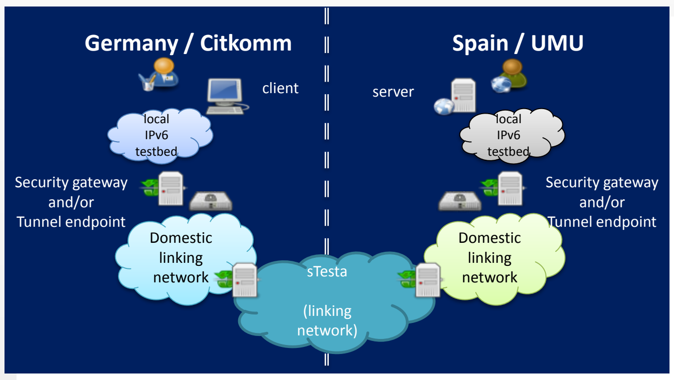
Where To Start From

The current situation in cross border eGov:

- Citizens connect to government services through the public Internet, provided by a number of local ISPs. Conversely, connection between administrations is often performed through private administrative networks, run by the government, to ensure security and privacy.
- Some member states have interconnected these private administrative networks through an international administrative network called sTESTA, enabling some of their eGov services for cross-border access.
- However, many of these networks (either public or private) are not ready for the use of IPv6 nowadays. Instead, they provide IPv4-only equipment that hinder a seamless transition to IPv6.
- Security and authentication are a major issue for cross-border eGovernment.

USE CASES

GEN6 evaluates authentication and secure communication based on the use case of cooperationg public workers. These scenarios make use of STORK for authentication and direct communication through government networks



ABOUT GEN6

This work was in part supported by the European Commission as part of the project »Governments Enabled with IPv6« (GEN6). GEN6 is about stimulating EU-wide deployment of IPv6 by means of best practices and guidelines. This work supports:

- national pilots to make a step further in IPv6 deployment in different sectors,
- cross-border pilots to demonstrate EU-wide interoperability of IPv6,
- communication activities and road shows to ensure dissemination in public administrations and with other relevant stakeholders.

Supported by EC,
Grant nr. 261584

University of Murcia
www.um.es/english

Fraunhofer FOKUS
www.fokus.fraunhofer.de

citkomm
www.citkomm.de

Ministry of Industry, Energy and Tourism
www.ipv6.es

Ministry of Finance and Public Administrations
administracionelectronica.gob.es

IPv6 eGov

IPv6-readiness for cross-border eGovernment services

University of Murcia, Fraunhofer FOKUS,
Citkomm, Ministry of Industry, Energy and Tourism,
Ministry of Finance and Public Administrations

IPv6-based support for cross-border eGovernment services

Cross-border eGovernment services are required in order to strengthen the Single-Market and to favour the mobility of EU citizens. Due to the imminent transition to IPv6, it must be assured that they are (and will be) prepared to interoperate using IPv6.

This project has the following objectives:

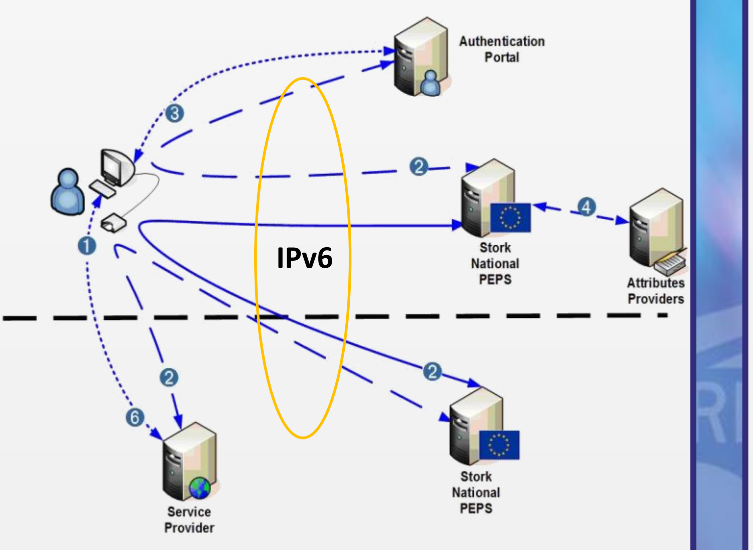
- **Identification of the technical arrangements needed for the interoperability of the IPv6 transition national strategies.**
- **Preparation of different transition scenarios with a mixed environment of IPv4 and IPv6 clouds in the government tiers (national, regional, universities…).**
- **Testing of the interoperability scenarios and compilation of a troubleshooting manual, roadmap of actions developed and guidelines.**
- **Strengthening the usage of IPv6 on public administration by means of learning by examples based on the experience of this pilot.**

CROSS-BORDER AUTHENTICATION Based On The Results From STORK

Strong authentication is one of the corner-stones of cross-border eGov services

Many member states deployed national eID systems in the last years enabling citizens to use government services online. These identification mechanisms have to be transferred to IPv6 for future use in cross-border government cooperation. GEN6 will make use of the STORK results to show how IPv6 enables authentication procedures:

- Authentication process based on the national eID cards issued by the origin member states.
- Citizens redirected from the target service to their national authentication authorities through different proxies via HTTP GET/POST requests.
- Citizens redirected back to the target service with the authentication outcome signed by the national authority.
- Different authentication systems, similar behaviour: STORK, GERMAN one. Proxies make interoperation possible.
- Services, proxies and authentication authorities need to be updated to IPv6.

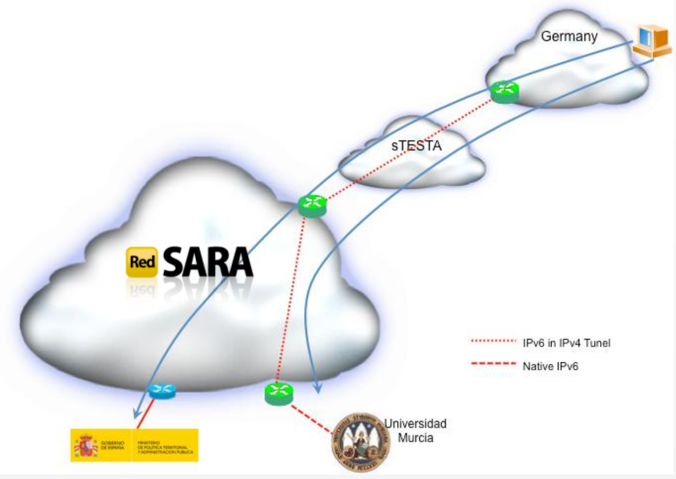


IPv6-ENABLED INTERCONNECTION OF CROSS-BORDER eGOV SERVICES

Enable the Member States' eGovernment services to interact through IPv6-enabled connections

Analyse current administrative communication infrastructures, and prepare an action plan to provide point-to-point IPv6 connectivity between member states. Currently there exists more than one option. GEN6 will evaluate the different paths and give recommendations about the options, their Pros and Cons:

- Promote the use of native IPv6 connection provided by ISPs, national gateways, etc.
- Define the use of IPv6 in IPv4 tunnels to go through non-IPv6 networks (e.g. sTESTA and DOI Backbone).

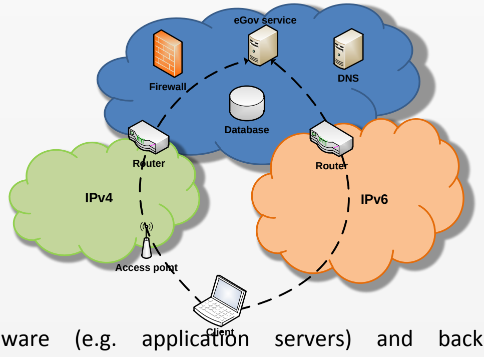


- Support the transition of sTESTA to a native IPv6 network.
- Adapt network equipment to the use of IPv6 (e.g. firewalls, routers, DNS servers).
- Configure web servers and applications to support IPv6 connections
- Provide good practice examples, drawbacks, advantages and procedures that will serve for future adaptations.

BASIC REQUIREMENTS FOR THE TRANSITION TO IPv6

Besides the changes on routers and network equipment, other actions are required to allow a smooth transition to IPv6

- Web servers need to be updated and/or reconfigured to listen on IPv6 addresses and accept IPv6 connections.
- The same holds true for DNS servers (IPv6 support, new AAAA-type entries for services, proxies, and authentication authorities.
- Firewalls need to be reconfigured to include IPv6-based rules, realizing the meaning of exiting IPv4-rules.
- Routers need to be made fit for IPv6 by upgrade (or replacement) and configuration; switches should be checked too (management access).
- All affected middle boxes (Proxies, application-layer gateways, load-balancers, etc.) must be checked, and upgraded if needed.



- Middleware (e.g. application servers) and backend applications (e.g. databases) must be configured and tested for IPv6 support.
- Used client applications (web browsers, terminal clients, and fat clients) must be checked for combatibility with an IPv6-enabled network environment.
- Where network monitoring is in place, this must not be extended to support IPv6 itself, plus also check the IPv6-reachability of any migrated service.
- It is best to start the migration in a dedicated testbed, where real-world applications and their processes can be tested before going live.