

## RFID Authentication Protocols

### Group Authentication/Proofs

Prove that a group of RFID tags are presented at the same time.

We are proposing more efficient solutions that shortens the time that the tags need to be in the reader field

Optimisation of performance and security in RFID tracking systems

### Distance Bounding

Cryptographic proof of proximity of two entities (provide upper bound on the distance between them)

Proximity identification based only on limited distance of communication channel vulnerable to relay attacks

Implement secure proximity systems for high-value systems

## Multiple SIA Architecture

### Access to multiple mobile networks/services with a single smart token

Currently, mobile networks rely upon a dedicated Subscriber Identity Application (SIA) hosted on a smart card so multiple cards are needed to access different types of networks.

This work explores the possibility of hosting more than one SIA on a single card, which would provide access to a multiple mobile technologies/services.

## Mobile Portal

### ID Verified Using Mobile/NFC

Use mobile handsets as a portal to read and verify identification tokens (e.g. Identification cards) via NFC. The information will be sent securely via the communication network for verification at the remote server.

Ubiquitous replacement for contactless smart card reader infrastructure.

## User-Centric Smart Cards

### Smart Card Properties

A smart card that can be customised by the user thereby providing flexibility and allowing for more ubiquitous use. For example, an issued ID card could be customised by its owner to contain loyalty or travel products.

Security framework to protect Individual applications on card.

### Users

Users would have control of the smart card. They could install and delete additional applications as they wish.

Reduced number of smart cards required by the user as a single card or NFC device could replace all other cards (ID, banking, transport etc).

### Organisations

Companies could offer their application in software form, e.g. available from their dedicated websites.

Companies can deploy applications without additional costs of a dedicated smart card platform and 'ownership' issues are simplified compared to current multi-application cards.