

Parallel session 9 Security and Trust – The Foundation for Building an eUnion

Session Description

Building an eUnion makes it easier for citizens and businesses to move and work in any EU Member State. This leads not only to an increasing flow of digital data but also to more severe security threats and specific challenges connected to privacy rights.

A secure exchange and storage of personal data requires innovative legal and technological solutions that can ensure an automatic compliance with privacy and security provisions as well as being user friendly and efficient. A balance that needs to be struck between increased efficiency and transparency on one hand, and security and privacy, on the other.

In this session, chaired by **Francisco García Morán**, (Director General for Informatics, European Commission) a panel of speakers with different backgrounds (IT, academia, industry, public sector) addressed, each from their own professional perspective, the need for secure infrastructure, capable to manage efficiently information.

Anne-Marie Eklund Löwinder, Quality and Security Manager of the Internet Infrastructure Foundation .SE (Sweden), described how communications and networking equipment requires to be at the same time secure, dynamic, robust and reliable, while Internet continues to be vulnerable to various problems connected to security and robustness. The Internet Infrastructure Foundation has surveyed how public authorities and other important bodies in the Swedish society manage their presence on Internet. The analysis underlines a lack of understanding and responsiveness, and consequently critical improvements are necessary, not optional. Mrs Lowinder, affirmed that the current regulatory framework is sufficient for open market operations and further regulations are not needed. On the other hand additional action would be necessary in terms of recommendations: the introduction of DNS Security Extensions (DNSSEC) securing the domain name system, for deployment of the next-generation Internet Protocol (IPv6), for best practice of robust and resilient network design. Separate identity authentication standards complicates sharing access among different groups. In this sense there is the need to avoid long lists of passwords but it is also important to introduce a Federated Identity based on open standards, which offers suitable protection of own personal integrity, and is technically neutral, cost effective, as well as available to different stakeholders coming from all parts of the society.

For **Tommi Nordberg**, Executive Vice President of Government Programs, Gemalto, Finland, while progress has been achieved to ensure a secure identification and access to eGovernment services (using eID, PKI authentication, signatures, etc.) the user experience has been disappointing and more focus on design of interfaces is needed to avoid loss of potential market. eGov 2.0 is a step towards an easier and more user friendly environment. The combination of e-ID smart cards and eGov 2.0 strong-authentication framework (PKI technology) did not just provide extra security, but it also provided end-user extra convenience. Such combination deserves furthermore easy adoption, mobility (e-ID cards can be used in multiple platforms), less dependence on users' technology skills, thus encouraging a more "security conscious" citizen behaviour, promoting a global, modern, competitive and socio-economically equal world. Several eID and eGov 2.0 approaches exist in Europe. It will be interesting to see, Nordberg affirms, when they will finally come to use by all the people in Europe and how they will work.

Kai Rannenberg, Mobile Business and Multilateral Security professor within Goethe University of Frankfurt, Germany, highlighted that trust into eGovernment requires multilateral security of the underlying infrastructure, especially concerning used identities. Mobile/ubiquitous/ambient systems coming ever closer to people call for user-friendly identity management and multilaterally secure identifiers. Prof. Rannenberg introduced the concepts of partial identities, strong sovereign identifiers, minimum disclosure. Every person has his own identity. This identity consists also of peoples' role, e.g. while using government services a person is well known whereas while he is shopping, he is almost anonymous. These different depictions of identity depending on the situation are represented by partial identities. A partial identity is a set of personal attributes of a user. A user can have several partial identities. Close to the physical world, a user changes his partial identity in computer networks while shifting between being anonymous and being fully identifiable. Such a change depends on the situation and on the role necessary for specific situation. Identity management systems support users which utilize role based identities and help to present the "right" identity in the right

context. Secure identities based on strong and protective identifiers that can communicate through more than one channel. Our current systems collect more information than is generally required. Users should have the possibility to decide what information disclose (minimum disclosure).

Andrej Tomšič, Deputy Information Commissioner of Slovenia, affirmed that fundamental principles of personal data protection must be respected when developing eGovernment systems and services thus avoiding eGovernment data protection pitfalls (data pollution, function creep effect, the threat of the “Big Brother’s one-stop shop”, internal threats such as the curiosity of public servants and security breaches). This can be done by ensuring transparency, providing for security & traceability of personal data processing, implementing best practices and international standards (such as AAA concept, ISO 2700 family standards and similar), educating and controlling internally civil servants and also by guaranteeing data subject the right of access to his own information. Legislative proposals that provide legal ground for personal data processing should properly consider privacy throughout the designing approach and also utilize privacy impact assessments. In doing so government bodies should establish good relations and cooperative initiatives with data protection authorities, the latter being entrusted with sufficient enforcement competencies. Tomšič concludes expressing a vision of a unified and connected Europe, able to deliver high quality services to its citizens and businesses whilst respecting the basic human right of privacy through privacy impact assessments, guaranteeing transparency and respecting personal data protection commandments, which are: legitimacy, lawfulness, fairness, proportionality, finality, data quality, accountability and data subject’s rights.

Discussions concentrated on the need of further regulations in this sector. Anne-Marie Eklund Löwinder affirmed that most of existing regulation is sufficient. Major requirement underlined was to start regulating only after developing practical solutions, in order to avoid deployment trouble which could arise in a second moment. A classical example are the regulations concerning eID. Francisco García Morán, stressed that EC has been implementing impact assessments of the new IT legislation. Discussion then moved towards the concept of “partial identity”, in particular concerning its straight connection to privacy issues, as well as to the role and to the responsibilities of the user who owns this identity.