
Entrust
Securing Digital Identities
& Information
SECURITY ON
USING ENCRYPTION TO
PROTECT SENSITIVE INFORMATION
Commonwealth Office of Technology
Security Month Seminars
October 29, 2013

Alternate Title?

"Boy, am I surprised."

"The Entrust guy who has mentioned PKI during every Security Month presentation for the past six years is going to talk about encryption!"

© Entrust, Inc. All rights reserved.

Is Encryption Unbreakable?

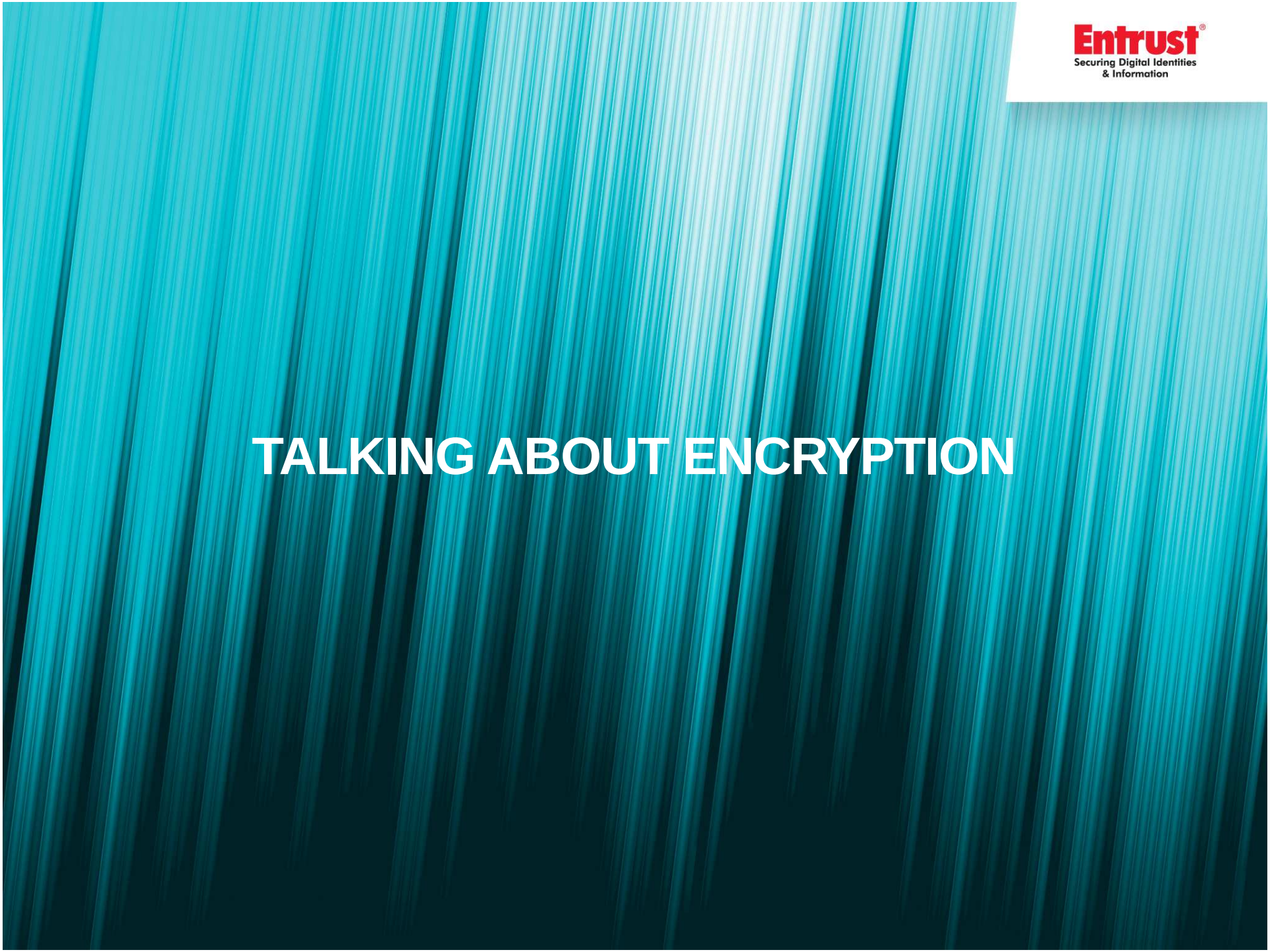
- A cryptographic system is said to be ‘computationally secure’ if
  - The cost of breaking the encryption is greater than the value of the protected information

  Or

  - The time required to crack the encryption is longer than the life time of the protected data

© Entrust, Inc. All rights reserved.

© Entrust, Inc. All rights reserved.


Entrust
Securing Digital Identities
& Information
TALKING ABOUT ENCRYPTION

Common Terms

- Encryption
  - The process of encoding or converting information so that it can only be read after it is decoded (decrypted)
  - Plaintext → Ciphertext → Plaintext
- Algorithm
  - A step-by-step method for calculating a function.
- Key
  - A unique piece of information that is used as one of the inputs of the encryption algorithm
- Key Length
  - The size (length) of the key expressed in bits
- Ciphertext = Algorithm(Key)(Plaintext)

© Entrust, Inc. All rights reserved.

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

© Entrust, Inc. All rights reserved.

Key Management

- The process for managing the lifecycle of cryptographic keys
  - Key Generation
  - Key Exchange (distribution)
  - Key Storage
  - Key Usage
  - Key Replacement
- Public Key Infrastructure (PKI)
- Commercial Enterprise Key Management Systems

© Entrust, Inc. All rights reserved.

More Encryption Terms

Symmetric Key Algorithms

- DES – Data Encryption Standard (also 'Triple DES')
- AES – Advanced Encryption Standard

Asymmetric Key Algorithms

- RSA – Rivest, Shamir, & Adleman (1977)
- DSA – Digital Signature Algorithm (FIPS)
- Elliptic Curve Cryptography

Hash Algorithms

- MD5 – Message Digest Algorithm
- SHA-1 – Secure Hash Algorithm
- SHA-2 – (SHA-224, SHA-256, SHA-384, SHA-512)
- SHA-3

© Entrust, Inc. All rights reserved.

Encryption Quality (Strength)

- Key length is not the only issue
- Quality of the key
  - Source?
    - Random number generators aren't perfect
    - Is the key password protected?
      - Password entropy
      - Dictionary attacks
- Quality of algorithms
  - New is Bad?
  - "Anyone who develops a new encryption algorithm is either a genius or a fool"

© Entrust, Inc. All rights reserved.

So How Should I Evaluate Encryption Tools?

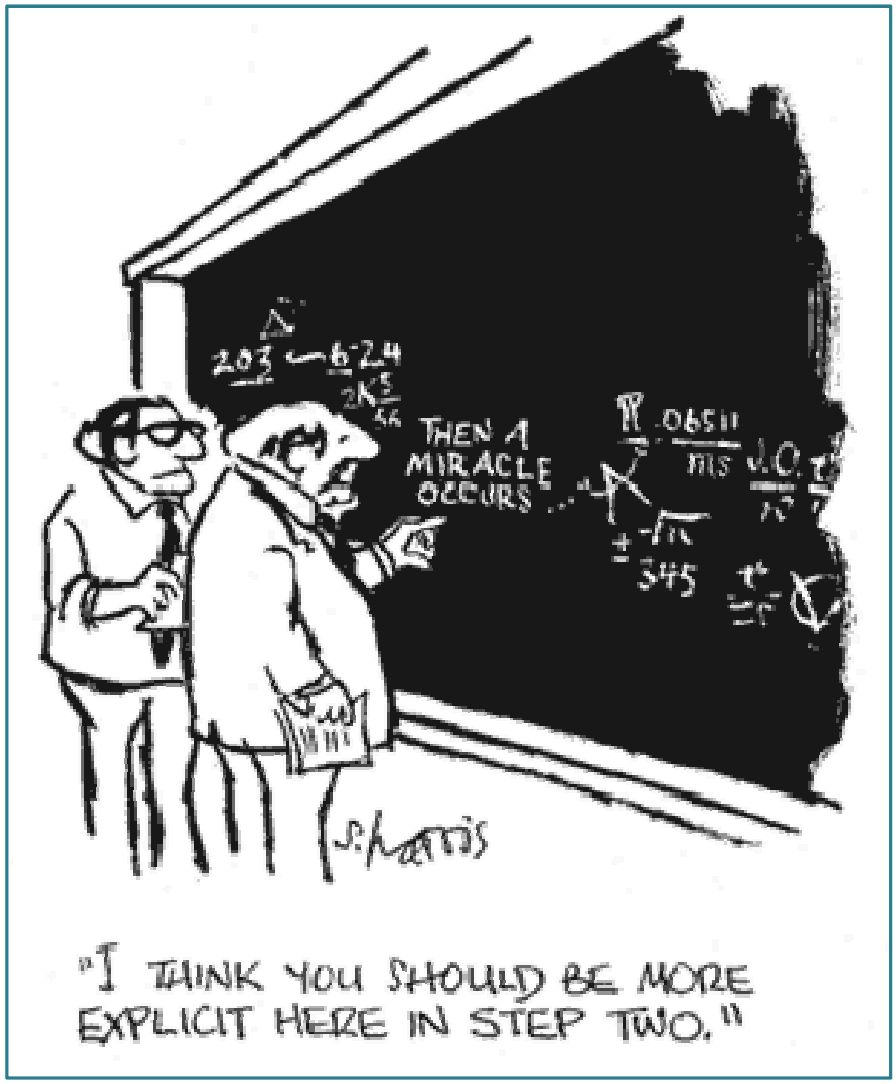
Option A – Do your own evaluation?

"An attacker using a general field number sieve would need to conduct an attack with complexity $O(\exp(((649+o(1))\cdot n)13(\log n)23))$ to factor the modulus (and thus break the private key), given a modulus of bit-length n."

Option B – Trusted Standards & Recommendations

- NIST Computer Security Division
  - NIST Special Publications (800 Series)
- IDManagement.gov
- NASCIO
  - State Identity, Credential, and Access Management Guidance
- Qualified Security Consultants

© Entrust, Inc. All rights reserved.



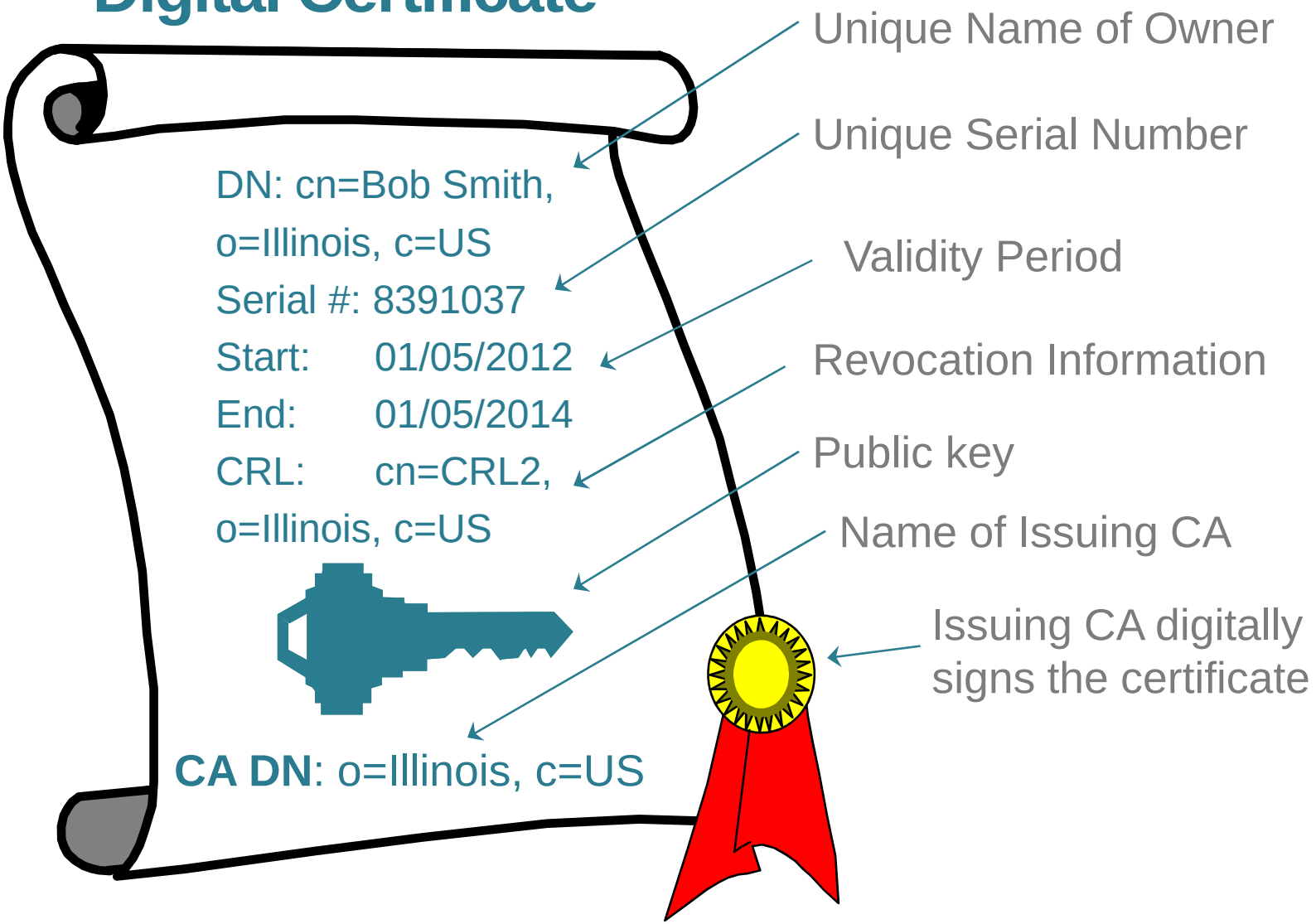
© Entrust, Inc. All rights reserved.

Symmetric vs. Asymmetric Encryption

- Symmetric Encryption
  - Encryption and decryption operations use the same secret key
  - Computationally faster operation
  - Key distribution can cause scalability issues
- Asymmetric Encryption
  - Also called Public Key Encryption
  - Each entity is issued a key pair
    - A public key which can be freely shared
    - A private key which is kept secret
  - Information encrypted with one key can only be decrypted with the other key from that pair
  - Mathematically 'impossible' to calculate the value of one key using the value of the other key

© Entrust, Inc. All rights reserved.

Digital Certificate

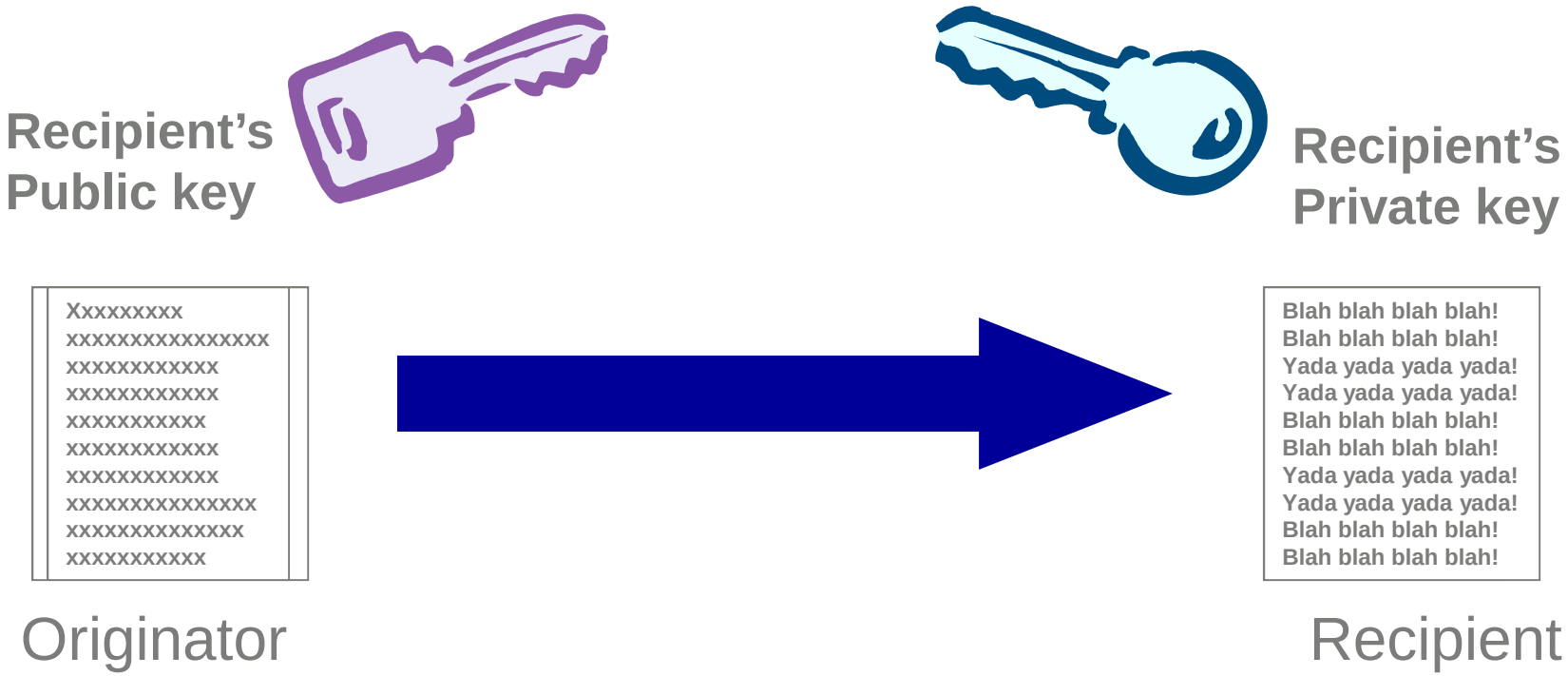


©Entrust, Inc. All rights reserved.

Public Key Encryption Process

Message originator encrypts the data using the recipient's public key

Recipient uses own private key to decrypt the data

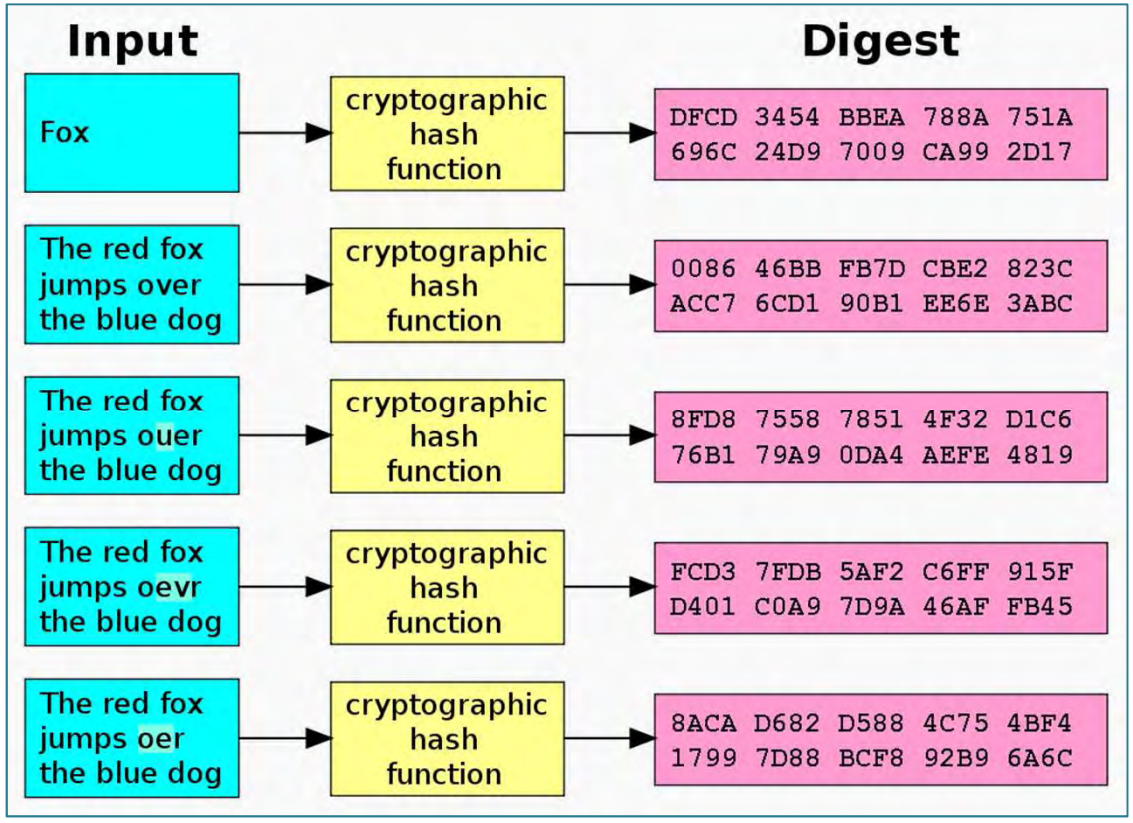


©Entrust, Inc. All rights reserved.

Encryption vs. Hashing

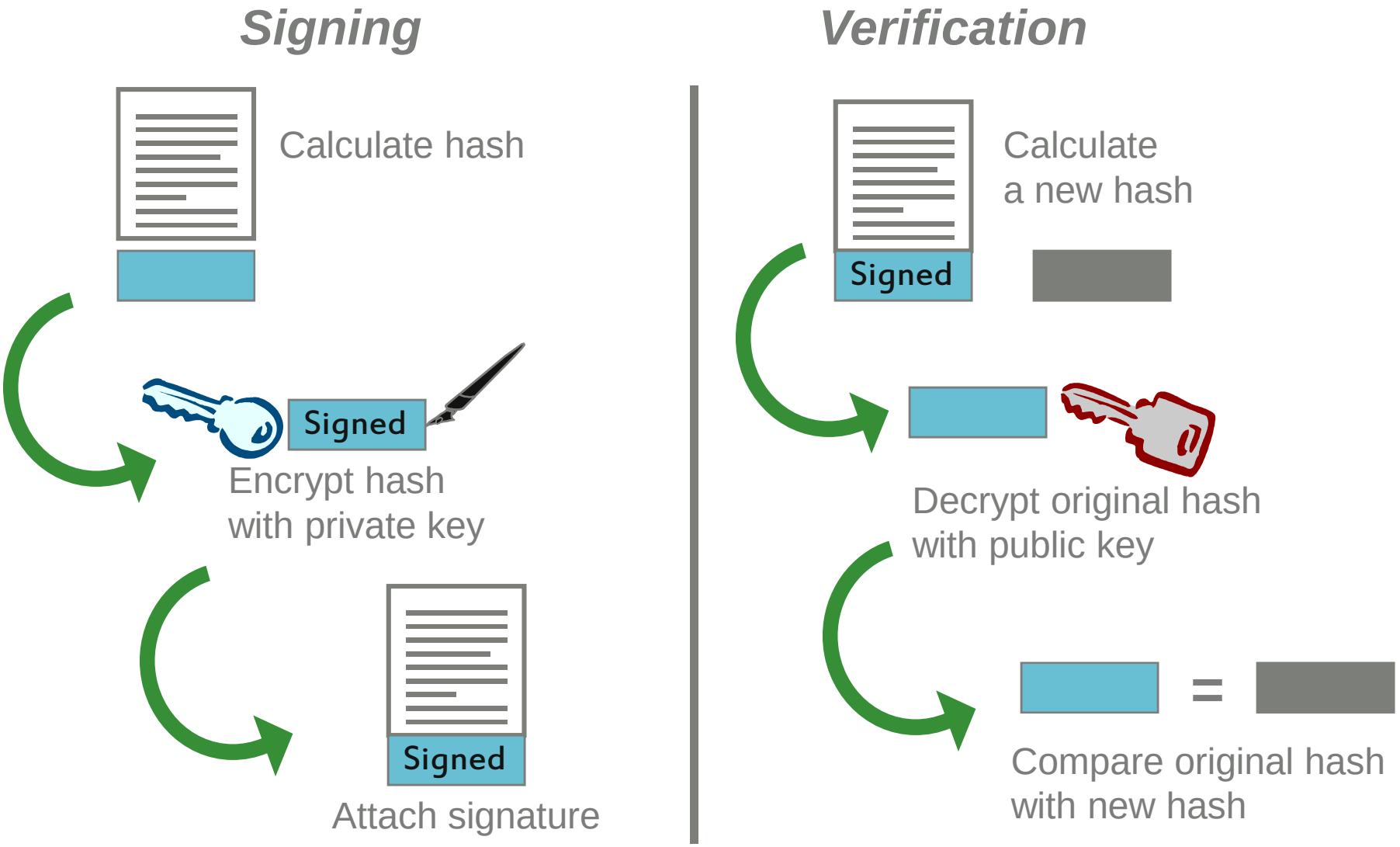
- A hashing function maps variable length data to a fixed-length value
- One-way (cannot determine the plaintext from the hash value)
- Salt & Pepper and Slow!

© Entrust, Inc. All rights reserved.



© Entrust, Inc. All rights reserved.

How Digital Signatures Work



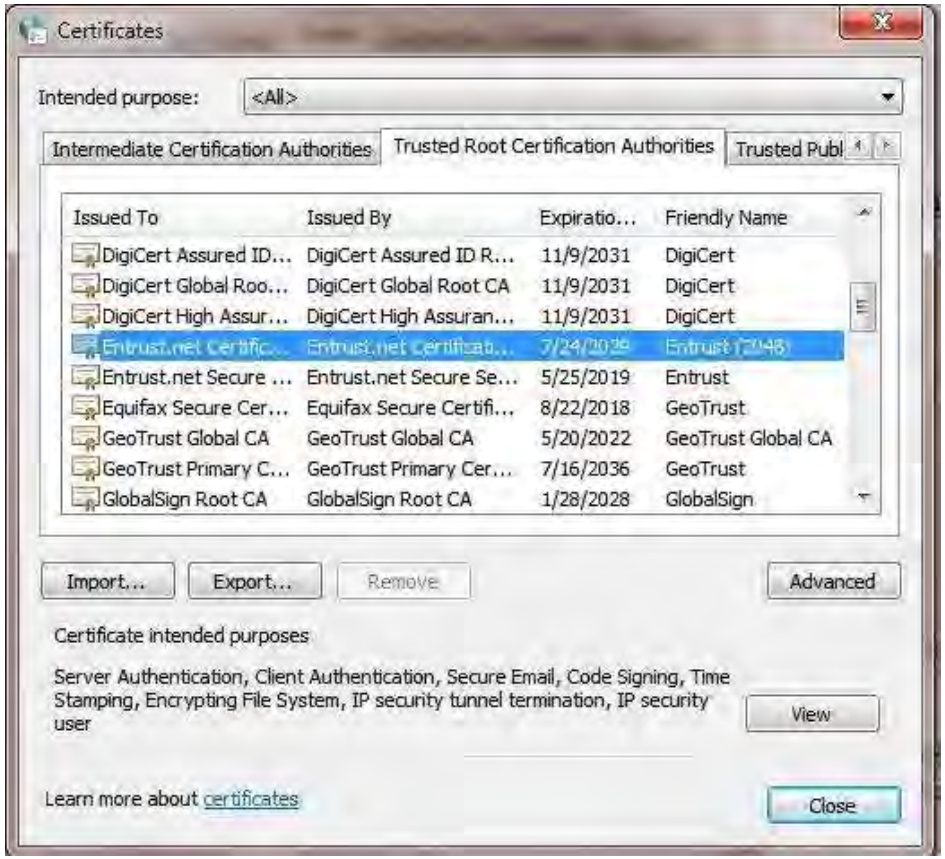
©Entrust, Inc. All rights reserved.

Self-Signed Certificates vs. Certification Authority

- Numerous utilities to create self-signed digital certificates
  - Microsoft Office, Adobe, OpenSSL, others
  - Can be useful for point solutions
  - Scaling problems similar to symmetric encryption
  - No verifiable authentication or issuance policies
- A Certification Authority should provide:
  - Centralized certificate management
  - Verifiable certificate status
  - Reviewable policies

© Entrust, Inc. All rights reserved.

Public vs. 'Private' Trust



© Entrust, Inc. All rights reserved.

Illinois Department of Central Management Services

CMS

Search

Bureau of Communication and Computer Services

Home | Services | Products | Support | Policies | Communications

Order Services

Contact Us

Home ▸ Services ▸ Catalog ▸ Security ▸ Cryptography

Cryptography (PKI)

Category: Security

Illinois was a pioneer among state governments in the area of PKI and strong encryption and was the first State to gain trusted status to the Federal PKI Bridge. There are roughly forty-eight State agencies, boards, commissions and units of local government utilizing digital certificates managed by BCCS.

CMS, by Legislative directive, is the sole source of digital certificates for State agencies, boards, commissions, universities and those who do business with them. This service can also be used by local, county and municipal governmental entities.

Digital Certificates
A digital certificate used to digitally sign a file, document or email, creates three points of assurance that an electronic communication is valid and unaltered.

A simple way of viewing this is that when two persons or two machines want to communicate electronically, both ends of the exchange are validated by a central (third party) Certificate Authority assuring that each end of the conversation is:

1. who it is suppose to be;
2. exchange between the two ends is both private and secured;
3. contents of the document have not been altered

RELATED RESOURCES

- What is PKI?
- Certificate Policy
- Certificate Practices Statement
- Get a Digital ID
- User Maintenance
- Forgot Password
- PKI FAQs
- Digital ID Subscriber Agreement
- Download the State of Illinois Root CA Certifiate
- Download the State of Illinois FBCS Cross Certificate
- Illinois Digital Signature Project Plan
- PKI News

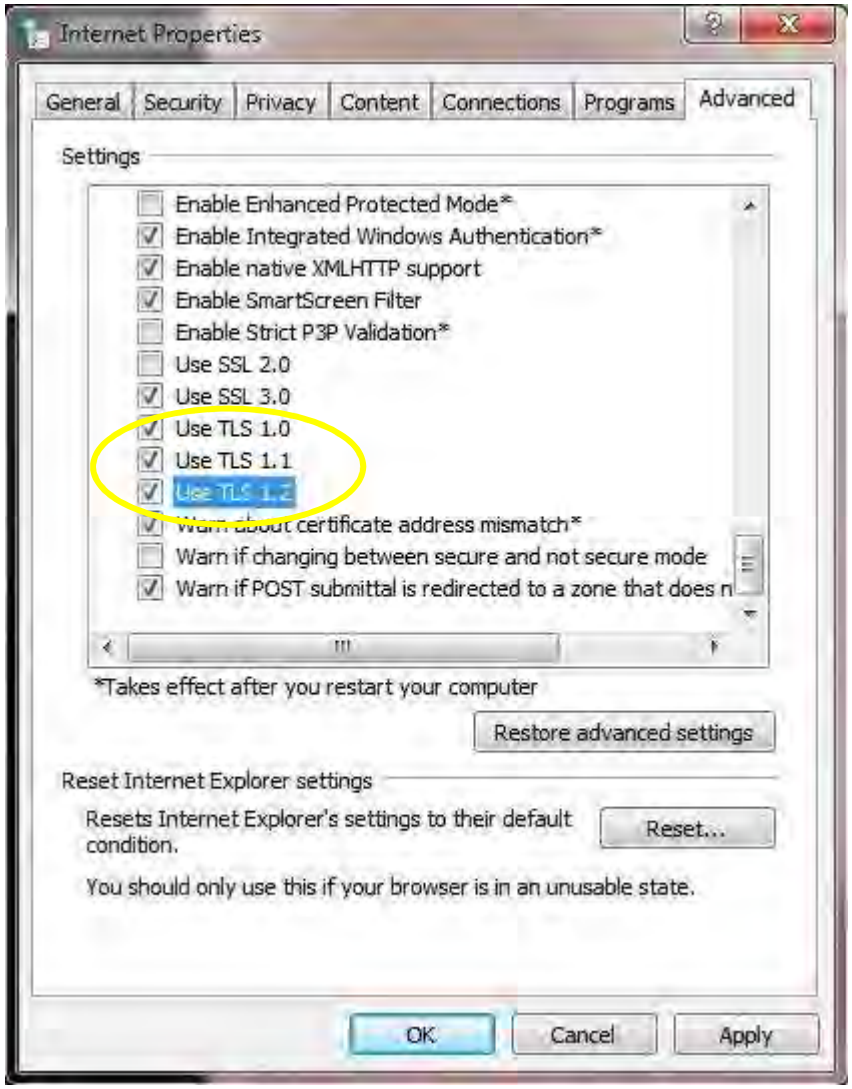
© Entrust, Inc. All rights reserved.

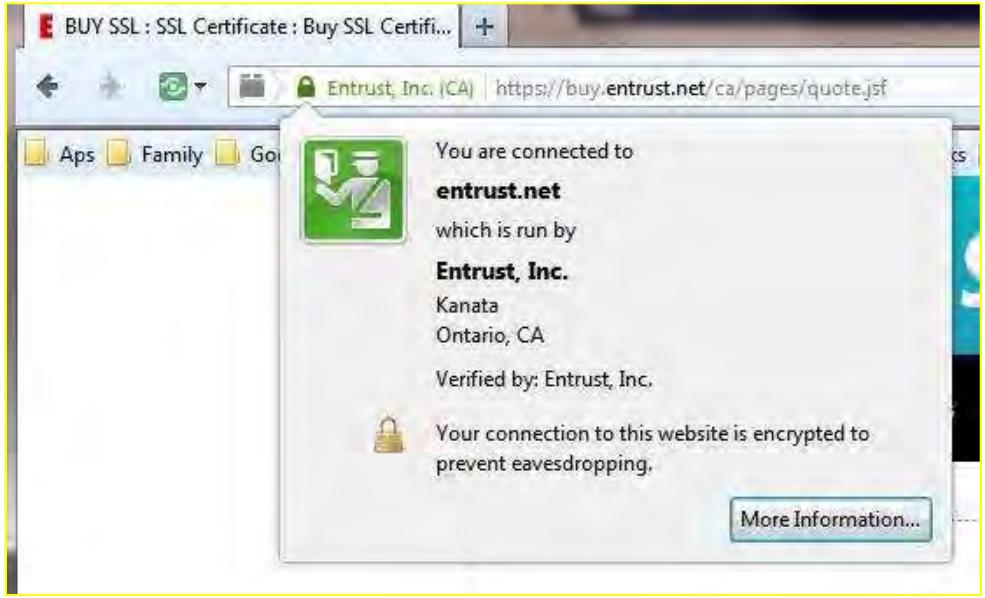

Entrust
Securing Digital Identities
& Information
USING ENCRYPTION TO PROTECT DATA

SSL & TLS

- Protocols to provide bidirectional authentication, privacy & message integrity over reliable communications protocols (TCP)
- HTTPS is actually HTTP data exchanged over a previously established SSL or TLS connection (HTTP over SSL over TCP)
- The application establishes an SSL connection
  - Client (browser) requests a secure page
  - Server (web site) sends digital certificate
  - Client verifies that certificate is trusted
  - Client uses public key to encrypt session (symmetric) key
  - Both Client & Server use session key to exchange data
  - Both Client & Server discard the session key when connection is terminated

© Entrust, Inc. All rights reserved.





© Entrust, Inc. All rights reserved.

VPN – Virtual Private Network

- A secure network segment that is logically isolated from the network as a whole – isolated through encryption rather than through physical or logical switching
- Generally requires configuration of the device
  - more intrusive than TLS but also more comprehensive security
- VPN operates at the operating system level. Securely connects the device so individual applications do not need to be security aware.
- Enable mutual authentication by issuing a certificate to both the VPN device and the client device

© Entrust, Inc. All rights reserved.

Wi-Fi Encryption (and Authentication!)

- WEP – In this case ‘Old is Bad’!
- At home
  - WPA2-PSK (sometimes labeled WPA2–Personal)
  - PSK = Pre-Shared Key
    - For personal use a passphrase of maximum allowed length
    - For more secure uses generate a random character string
- In the Enterprise
  - WPA-Enterprise enables authentication using a Radius server
  - Other 802.1x authentication methods

© Entrust, Inc. All rights reserved.

© Entrust, Inc. All rights reserved.

"Full" Disk Encryption

- Hard Drives
  - Typically used to encrypt the contents of a laptop hard drive
  - Solution should also encrypt swap files and temp files
  - Security depends on strong user credentials to the device
  - Protects against 'coincidental' breaches of information
- Smart Phones
  - Also probably not "hacker proof"
  - But makes it really hard for the guy who finds your phone in a taxi to dial your daughter's phone number or find your mother's home address!

© Entrust, Inc. All rights reserved.

File & Folder Encryption

- May require a separate application or be installed as a function of the operating system
- Encryption may use public key (digital certificate) or a passphrase as the encryption key
- Encrypt sensitive files that will be:
  - Sent to another person by email
  - Transported on portable media (CD's, USB Drives, etc.)
    - Including backup files!
  - Stored in cloud services (Dropbox, Box, Google Drive)
  - Uploaded over an unsecured connection

© Entrust, Inc. All rights reserved.

Protecting Information in Email

- S/MIME
  - Secure Multipurpose Internet Mail Extensions
  - Encrypts the message body and attachments
  - Designed for end-to-end protection
  - Requires email clients that are S/MIME capable
- Encrypted File Attachments
  - Message body is sent as plaintext
  - No email client requirements
- TLS over SMTP
  - Encryption only takes place between SMTP relays
  - Does not prevent the use of S/MIME or encrypted attachments

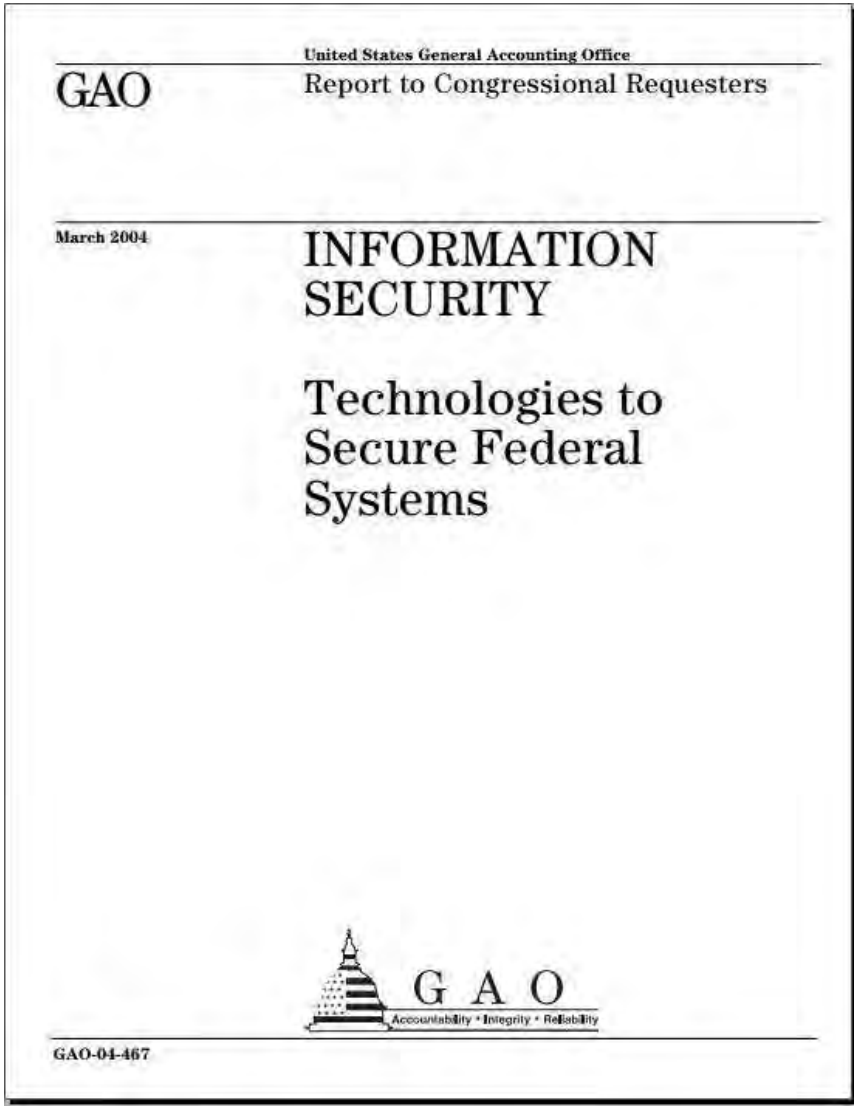
© Entrust, Inc. All rights reserved.

Not Just For Work!

- Personal uses for encryption
  - Secure storage on a shared computer
  - Email attachments
  - Cloud storage
- No-Cost Personal Encryption Solutions
  - TrueCrypt
    - Create an encrypted virtual disk on a drive
  - AxCrypt
    - Encrypt individual files
  - OpenPGP or GnuPG
    - File & folder encryption
    - Email message encryption*

© Entrust, Inc. All rights reserved.

© Entrust, Inc. All rights reserved.



United States General Accounting Office

GAO

Report to Congressional Requesters

March 2004

INFORMATION SECURITY

Technologies to Secure Federal Systems

GAO

Accountability * Integrity * Reliability

GAO-04-467

© Entrust, Inc. All rights reserved.

Thank You!

Brent Crossland

Entrust, Inc.

State Government Initiatives

brent.crossland@entrust.com

o: (217) 953-0773

m: (217) 341-7467

© Entrust, Inc. All rights reserved.