Mehta Ketan

From: Anders Rundgren [anders.rundgren@telia.com]
Sent: Sunday, November 21, 2004 2:37 PM
To: draftfips201@nist.gov
Subject: Comments on Public Draft FIPS 201

Ladies & Gentlemen,

I did not use the comment form as this input is not about details but rather about the entire framework. The input is based on about eight years of experiences with smart ID cards in Scandinavia.

Human readable IDs vs. Electronic IDs
==========
I personally don't think that the combination of a human-readable ID (badge) and electronic authentication devices is the optimal solution. The reason is that the form factor of the latter becomes constrained and that the applicable use cases are entirely different. As a representative of a major US computer security company, I can testify that USB tokens is much hotter item than smart cards to take an existing example.

Badges as ID cards
==========
Regarding badges, they come in many flavors and for certain usages they are intended to authenticate the user as a valid representative but not necessarily containing the person's full identity. The reason for this is that certain more or less public roles may need some privacy protection in order to reduce potential harassment by clients (citizens).

Due to this I believe that PIV should only rely on electronic data and let badges continue to be subject to local requirements. The armed forces and hospitals probably do not have the same requirements.

Specifying contents and procedures, but leaving form factor
==========
Due to the very intensive developments going on in mobile devices, I believe it is premature to standardize the "container". Or maybe, define an initial form factor and interface, but leave the door open to other schemes like the ones the Trusted Computing Group are working with (=using mobile phones and PDAs as universal multi-credential security containers). More detailed information is available upon request.

Regards
Anders Rundgren
Developer of mobile security technology
Member of Trusted Computing Group