Solving the HIPPA email Encryption Problem

Bill Pankey
Tunitas Group
bpankey@tunitas.com

Agenda

- Is there a problem?
- What are the business requirements?
- Critical evaluation of solution alternatives
- Rethinking s/MIME and PKI

HIPAA's Encryption Requirement

- ***Standard*** **~**
  "Transmission Security: Implement technical security measures to guard against unauthorized access to PHI that is being transmitted over an electronic communications network"
  45 CFR 164.312 (e)(1)

- ***Addressable Implementation Feature*** **~**
  "implement a mechanism to encrypt electronic protected health information whenever deemed appropriate"
  45 CFR 164.312 (e)(2)(ii)

  Clearly, **email containing PHI subject to this provision**

Addressable Implementation

- **Addressable implementation features are *not* optional, they must be *addressed;* HCO must either:**

  1 **implement the feature**

  or

  2 **document why its is not "reasonable and appropriate" to implement feature,**

  and

  implement an equivalent alternative measure when "reasonable and appropriate"

"Addressing" Encryption

- **No real 'equivalent alternative' to encryption**
  - **encryption is *the* confidentiality control for public network (Internet) communication**
    - confidentiality threat *might* be reduced thru use of steganography (hiding messages in host files) but such methods not widely deployed
- **"No encrypt" response then dependent on the argument that encryption is *NOT* "reasonable and appropriate" for email communication**
  - **can't argue on cost basis, encryption is 'free'**
    - software bundled with all commercial email software
    - only significant cost is management related
  - **on what basis then?**

"Reasonable and Appropriate"

- **Not terms of art for security profession, so absent guidance must rely upon ordinary dictionary meaning**
  - **reasonable ~ "not extreme or excessive"**
  - **appropriate ~ "suitable [to some purpose]"**
- **Test would seem to be whether or not email encryption protects against a "reasonably anticipated" threat**
  - **failing encryption, the HCO should argue that risks are so inconsequential as to not warrant efforts to remediate**

Caveat

- **HHS *apparently* considers 'reasonable and appropriate' independent of *objective* risk of internet transmission, per Karen Trudel,**

  1. HCO sending large number of transactions should encrypt (presumably when sending to doctor A); Doctor B need not encrypt when sending to doctor A ~ interview with Computer World, Feb 20, 2003

  2. "encrypt when you *feel* that it is right for your organization" ~ HHS conference call, Feb 28, 2003

in other words, the patient's expectation of privacy is a function of to whom the patient provides the sensitive information

Back to Basics ~ Interception Risk

- **Components of Internet mail delivery**
  - mail user applications
  - sender SMTP relay
  - DNS to locate recipient SMTP relay (MX records)
  - potential mail transfer agents (intermediate SMTP relay)
  - recipient SMTP relay
  - recipient POP / IMAP servers
  - Various routers (sender, receiver, Internet backbone) for delivery to appropriate IP
- **No confidentiality service in SMTP delivery**
- **Failure to 'secure' any of above services places confidentiality at risk**

Back to Basics ~ Interception Risk

- **Enterprise SMTP and DNS servers are highly vulnerable as directly accessed from Internet**
  - **Mitre "Common Vulnerability and Exposure" database list scores of known SMTP and DNS vulnerability**
    - particularly subject to buffer overflow
- **Attacks allow for hacker to control SMTP and / or underlying OS, poison DNS cache, etc**
  - **redirection / misdirection of email expected result**
- **Attacks against routers**
  - **when was the last time were your routers patched?**
    Hint: **either Dec 31, 1999 or Jan 1, 2000**

Back to Basics ~ Interception Risk

- **w/o encryption, *sender* can't ensure confidentiality**
  - **subject to any compromise in security of Internet backbone routers, DNS system or receiver's SMTP / POP servers**
  - **assurance of confidentiality would depend primarily on trust in the diligence performed by *unknown* parties, e.g.**
    - DNS sources, backbone providers, recipient's ISP
- **These risks largely independent of sender**
- **Since the threat exists, best opportunity to address w/o actually encrypting is to argue the inconsequentiality of the confidentiality threat to Internet email**

Arguing Inconsequentiality

- **ABA Formal Ethics Opinion 99-413**
  - **plaintext email provides 'reasonable expectation of privacy'**
    - no less secure than telephone, fax, US & 'commercial' mail
    - same expectation should be afforded email as other modes !
  - **plaintext email OK for use by attorney for communication of confidential client information**
- **Arguments in support of 'reasonable expectation'**
  - **Obscurity of any single message**
  - **Electronic communications privacy act (EPCA)**
  - **Little evidence of substantial amount of email interception**

Counters

- **Relative security claim may be wrong on the facts**
  - **e.g. Sendmail exploits where specifically crafted message gives control of SMTP relay to intruder**
    - "From" headers sufficient to give sender effective control over sendmail implementation and underlying OS
  - **e.g. automatic filtering of TO, FROM and contents of email**
    - Mailsnarf used in conjunction with arpRedirect ~ advertised as the most effective way to violate ECPA
    - online bookseller eLibris interception of email directed to and from Amazon.com
- **Criminality of act does not, in itself, prevent the act**
- **Sender may be the last to know of confidentiality breach, if at all**
  - **direct experience may not be the best guide**

Addressablity begs the question

- **To what extent can the HCO 'reasonable and appropriate security' depend on *mere trust* in diligence of 3rd parties?**
  - **Expectation that ISP 'secure' their servers and routers, restricting access to 'maintenance' functions only**

  failing that

- **To what extent must the HCO evaluate the capability of these 3rd parties to adequately restrict access to HCO's messages**
  - **especially when the providers of that service explicitly discount confidentiality guarantee**

Caveats when not encrypting

- **Failure to encrypt raises minimum standard relative to protection of SMTP, POP and DNS servers**
  - **also need greater diligence in ISP selection**
- **Recognize that acting contrary to 'best practices' recommendation of technical security community,**
  - **AICPA WebTrust confidentiality principle**
  - **COBIT 'trusted path' control objective**
  - **VISA Account InfoSec Standards**
  - **ASTM Internet Security Guidelines**
  - **watch for NIST SP 800-53 "Minimum Security Controls …"**
- **Expect to be 'the last to know' of breach; develop (HIPAA required) incident response accordingly**

Non functional
Business Requirements

Encryption Challenges

- **Protection of email's business value by ensuring:**
  - **'routine processing' by recipients**
  - **appropriate scope**
- **Non interference with other obligations**
  - **protection of enterprise resources from malware & other**
  - **appropriate disclosure monitoring**
  - **inclusion of information into formal system of records**
- **Effective resource management**
  - **minimize end user training / support issues**

What is often missed #1

- **Cannot implement *effective* encryption technology 'unilaterally'**
  - encryption has no value w/o recipient decryption
  - business partner cooperation required
- **Recipients have computing requirements, that may detract from 'utility' of sender's solution**
  - e.g. virus inspection at enterprise boundary
  - e.g. enterprise software discipline which requires evaluation of software (such as plug-ins) before installation
- **Encryption methods are best 'negotiated'**

Interference

- eMail encryption may interfere with application of enterprise policy
- Evaluation of policy predicates requires an examination of *plaintext* content of email
  - e.g., virus filtering compares virus signature with file contents
  - e.g., audit of the appropriateness & destination of enterprise email
  - e.g., eMail potential source of patient health info, need some procedure to recognize and handle as such
- Locus of encryption is important
  - impacts where policy can be implemented

End user difficulties

- Carnegie Tech study "Why Johnny can't encrypt" points to significant end user difficulties in using PGP
  - CareGroup 'nightmare' when trying to support s/MIME desktop encryption of email using Notes
- Usability concerns are due to the technology's abstractness and the uncertain motivation for it
- Encryption at enterprise boundary avoids most encryption related end user support
  - Is email encryption required at enterprise desktop?
  - Are enterprise network controls sufficient to ensure confidentiality prior to Internet transfer?

Some conclusions

- eMail encryption is most cost effective when accomplished at enterprise boundary
  - ensure availability of plaintext for application of enterprise policy manager
  - avoid potentially large end user support costs
- Encrypt whenever you can
  - significant encryption cost is parameter negotiation
  - once procedures negotiated, primary cost of encryption cost is bandwidth / silicon related

Some Conclusions

- **Important to address how external parties will send email securely to your domain**
  - **total cost calculations should address all aspects of email security**
  - **productivity / management costs associated with business partner's security solutions**
- **Recognize that sometimes encryption may not be possible with chosen solution**
  - **business partner non participation**
  - **need policy to address when plaintext message should be sent by alternative means**

Critical Review

Functional Requirements
Secure eMail Models
Advantages / Disadvantages
Conclusions

Common Requirements

- Encrypt message with symmetric key algorithm
  - key typically is randomly generated on a per message basis
  - same key used for encryption / decryption
- Mechanism to securely transmit message key to intended recipient
- Software support for decryption by recipient
- Source and message authenticity typically provided as adjunct to encryption solution

eMail Encryption Models

- **Public Key Standards based**

  1 **message level encryption**

  - S/MIME and DOMSEC
  - pgp/MIME

  4 **transport level encryption**

  - eSMTP STARTTLS

- **Proprietary solutions**

  2 **Web browser email over SSL/TLS**

  3 **Outsource Security Infrastructure**

1. Public Key Message encryption

- **S/MIME and PGP are ‘conventional methods for email encryption**
  - **randomly generate ‘message key’**
  - **encrypt message contents with symmetric key algorithm**
  - **encrypt message key using public encryption key of recipient and asymmetric encryption (RSA, Diffie-Hellman, etc)**
  - **‘envelope’ resulting ciphertext using standard format defined by s/MIME or pgp/MIME**
  - **recipient recovers message key using recipient's private decryption key**
  - **recovers message plaintext using the transmitted message key**

Advantages

- **Broad support thru bundled s/MIME capability**
  - **Outlook, Outlook Express, Netscape Messenger, Eudora, Notes, Groupwise, Pegasus, Mozilla, kMail …**
    - encryption and signature automatic with properly configured client
  - **pgp has been historical favorite of health plans & clearinghouse**
- **Ability to deliver confidential messages using ordinary SMTP mail**
- **In principle, no requirement to issue authentication credentials to external mail recipients**

DisAdvantages

- **Support generally lacking for non POP / IMAP consumer oriented email services, (e.g. AOL, Hotmail)**
  - **is this an issue with healthcare B2B or B2b email?**
- **Requires public key certificate of recipient**
  - **slow deployment of PKI**
  - **uncertain source for recipient's certificate ~ Verisign demonstrably *not* the answer**
- **Potential for high end user support costs if implementing at enterprise desktop**
  - **costs generally encapsulated in certificate cost**

Enterprise Implementation

- Information about source and target encapsulated in encryption / signing certificates
- s/MIME gateway products manage crypto at server level thru use of 'proxy' certificates
  - common public encryption key
  - certificates created as needed to bind common public key to distinct rfc822 email addresses of internal users
  - to external parties, gateway is transparent; indistinguishable from 'end to end' s/MIME
- DOM-SEC (rfc 3183) disambiguates domain level from end entity encryption and signing
  - naming standards for domain encryption / signing certs

2. Secure Web (browser) mail

- eMail is redirected to sender's enterprise store
- Recipient pulls mail from the store using HTTPs
- Message encryption and key exchange is provided at transport layer thru use of SSL / TLS
- Recipient authenticates to (sender's) web mail server

Account Management Issues

- "Account' must be established for individual recipient
  - involves an 'out of band' diligence process if security benefit to be achieved
- Some business partner role when recipient in a member business partner's workforce
  - authorization
  - account maintenance in light of workforce changes
- Synchronization with business partner's web strategy
  - potential for conflicting point solutions

Advantages

- **Works for the 'least common denominator' recipient.**
  - send secure mail to *any* recipient as only requires browser
- **Better management over 'inbound' return messages**
  - utilize web forms to structure response
- **Provides control over message disposition**
  - no reliance on external SMTP relay
  - provides some control over recipient storage, forwarding, copy / paste, etc
- **Feedback regarding end user receipt of mail**
  - ability to log the download of specific messages

DisAdvantages

- ‘One size fits all’ solution is cost inefficient
  - little ability to leverage recipient’s security infrastructure
- Account creation for external recipients
  - latency in delivery of ‘first’ message
  - potential for scalability issues and high support costs
  - uncertain policy and procedure
- New workflow requirements for recipient
  - leave email client to logon onto sender’s webmail site
  - difficult to maintain integrated email logs
- May encounter acceptance issues (by recipient)
  - inconvenient web forms

Improving the Model

- **Cost inefficiencies may be addressed by 'federation' of authentication credentials**
  - **sender verifies logon credential with 'authentication server' of business partner or other trusted source; attempts at cross domain SSO.**
    - Reach dependent on trading partner cooperation
  - **standards support thru SAML**

3. Outsource Security Infrastructure

- **Outsource supporting multiple delivery modes**
  - **SMTP using proprietary 'plug-in' (sender & recipient)**
  - **webmail**
- **Implemented at enterprise boundary & / or desktop**
- **Outsource establishes and maintains directory & account information of external recipients**
- **Multiple levels to service**
  - **directory service providing recipient encryption parameters. Mail subsequently sent using ordinary SMTP**
    - essentially a proprietary version of s/MIME
  - **resource to stage mail for subsequent delivery via webmail**
    - sender redirects mail to resource for subsequent pickup

Issues

- **Business partner's diligence in approving installation of proprietary plug-in**
  - **what motivates trading partner enterprise to do this in a timely fashion?**
  - **how does use of plug-in coincide with application of recipient enterprise policy**
    - e.g virus scanning, archiving, etc
- **What assures appropriate diligence by outsource?**
  - **reliance on vendor claims re proprietary swft & procedure**
  - **no clear evaluation guidelines like, say,**
    - ASTM e2212 Healthcare Standard Certificate Policy (PKI)
    - NIST FIPS 140-2 (cryptographic performance standards)

Advantages

- **Standard ASP value proposition**
  - lower entry cost
  - ‘pay with use’ pricing
- **Substitutes trading partner management problem with potentially simpler vendor management one**
  - may be more efficient use of enterprise resources

DisAdvantages

- **Uncertain total cost benefit**
  - Value proposition depends upon outsource's success
  - 'For profit' outsource most likely requires ROI greater than nonprofit HCO's internal 'hurdle rate'
  - If outsource does not acquire cost efficiency with scale, then value proposition unsound
- **Reliance on proprietary procedures**
  - conventional wisdom distrusts 'private' security
- **Promised benefits may depend on recipient use of proprietary plug-in**
  - enterprise must 'sell' outsource solution to maximize its obtained benefit

eSMTP STARTTLS

- **Transport layer security built into SMTP Relay**
  - **eSMTP command allows supplicant to request TLS handshake**
    - server authenticates with certificate, optional client auth
    - negotiation of encryption parameters
- **Relay to Relay encryption**
  - **confidentiality protection while data is in transit between SMTP relays ~**
    - does not protect against compromise of relay
    - traffic decrypted at relay for subsequent delivery / forwarding
- **Fair product support**
  - **Sendmail, Exchange, Notes**
  - **email security products, e.g. CertifiedMail, Tumbleweed**

Issues

- **Current utility probably limited to 'direct SMTP' with affiliated payers / providers and business associates**
  - **may not work for many HCO that outsource various SMTP functions**
  - **senders generally will not know how to authenticate receiver's *legitimate* ISP**
- **Has architectural implementations**
  - **must be implemented before any plaintext filtering or transformations**

Conclusions

- **Segmentation of recipient space**
  - hybrid solution may be required: B2B, B2b, B2C targets have differing capabilities & requirments
- **Utility of secure webmail greatest in B2C applications**
  - some HCO have abandoned webmail approaches due to business partner ‘acceptance’ issues
  - consumers have limited number of healthcare suppliers, ‘exceptional’ processing of particular HCO’s message less problematical
- **Requirement for standards based solution**
  - potentially highest acceptance rate in B2b sector

Some Vendors

- Vendor (Model)
  - CertifiedMail (2,3,4)
  - ClearSwift (1,2)
  - Hilgraeve (3)
  - OmTool (1,2)
  - Sigaba (3)
  - TFS (1,2)
  - Tumbleweed (1,2)
  - Zixit (3)
  - …. Many more

- Must test limits of vendor support for standard - sometimes incomplete, e.g. ‘send but not receive’
- Tend to hybridization in order to increase scope of solution
- good vendor review in Feb 2003, SC Magazine

Rethinking s/MIME
&
the ‘Death’ of PKI

The Problem with PKI
New Models for Certificate Distribution
Ongoing Trials in California

Some indications of life to PKI ...

- Limited HCO enterprise application, ie Kaiser
- Pharmaceutical and medical device manufacturers implementing digital signatures in response to CFR 21 Part 11
  - Johnson & Johnson
- Recent Federal Government PKI deployment conference driven in part by GPEA
  - 200 + attendees from many Fed agencies
- PKI is central to Win2k / Win2003 security
  - certs in every win2k / XP pro workstation
  - MSFT distributed certs on smart card to 60K employees
  - PKI becomes part of the enterprise infrastructure

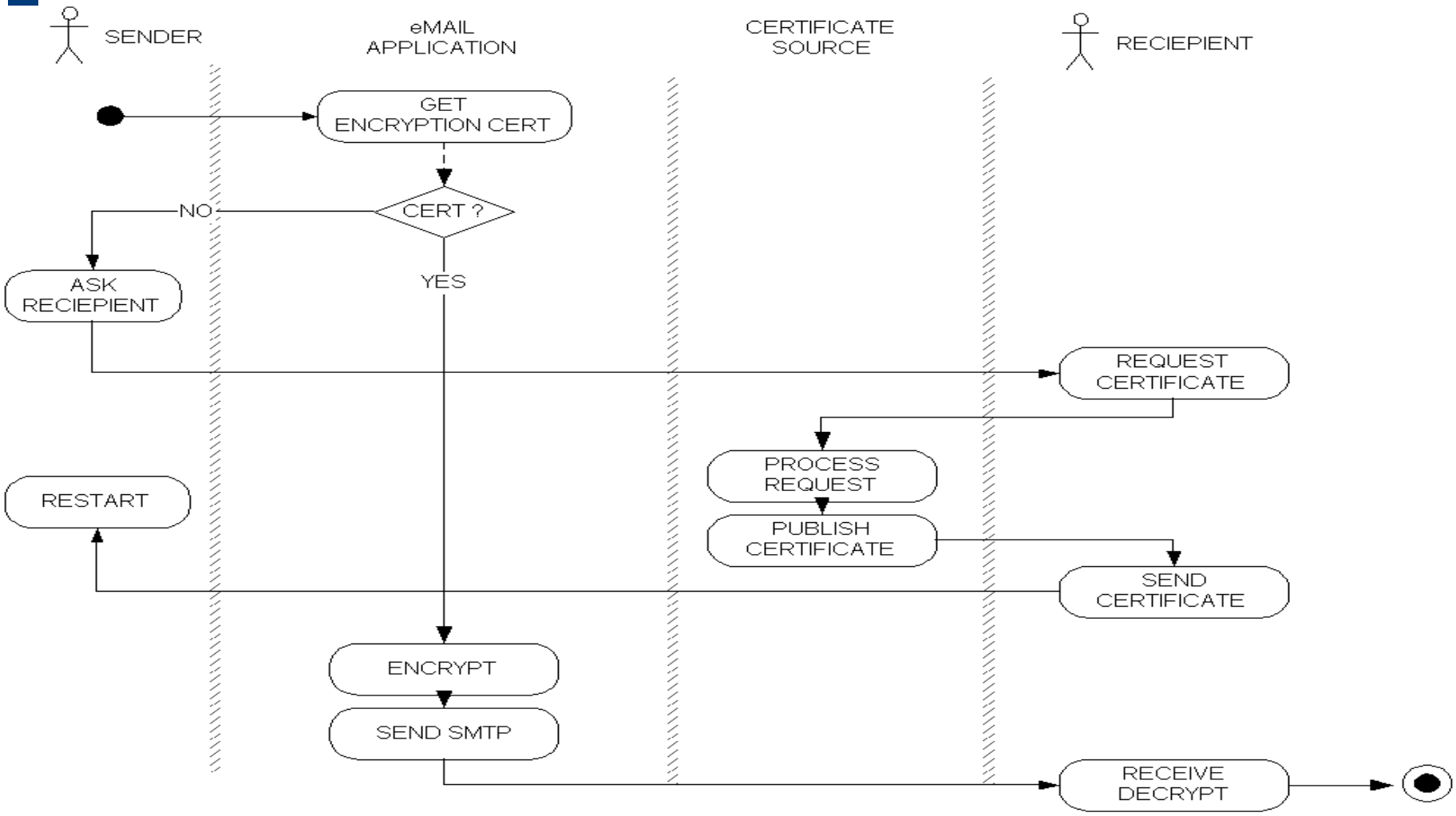
What about email support?

- **Current PKI utilization focuses on enterprise application; exposure to trading partners 'on the shelf'**
  - **absent broad PKI deployment, HCO do not recognize case for publishing internal certificate directory**
- **Secure eMail requires the certificates of recipients; i.e. PKI must be deployed *outside* the enterprise**
- **s/MIME use awaits reliable source for recipient's certificates**

Problem with PKI

- **Approach to industry scale PKI based on on a 'consumer pull' model where cert distribution awaits subscriber request**
  - **implemented in PKCS#10 and CRS**
  - **subscriber creates key pair and sends public portion to CA; CA writes and publishes certificate**
- **Inappropriate assignment as technical responsibilities fall to unprepared end users**
  - **"what is a certificate?"**
  - **"why should I be concerned about this?"**
- **Poor workflow design that places 'unprepared' in middle of cert request / distribution process without adequate feedback mechanism**

Typical s/MIME Workflow



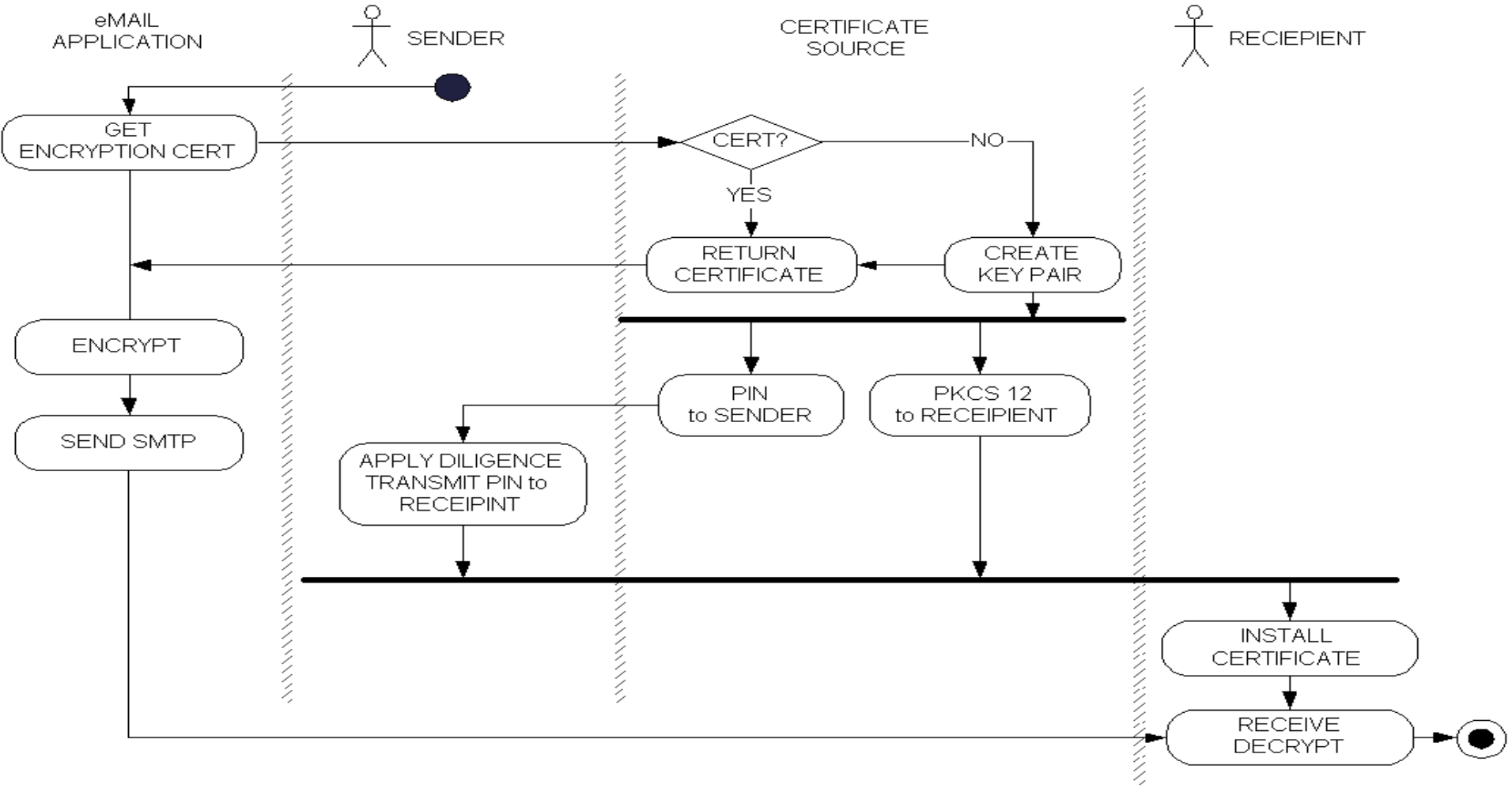
Implementation Deficiencies

- **Process suffers from lack of enterprise P&P**
  - if recipient does not have a cert, what instruction is communicated and by whom?
  - what happens to the message while awaiting receipt of receipient's certificate?
- **Lack of feedback mechanism**
  - sender uncertain about if and when recipient initiates / completes cert application
  - error reporting?
- **Usability issues with CRS / PKCS#10 based applications**
  - must simplify end user task

Improving the Workflow

- **Simplify requirements placed on end users, both sender and recipient**
  - **seek 1-click process**
- **Minimize latency in certificate acquisition**
  - **allow message encryption to proceed w/o awaiting completion of cert related diligence**
  - **improves reliability and security of system**
- **Support feedback to sender on status of message delivery and certificate application**

Improved s/MIME Workflow



Industry Trial

- **Ongoing California effort to address broad applicability of standards based email solutions**
  - **5 hospital systems; large multi-state to small regional**
  - **4 commercial payers; (3 'unofficially')**
  - **2 professional associations; physicians, transcriptionist**
  - **vendors; PKI software, email gateways, OS**
- **Goals**
  - **trial the 'improved s/MIME related workflow"**
  - **develop business strategies, especially with respect to**
    - specific health plans
    - SME business associates
  - **develop the email security business case**
  - **establish some 'best practices' guidelines**

For more info

- **To audit the California workgroup activity and receive its work product, email**
  - **to: subscribe@tunitas.com**
  - **subject: community trial**

Last Words

- **eMail security is difficult due to heterogeneity of communication targets**
  - **involves more than mere configuration of vendor product**
- **Important to first understand your organization's use of electronic mail; need to audit**
  - **who in the organization is sending confidential info by email**
  - **to whom. What are the actual (rather than assumed) capabilities of these targets**
  - **for what purpose**

Some References

- NIST SP 800-45 “Guidelines on Electronic Mail Security”
  - http://csrc.nist.gov/publications/nistpubs/800-45/sp800-45.pdf
- “Why Johnny Can’t Encrypt”
  - http://www.cs.cmu.edu/~alma/johnny.pdf
- “Solving Healthcare’s eMail Security Problem”
  - http://www.giac.org/practical/GSEC/Bill_Pankey_GSEC.pdf
- PK3i White Papers related to secure email and PKI
  - http://www.pk3i.com/whitepapers/