NISSC '97 Internet Security Track
Wednesday, October 8, 2:00-3:30 p.m.
Panel Session: Public Key Infrastructure -- Issues and Challenges

Chair:

Warwick Ford
Director, Advanced Technology
VeriSign, Inc.
One Alewife Center
Cambridge, MA 02140
(617) 492-2816
wford@verisign.com

Panelists:

Taher Elgamal
Chief Scientist
Netscape Communications Corporation
685 Middlefield Road
Mountain View, CA
(415) 937-2898
elgamal@verisign.com

Donna F. Dodson
NIST PKI Program Manager
National Institute of Standards and Technology, Bldg 820, Rm 426
Gaithersburg, MD 20899
(301) 975-2921
donna.dodson@nist.gov

Tom Manessis
Visa
PO Box 8999
San Francisco, CA 94128
(415) 432-7011
tmanessi@visa.com

Ted Humphreys
Director, XiSEC Consultants Ltd
2 Denham Court
Martlesham Heath
Ipswich IP5 3TF UK
+44-1473-626615
ted@xisec.demon.co.uk

Panel Session:
Public Key Infrastructure - Issues and Challenges

Chair
Warwick Ford, VeriSign, Inc., Cambridge, MA

Panelists
Taher ElGamal, Netscape Communications Corp., Mountain View, CA
Donna Dodson, National Institute of Standards and Technology, Gaithersburg, MD
Tom Manessis, Visa, San Francisco, CA
Ted Humphreys, XiSEC Consultants Ltd., Ipswich, UK

While public-key infrastructure has been a topic of academic study, technology development, and experimentation for several years, it is only comparatively recently that efforts have been made to deploy public-key infrastructure on a large scale in direct response to real business and government needs. As a consequence of these large-scale deployment efforts, we have recently gained an enormous amount of insight into the practical barriers that continue to make wide-scale deployment of public-key infrastructure more difficult than many once believed.

This panel session examines the main issues and challenges in the development and deployment of public-key infrastructure. These issues and challenges will be examined from four different perspectives:

- **The Software Industry:** Commercial products that either employ or contribute to the provision of public-key infrastructure are now readily available from the major software vendors. How successful are these products or product features? What are the main challenges faced by the software vendor? What changes in direction might we expect in the next year or so?
- **Government:** Governments have largely led the way in early public-key infrastructure research and experimentation, but that role has now, by and large, been made redundant, because of the advances into commercialization of the technology. What role does/should government now have with respect to public-key infrastructure? Is government the natural facilitator of public-key infrastructure interoperability? Should government lead the way in setting security standards for public-key infrastructure product or service providers? What can we gain from experiences overseas?

- **A Major Commercial Application:** One of the first commercial applications to commit to the adoption of public-key infrastructure was that of Internet-based bank card payments, through the Secure Electronic Transaction (SET) initiative. After almost two years of design and development work, large-scale deployment of SET is on its threshold. What major lessons have been learned so far in the SET project? How can other public-key infrastructure application endeavors benefit from the SET experience?
- **Commercial Public-Key Infrastructure Service Provision:** The past 12 months represent the best testing ground to date for determining the commercial viability of public-key infrastructure service provision as an industry in its own right. What has been learnt so far? What issues do such an industry face?

Each panelist (including the Chair) will present an opening statement, addressing the panel topic from one or more of these perspectives. Substantial time will be reserved for interactive question and answer with the floor.