

FI PPP 2nd Usage Area Workshop: EADS Astrium Position Paper

1. *What use case and scenario in your area would you consider the most appropriate and representative one for large-scale experimentation with the Future Internet platform to be built starting from 2013 (please refer to the documents referred to on the above websites for inspiration)?*

There are three scenarios that we consider representative, all with a focus on public service provision using the Future Internet:

- a. *Critical Infrastructure Protection*: A hybrid terrestrial/satellite infrastructure connecting sensors or aggregated sensor systems to control centres at regional, national and European levels, integrated with the Internet, but offering resilience and security functions over and above those available today.
 - b. *Bridging the Digital Divide*: Provision of a seamless data transport mechanism that supports a service provision that is adapted to varying communications capabilities across both the digital cities and into remote rural communities over multiple terrestrial wired and wireless supports as well as mobile and fixed satellite infrastructure.
 - c. *Pan-European Service experiments*: Use of satellite backbone to bridge a number of disparate user communities with varying levels of user sophistication and IT infrastructure as well as cultural, administrative and legal traditions and practices in order to study high-level issues of interworking on common themes involving e-government
2. *What innovative Internet functionality and technologies would you consider important for your suggested use case and scenario (e.g. context awareness, sensor networks, advanced real time processing capabilities handling huge volume of data, ad hoc service composition and mash-up, managed broadband connectivity and services, embedded media support for interfaces easing the interpretation of processed contextual data, etc.)?*

Public service and e-government applications have specific characteristic requirements for security, privacy, availability and resilience. Therefore questions of interworking, failover and fallback, overall service and network management are raised by these applications. In particular we believe that Policy-Based Network Management and Security technologies need to be developed and deployed to enable this functionality. These technologies must intervene both within and between different communications technology domains, as well as across regional and national boundaries. They must operate both within and between IMS sub-systems as well as enabling end-to-end service provision with the required capabilities.

3. *Which of the identified functionalities would you expect the Future Internet core technology platform to deliver to support your and other usage area scenarios?*

The platform should provide a range of data transport services with facilities to support virtualisation and flexible network and security management architectures.

4. *What kind of experimentation environment would you consider necessary for broad large scale testing of the platform to be developed in your use area? What would be needed to experiment new services and applications cutting across use areas (services and application mash-up) and building a new services and application ecosystem around the prototype implementations of the platform?*

The primary requirement for these environment would be service availability across a variety of user communities distributed geographically and politically, with interfaces to European, national and regional government and government agencies.

5. *How do you see the potential role of your organisation in the FI-PPP, in the context of Usage areas taking a prominent role in the Initiative, to ensure an appropriate application driven approach?*

Astrium has capabilities in the provision of satellite-based resilient and secure communications infrastructure. We have close links with governmental service-providers and and-user organisations in a variety of areas, including crisis intervention, infrastructure monitoring and management, security services, and other related areas. We act as both systems developers/suppliers and service providers.