NIST Special Publication 800-49

Federal S/MIME V3 Client Profile

C. Michael Chernick

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

C O M P U T E R S E C U R I T Y

November 2002

NIST Special Publication 800-49

Federal S/MIME V3 Client Profile

Recommendations of the
National Institute of Standards and Technology

C. Michael Chernick

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

November 2002

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Reports on Information Security Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-46
Natl. Inst. Stand. Technol. Spec. Publ. 800-31, 26 pages (November 2002)
CODEN: NSPUE2

Acknowledgments

NIST would like to thank the many people who assisted with the development of this profile. We are grateful for the support that we received from members of the Internet Engineering Task Force (IETF), IETF's Public-Key Infrastructure Group (X.509) (PKIX) and S/MIME Working Groups. Special thanks are due to John Pawling, Jim Schaad, Russ Housley, Blake Ramsdell, and Tim Polk.

Executive Summary to the Federal S/MIME V3 Client Profile

(For Procurement Officials, Implementers, Vendors and Others Interested in Specifying S/MIME Technology)

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a set of specifications for securing electronic mail. S/MIME is based upon the widely used MIME standard [MIME] and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered by S/MIME are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer's certificate(s).

To understand S/MIME it is useful to understand some of the history of Internet e-mail. In the past twenty-five years or so, Internet e-mail has evolved from a simple text-based (ASCII) transfer of messages designed for researchers into a more sophisticated messaging system capable of communicating a wealth of digital information (e.g., photographic images, computer files, sound clips, cinema) to many millions of people around the world.

Internet e-mail was designed for a small community of trusted researchers (primarily at university and government sites) for exchanging text-based messages, and thus security was not a goal in its design. Over the years many deficiencies in Internet e-mail have been overcome to a certain extent through the use of a technology called Multipurpose Internet Mail Extensions (MIME). Employing MIME for messaging allows the use of multiple-text effects (e.g., bold, italic, various font sizes, and colors) as well as the transfer of digital information. MIME by itself also does not address security issues. However, a set of security features has been developed and added to MIME to form what is known as S/MIME (Secure MIME).

S/MIME adds features to e-mail messaging including privacy (using encryption), authentication of sending party (using digital signatures), integrity (non-alteration of messages), etc. S/MIME V3 is the latest version of S/MIME and is supported in whole or part by several vendors with "Commercial-Off-The-Shelf" (COTS) products.

Because S/MIME still uses the same extant Internet e-mail technology that has been widely deployed for many years, it is not necessary to modify or replace e-mail "servers" to accommodate S/MIME. Rather S/MIME functionality may be added to e-mail "client" software. By not disturbing the underlying e-mail server/message transfer system, S/MIME allows gradual migration from non-secure to secure e-mail messaging, rather than requiring a large, possibly abrupt change in technology.

Like other services and protocols used by the Internet community, S/MIME has been under development for many years, with the main components specified by the Internet Engineering Task Force (IETF), a technical body that issues specifications that serve as standards for vendor

implementation. These specifications are known as "Request for Comments"[1] (RFCs). The IETF RFCs for S/MIME reference important standards issued by the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU). In addition, the U.S. National Institute of Standards and Technology (NIST) has issued certain Federal Information Processing Standards (FIPS) that are used to specify requirements for cryptographic algorithms and related hardware/software modules used by S/MIME. Thus, implementers and users must adhere to a very large set of “standards.”

Furthermore, because standards developers allow many options within communications systems, even if all standards are rigidly adhered to, interoperability may not be possible due to differing choices of options selected by different vendors. For example, if vendor A chooses to implement signed receipts and vendor B chooses not to, then the signed receipts requested by the user of vendor A's products will never be sent by vendor B's product although neither implementation violates the standards.

To help assure that S/MIME products can interoperate and meet the e-mail security needs of federal agencies both with respect to security features, and adequate cryptographic algorithms, NIST has developed this Federal S/MIME V3 Client Profile. This profile states requirements for implementing sets of cryptographic algorithm suites specified elsewhere by the standards development organizations. The profile specifies a set of e-mail security features (e.g., encrypted e-mail, signed receipts) that are mandatory to be implemented. In the definition of this Profile, NIST’s intention is never to violate underlying S/MIME standards, but rather to provide additional specificity within the standards.

While NIST believes that use of this profile will help assure interoperability of the near term secure e-mail products, NIST anticipates that future revisions of the profile will be required to reflect new cryptographic algorithms and related attacks, new underlying S/MIME standards, and new e-mail security features required by federal agencies.

The use of S/MIME requires the establishment of a Public Key Infrastructure (PKI) to support each sender and recipient of S/MIME messages. While the details of PKI are out of scope for this document, it is important to note that PKI is used to provide mechanisms to establish the identity of S/MIME users (known as authentication) and to provide for digital signatures, confidentiality, non-repudiation of sender, etc. X.509 Certificates are used to bind an entity’s identity and public key for secure operations for S/MIME and other PKI-enabled secure applications. For a further understanding of PKI, see [Kuhn01], [Housley01], or [Adams00] in the References clause.

[1] (Note: The RFC name is a misnomer, but is retained for historic purposes, and is well-known in the Internet development community.)

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.