Copyright (C) 1996 IEEE. See full copyright notice at Table of Contents.

Panel on Public-Key Infrastructure

Warwick Ford, Chair

Bell-Northern Research
Ottawa, Canada
wford@bnr.ca

Abstract

This panel session will address issues relating to the deployment and evolution of public-key infrastructures, focusing on the question: How many "credentials" do I need? The panel comprises experts in the field of public-key infrastructures who are able to address this question from a variety of perspectives, including the credit card industry perspective, the application software vendor perspective, and the commercial public-key infrastructure service provider perspective.

Overview

This panel will focus on the question: How many "credentials" do I need?

In the emerging public-key technology world, it is feasible that one set of private "credentials" embodied, for example, in a smart-card, token, or password-encrypted personal file, can be used for many different application purposes. Such purposes might include, for example, protection of casual E-mail and Web accesses, protection of financial transactions, and protection of communications with the government.

Furthermore one set of "credentials" can conceivably support multiple personal roles, such as a private citizen role and an organizational representative role.

But is such credentials-sharing really achievable? Will I end up with one set of "credentials" or with so many "credentials" in different physical forms that a wallet-full of plastic cards will look elegant in comparison?

And,... what will it cost?

The panelists have been invited on the basis of their abilities to address the focus question from different perspectives:

- the credit card industry perspective;
- the application software vendor perspective;
- the commercial public-key infrastructure service provider perspective.

Panelists

The panelists are as follows:

John Wankmueller, MasterCard International
(credit card industry perspective)

John Wankmueller is Director, Technology Assessment, at MasterCard International. He is leading the design of the infrastructure and development of standards for securing MasterCard electronic commerce transactions.

Taher ElGamal, Netscape Communications
(application software vendor perspective)

Taher ElGamal, a well-recognized researcher in public-key technologies, is now Chief Scientist at Netscape Communications Corporation in Mountain View, CA.

Michael Baum, Verisign Inc.
(commercial public-key infrastructure service provider perspective)

Michael Baum is Vice President, Practices and External Affairs, at Verisign, Inc. Michael has an extensive background working on the legal and commercial aspects of digital signature systems.