

**Mini-track title: E-Government Trust and Information Security Issues and Concerns**  
**Track: E-Government**

**Mini-track Chair(s):**

1. Dr Ramzi El-Haddadeh\*,  
Brunel Business School, Brunel University  
[csstrre@brunel.ac.uk](mailto:csstrre@brunel.ac.uk)  
Tel: +44 (0)1895267099

2. Dr Vishanth Weerakkody  
Brunel Business School, Brunel University  
[Vishanth.Weerakkody@brunel.ac.uk](mailto:Vishanth.Weerakkody@brunel.ac.uk),  
Tel: +44 (0)1895267099

**Description:**

In the rapidly growing world of ICT, various public sector organizations including e-government have focused their efforts towards digitalizing their services to their customers or citizens through the Internet. Such digitizing of information is known as e-government and implies that information is exchanged among different parties over the Internet. However, a major concern over trust, protection and safety of such information demands a high level of security within e-government organisations. In this context, the role of e-government, trust and information security activities is to ensure confidentiality, availability, integrity, authentication and non repudiation of information in addition to providing more comprehensive understanding of user acceptance of such electronic service. In general, the prescription of information security is mainly associated with technical and technological aspects. However, there are considerably various embedded issues such as processes, judicial factors and strategies that impact upon information security when delivering e-enabled public services to citizens, businesses and other government and non government agencies.

On a strategic level, public administration has security obligations and responsibilities for a wide range of electronic processes in the various public sector fields and includes many parties that are closely involved in it. These security strategies are not very clear upon first inspection. By comparison, e-commerce builds on clearly defined strategies and goals based on obvious trust and security strategies for two-way interaction. The aim of this minitrack is to provide a common platform for discussion and presentation of original research that highlights strategic, technical, organizational, judicial or other factors that influence trust and information security when delivering an e-government service .

**Suggested topics:**

- Trust issues in E-Government adoption and diffusion.
- Information systems security design and management in E-Government.
- Risk analysis of information security in E-Government.
- Developing strategies for assessing security risks in E-Government.
- Trust, behavioural, cultural and judicial issues influencing information security in EGovernment.
- Technical factors influencing information security E-Government.
- Strategic and management issues influencing information security in E-Government.
- Information security infrastructure development for electronic service delivery in EGovernment.
- Impacts of emerging technologies on security and privacy and its adoption in EGovernment.
- Best practices in implementing and managing information security for E-Government.
- Evaluation of information security protocols that are used in e-government contexts