

**RFID and Identity Management - An Anonymity and Multiple Identity Card Prototype:**

The Smart Cities Group of the MIT Media Lab has conceived and developed an innovative use of RFID for identity cards that is designed to protect privacy by allowing for use of multiple lawful pseudonyms. Up to now, RFID has been considered a potential concern from a privacy perspective, largely because of the potential to read the information from an identity card wirelessly, possibly without the knowledge or consent of the card holder. This concept demonstrates that RFID can be used to enhance privacy, by enabling tightly controlled separation between multiple lawful identities for a given person. By using a mechanical system to shut off power potential to chips, and giving the user manual operation to turn on just one chip at a time, this prototype allows people to exercise control over who gets what information about them.

Unlike a single national ID, or a widely used unique identifier, it is possible through the concept of MultiIdentity Cards for a person to have one chip for, say, an employee access card, another as a driver license, another as a retail loyalty card and another for e-commerce, for example. The chip information can be designed such that no chip can be linked directly to another. However, in the event of a lawful warrant or other legal process, it can be possible to discover the user of any given identity. By turning all the chips to the off mode, the user can enter a digital stealth mode, never emitting any information wirelessly.

This concept was conceived by Daniel Greenwood, Lecturer at the Media Lab and the implementation was engineered and constructed by Peter Schmitt, Masters student at the Media Lab. They are now working on a more elegant design of the concept, using a thumb slider to toggle between the chips, and another design using a button set to activate the chips easily. These designs also rely upon mechanical operations to turn on and off each chip, thereby eliminating the possibility that an unauthorized user could secretly activate a chip by remote electronic transmission without the knowledge or consent of the card holder. This is because the card holder must physically turn on or off a given chip before it is capable of transmitting. All designs, however, allow a user to choose to leave any given chip in the "on" mode, for ease of use in such applications as parking or building access, when the card holder may wish to keep the card in a wallet or purse for routine, convenient use.

Both Peter and Dan are with the Smart Cities Group of the Media Lab, led by Professor William Mitchell. We wish to thank HID incorporated for their donation of the chips, the reader and other support that made this project possible.

[LINK TO THE VIDEO OF THE FIRST PROTOTYPE](#)

[LINK TO LAW REVIEW ARTICLE OUTLINING GENERAL LAWFUL BASIS OF ANONYMITY AND MULTIPLE IDENTITIES BY ANY PERSON, PROVIDED NO INTENT TO COMMIT A CRIME OF A FRAUD.](#)

ECITIZEN.MIT.EDU The MIT E-Commerce Architecture Project