system, which is essential as sensitive data are exchanged. TESTA has proven to be highly reliable and to deal with our load without any problems. Next steps we consider, are the TESTA PKI and DNS services, to further enhance our service level."

Herman Grooters, Manager Operations EUCARIS, on behalf of the Netherlands Vehicle Authority (RDW)
eucaris2help@rdw.nl

ECRIS: *"The European Criminal Record Information System (ECRIS) was established in 2012 to facilitate the exchange of information on criminal records throughout the European Union. It enables the electronic interconnections between EU countries and puts rules into place to ensure that information on convictions contained in the national criminal records systems can be exchanged through an electronic standardised format, in a uniform and speedy way, and within short legal deadlines. Currently all EU countries are connected to the ECRIS and the exchanges reached in 2016 around the 2 million messages over the TESTA network. The ECRIS users are also using the secured TESTA FTP service which was recently migrated to TESTA-next generation."*

Jaime Lopez Loosvelt,General Criminal Law Unit, DG Justice and Consumers, European Commission
JUST-CRIMINAL-RECORD@ec.europa.eu

DG TRADE: *"Dual use Items are goods and technologies that can be used for both civilian and military applications and/or can contribute to the proliferation of Weapons of Mass Destruction (WMD). The trade of such items is subject to controls to prevent the inherent risks they may represent to international security. The controls derive from international obligations (in particular UN Security Council Resolution 1540, the Chemical Weapons Convention and the Biological Weapons Convention) and are in line with commitments agreed upon in multilateral export control regimes.*

The Dual Use System (DUES) offered by the Commission is used by all the Member States in order to share information on Dual Use export transactions and enforce the controls at European level. The information available in the DUES system is highly sensitive, this is why all DUES communications are exchanged over the secured TESTA network thereby ensuring the appropriate level of data confidentiality and integrity.

Thanks to the DUES system and TESTA network, the EU is able to control the export, transit and brokering of dual-use items and are both key instruments in contributing towards international peace and security."

Jean-Marc Reynders,Information Technology and IT systems Unit, DG TRADE,European Commission
TRADE-SERVICE-DESK@ec.europa.eu

European Union Intellectual Property Office: *"For us, TESTA is the vehicle to communicate digitally among the EU agencies and with the EU institutions. Typically we are in contact with our parent DG and other EU agencies in our policy areas, as well as Member States. Because we are decentralized and because we now live in a digital world, for us telecommunications are very important. So being able to communicate electronically in a safe way is even more important for us. TESTA is the network we use and we are very happy with the completeness of our stakeholders linked to the network, the fact that it is secure and the fact that is has a good track record of availability."*

Diego Eguidazu, Deputy Director for ICT Services, Digital Transformation Department, Diego.Eguidazu@euipo.europa.eu

"The future needs reliable and secure electronic communication between the public administration of the Member States. TESTA is THE solution for Germany."
Constanze Bürger, IT and Network Infrastructures in the public administration, Federal Ministry of the Interior of Germany
Constanze.buerger@bmi.bund.de

AGID Italy: *"We are managing the IT connection to TESTA since 15 years at the Agenzia per l'Italia Digitale. All national Italian public administration is connected to the National Public Administration's Network (the so called SPC network) and the SPC network itself is connected to TESTA. Through TESTA we have one single point of interconnection by which we are able to deliver services to Italian Public administration. Our administrations are very satisfied with the services provided by TESTA."*

Marino Di Nillo, Soluzioni per la Pubblica Amministrazione
dinillo@agid.gov.it

Swedish Civil Contingencies Agency, Sweden: *"I can definitely recommend TESTA. For me, this is the only connection point towards other European agencies because it meets the standard of security, encryption and resilience."*

Anders Hagland, Service Owner
Anders.hagland@msb.se

SE "Infostruktūra", Lithuania: *"We have connected some 19 national administrations, departments and services to TESTA so far, among other the police department and the social security service. The last service we managed to connect in 1,5 hours only. TESTA made our life definitively easier. The network is causing neither problems nor delays, with the connected services running correctly. What can you expect more?"*

Algimantas Inčius, Acting Managing Director SE "Infostruktūra", Secure State Data Communication Network (SSDCN) operator
Algimantas.incius@is.lt

FIU.NET - a decentralised computer network

Designed to connect EU Financial Intelligence Units - FIUs, using modern technology and computers to bilaterally exchange financial intelligence information.

DUBLINET – e-mail exchange system

Based on the COMMISSION REGULATION (EC) No 604/2013, laying down detailed rules for establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national.

The secure electronic means of transmission referred to in Article 18 of Regulation (EC) No 1560/2003 shall be known as 'DubliNet'. Exchange of asylum seekers data between Dublin Member States in a secured way.

TESS – Telematic for Social Security, a system using FTP

TESS is a European project to speed up and simplify administrative procedures in order to improve the acquisition of entitlement and the granting and payment of social security benefits to migrant workers and other persons who have exercised their right of free movement.

The application uses two dedicated ftp servers hosted on the TESTA Central Platform to store and fetch documents between Healthcare and Pension Administrations of Member States.

TESS is expected to be replaced by the currently under development / implementation system: EESSI (Electronic Exchange of Social Security Information) in a transition phase 2017-2019.

4.5 Costs

TESTA costs are related to the setting-up, operation and maintenance of the network and the use of TESTA services.

The European Commission (DG DIGIT) is accountable to TESTA users for the TESTA network, specifically the EuroDomain and Central Service Domain (CSD).

The Member States Administrations, European Agencies and EC DGs that own applications running over TESTA are responsible for the operation and maintenance of:

- networks within their own Local Domains;
- applications using the TESTA network and services.

The specific costs of accessing TESTA should be discussed on a case by case basis.

The fixed costs of one national LDCP connection are paid for by the Commission. Any other direct connection costs are paid for by its users.

The standard bandwidth provided to TESTA users is 10 Megabits/s. Higher bandwidth can be made available as well upon justification.

Annex VI to the Memorandum of Understanding covers the principles applied to the use of TESTA by non-Community projects, including the need for a financial contribution and the corresponding fee. A non-Community project is a project leading to information exchanges between administrations or to eGovernment services at a European level but whose legal basis is not or not directly deriving from a Community legal act.

4.5.1 Contractual costs

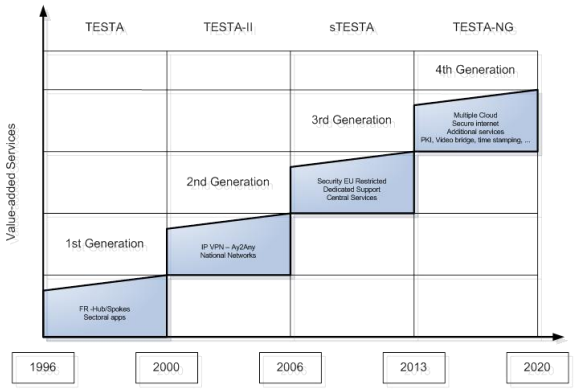
A pre-requisite of using TESTA Services for all administrations joining the TESTA network is to agree on a Memorandum of Understanding (MoU) on the quality of services. This is necessary to guarantee the same overall service level between administrations.

DG DIGIT remains the technical system owner of the TESTA communication platform and manages the Framework contract and the Eurodomain Specific Contract(s).

The TESTA service provision contract is of pre-defined and limited length. The services of TESTA are intended to continue in the future and migration from one network to another is carefully planned to go smoothly.

The contractual advantage of TESTA for the administrations is that the contractual arrangements are regulated centrally.

TESTA is in constantly developing and changing.


TESTA
TESTA-II
sTESTA
TESTA-NG
4th Generation
3rd Generation
Multiple Cloud
Secure internet
Additional services
PKI, Video bridge, time stamping, ...
2nd Generation
Security EU Restricted
Dedicated Support
Central Services
1st Generation
IP VPN – Ay2Any
National Networks
FR -Hub/Spokes
Sectoral apps
Value-added Services
1996
2000
2006
2013
2020

4.6 TESTA Information Dissemination Points

4.6.1 All parties

The following TESTA Information Dissemination Points are available to all TESTA stakeholders:

- ISA^2 Team:
  Email: ISA2@ec.europa.eu
  ISA^2 web site: http://ec.europa.eu/isa/ready-to-use-solutions/isa2/stesta_en.htm
- TESTA Head of Section and Security Officer in the Commission:
  Contact: Philippe Schultz
  Email: Philippe.Schultz@ec.europa.eu
- TESTA Programme Officer (PO) in the Commission:
  Contact: Aldo Grech
  Email: Aldo.Grech@ec.europa.eu
- TESTA Stakeholders manager:
  Contact: Sophie Devleeschouwer
  Email: sophie.devleeschouwer@ext.ec.europa.eu

  Email: DIGIT TESTA
  DIGIT-TESTA@ec.europa.eu

4.6.2 TESTA users

- TESTA portal
  Accessible only to those who already have an TESTA connection
  Site address: https://demo.portal.testa.eu/Pages/default.aspx
- TESTA SOC Helpdesk
  Accessible 24/7 only to authorized persons in English via phone, mail and Web Portal.
  Only issues concerning the EuroDomain, interconnections with the Local Domain or the Domain of another competent administration may be addressed to the TESTA SOC Helpdesk.
  Email: TESTAng.soc@t-systems.sk

  Phone: +49 69/426 965 3027.
- CircaBC
  Accessible only to authorized persons.
  Site address: https://circabc.europa.eu/faces/jsp/extension/wai/navigation/container.jsp

5. Acronyms

CMT	Core Management Team
CSD	Central Service Domain
EU	European Union
FTP	File Transfer Protocol
IDA(BC)	Interoperable Delivery of European eGovernment Services to Public Administrations (Business and Citizens)
ISA(2)	Interoperability Solutions for European Public Administrations
LAN	Local Area Network
LDCP	Local Domain Connection Point
Mbps	Mega bit per second
MoU	Memorandum of Understanding
MPLS	Multi-Protocol Label Switching
NSA	National Security Agency
TAP	Turnkey Acces Point
SLA	Service-Level Agreement
SOC	Security Operation Centre
TESTA	Trans-European Services for Telematics between Administrations