

Procedure 1607 PR.01
Endorsed Encryption Implementation Procedure
 Revision Date 2/25/03

Endorsed Encryption Implementation	1
Overview	1
Rationale for Procedures	1
Current Encryption Recommendations	2
SSL/TLS:	2
Special Situations/Exceptions for Encryption Methods	3
Additional Comments	3
Revision History:.....	4

Endorsed Encryption Implementation

Overview

These encryption implementation procedures are designed to supplement the Yale University Policy [1607](#) Information Technology Appropriate Use Policy section 1607.2 F, which states:

Encryption of Data. Users are encouraged to encrypt files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks. The University makes available software and protocols endorsed by the Information Security Office that provide robust encryption, as well as the capability for properly designated University officials to decrypt the information, when required and authorized under this policy. Users encrypting information are encouraged to use only the endorsed software and protocols. Users who elect not to use endorsed encryption software and protocols on IT Systems are expected to decrypt information upon official, authorized request. (See Policy [1607](#) - Information Technology Appropriate Use Policy section 1607.2 Conditions of University Access.) A staff member may only encrypt with the permission of his or her supervisor.

These encryption implementation guidelines, including endorsed software and procedures, will be updated as technical solutions and University requirements change.

Rationale for Procedures

To support preservation of access to important data, the University has developed recommendations for *data recovery* (salvaging data stored on damaged media, such as magnetic disks and tapes) of encrypted *persistent data* (information that endures beyond a single instance of use). Business continuity in the event of a disaster, such as the endangerment of data access (loss of key personnel or passwords) for a University owned computing device is a serious concern, as is the concern that a Yale-owned computing device could use encryption to hide illegal activities.

The University has also established minimum standards for encryption to ensure that sensitive data is protected from disclosure, both when 'in transit' over computer networks and when stored on computing devices including servers, desktop machines and portable devices such as a PDA. The University is presently not concerned with maintaining a central *data recovery* decryption capability if it would prevent use of network privacy. Nor is the University planning to require the ability to decrypt traffic in transit over the campus network. The University understands that there are privacy concerns attached to these capabilities, as well as deployment problems.

It is also recognized that in the future federal or state law enforcement may ask for the capability to monitor and decode traffic in transit and that circumstances may lead Yale University Information Security to desire this same capability. However, the University currently believes that our capability to monitor encrypted network traffic at the endpoint(s) from system operators/owners/administrators is the most reliable implementation. These system operators/owners/administrators are required to cooperate with

requests for decryption under the conditions specified in Yale University Policy [1607](#) Information Technology Appropriate Use Policy.

Information that is directly related to the business of Yale University (finance & administration, HR, student affairs, legal, primary source clinical and research data) should only be encrypted using a *University approved method* (e.g., PGP) which provides the ability for Yale to recover the data in the event of an emergency.

Current Encryption Recommendations

Currently, the only *University recommended method* for encrypting data (email, files, documents, disks) stored on Yale University owned computer systems is PGP (Pretty Good Privacy) software.

PGP (Pretty Good Privacy) -- data should be:

- Encrypted using PGP software (version 6.0 or later) using the default CAST cipher (*cipher text* is unreadable until it has been converted into *plain text*, decrypted, with a key).
- Encrypted to the Yale ITS ADK (Additional Decryption Key) associated with the name itsiso.adk@yale.edu (fingerprint EE59 62A3 2193 6F7E 63D1 ECBC A42D 1AFE CBE3 F022) in addition to the other public keys to which the data is being encrypted. (ADK was added to the PGP software, so that government or other third parties like the University, could have a back door to PGP encrypted data)
- Encrypted only to public PGP 5/6 (Diffie-Hellman, not RSA) keys which have been stored on the Yale PGP Key servers (the LDAP and secure LDAP – LDAPS – servers) and are "signed" by the Yale ITS Certificate Authority Signing Key (KeyID # 0x102F1F65, fingerprint B876 3F26 CABA F0B5 B3DD 7679 8DF5 44F1 102F 1F65).
- Both the Yale ITS ADK and Certificate Authority Signing Key public keys are available for download via LDAP and "Secure" LDAP via the Yale PGP Key servers available via the name "PGPKEYS.ITS.YALE.EDU" (<ldap://pgpkeys.its.yale.edu/> and <ldaps://pgpkeys.its.yale.edu/>)

PGP software that implements the above policies is downloadable for use by Yale faculty, staff and students who must conduct secure business, research or clinical activity on behalf of the University. For more information see:

- [ITS Information Security](#): (Central Campus)
- [ITS-Med Information Security](#) (Medical Campus)

SSL/TLS:

Secure Socket Layer-SSL (versions 2 or 3) or Transport Layer Security -TLS protocol is recommended for transmission of Yale University data via the World Wide Web on either the local campus network or the Internet:

- Use © VeriSign Web server certificates and Web servers which support SSLv3/TLSv1 in strong encryption mode (128 bit or higher symmetric/bulk encryption, 1024 bit or higher public key encryption).
- © VeriSign Web server certificates can be obtained (for a fee) either the Yale University Information Security Office [Verisign On-Site program](#) or directly from © [VeriSign](#).
- The private key associated with the SSL Web server should be secured appropriately on the host OS (e.g. Windows NT/2000/XP or Unix) and should be provided on request by the University.
- The above stipulations do not apply if 1) you are testing encryption protocols or 2) if this is a private server (departmentally owned, not owned or managed centrally by ITS or ITS-Med)

Special Situations/Exceptions for Encryption Methods

(other than PGP/SSL implementations described above)

1. Login and access to Yale University owned servers is endorsed for the following secure protocols:
 - SSH 1 & 2
 - Kerberized Telnet (Note: should be used in encryption AND authentication mode).
 - Kerberized POP (Note: does not provide e-mail content nor traffic encryption)
 - IMAP over SSL
 - FTP over SSL
 - SMTP over SSL
 - [NetMeeting](#)
 - [pcAnywhere](#) (versions 8x, 9x & 10.x)
 - [NT Terminal Server Client](#)
 - [Citrix ICA](#)
2. The [University Audit department](#) currently has a requirement for independent private encryption of audit information kept on auditor's hard disks and servers.
3. [HIPAA](#) (Health Insurance Portability and Accountability Act) compliance: Yale University must adhere to requirements of the Federal government (e.g., HIPAA and Federal agencies), business partners, as well as those imposed by contractual relationships ([CHIME](#), vendors, University consortia, etc.). **If the data is *primary source PHI-Protected Health Information* for TPO (treatment/payment/operations) or primary source PHI for approved research or pre-research, the only allowable method for encryption is the Yale University implementations of PGP. If the data does not meet these criteria, other encryption methods are allowable, such as**
 - Windows 2000 [EFS](#)
 - MacOS 9 - [Apple File Security & Apple Verifier tools](#)
 - MacOS X - [Disk Image Encryption](#)
 - S/MIME - Secure Multi-Purpose Internet Mail Extensions
 - Non-Yale implementations of PGP

Additional Comments

Windows 2000 EFS (Encrypted File System): Windows 2000 and Windows XP have the capability to escrow the keys used for the Encrypted File System by designating Trusted Agents' given data recovery privileges. A Yale University implementation is not currently in place, but it will be in the future and that implementation will require that your machine be a part of the Yale Windows 2000 [Active Directory](#) domain hierarchy.

Apple **MacOS 9** does not appear to support enterprise-wide data recovery or key escrow capabilities in their current file encryption system.

Apple **MacOS X** does not currently appear to support enterprise-wide data recovery or key escrow capabilities in their current file encryption system, but these features may be added in future releases.

S/MIME holds the most promise of achieving a universal, ubiquitous and user-friendly email security and privacy solution. PGP is currently a niche product being used for email by approximately 200 Yale clients. We believe that S/MIME will be required in the future by some business partners and health system consortia (CHIME) for secure Internet email. However, a Yale University PKI infrastructure

implementation will be required for effective use of the S/MIME protocol. Public Key Infrastructure (PKI) is the term used to describe the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys, and it supports enterprise-wide data recovery capabilities.

The University is planning to do implement S/MIME once our PKI infrastructure is in place. In addition to being required for S/MIME, a PKI and X.509 certificates will be needed for other University applications such as access to licensed bibliographic material, restricted health Web sites, and VPN (Virtual Private Networks).

There are other requirements for implementation of S/MIME, but none should prove insurmountable:

- The Eudora E-mail client doesn't support S/MIME natively. It requires a separate licensed commercial plug-in be purchased and installed for each Eudora client.
- S/MIME certificates are not completely portable between Netscape, Microsoft and other S/MIME e-mail clients requiring some additional effort to create interoperable certificates.
- There is no Internet, nor interoperable standard method of providing either key escrow or enterprise data recovery to encrypted S/MIME messages. A Microsoft Exchange server (Exchange is not currently supported by ITS or ITS-Med) has this capability, but it is not provided in a non-proprietary method by other S/MIME email clients. End-users could additionally encrypt each message to a special 'data recovery' key, but this is not a preferred solution.

Revision History:

February 23, 2000

February 25, 2003

The official version of this information will only be maintained in an on-line web format. Any and all printed copies of this material are dated as of the print date. Please make certain to review the material on-line prior to placing reliance on a dated printed version.
