

## PAMPAS

### Workshop on Requirements for Mobility, Privacy and Security

#### Future Research Priorities

##### Drivers

Over the coming years identity management will increase in complexity as the balance of power and sophistication of relationships (enterprise, B2C, G2C, Social) develop in line with new opportunities brought about by modern technology.

Furthermore, we believe that any scheme should be predicated on the belief that the citizen owns their ID. What this means is that the citizen wants to be able to authorise and manage the use of their identity. They want to define the protection and avoid the 'lock in' traditionally associated with convenience.

Scenarios that we envisage becoming common practice and likely to challenge the way we manage identity include:

- Dual use appliances used for both work and leisure activities and therefore affording protection to user owned data and data owned by a third party.
- Shared appliances where two or more users use a single device of totally independent applications.
- Multi-relationship where a device is used by its owner to maintain multiple independent relationships, effectively isolating the relationship's partners from each other. A typical example of this is a contractor who has several different employers.
- Support for highly mobile users where establishing trust in the environment is more challenging due to unfamiliarity and increased complexity.

This change in emphasis from a centralised model of ID management has a bearing on the architecture required. Peer-to-peer models become as equally plausible as those of the more traditional client-to-infrastructure interactions.

##### Technologies

Technology is starting to emerge that can establish and measure trust, and control the use of data. Trusted operating systems provide many of the controls necessary to protect sensitive information in complex multi-user environments. TCPA (Trusted Computing Platform Alliance) defines a means of determining whether a platform can be trusted. Identifier Based Encryption (IBE) sets a new standard for cryptosystems where identity and the need for lightweight protocols are key requirements.

Stephen Crane

Hewlett-Packard Laboratories Bristol, UK