Secure E-mail: An Implementation Success Story

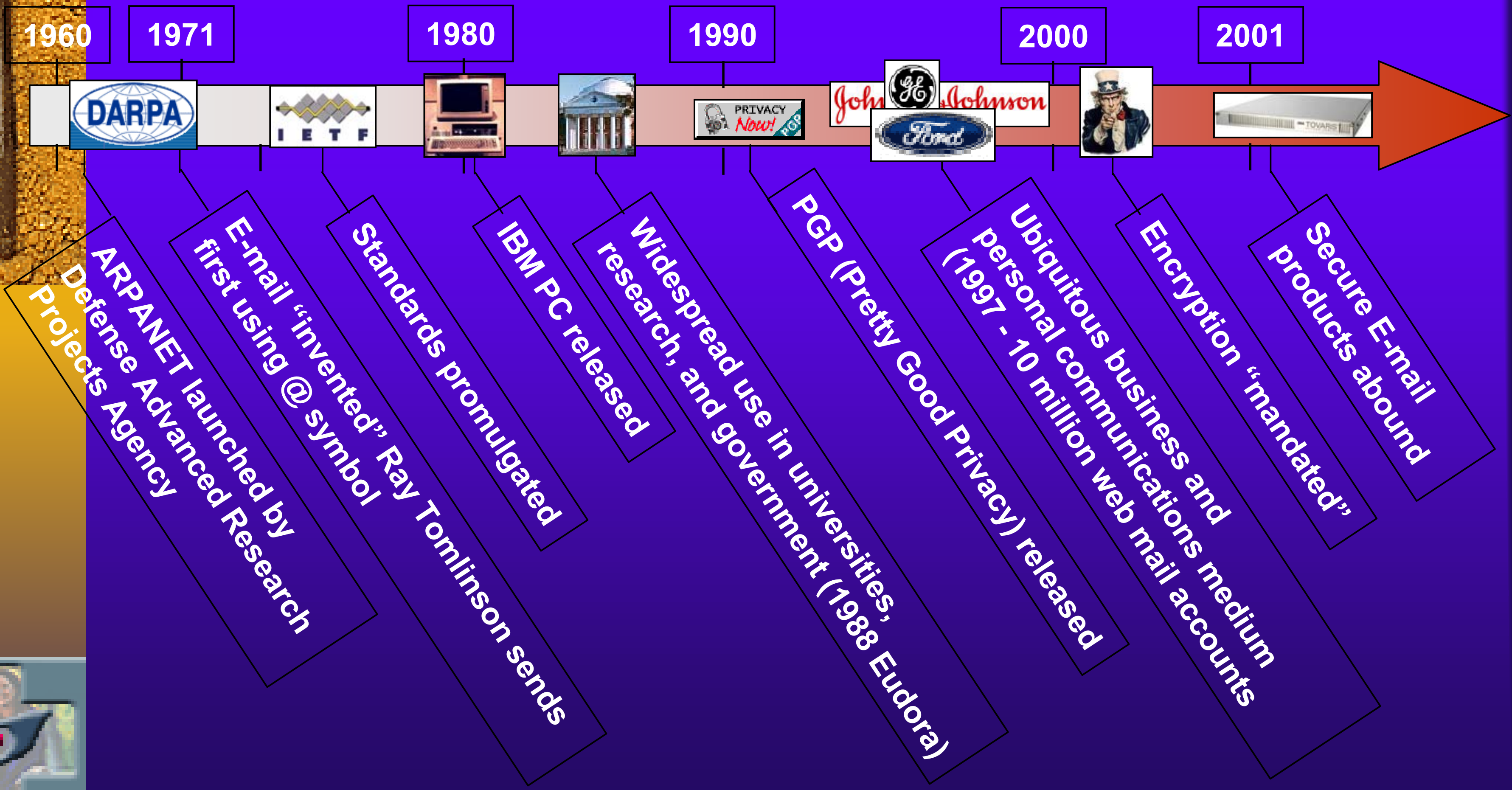
How Texoma Healthcare System Identified & Addressed its Secure E-mail Requirements

Presented by
Jeff Kerber, Former Corporate Privacy Officer
and HIPAA Compliance Director
Texoma Healthcare System
March 8, 2004

Agenda

- A Brief History of E-mail
- The Obligatory HIPAA Review
- Vulnerabilities and Cryptography
- The THCS Experience
- The Highlights and “Take-aways”

Brief History of E-mail

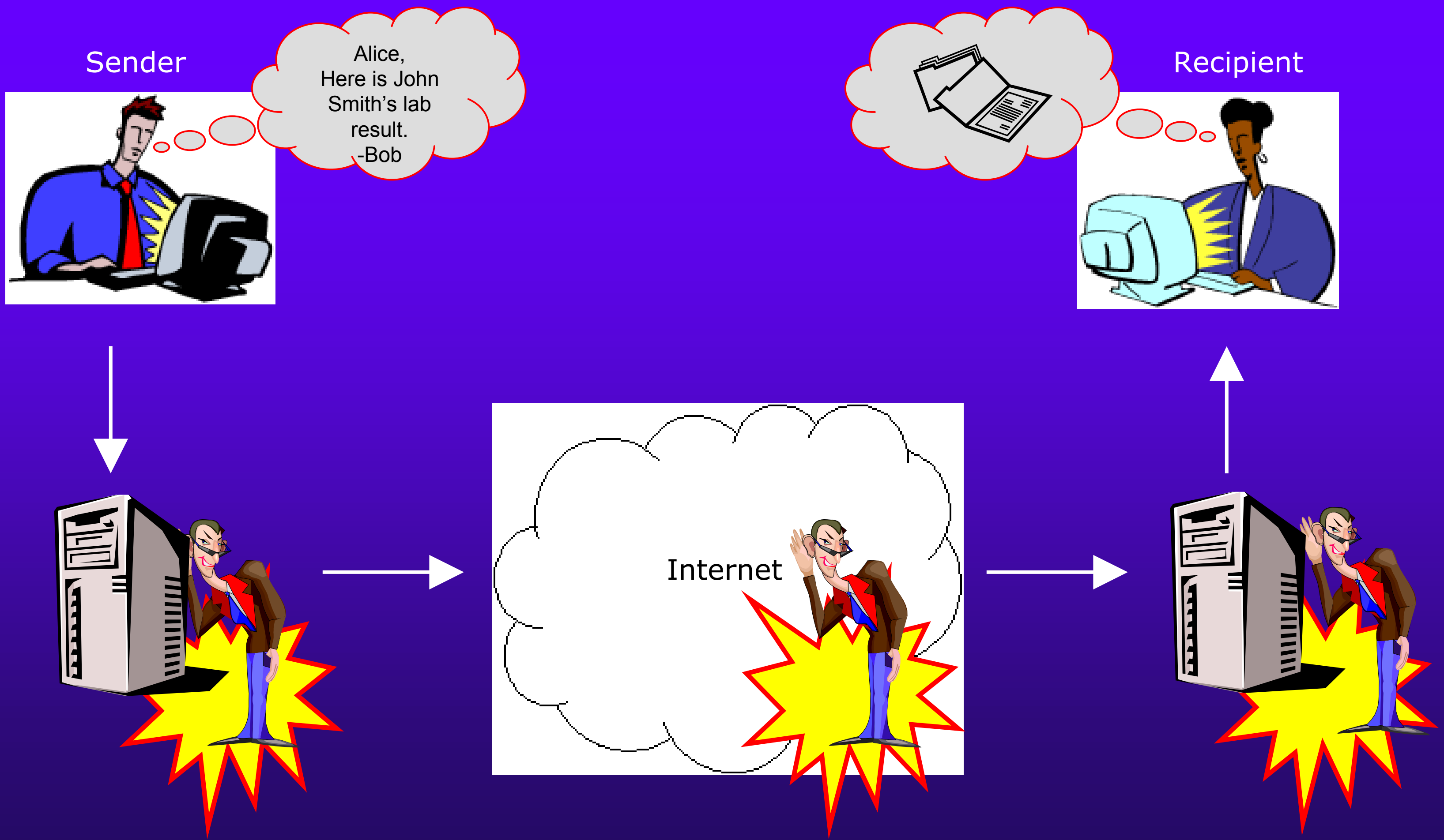


- 1960 – ARPANET launched by Defense Advanced Research Projects Agency
- 1971 – E-mail "invented" Ray Tomlinson sends first using @ symbol
- Standards promulgated
- 1980 – IBM PC released
- Widespread use in universities, research, and government (1988 Eudora)
- 1990 – PGP (Pretty Good Privacy) released
- Ubiquitous business and personal communications medium (1997 - 10 million web mail accounts
- 2000 – Encryption "mandated"
- 2001 – Secure E-mail products abound

The Obligatory HIPAA Review

- Defining Covered Entities
- The Privacy Rule and Security Rule
  - 164.530(c)(1) and (2) a.k.a. “Mini-Security Rule
  - Security Rule, Technical Specifications 164.312 (a)(2)(iv) (Addressable)
  - Security Rule, Technical Specifications 164.312 (e)(2)(ii) (Addressable)
- April 14, 2003 and April 21, 2005
- Reasonable Effort

E-mail Security Vulnerabilities



Sender

Alice,
Here is John Smith’s lab result.
-Bob

Recipient

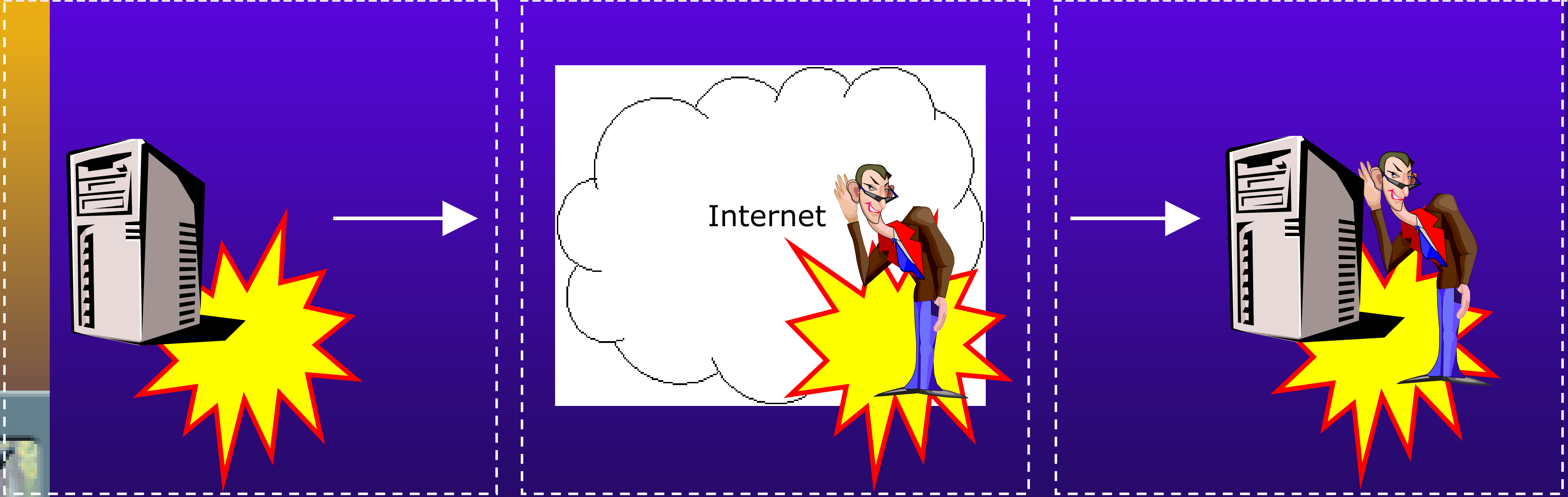
Internet

Potential Attacks

- Mail server hack
- Malware install
- Intranet sniff
- Unencrypted E-mail

- Internet sniffing
- DNS spoofing
- Mail router hack
- Unencrypted E-mail

- Mail server hack
- Malware install
- Intranet sniff
- Unencrypted E-mail



Encryption is a Solution

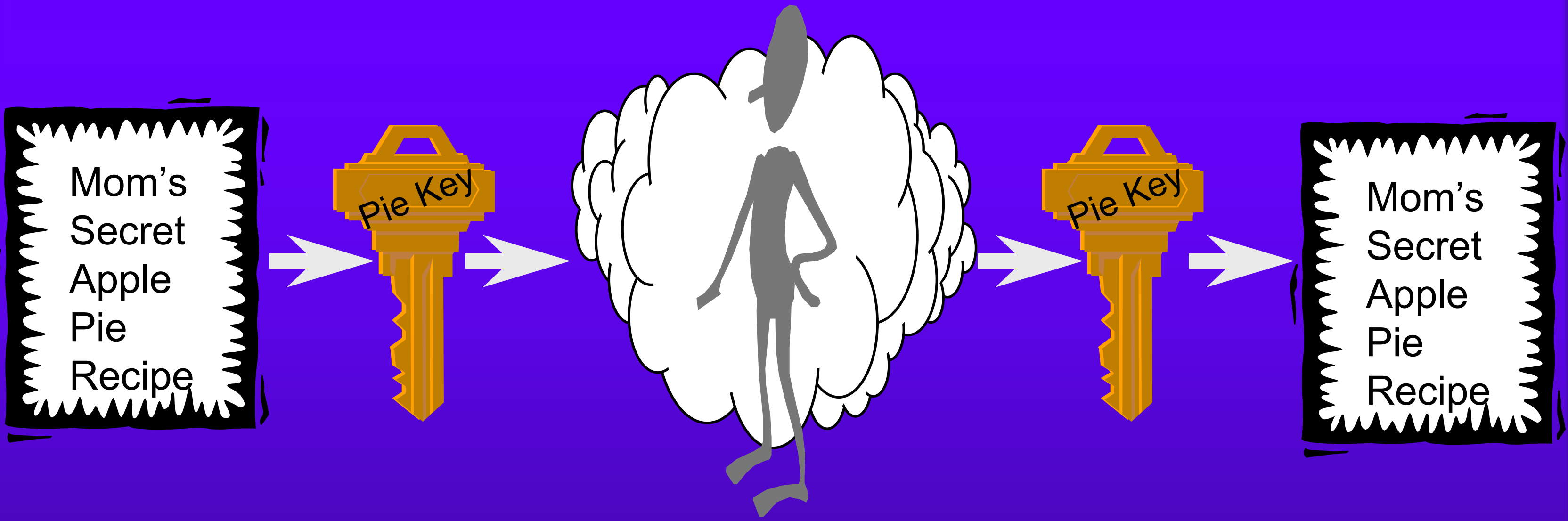
- Mail server hack
- Malware install
- Intranet sniff
- Unencrypted E-mail

- Internet sniffing
- DNS spoofing
- Mail router hack
- Unencrypted E-mail

- Mail server hack
- Malware install
- Intranet sniff
- Unencrypted E-mail

ADDRESSED WITH ENCRYPTION

Cryptography Concepts: Symmetric Cryptography

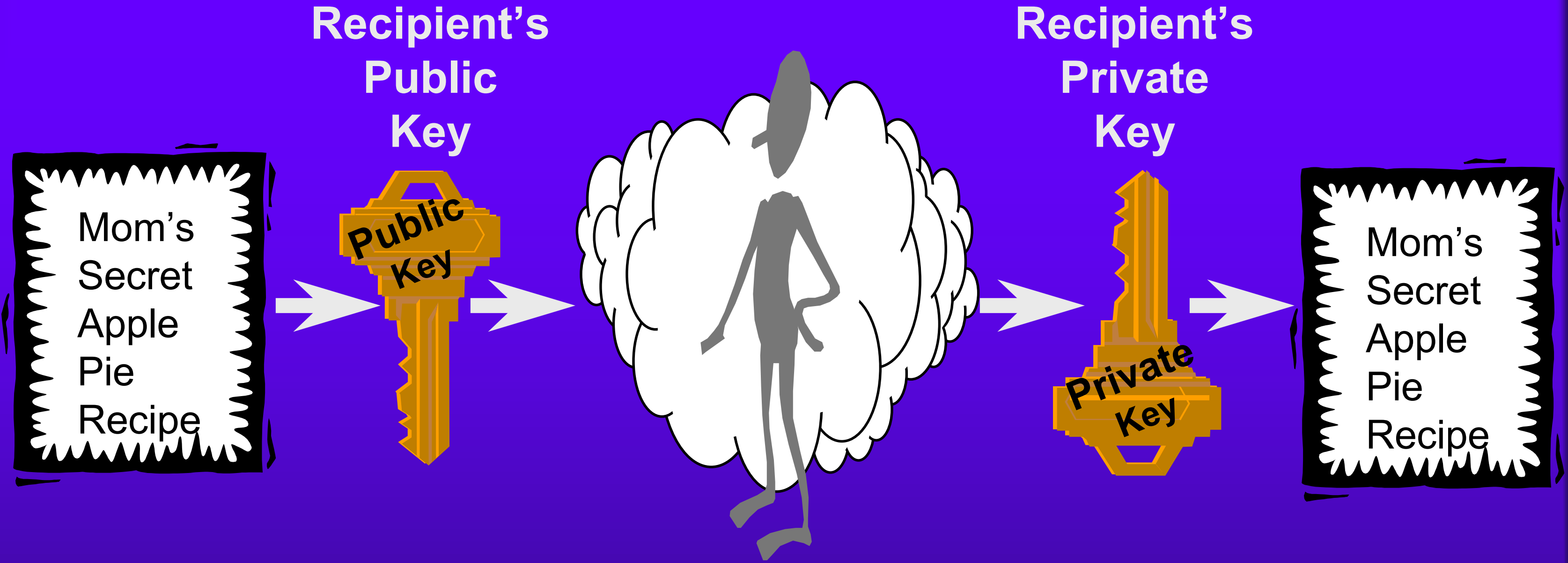


The same key is used to encrypt and decrypt the data.
DES is one example, RC4 is another.

Cryptography Concepts:
Symmetric Cryptography

- Advantages
  - Secure
  - Widely Used
  - The encrypted text is compact
  - Fast
- Disadvantages
  - Complex Administration
  - Requires Secret Key Sharing
  - Large Number of Keys (# Keys = N*(N-1)
  - No non-repudiation
  - Subject to interception

Cryptography Concepts: Asymmetric Cryptography



What is encrypted with one key,
can only be decrypted with the other key.
RSA is one example, Elliptic Curve is another.

Cryptography Concepts: Trusting the Public Key

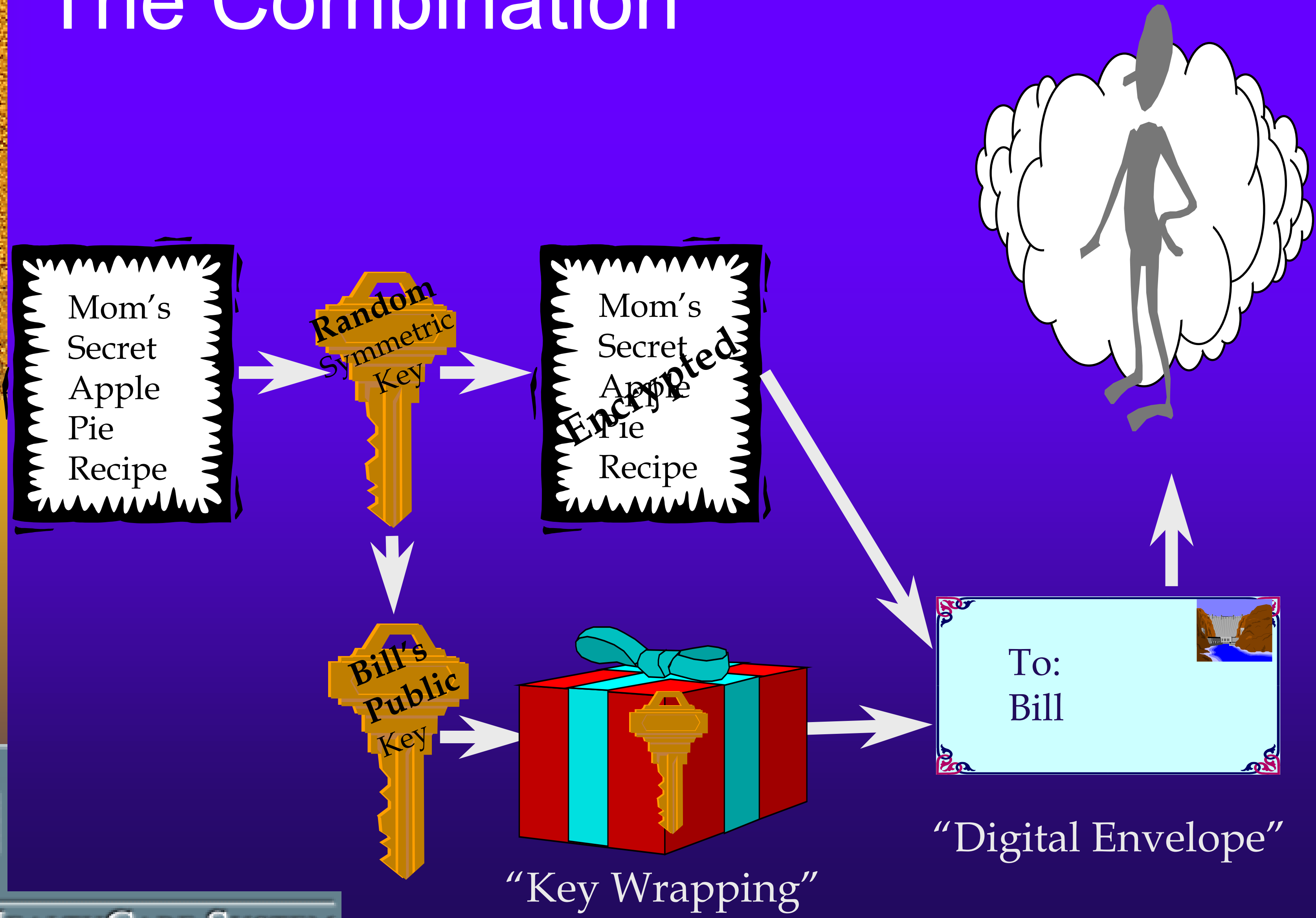
X.509 Digital Certificate

*"I officially notarize the association between this particular **User**, and this particular **Public Key**"*

Cryptography Concepts: Asymmetric Cryptography

- Advantages
  - Secure
  - No secret sharing
  - No prior relationship
  - Easier Admin
  - Many fewer keys
  - Supports non-repudiation
- Disadvantages
  - Slower than symmetric key
  - The encrypted text is larger than a symmetric version

Cryptography Concepts: The Combination



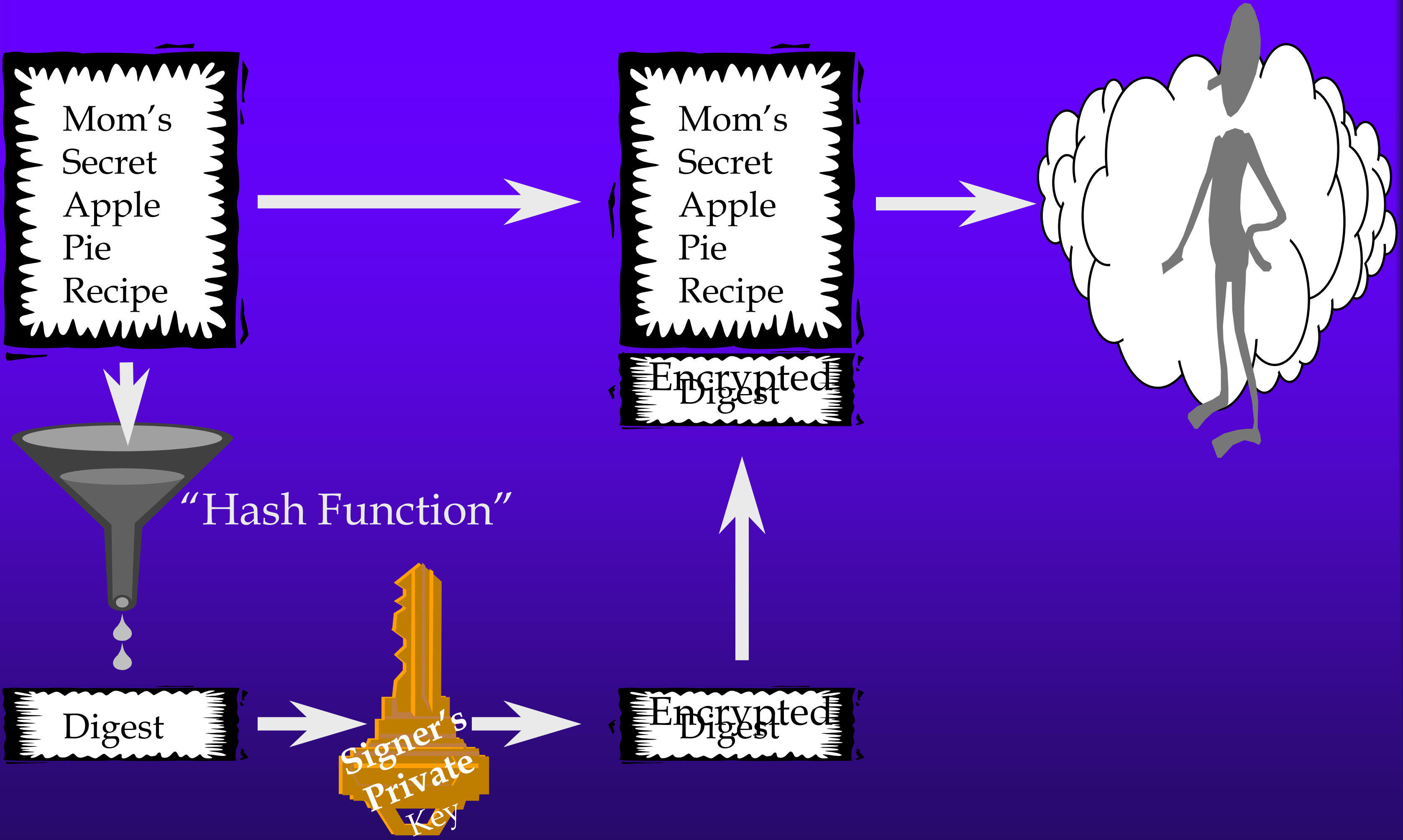
"Key Wrapping"

"Digital Envelope"

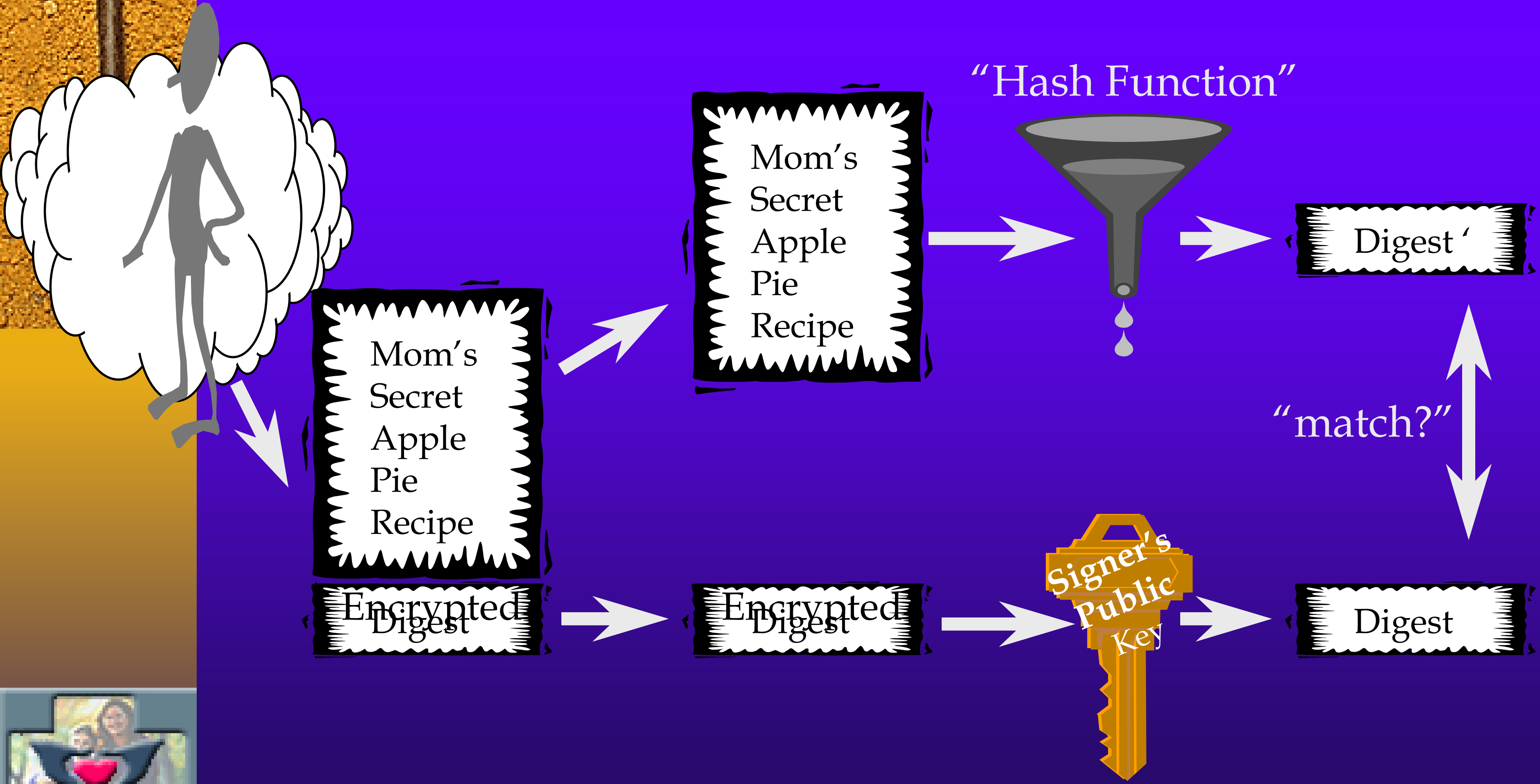
Cryptography Concepts: The Combination

- ♦ You get the best of both worlds
  - – The benefits of Symmetric Key
    - Speed
    - Compact Encrypted Text
  - – The benefits of Public Key
    - Simpler Key management
    - Digital Signature
    - Non-Repudiation

Cryptography Concepts: Digital Signatures



Cryptography Concepts: Digital Signatures

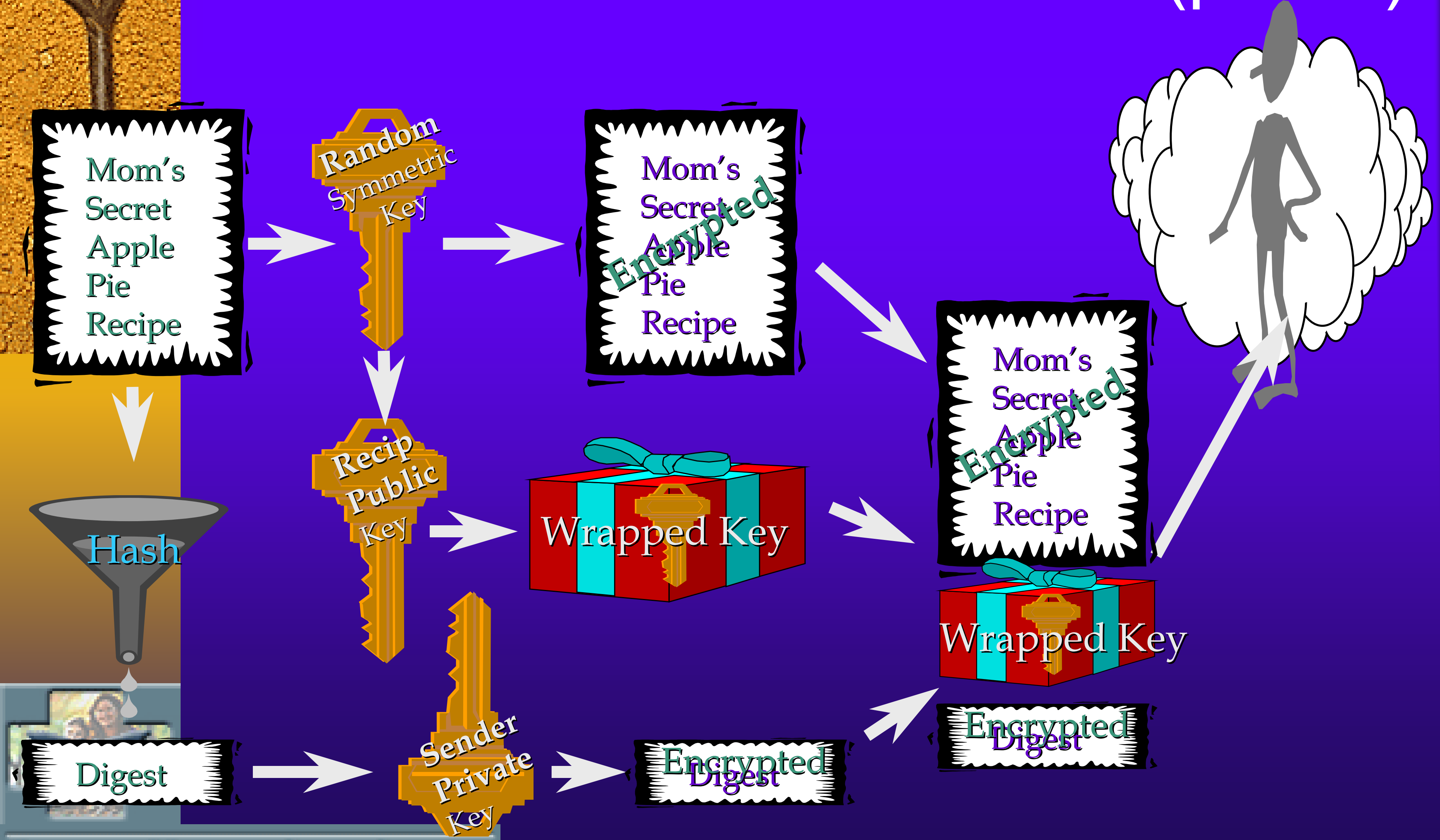


TEXOMA HEALTHCARE SYSTEM

Cryptography Concepts: The Secure E-mail Problem

- What would the steps be to do send a message with the following properties:
  - It cannot be read by anyone but the intended recipient
  - The recipient can assure it was not modified in transit
  - The recipient can verify who authored the message
  - The recipient cannot later claim that they didn’t send it

Crypto Concepts:
The Secure E-mail Solution (part 1)



Mom's Secret Apple Pie Recipe

Random Symmetric Key

Encrypted Mom's Secret Apple Pie Recipe

Hash

Digest

Recip Public Key

Wrapped Key

Sender Private Key

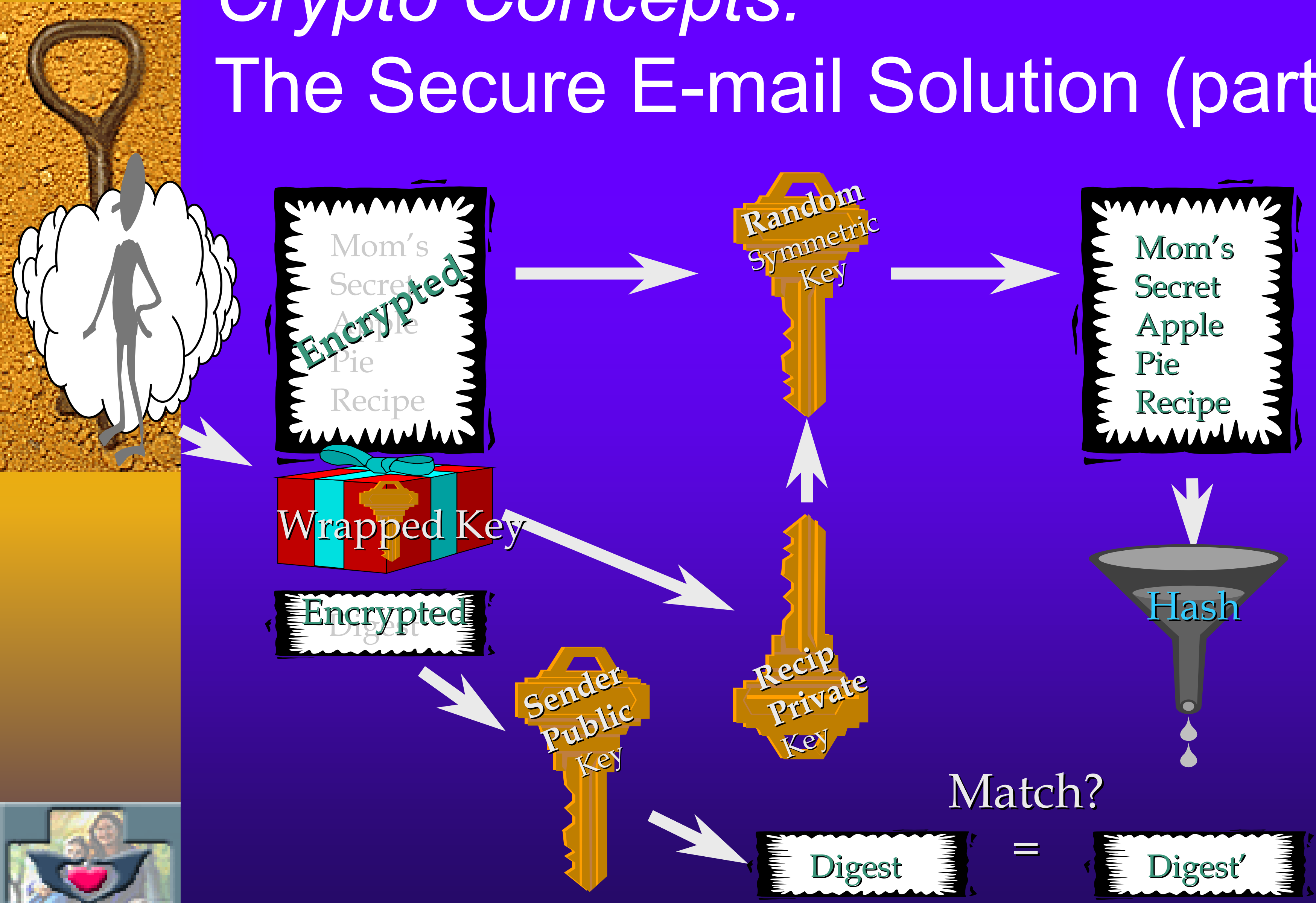
Encrypted Digest

Encrypted Mom's Secret Apple Pie Recipe

Wrapped Key

Encrypted Digest

Crypto Concepts: The Secure E-mail Solution (part 2)



The THCS Experience

- Our decision-making team
  - CIO and CFO
  - HIPAA Compliance Officer, CPO
  - Operations
  - Decision Support
  - Network Manager
  - IS Support Services

The THCS Experience

- Requirements Analysis
  - Ease of use
  - Zero client footprint (senders and recipients)
  - Key distribution and management
  - Proven encryption technology
  - Control of message store

The Three Challenges of Secure E-mail

- ❑ THCS users can’t use encryption—it’s too difficult!
- ❑ How do we send secure messages to recipients with no digital certificate?
- ❑ Manual certificate exchange is impossible to manage with our business partners.

The THCS Experience

- **Minimum system requirements for SecureMessenger message retrieval**
  - Message retrieval is intuitive
  - Message links are common industry practice (airlines, banks, greeting cards)
  - Works with AOL, Yahoo!, Hotmail
- **Can’t assume recipients will be able or willing to download, install, or use a plug-in or separate secure E-mail application**
  - Individual recipients
  - Physicians
  - Business Associates

The THCS Experience

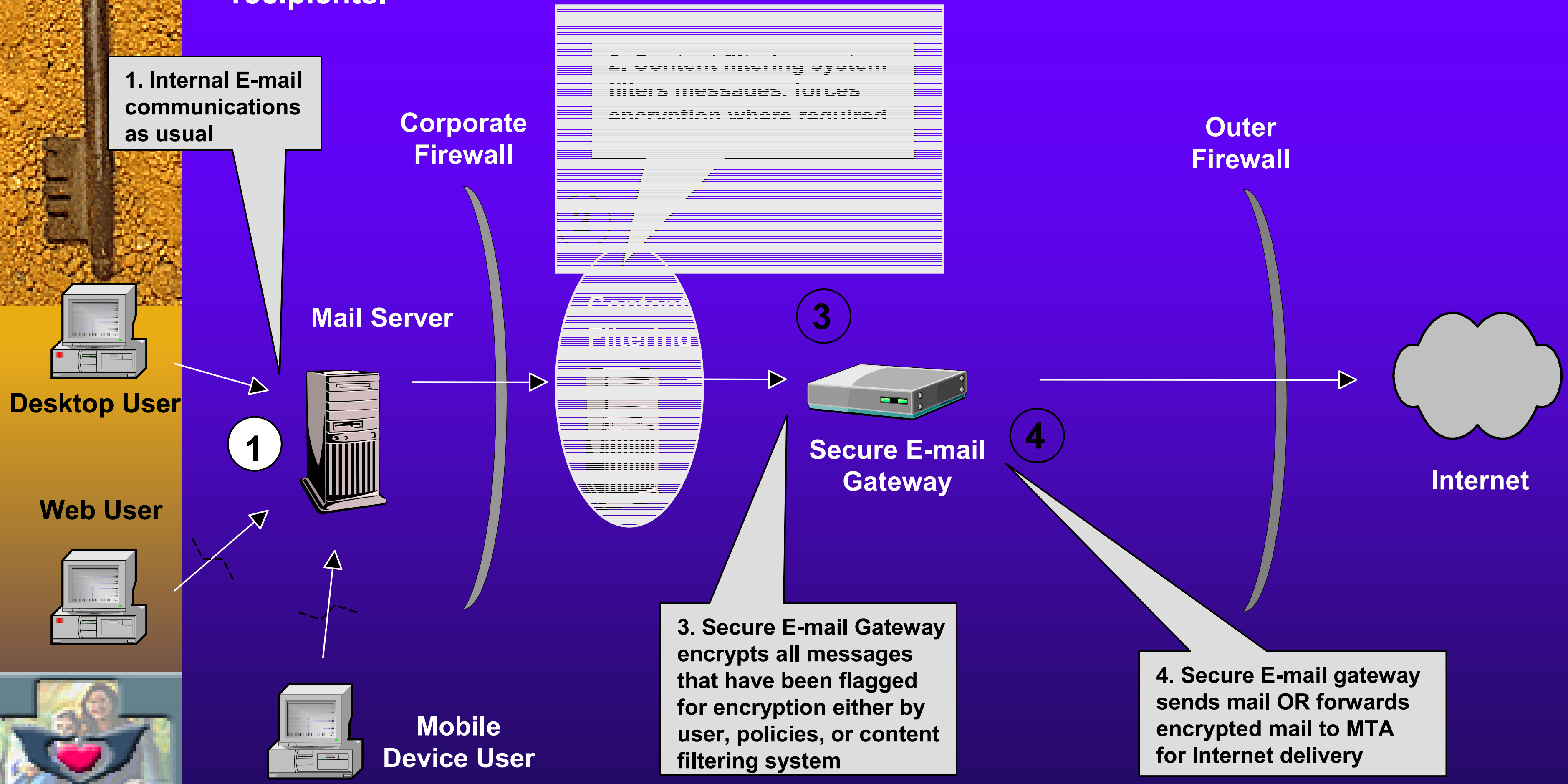
- Product Review and Selection
  - Concentrated on secure messaging vendors
  - Avoided complicated PKI vendors
  - Understood HIPAA regulations
  - Demos
  - In-house trials

The THCS Experience

- Implementation and Integration
  - Well-documented install preparation and process
  - Drop it in and go
  - Excellent training

Secure E-mail Gateway

E-mail security appliance component provides seamless E-mail encryption and decryption services to THCS employees, clinicians, other enterprise users, and remote recipients.



1. Internal E-mail communications as usual

2. Content filtering system filters messages, forces encryption where required

3. Secure E-mail Gateway encrypts all messages that have been flagged for encryption either by user, policies, or content filtering system

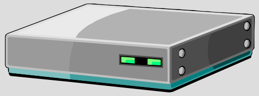
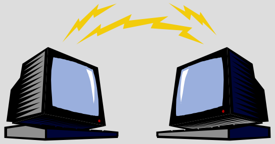
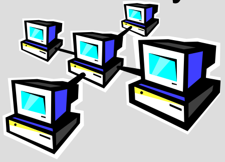
4. Secure E-mail gateway sends mail OR forwards encrypted mail to MTA for Internet delivery

Unified Secure Messaging Platform

S/MIME Appliance

Universal Secure Delivery

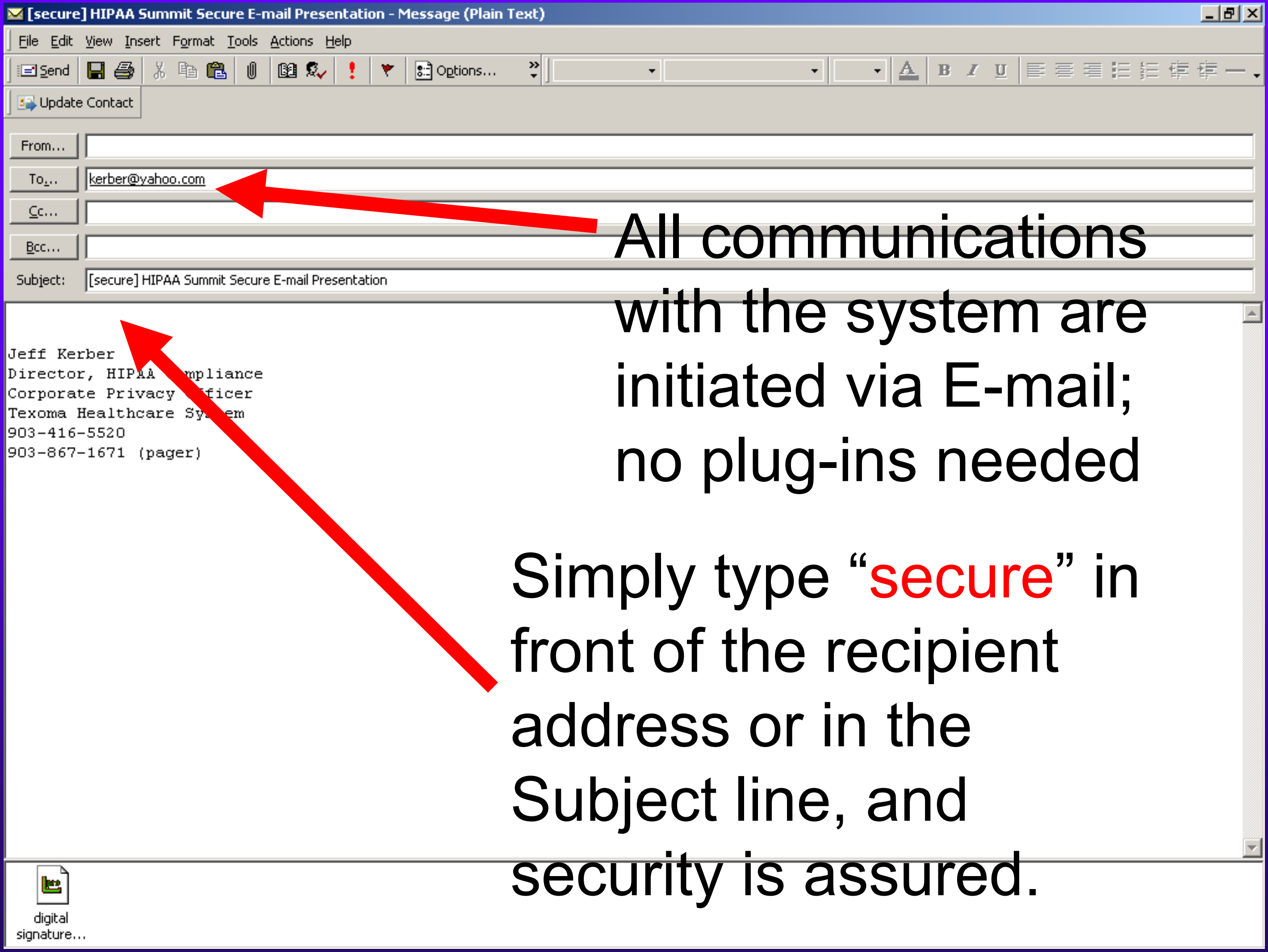
Global Certificate Network

Product	Description
Secure E-mail Gateway 	• Plug-and-play E-mail security appliance • Automatic certificate lookup and harvesting • Automatic encryption and decryption • Digital signatures
Secure Web Server 	• Secure E-mail Gateway universal secure messaging feature • Enables secure E-mail to any recipient, requiring only: – Web browser (SSL-capable) – E-mail address and application
Secure Gateway Network 	• Scalable backbone network • Connects Secure E-mail Gateway appliances • Management and distribution of standard X.509 digital certificates (public keys) • Automatic certificate lookup on every message

The THCS Experience

- Authentication of Non-S/MIME Recipients
  - Establishing a pass phrase
  - Communicating the pass phrase

Sending Secure E-mail: Manual Message Flag


[secure] HIPAA Summit Secure E-mail Presentation - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Send
Options...
Update Contact
From...
To...
Cc...
Bcc...
Subject:
digital signature...

To: kerber@yahoo.com

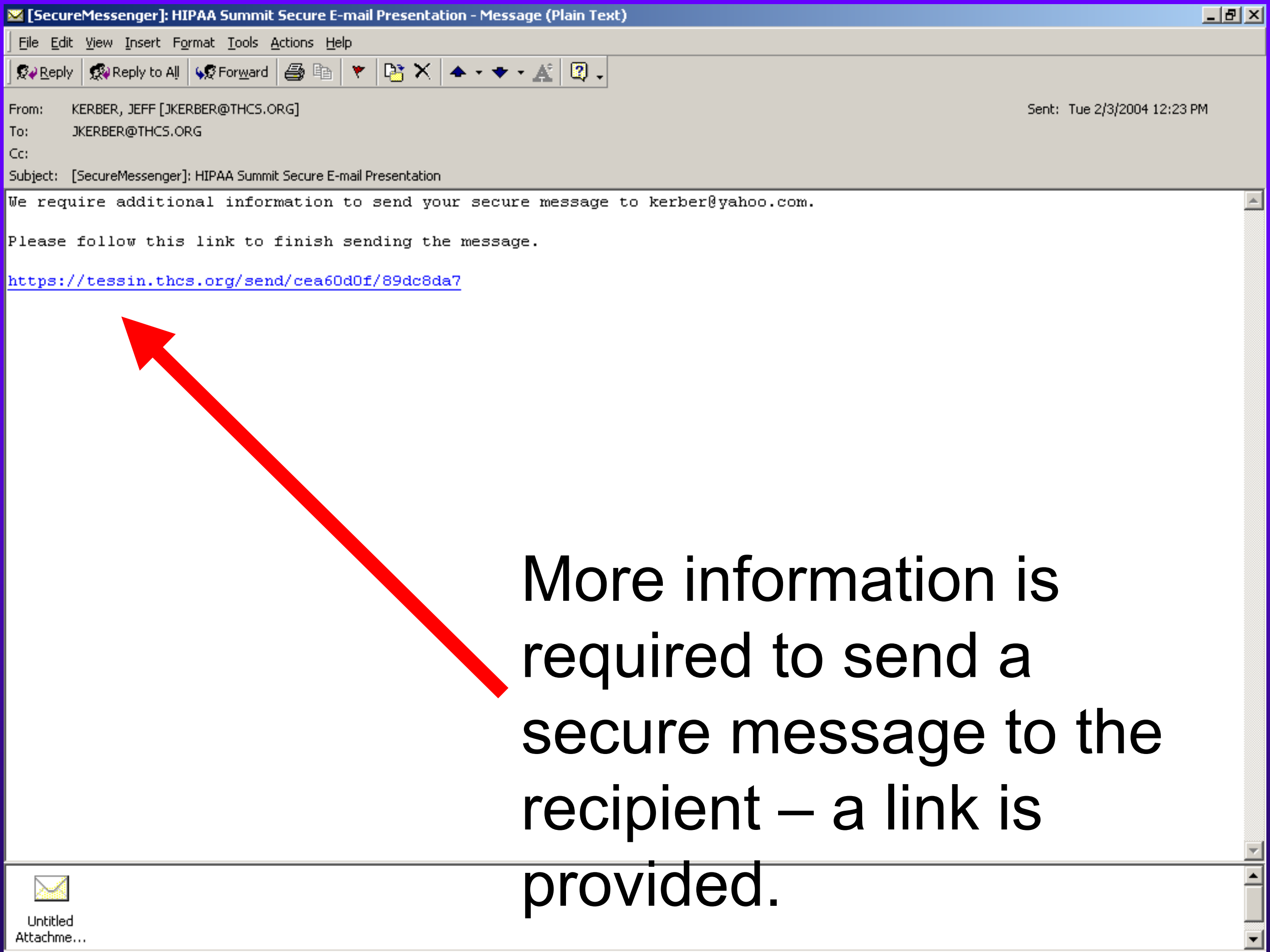
Subject: [secure] HIPAA Summit Secure E-mail Presentation

```
Jeff Kerber
Director, HIPAA Compliance
Corporate Privacy Officer
Texoma Healthcare System
903-416-5520
903-867-1671 (pager)
```

All communications with the system are initiated via E-mail; no plug-ins needed

Simply type "secure" in front of the recipient address or in the Subject line, and security is assured.

Sending Secure E-mail: Manual Message Flag



[SecureMessenger]: HIPAA Summit Secure E-mail Presentation - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward
Untitled Attachme...

From: KERBER, JEFF [JKERBER@THCS.ORG]

Sent: Tue 2/3/2004 12:23 PM

To: JKERBER@THCS.ORG

Cc:

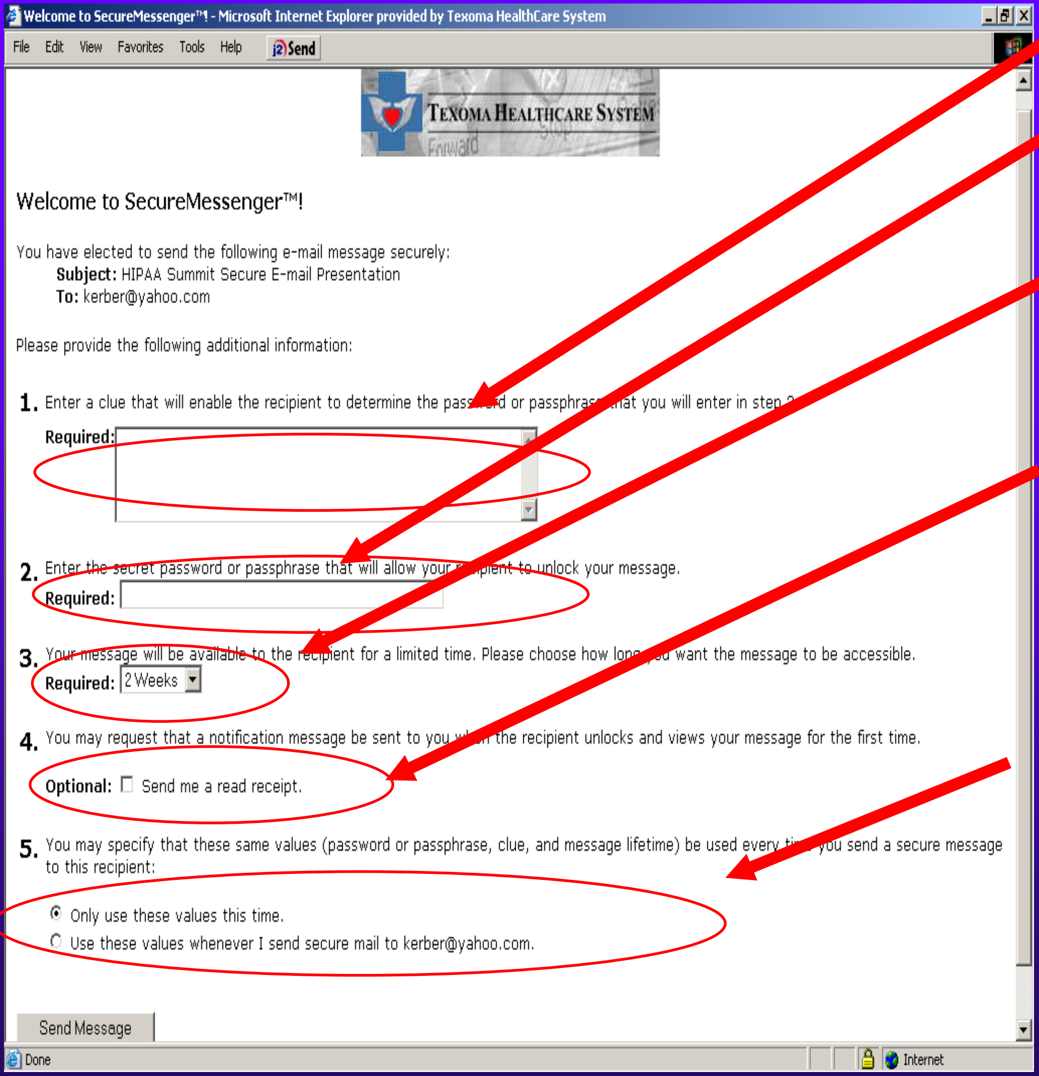
Subject: [SecureMessenger]: HIPAA Summit Secure E-mail Presentation

```
We require additional information to send your secure message to kerber@yahoo.com.

Please follow this link to finish sending the message.

https://tessin.thcs.org/send/cea60d0f/89dc8da7
```

More information is required to send a secure message to the recipient – a link is provided.

Texoma HealthCare System

Sending Secure E-mail: Preparing to Encrypt


Welcome to SecureMessenger™! - Microsoft Internet Explorer provided by Texoma HealthCare System
File
Edit
View
Favorites
Tools
Help
j2Send
TEXOMA HEALTHCARE SYSTEM
Done
Internet

Welcome to SecureMessenger™!

You have elected to send the following e-mail message securely:

Subject: HIPAA Summit Secure E-mail Presentation
To: kerber@yahoo.com

Please provide the following additional information:

1. Enter a clue that will enable the recipient to determine the password or passphrase that you will enter in step 2.

Required:

2. Enter the secret password or passphrase that will allow your recipient to unlock your message.

Required:

3. Your message will be available to the recipient for a limited time. Please choose how long you want the message to be accessible.

Required: 2 Weeks

4. You may request that a notification message be sent to you when the recipient unlocks and views your message for the first time.

Optional: ☐ Send me a read receipt.

5. You may specify that these same values (password or passphrase, clue, and message lifetime) be used every time you send a secure message to this recipient:

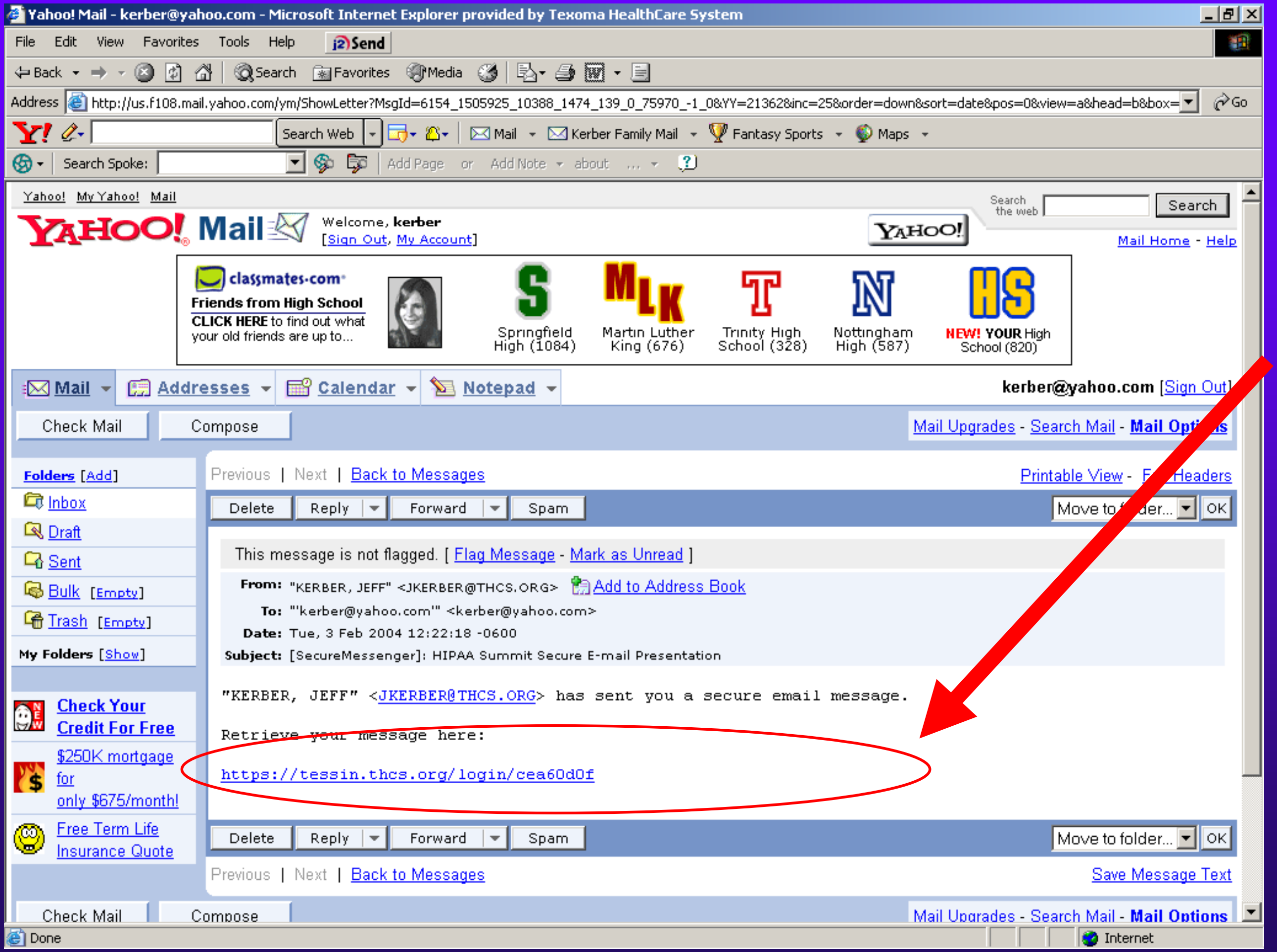
● Only use these values this time.
○ Use these values whenever I send secure mail to kerber@yahoo.com.

Send Message

1. Enter clue (challenge)
2. Enter password (response)
3. Establish message lifetime
4. Request real-time message tracking/delivery receipt
5. Click button to always use this clue/password and other settings for this recipient

TEXOMA HEALTHCARE SYSTEM

Sending Secure E-mail: Recipient Notification



Yahoo! Mail - kerber@yahoo.com - Microsoft Internet Explorer provided by Texoma HealthCare System

Address http://us.f108.mail.yahoo.com/ym/ShowLetter?MsgId=6154_1505925_10388_1474_139_0_75970_-1_0&YY=21362&inc=25&order=down&sort=date&pos=0&view=a&head=b&box=

Welcome, kerber [Sign Out, My Account]

kerber@yahoo.com [Sign Out]

This message is not flagged. [Flag Message - Mark as Unread]

From: "KERBER, JEFF" <JKERBER@THCS.ORG> Add to Address Book

To: "'kerber@yahoo.com'" <kerber@yahoo.com>

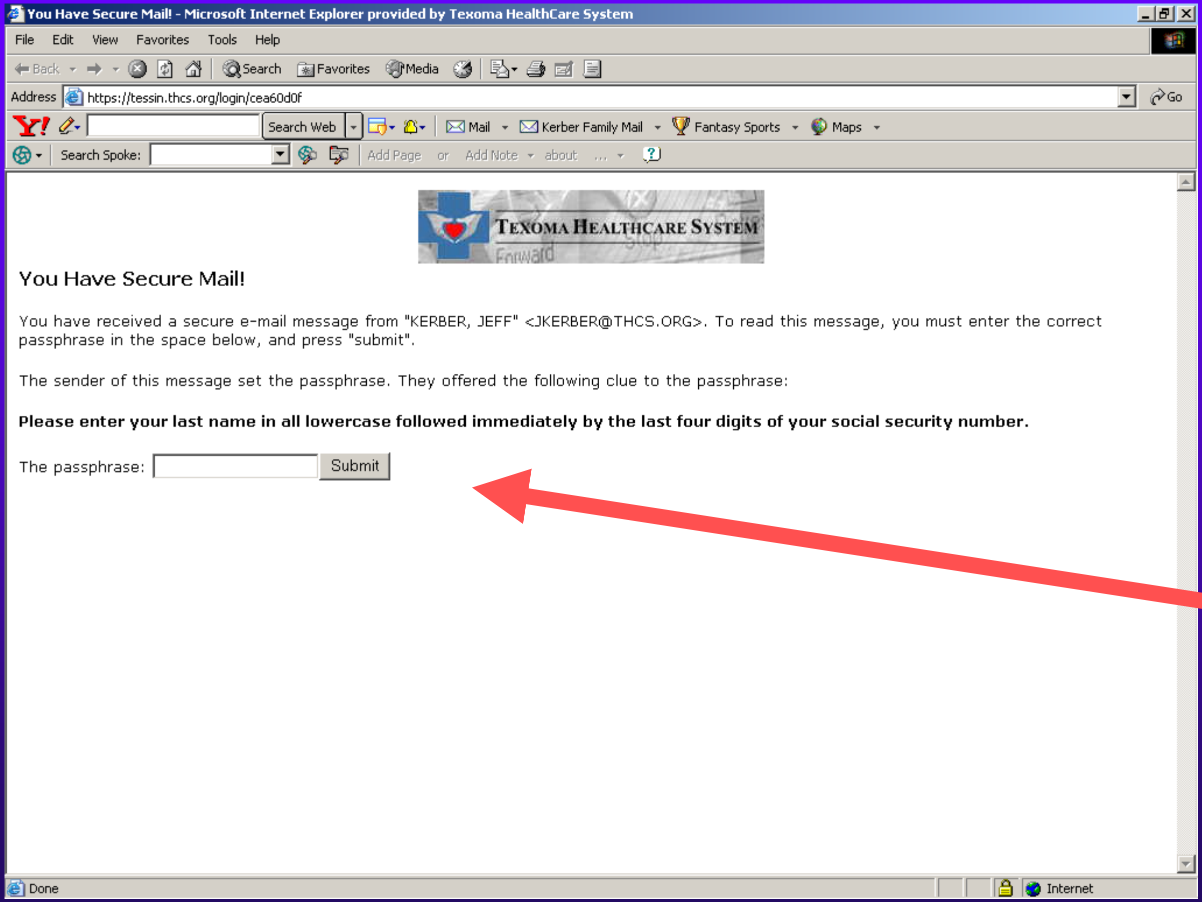
Date: Tue, 3 Feb 2004 12:22:18 -0600

Subject: [SecureMessenger]: HIPAA Summit Secure E-mail Presentation

```
"KERBER, JEFF" <JKERBER@THCS.ORG> has sent you a secure email message.

Retrieve your message here:

https://tessin.thcs.org/login/cea60d0f
```

Link will invoke web browser and establish the secure SSL connection for the recipient.

Sending Secure E-mail: Preparing to Decrypt


You Have Secure Mail! - Microsoft Internet Explorer provided by Texoma HealthCare System
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://tessin.thcs.org/login/cea60d0f
Go
Search Web
Mail
Kerber Family Mail
Fantasy Sports
Maps
Search Spoke:
Add Page or Add Note about
TEXOMA HEALTHCARE SYSTEM
Forward
Stop
Done
Internet

You Have Secure Mail!

You have received a secure e-mail message from "KERBER, JEFF" <JKERBER@THCS.ORG>. To read this message, you must enter the correct passphrase in the space below, and press "submit".

The sender of this message set the passphrase. They offered the following clue to the passphrase:

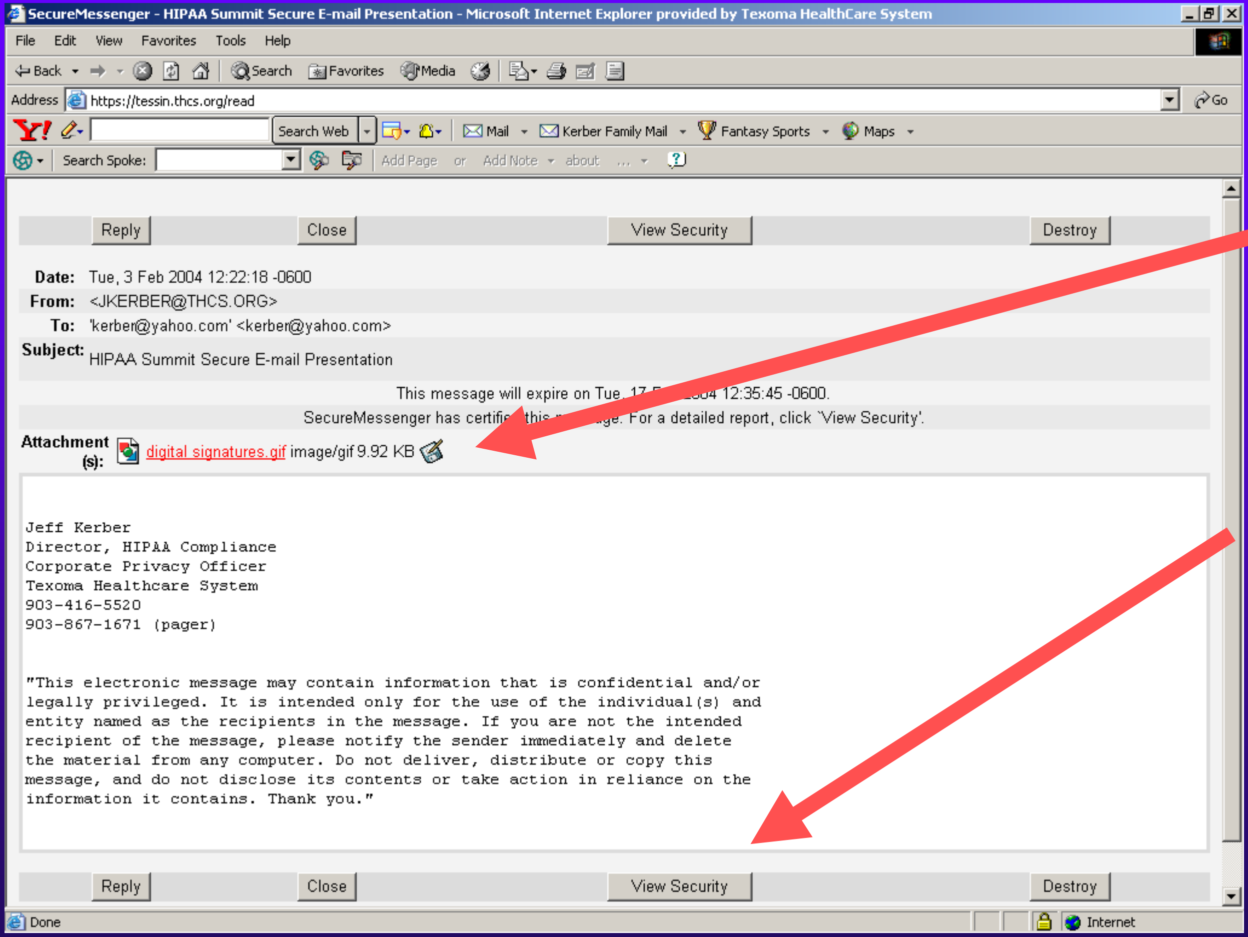
Please enter your last name in all lowercase followed immediately by the last four digits of your social security number.

The passphrase: ______ Submit

Recipient authenticates him/herself to receive secure message:

- Password
- Account number
- Provider number
- Shared secret

Sending Secure E-mail: Message Pickup


SecureMessenger - HIPAA Summit Secure E-mail Presentation - Microsoft Internet Explorer provided by Texoma HealthCare System
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://tessin.thcs.org/read
Go
Search Web
Mail
Kerber Family Mail
Fantasy Sports
Maps
Search Spoke:
Add Page or Add Note about
Reply Close View Security Destroy
Done
Internet

Date: Tue, 3 Feb 2004 12:22:18 -0600
From: <JKERBER@THCS.ORG>
To: 'kerber@yahoo.com' <kerber@yahoo.com>
Subject: HIPAA Summit Secure E-mail Presentation

This message will expire on Tue, 17 F[illegible] 2004 12:35:45 -0600.

SecureMessenger has certifi[illegible] this [illegible]age. For a detailed report, click `View Security'.

Attachment (s): digital signatures.gif image/gif 9.92 KB

```
Jeff Kerber
Director, HIPAA Compliance
Corporate Privacy Officer
Texoma Healthcare System
903-416-5520
903-867-1671 (pager)


"This electronic message may contain information that is confidential and/or
legally privileged. It is intended only for the use of the individual(s) and
entity named as the recipients in the message. If you are not the intended
recipient of the message, please notify the sender immediately and delete
the material from any computer. Do not deliver, distribute or copy this
message, and do not disclose its contents or take action in reliance on the
information it contains. Thank you."
```

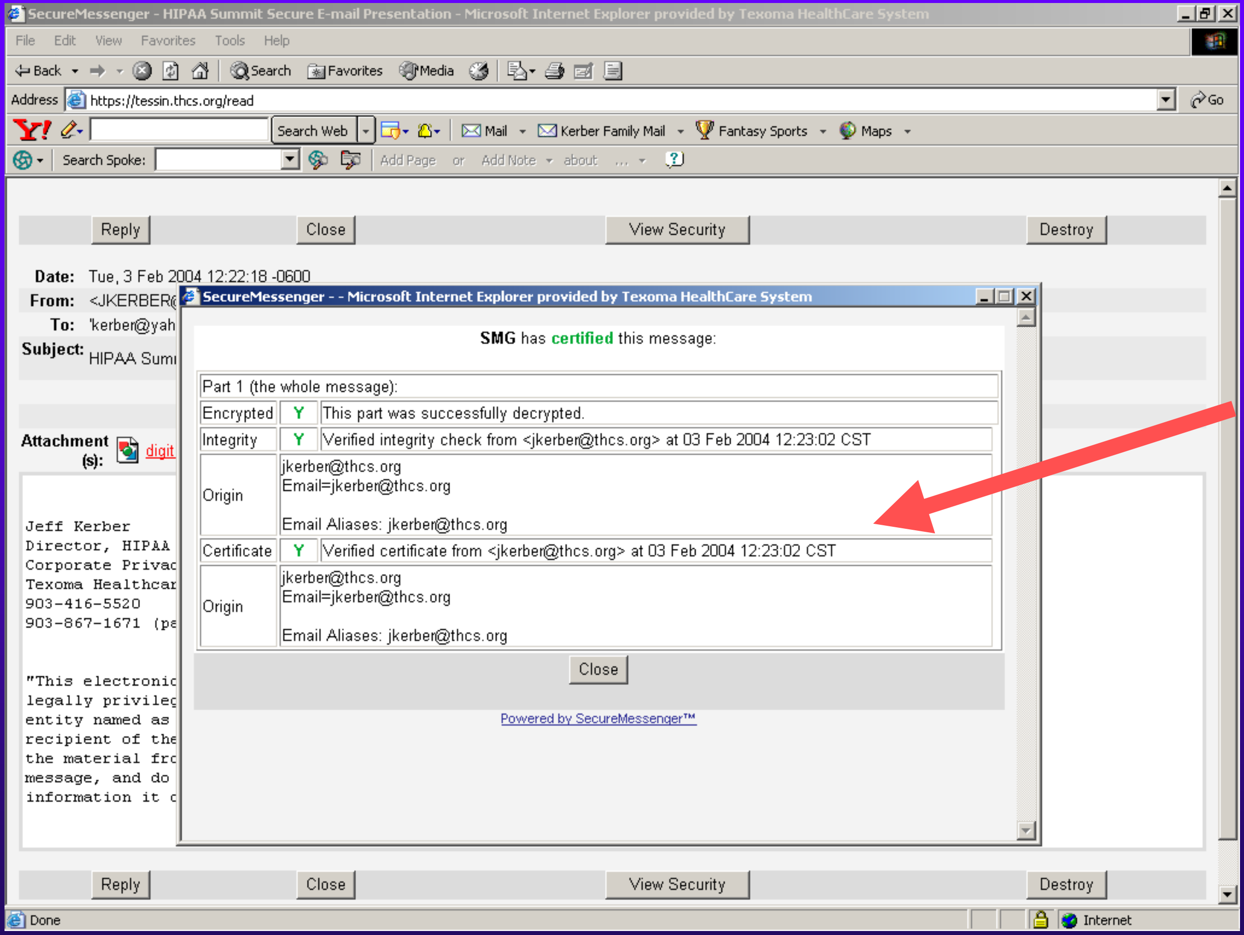
Recipient sends a secure reply with attachments

View security level and digital signature

Tovaris user views message reply in her inbox, securely

TEXOMA HEALTHCARE SYSTEM

Sending Secure E-mail: Message Verification/Non-repudiation


SecureMessenger - HIPAA Summit Secure E-mail Presentation - Microsoft Internet Explorer provided by Texoma HealthCare System
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://tessin.thcs.org/read
Go
Search Web
Mail
Kerber Family Mail
Fantasy Sports
Maps
Search Spoke:
Add Page or Add Note about ...
Reply
Close
View Security
Destroy

Date: Tue, 3 Feb 2004 12:22:18 -0600
From: <JKERBER@
To: 'kerber@yah
Subject: HIPAA Summ

Attachment (s): digit

```
Jeff Kerber
Director, HIPAA
Corporate Privac
Texoma Healthcar
903-416-5520
903-867-1671 (pa

"This electronic
legally privileg
entity named as
recipient of the
the material fro
message, and do
information it c
```

SecureMessenger - - Microsoft Internet Explorer provided by Texoma HealthCare System

SMG has certified this message:

Part 1 (the whole message):		
Encrypted	Y	This part was successfully decrypted.
Integrity	Y	Verified integrity check from <jkerber@thcs.org> at 03 Feb 2004 12:23:02 CST
Origin		jkerber@thcs.org Email=jkerber@thcs.org Email Aliases: jkerber@thcs.org
Certificate	Y	Verified certificate from <jkerber@thcs.org> at 03 Feb 2004 12:23:02 CST
Origin		jkerber@thcs.org Email=jkerber@thcs.org Email Aliases: jkerber@thcs.org

Recipient verifies encryption, signature integrity, originator identity, and certificate validity

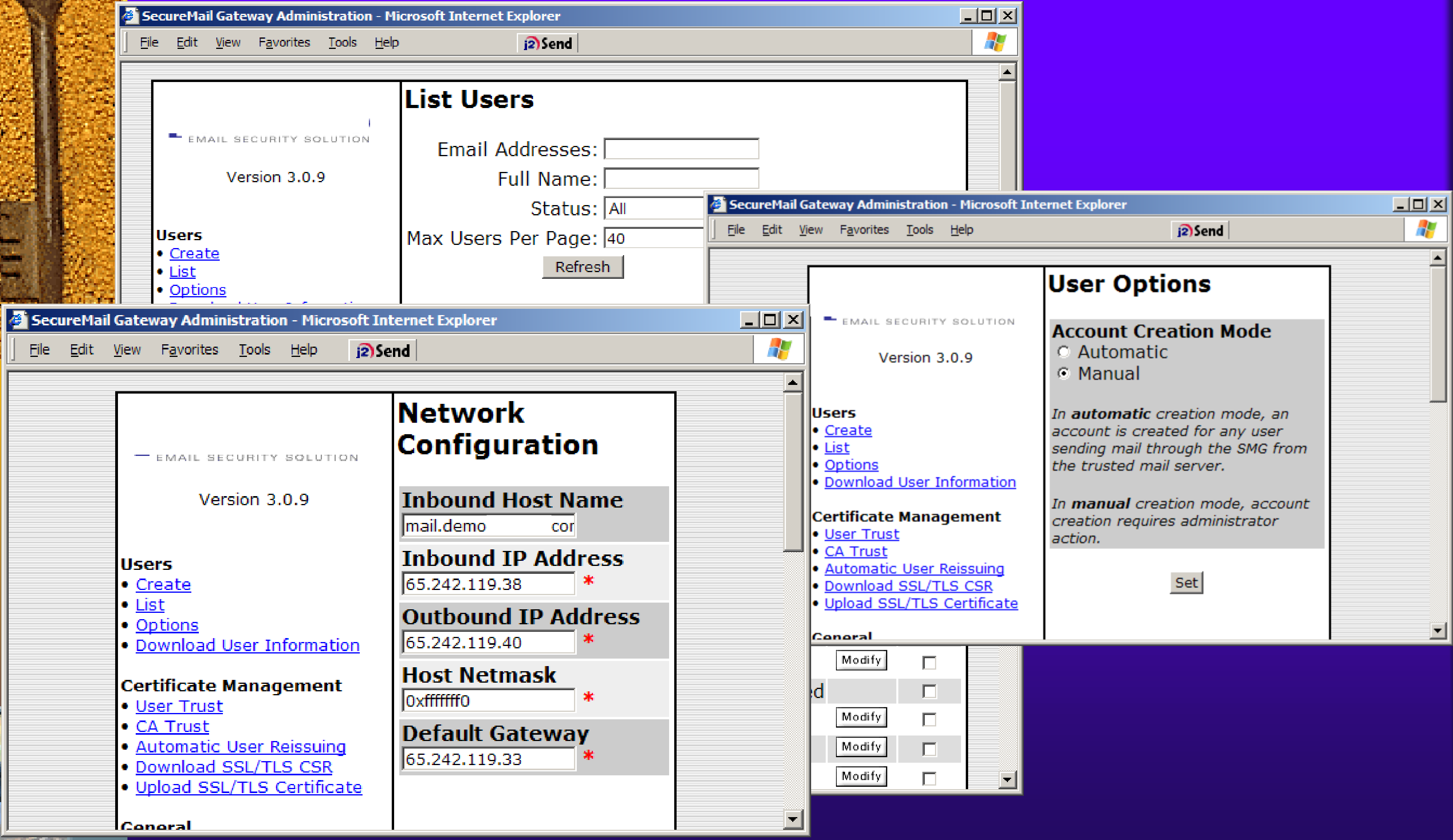
Sending Secure E-mail: Replies by the Recipient

- Recipient can reply securely back to sender, with unlimited file attachments. Original sender receives secure message in his own inbox when message has been replied to by recipient.

Sending Secure E-mail: Message Tracking

- Sender receives instant, secure notification by E-mail when Secure Messenger message has been retrieved by recipient.

Simple Web Administration


SecureMail Gateway Administration - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
i2Send

EMAIL SECURITY SOLUTION

Version 3.0.9

Users
- Create
- List
- Options

List Users

Email Addresses:

Full Name:

Status: All

Max Users Per Page: 40

SecureMail Gateway Administration - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
i2Send

EMAIL SECURITY SOLUTION

Version 3.0.9

Users
- Create
- List
- Options
- Download User Information

Certificate Management
- User Trust
- CA Trust
- Automatic User Reissuing
- Download SSL/TLS CSR
- Upload SSL/TLS Certificate

General

User Options

Account Creation Mode

○ Automatic

● Manual

In ***automatic*** *creation mode, an account is created for any user sending mail through the SMG from the trusted mail server.*

In ***manual*** *creation mode, account creation requires administrator action.*

SecureMail Gateway Administration - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
i2Send

EMAIL SECURITY SOLUTION

Version 3.0.9

Users
- Create
- List
- Options
- Download User Information

Certificate Management
- User Trust
- CA Trust
- Automatic User Reissuing
- Download SSL/TLS CSR
- Upload SSL/TLS Certificate

General

Network Configuration

Inbound Host Name
mail.demo cor

Inbound IP Address
65.242.119.38 *

Outbound IP Address
65.242.119.40 *

Host Netmask
0xfffffff0 *

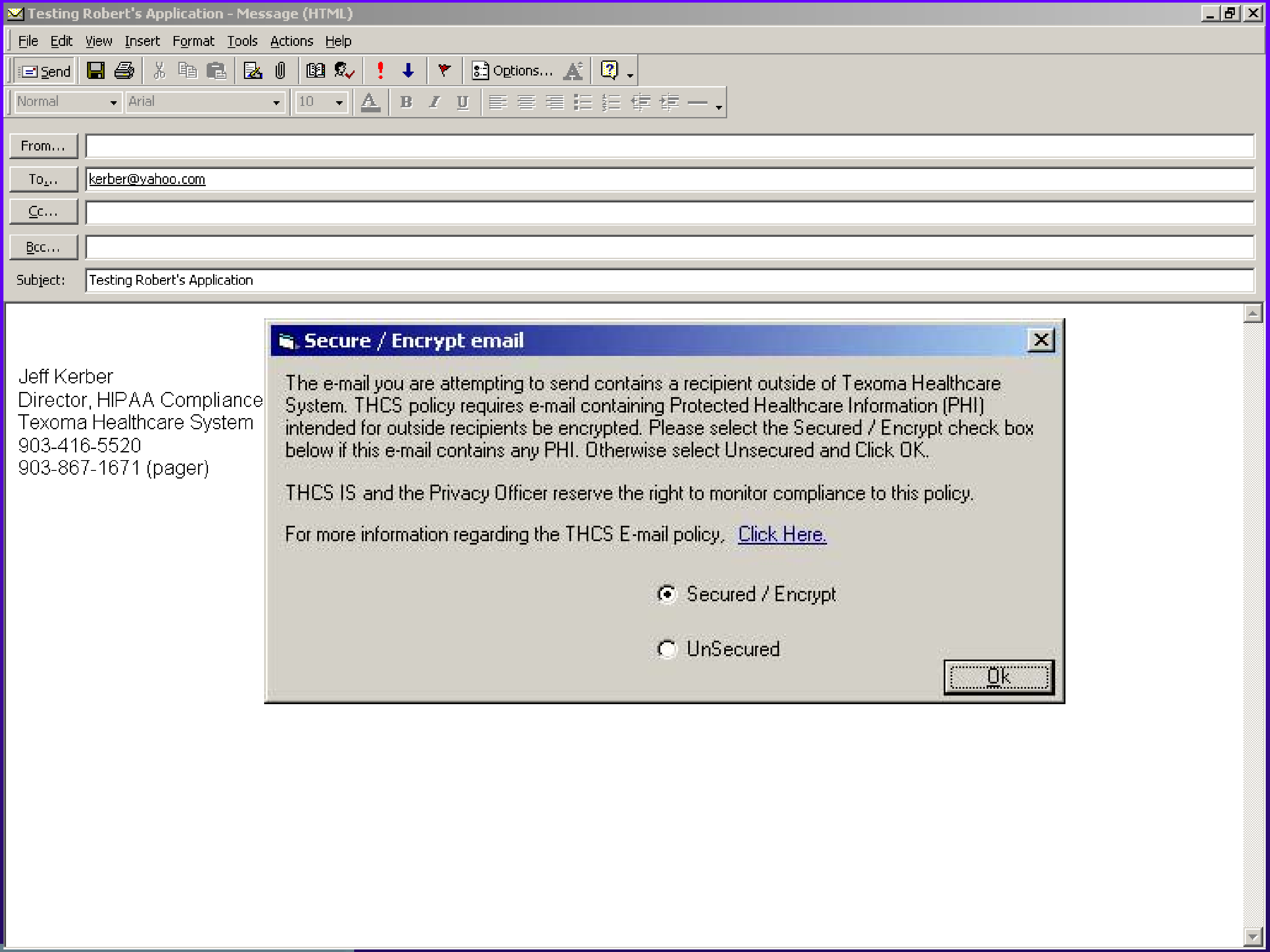
Default Gateway
65.242.119.33 *

TEXOMA HEALTHCARE SYSTEM

The THCS Experience

- Usage and Maintenance
  - What maintenance?
  - Measuring usage
  - Assuring usage

Addressing User Compliance



Testing Robert's Application - Message (HTML)
File Edit View Insert Format Tools Actions Help
Send
Options...
Normal
Arial
10
B I U

From...

To... kerber@yahoo.com

Cc...

Bcc...

Subject: Testing Robert's Application

Jeff Kerber
Director, HIPAA Compliance
Texoma Healthcare System
903-416-5520
903-867-1671 (pager)

Secure / Encrypt email

The e-mail you are attempting to send contains a recipient outside of Texoma Healthcare System. THCS policy requires e-mail containing Protected Healthcare Information (PHI) intended for outside recipients be encrypted. Please select the Secured / Encrypt check box below if this e-mail contains any PHI. Otherwise select Unsecured and Click OK.

THCS IS and the Privacy Officer reserve the right to monitor compliance to this policy.

For more information regarding the THCS E-mail policy, Click Here.

● Secured / Encrypt

○ UnSecured

Addressing Three Secure E-mail Challenges

- ☒ THCS users can't use encryption—it's too difficult!
  - ✓ No client application or plug-in—Secure E-mail Gateway is a fully integrated E-mail security device
- ☒ How do we send secure messages to recipients with no digital certificate?
  - ✓ Secure Messenger Web delivery to all recipients with no remote storage of keys or messages
- ☒ Manual certificate exchange is impossible to manage with our business partners.
  - ✓ Certificate harvesting and Secure Network automates certificate distribution, retrieval and management activities

Key “Take-aways”

- “Reasonable effort” toward HIPAA compliance
- Turn-key E-mail security with little user overhead
- Able to send secure E-mail to any recipient
- Little to no ongoing management burden
- Able to find and retrieve recipients’ certificates by default on every message sent
- Able to integrate secure E-mail with mail system, anti-spam/virus and content filtering systems
- Plug into existing data sources for seamless web delivery and authentication

Secure E-mail: An Implementation Success Story

How Texoma Healthcare System Identified & Addressed its Secure E-mail Requirements

Presented by
Jeff Kerber, Former Corporate Privacy Officer
and HIPAA Compliance Director
Texoma Healthcare System
March 8, 2004