TITLE   ACCESS CERTIFICATES FOR ELECTRONIC SERVICES

PANEL CHAIR   JUDITH A. SPENCER
                           GENERAL SERVICES ADMINISTRATION
                           OFFICE OF INFORMATION SECURITY

PANELISTS   STANLEY J. CHOFFREY
                           GENERAL SERVICES ADMINISTRATION
                           OFFICE OF INFORMATION SECURITY

                           GEORGE DATESMAN
                           MITRETEK SYSTEMS

                           DAVID TEMOSHOK
                           GENERAL SERVICES ADMINISTRATION
                           OFFICE OF GOVERNMENTWIDE POLICY

                           [TBD]

SUMMARY OF TOPICS

SPENCER TOPIC: One of the primary goals of the NII is to facilitate public access to the services offered by Federal agencies through use of information technologies, including on-line access to computers for purposes of reviewing, retrieving, and exchanging information. Access to some Federal computer systems can only be granted when the agency is provided with assurance that the individual attempting access has been properly identified and authenticated as being authorized to access the computer system and the information requested. Public Key cryptography, which includes digital signature technology, can play an integral role in providing this end-to-end security of information in terms of confidentiality, integrity, and proof of origin. The chair will discuss the issues affecting ACES and describe the panelist's role in addressing solutions.

SPENCER BIO: Ms. Spencer is the Director, Center for Governmentwide Security in the Office of Information Security, Federal Technology Service, General Services Administration. Ms. Spencer's 24 year career in Information Systems Security began with a three year enlistment in the U.S. Army followed by five years at the Lexington-Blue Grass Army Depot before moving to GSA in 1983. Since, joining GSA, Ms. Spencer has participated in the management of the STU-II, STU-III, and MISSI Civil Domain. She is currently leading the project to provide a government-wide solution using public key technology to enable interaction with the public via the Internet.

CHOFFREY TOPIC: Public Key Infrastructure (PKI) certificates, issued by a trusted third party who has identified the individual or entity, is the enabling technology for widespread access to Federal computer systems. In support of this goal, the General Services Administration's Office of Governmentwide Policy and Federal Technology Service (FTS) have initiated a project aimed at providing commercial public key

certificate services to the American public. This initiative is referred to as Access Certificates for Electronic Services or ACES.

Specifically, the FTS will release a contract for services that will require industry to:

* Provide a specified level of identity proofing for individuals members of the public;
* Issue a public key certificate binding the individual's identity to a unique digital signature; and
* Verify the validity of the certificate upon demand

The presentation will present an overview of the ACES architecture and provide insight to technical issues.

CHOFFREY BIO: Mr. Choffrey is the senior technical specialist to the Director, Center for Governmentwide Security. The Center is tasked with providing public key infrastructure services in support of Electronic Commerce and Electronic Messaging government-wide. Mr. Choffrey has extensive experience in PKI technology to include DOD's Fortezza Security system as well as commercial PKI systems. Mr. Choffrey's security background includes projects from classified secure voice system to network encryption systems for both classified and sensitive systems. He is currently the technical lead on the GSA Access Certificates for Electronic Services (ACES) initiative. Mr. Choffrey was previously the Chief of GSA's East Coast Special Facility, which was a government-wide operations center for electronic key management systems in support of voice and data encryption devices.

DATESMAN TOPIC: The ACES program was developed in response to requirements or granting and limiting electronic access to government services and information to those persons who are legally entitled to such access. To accomplish this requires the collection, verification, and maintenance of identity information relating to those persons who elect to participate in the ACES program. Comments, suggestions, and concerns about the handling, use, and protection of this personal identity information were actively solicited from interested individuals and groups. The information they provided became an important part of the foundation materials used to develop specifications for the ACES program. The presentation presents those comments, suggestions, and concerns and links them to the specific ACES program features that respond to them.

DATESMAN BIO: Dr. George H. Datesman, Jr., is a senior engineer with Mitretek Systems, Inc., Telecommunications and Networking Division. He holds Ph.D. from University of East Georgia. Dr. Datesman's experience includes Federal Bureau of Investigation's (FBI's) Integrated Automated Fingerprint Identification System (IAFIS) and National Crime Information Center (NCIC) 2000 procurements. His current activities involve assisting GSA in defining Governmentwide PKI policy and related privacy issues.

TEMOSHOK TOPIC:

This presentation will cover the Business Relationships of the ACES PKI. The following topics will be highlighted:

Roles and responsibilities among ACES PKI parties;

ACES Operating Rules;

ACES Relying Party and Subscriber Agreements;
Relationship of ACES PKI to other PKI.

TEMOSHOK BIO: David currently serves as Leader of the Federal Electronic Commerce Policy Office, General Services Administration. This Office is responsible for governmentwide policies and services delivery for electronic commerce initiatives and new technologies. In February 1997, David was appointed Director of the Federal Smart Card Task Force. The Task Force was created by the President's Management Council to provide leadership and coordination for the planning, development and implementation of smart card systems across the Federal Government.

In December 1993 David was appointed to serve as the Director for Systems Design and Development for the Federal Electronic Benefits Transfer (EBT) Task Force. The Federal EBT Task Force was created by Vice President Gore to direct the rapid implementation of systems to deliver both federal and state government benefits electronically on a nationwide basis. EBT systems are now operational in 30 states and 18 additional states are in the process of implementing contracted EBT services.

Prior to these appointments David has served as the USDA Director of Grants Management and has served in numerous other managerial and financial management positions in public administration.

David has received undergraduate and graduate degrees from the University of Rochester, NY, and the Pennsylvania State University.