

Health with HIPAA

Prophets, Contrarians and Carpetbaggers

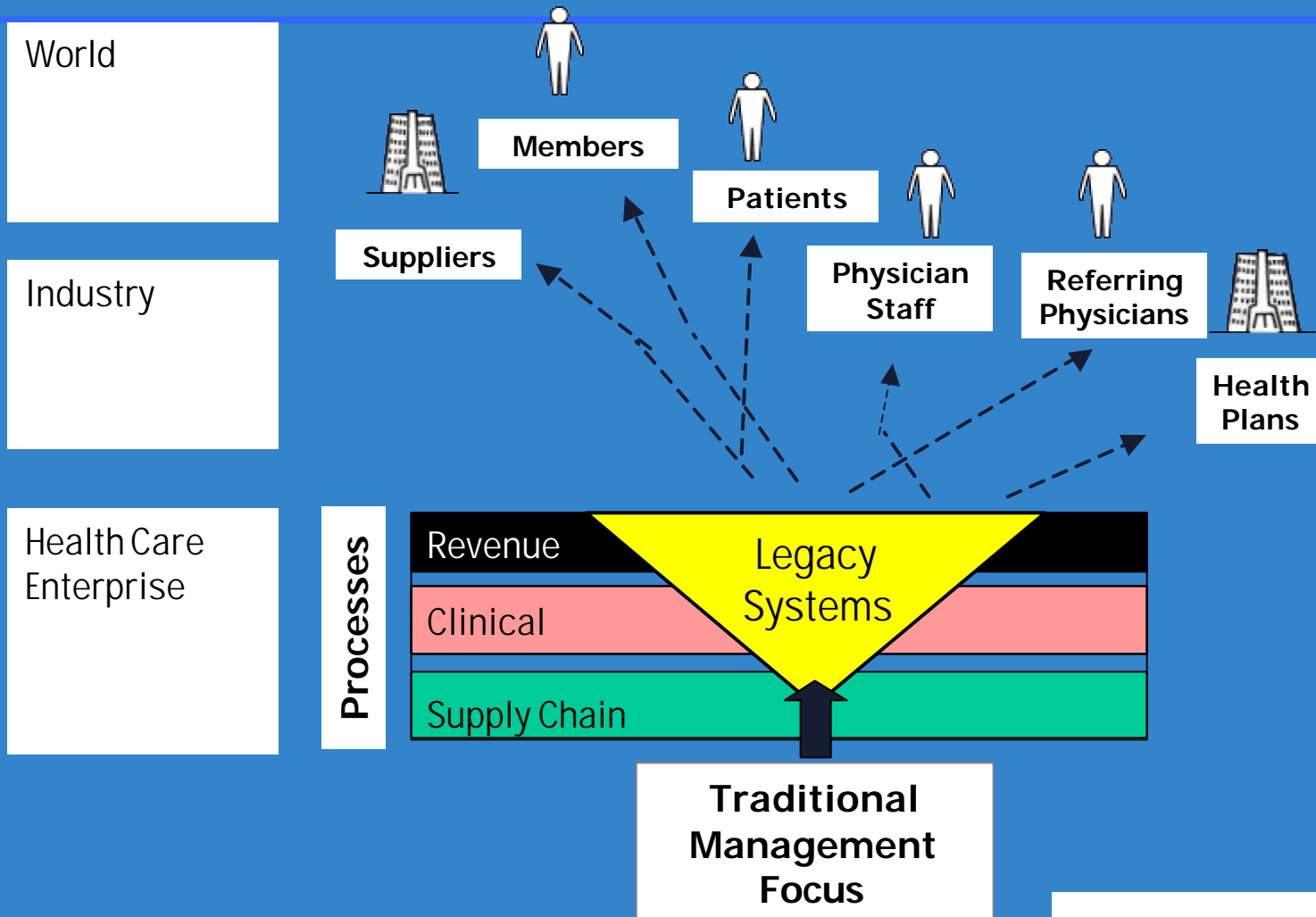
Joel F. French
President and CEO
ComTrustÒ, LLC
248-763-0671
Jfrench@comtrust.com
www.comtrust.com



Discussion Framework

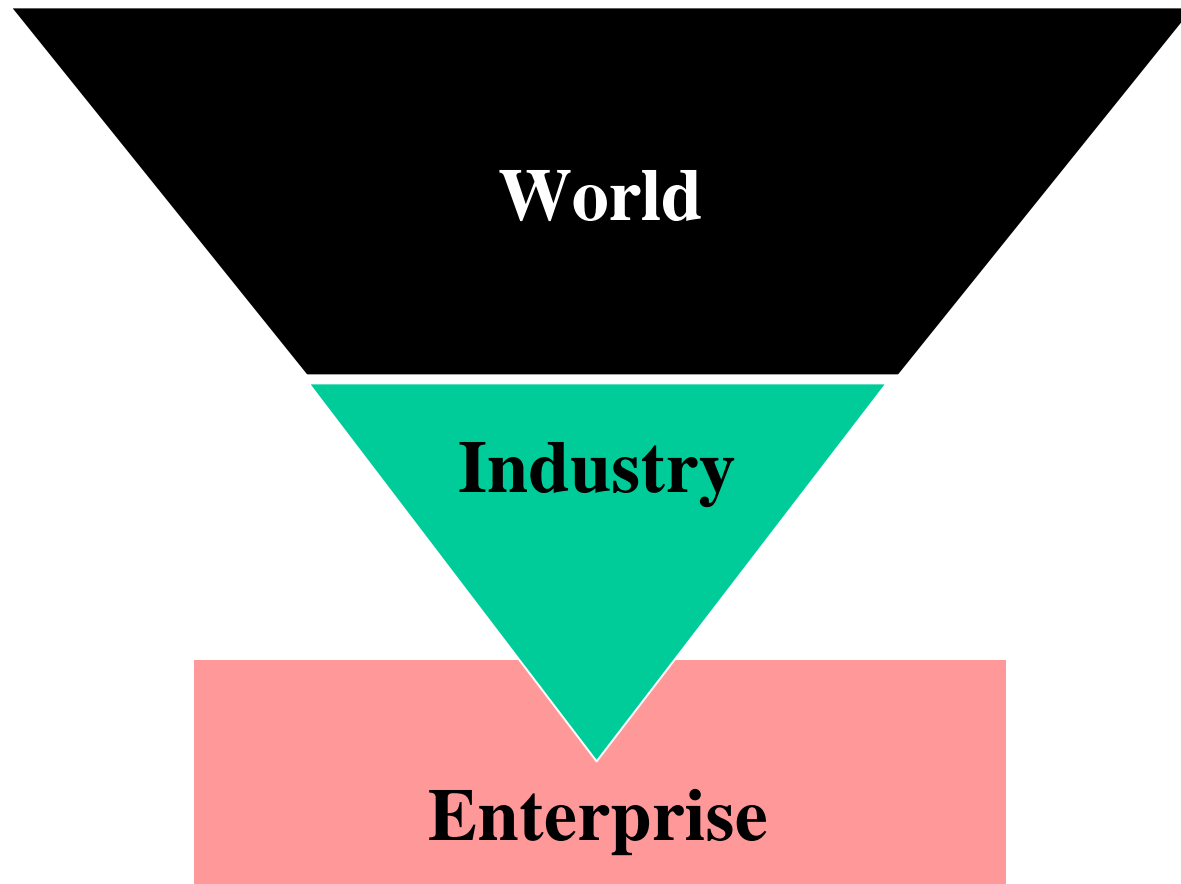
- Transitioning from requirements to reality
- Industry readiness
- Identifying business value and risks
- Range of solution alternatives
- The role played by PKI

Management Paradigm Inversion





Today's Information Marketplace



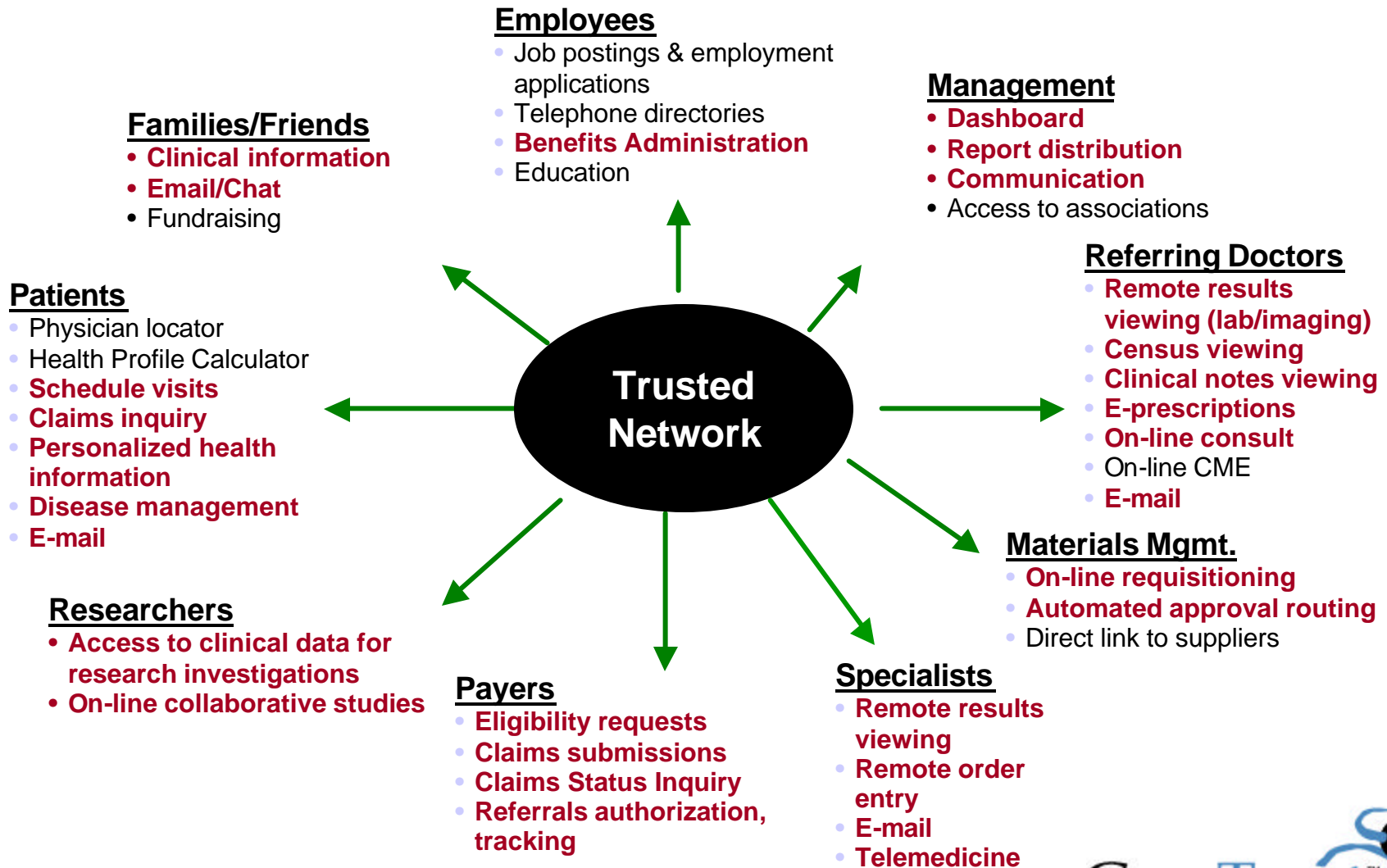
"Our web is secure!"

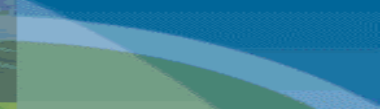
"Yeah....
Unassailable!"





Opportunities and Requirements





The Tip of the Iceberg

- ◆ Service and performance improvements hidden “below the water (on)line”, such as online scheduling, referrals, census, orders and results access, online communications, etc., all require strong security



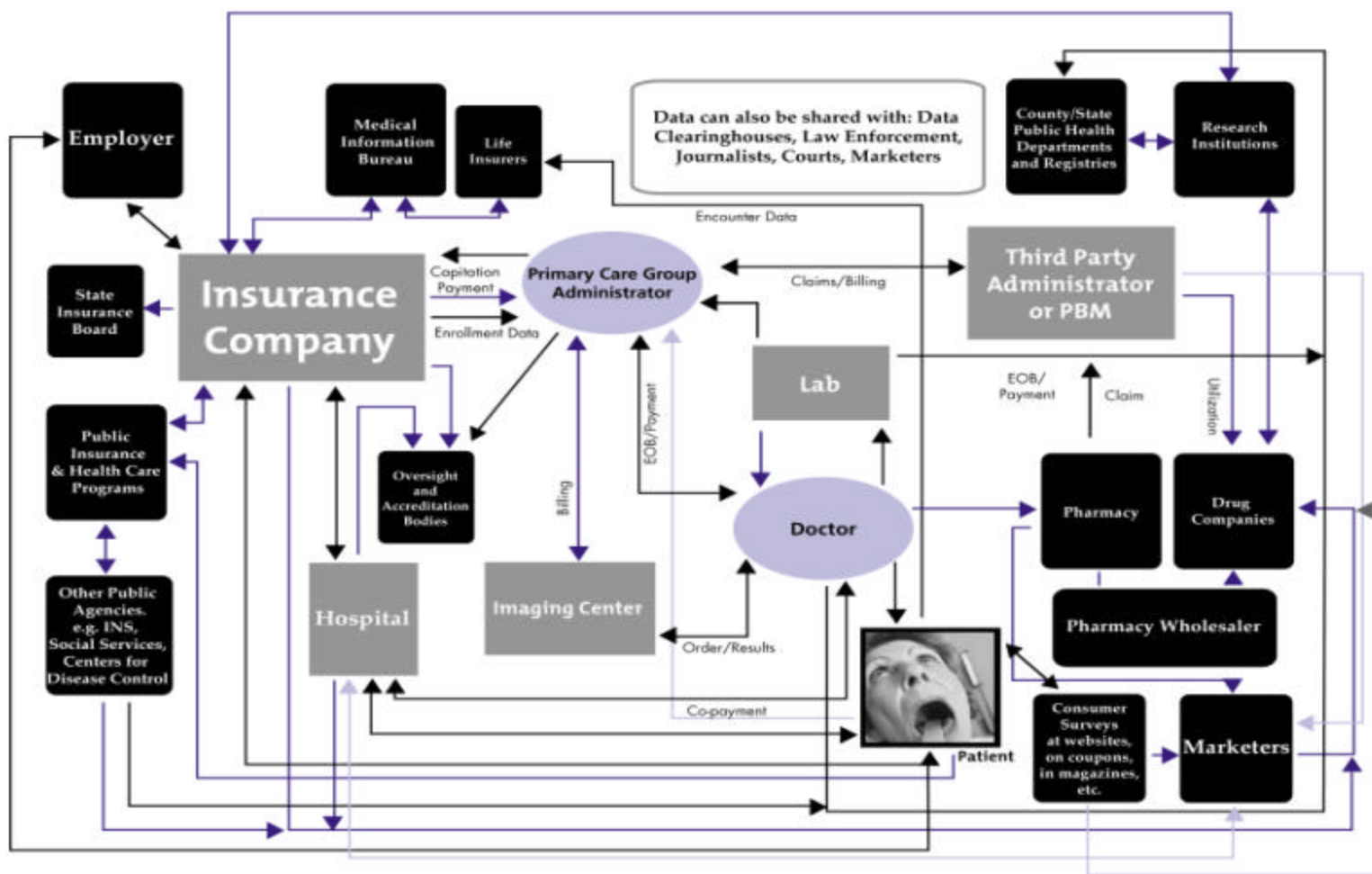
Results achieved so far by innovative market leaders

Incremental business benefits and market advantages enabled by securing cross-enterprise communications and transactions

Do You Know Where Your Medical Information Goes?

Sample Data Flow

Based on a presentation developed by the California HealthCare Foundation



Please note that the explanations are meant to be illustrative. They are not comprehensive.

Source: Health Privacy Project – Institute for Healthcare Research and Policy, Georgetown University

BusinessWeek

PRIVACY ON THE NEWS
What Should Be Done



Protecting medical privacy

IMAGING

THE INDUSTRY STANDARD

ADVERTISING AND MARKETING
SPECIAL REPORT

THE Privacy Problem



healthcare
INFORMATICS
Security on the Web

PLUS:

Staff Schedules

Spotlight: CPR Systems

The Many of a CIO

Forbes digital

Spotlight: CPR Systems

The Many of a CIO

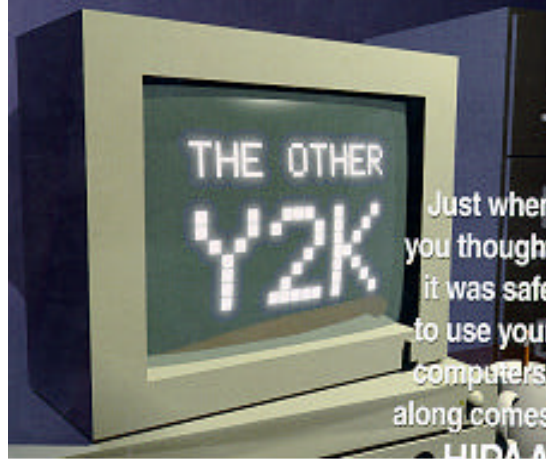
MEDIA & POLITICS

Medical privacy

Healthcare Weekly Business News January 31, 2000

TIME digital

ALSO DIGITAL E-BUSINESS RISK-TAKING



THE OTHER Y2K

Just when you thought it was safe to use your computers, along comes Y2K

WHO'S WATCHING

Who's watching you? Called programs spy on you port back by home. More than 22 million have unwittingly loaded them.



How to Protect Your

PRIVACY

ComTrust Your Key to Secure Communications



OPEN LETTER TO THE PRESIDENT
RED HERRING
THE BUSINESS OF TECHNOLOGY



Privacy
Why it will shape e-commerce in 2001

digital E-BUSINESS

Stealing privacy



BUILD SECURITY





Their Fear is Warranted

- **Major Non-Profit Health Plan:** 858 patient records **emailed** to unintended recipients over the Internet.
- **Major West Coast University Medical Center:** **Hacker** downloads medical records on 4,000 cardiology patients.
- **Major Cancer Center:** 12,000 patient records **compromised** and fraudulently used.
- **Major Mid-Western University Health System:** Thousands of patient records left exposed to the public on the **Internet** for months.
- **Major For-Profit Health Plan:** Accidentally **sent** private information to wrong doctors for 12,000 patients.



Balance Risk with Business Needs

Access

- Connectivity
- Speed of Access
- Ease of Use
- Workflow
- Convenience

Security

- Authentication
- Authorization
- Policy
- Accountability
- Data Integrity

Policy Management

Beyond HIPAA – Examples of Other Regulations

DEA – Fed. Reg., Vol. 67, No. 8 (1/11/2002) proposed regs. for

- Ordering Schedule IV controlled substances electronically
- Electronically writing, signing and transmitting prescriptions
 - Proposed DEA Root CA
 - Face-to-Face
 - 2 Factor Authentication
 - Private Key with Token Protection

FDA – Title 21 CFR 11 (3/20/97)

Regulations governing use of electronic records (e.g., encryption and signatures) covered by the Federal Food, Drug and Cosmetic Act and the Public Health Service Act



Standard Bodies – Security Requirements

- **ISO – 17799 , 7498-2**
- **ASTM – 1762, E-2084-00**
- **HL7 – Version 3.0**
- **ANSI, IETF, AICPA, W3C and e-i-e-i-o**

HIPAA Resources / Links

- **HHS Fact Sheet & Additional HIPAA information**

<http://www.gcd.com/seminars/publist.asp?groupid=3&areaid=4>

- **Overview of HIPAA's Security Concepts**

<http://rr.sans.org/legal/compliance.php>

- **Overview of the HIPAA Proposed Security Regulations Presentation**

<http://www.ehcca.com/presentations/ehc-info3/parmigiani.pdf>

- **American Bar Association PKI Assessment Guidelines (PAG)**

<http://www.abanet.org/scitech/ec/isc/pag/pag.html>

- **Additional Resources and Links**

<http://www.comtrust.com/resources>



French's 2nd Law

All online transactions begin with identity. Absent reliable mechanisms to secure online communications and transactions across enterprise boundaries, the promise of the web to deliver business improvements is illusory.



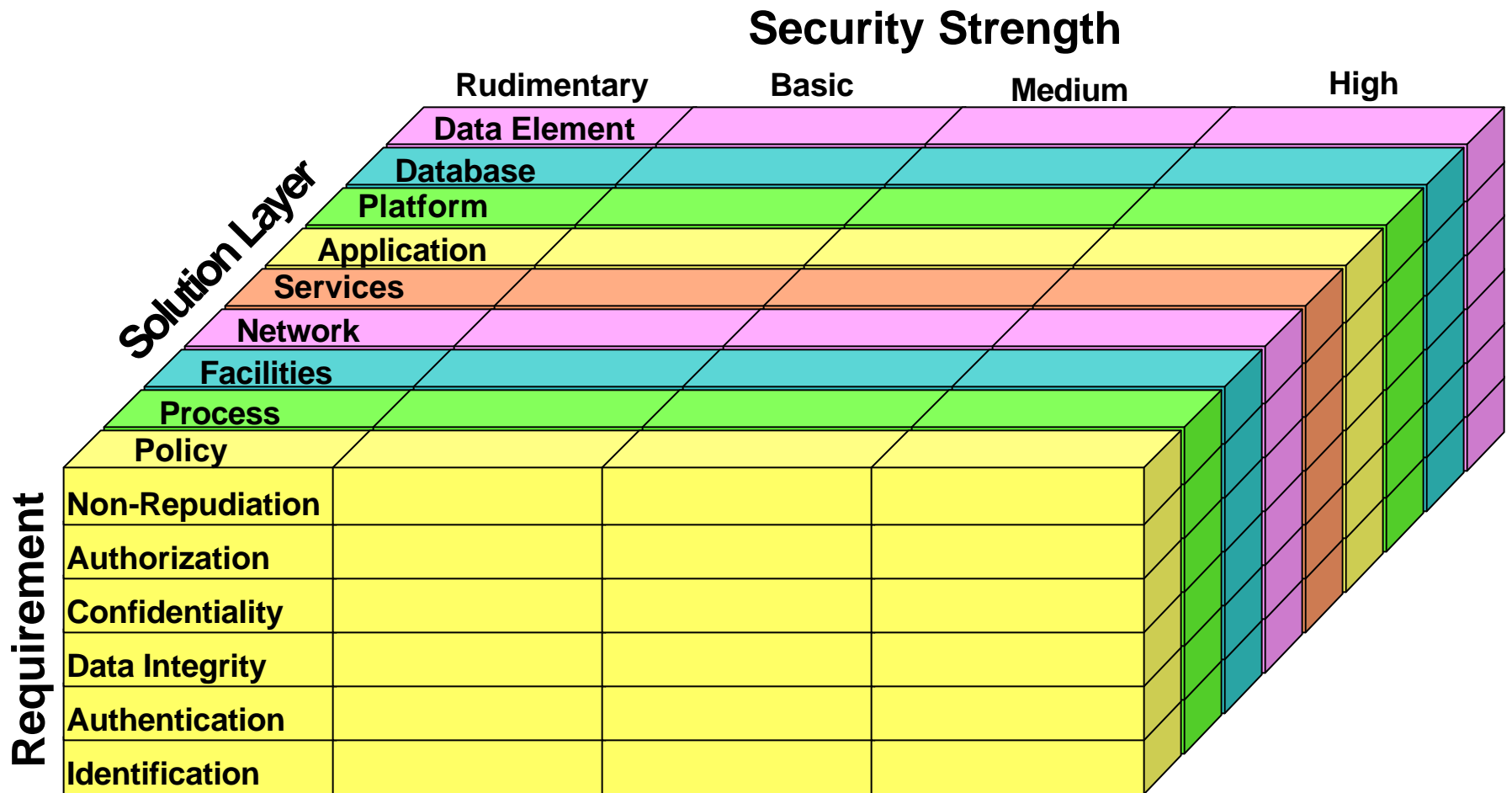
Healthcare Trust Issues

- Identification
- Authentication
- Access Control
- Authorizations
- Auditing
- Non-repudiation
- Digital signature
- Digital receipt
- Time stamp
- Confidentiality
- Data Integrity

Who are you?
How do we know?
Where can you go?
What can you do?
What did you do?
Can we prove it?
Did s/he sign for it?
Did s/he receive it?
When was it sent?
Was it kept private?
Did anyone tamper?



Multi-Dimensional Requirements





Requirement: Authentication

- Strong authentication requires both something you *know* AND either something you *have* or *are*.
 - ◆ Something you know
 - ◆ Passwords, combination to safe
 - ◆ Something you have
 - ◆ Keys, tokens, badges
 - ◆ Something you are
 - ◆ Fingerprint, signature, iris pattern, keystroke pattern



Aren't Passwords Enough?

Low security...

71% unauthorized break-ins by corporate insiders!

2000 CSI/FBI Computer Crime Survey

84% of bank fraud is committed by in-house staff.

Bank Technology News- Survey 2000, Cap Gemini Ernst & Young

... high frustration...

40% of all help desk calls are for forgotten passwords.

Gartner Group

... and costly.

Each year companies spend up to \$200-\$300 per user trying to maintain secure passwords.

Gartner Group, Forrester Research



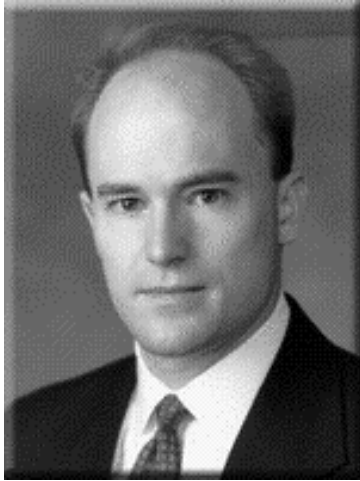


Token Authentication




Smart Cards or Proximity Cards

Front




Joel French, MD
Proctologist

Back



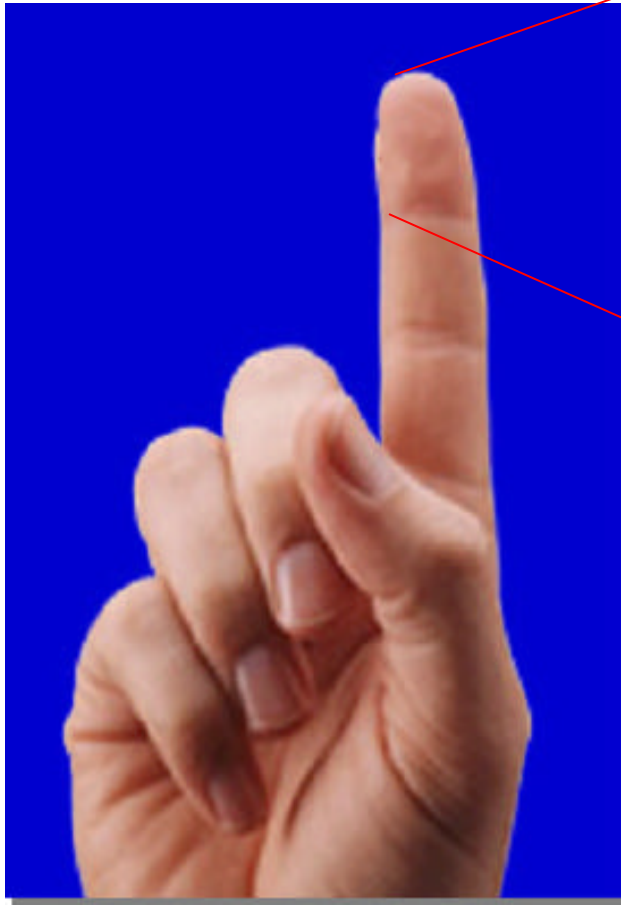
If Found, Return to:
ComTrust, LLC
7 McKee Place
Cheshire, CT 06410

Help-Line:
(800) 230-5462
registrar@comtrust.com





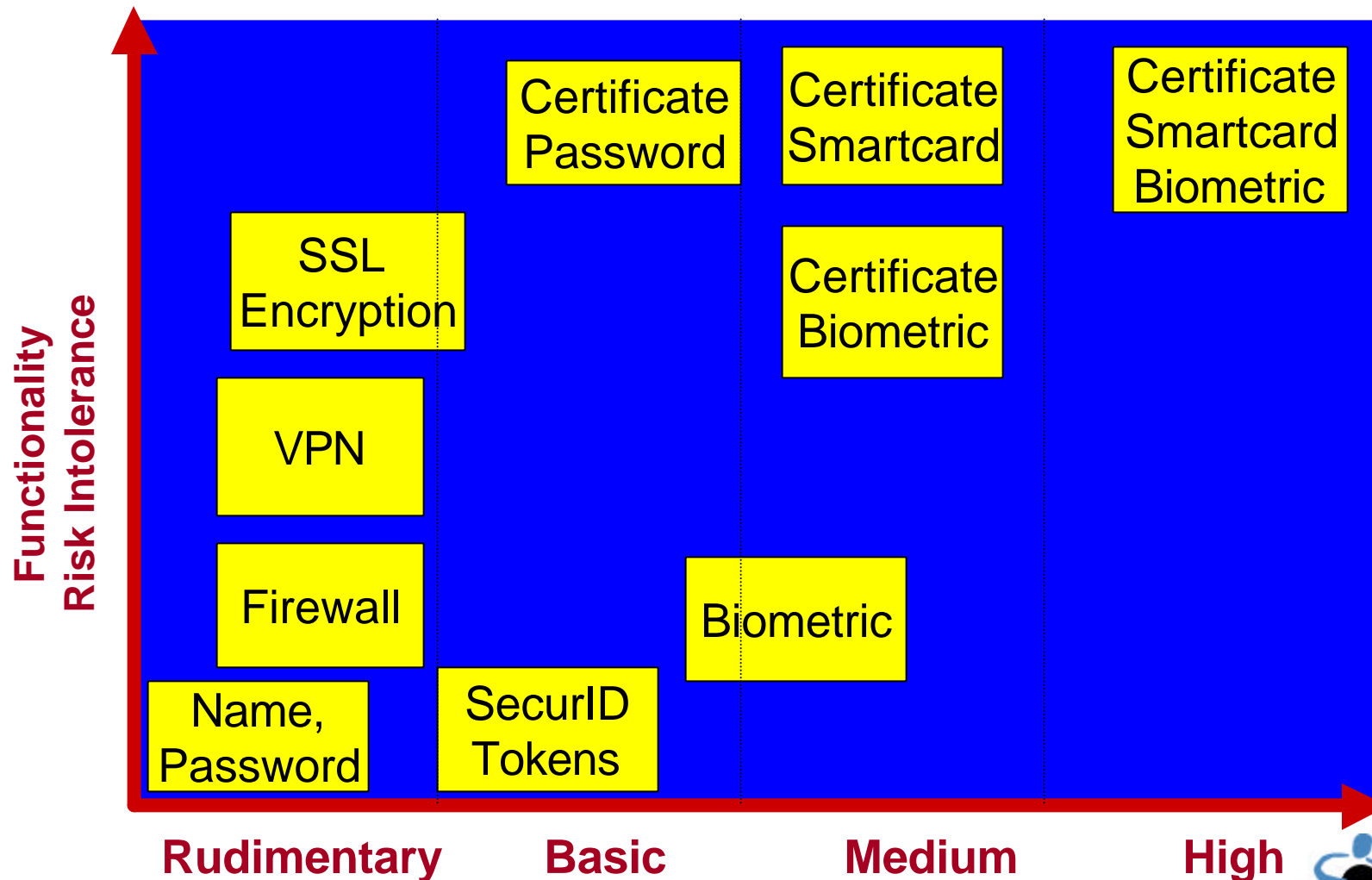
Fingerprint Authentication



- ✓ Convenience
- ✓ Never forget it
- ✓ Can't lose it
- ✓ Unique to individual
- ✓ Cannot be shared

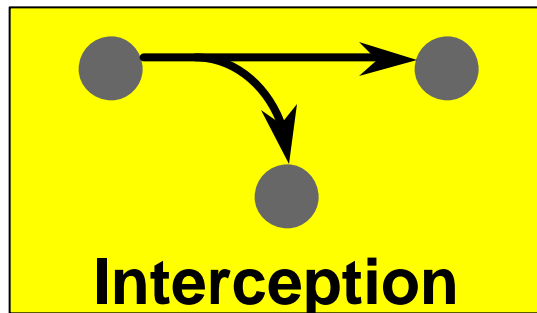


Business Need Drives Security Solution





Requirement: Confidentiality / Privacy

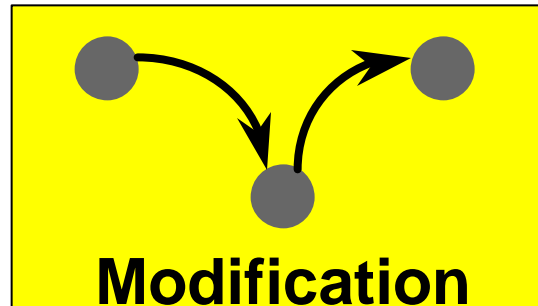


unauthorized revealing of information

Confidentiality - Assurance that content can only be read by the intended recipient. Encryption prevents others from viewing confidential information.



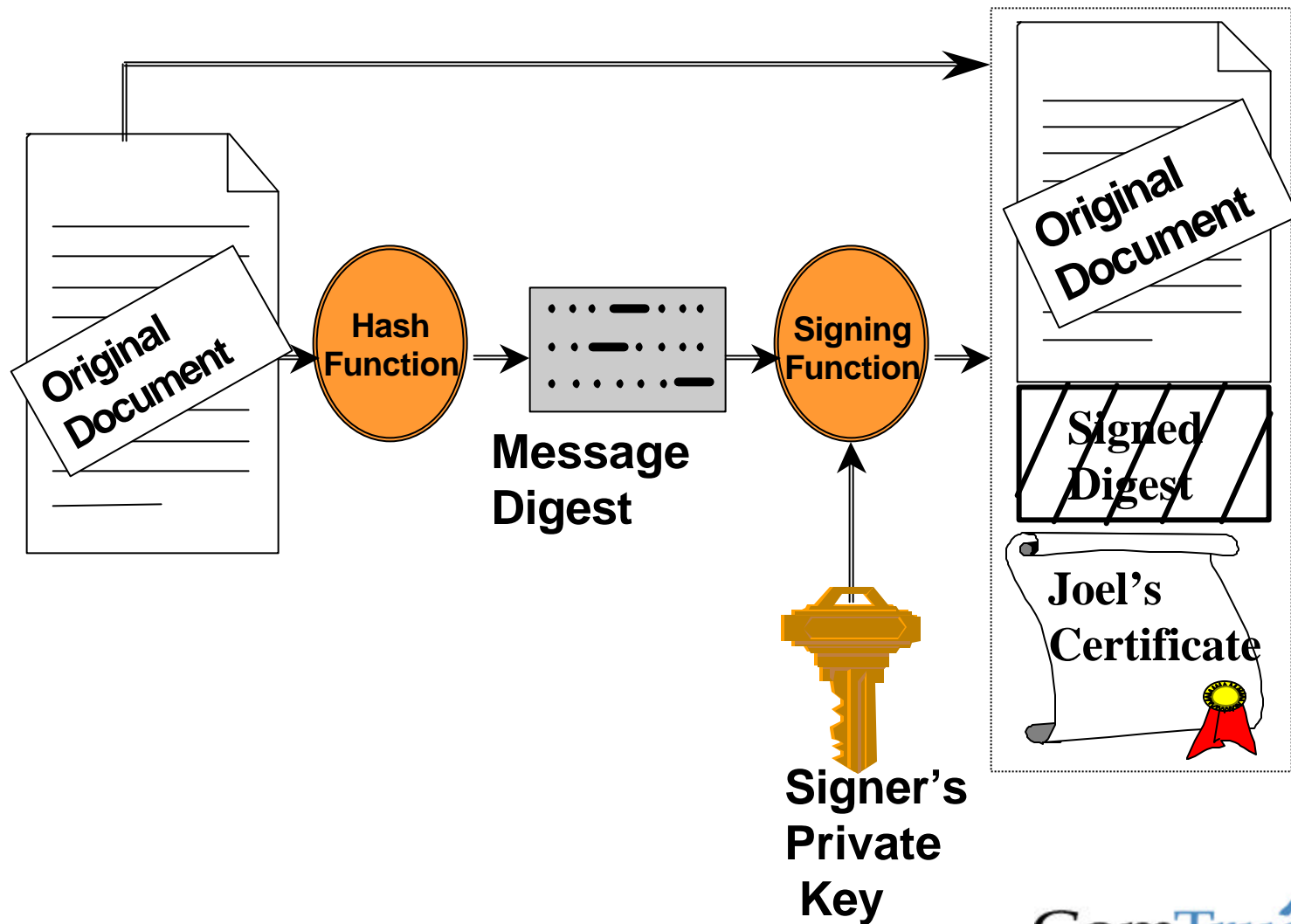
Requirement: Data Integrity



undetected alteration, or destruction of data

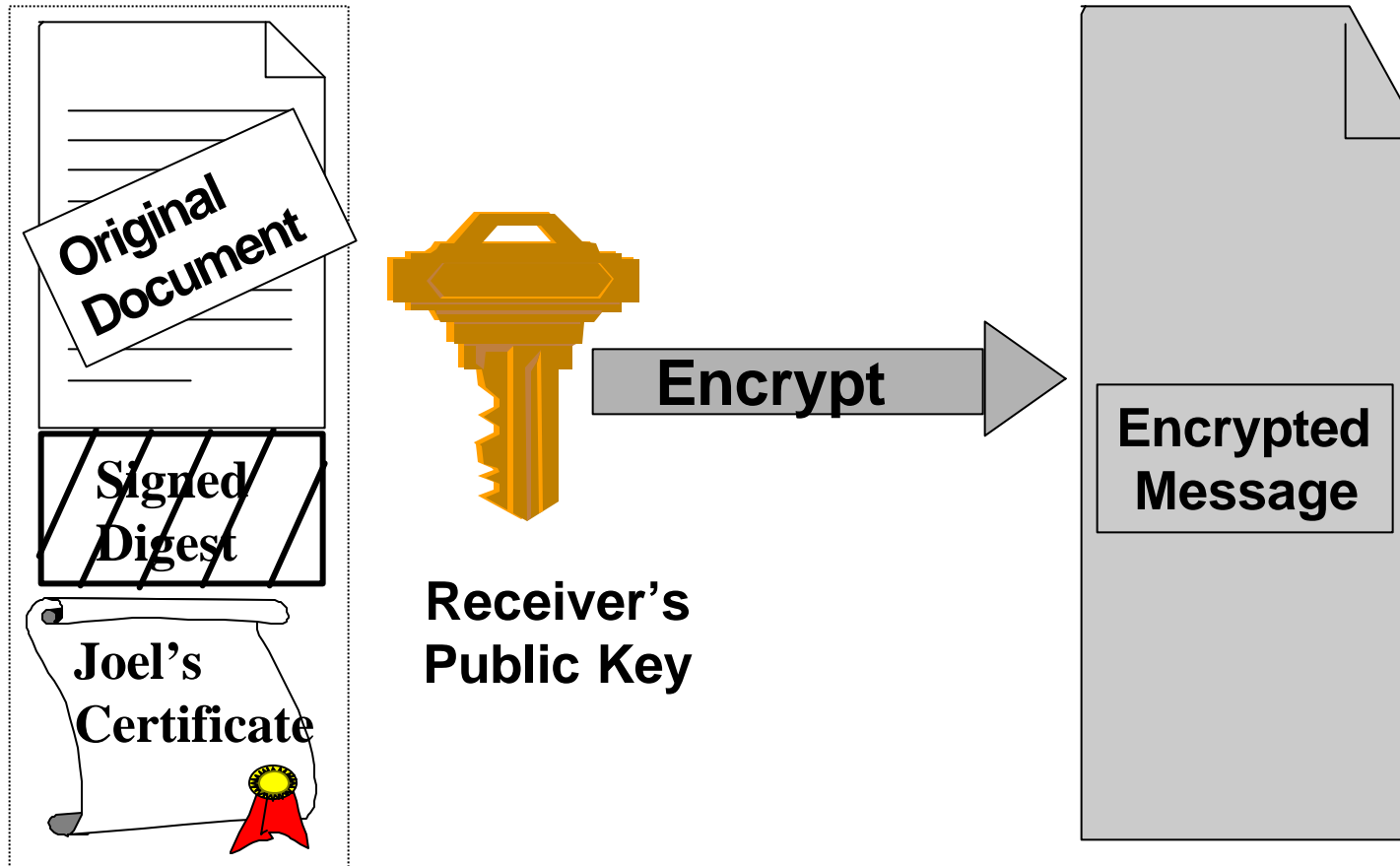
Integrity - A guarantee provided by electronic Digital Signature that contents of a message were not unaltered.

Requirement: Digital Signature “Signing”



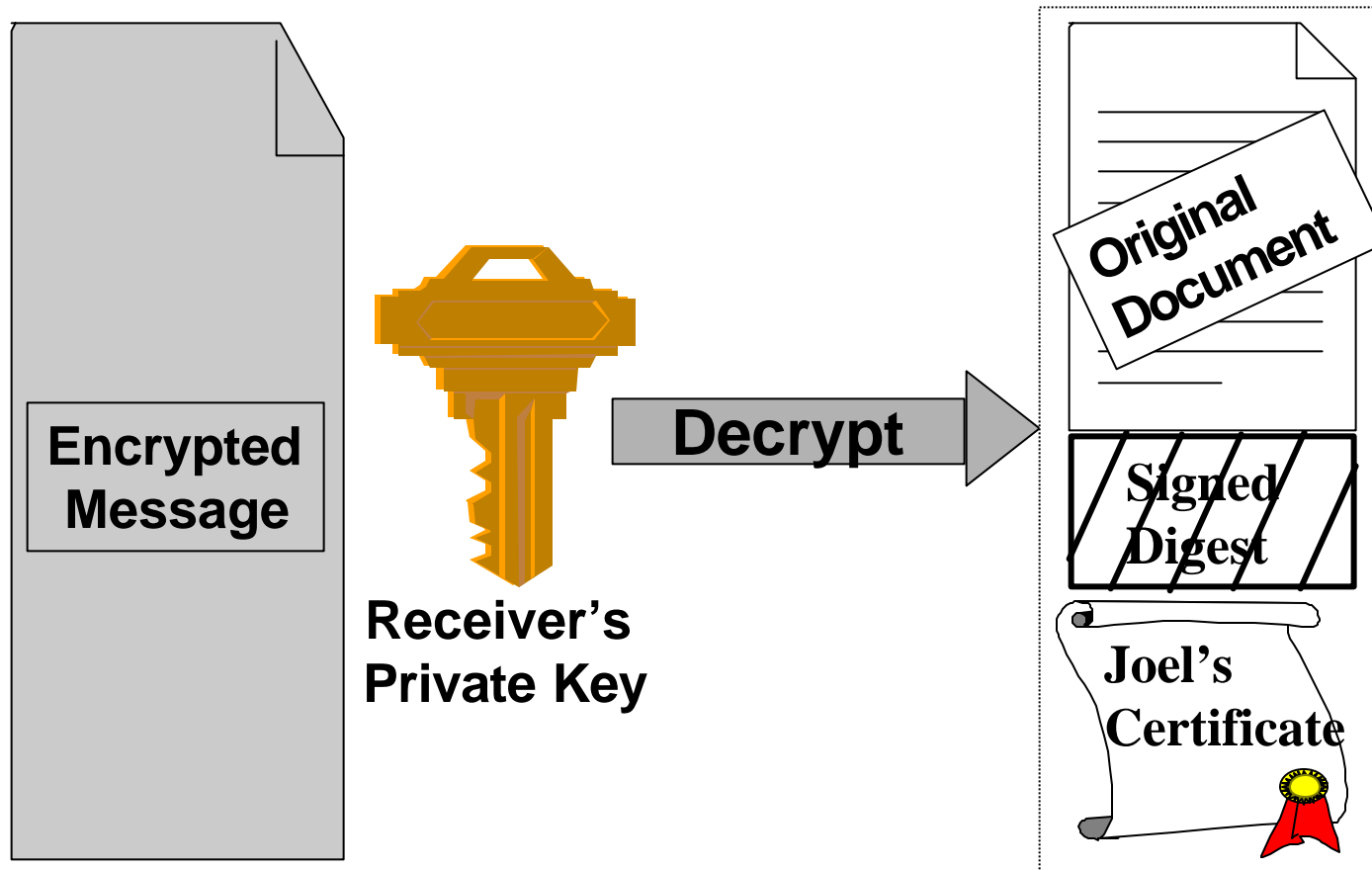


Requirement: 128 bit Encryption



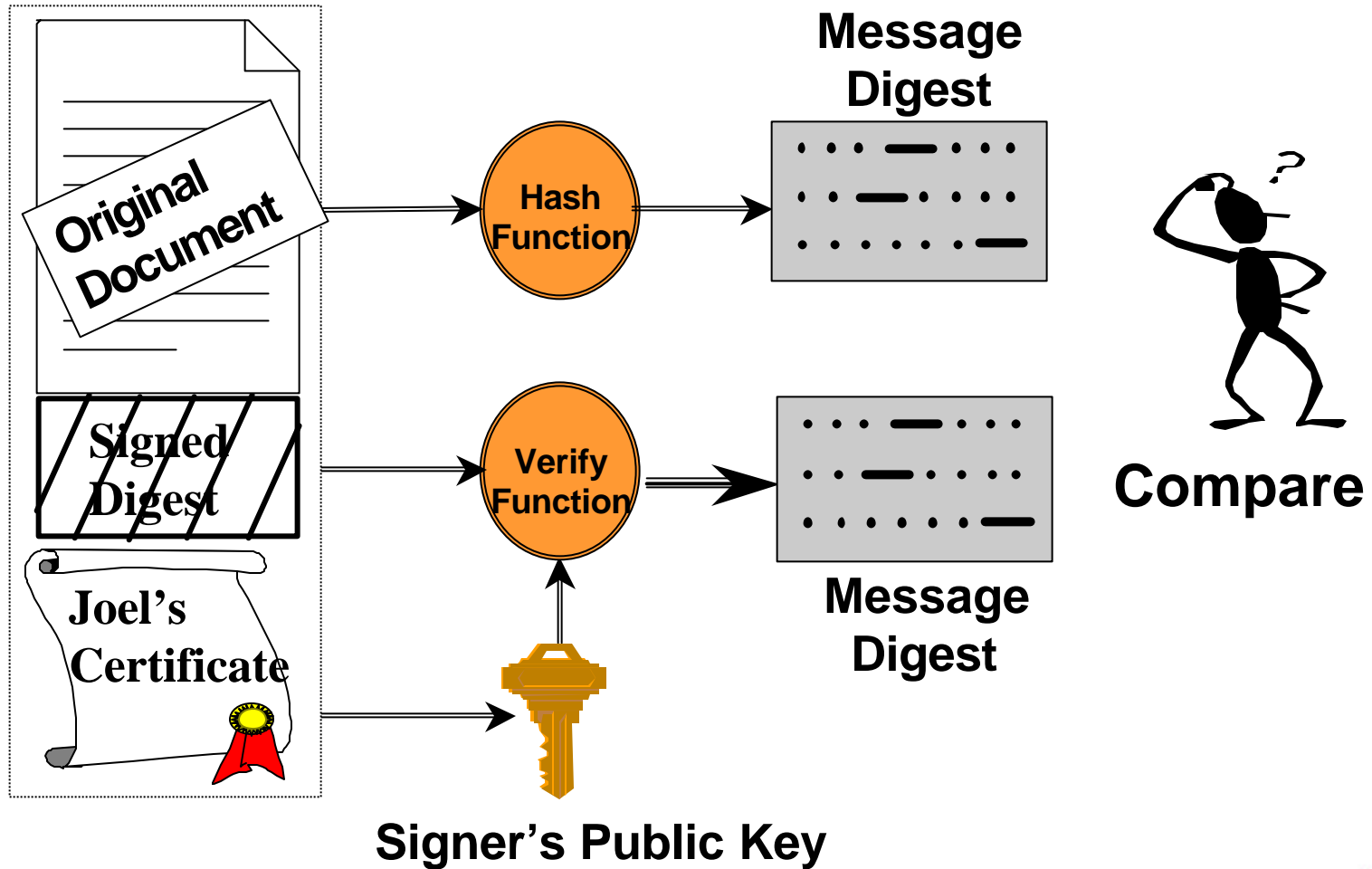


Requirement: Decryption





Requirement: Verification





What is Public Key Infrastructure?

- A combination of technical and procedural measures to ensure:
 - **accuracy** of identity and/or credentials
 - inextricable **binding** of identity and credentials to cryptographic keys used for digital signature
 - **validity** of identity, credentials and binding at time of transaction

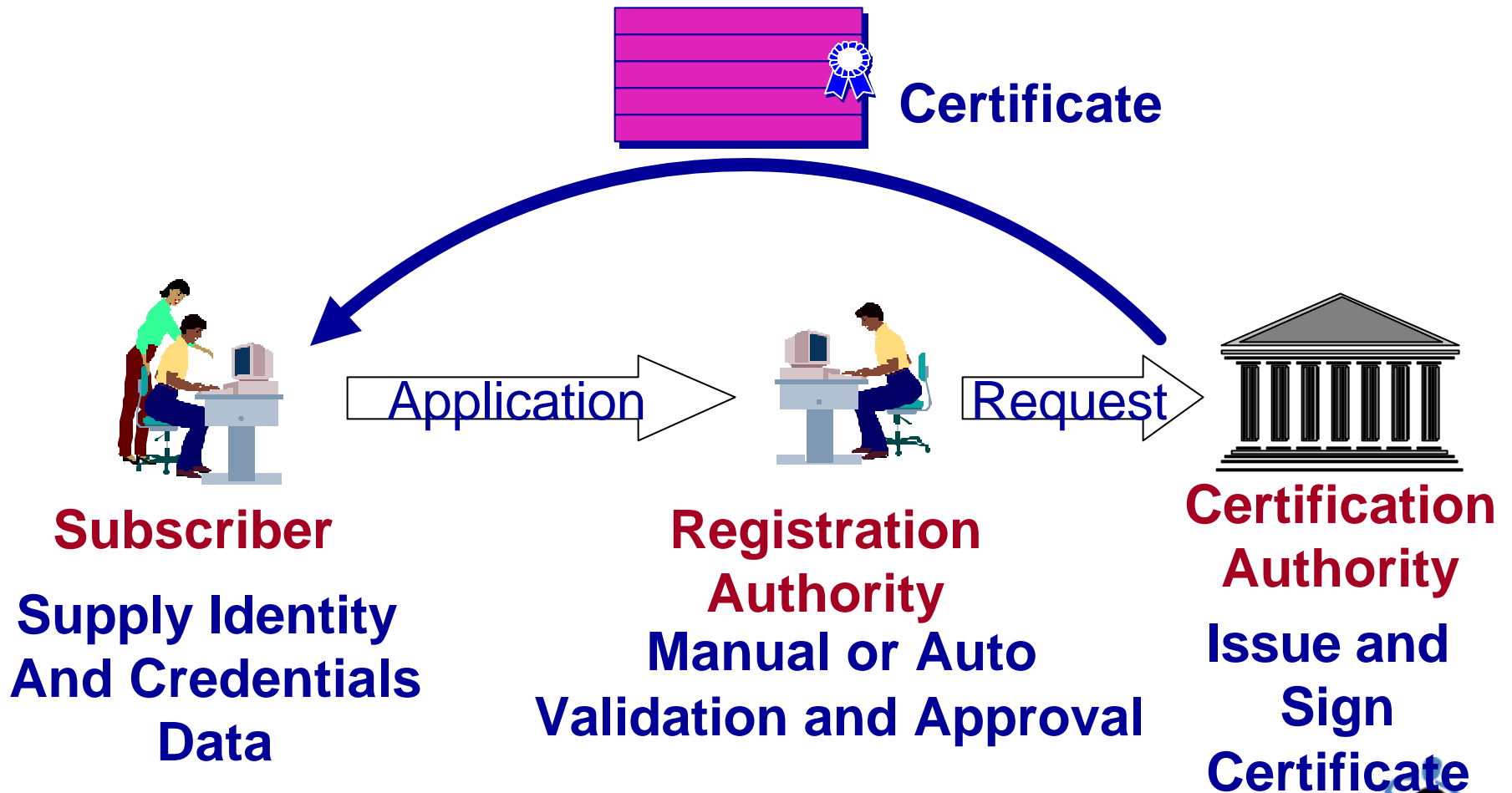


What Can Certificates Do?

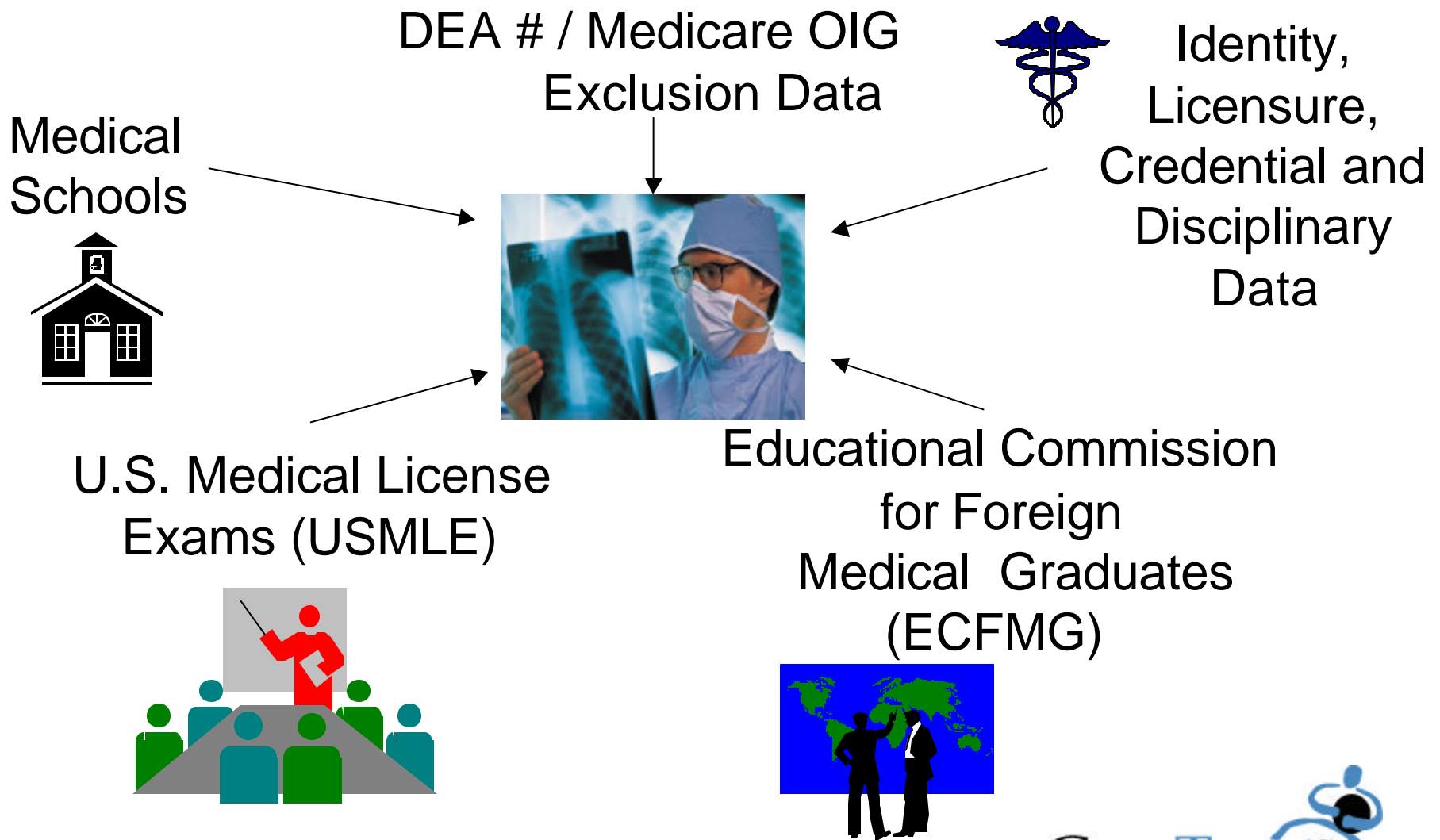
Provide portable, un-forgable attributes that convey:

- **Identity** (e.g. name, org, title/apparent authority)
- **Credentials** (e.g. MD, DO, CPA, Esq)
- **Authorizations** (explicit authority, limitations on authority - e.g. \$1MM signature authority, controlled substances)
- **Agency** (e.g. Power of Attorney)

Certificate Application



Physician Authentication / Validation



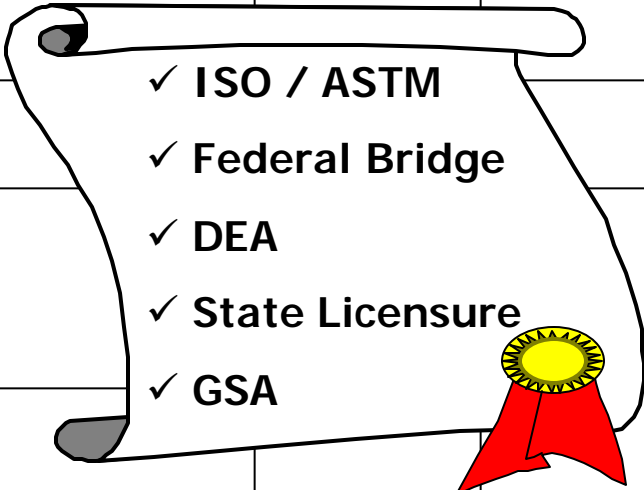


Why is Healthcare Policy Important?

- Policies define Levels of Trust
- CPS defines procedures/rules for trust
- Subscriber/Relying Party Contractual Agreement
 - Identity Proofing
 - Data Protection
 - Data Integrity
 - Signature/Authority

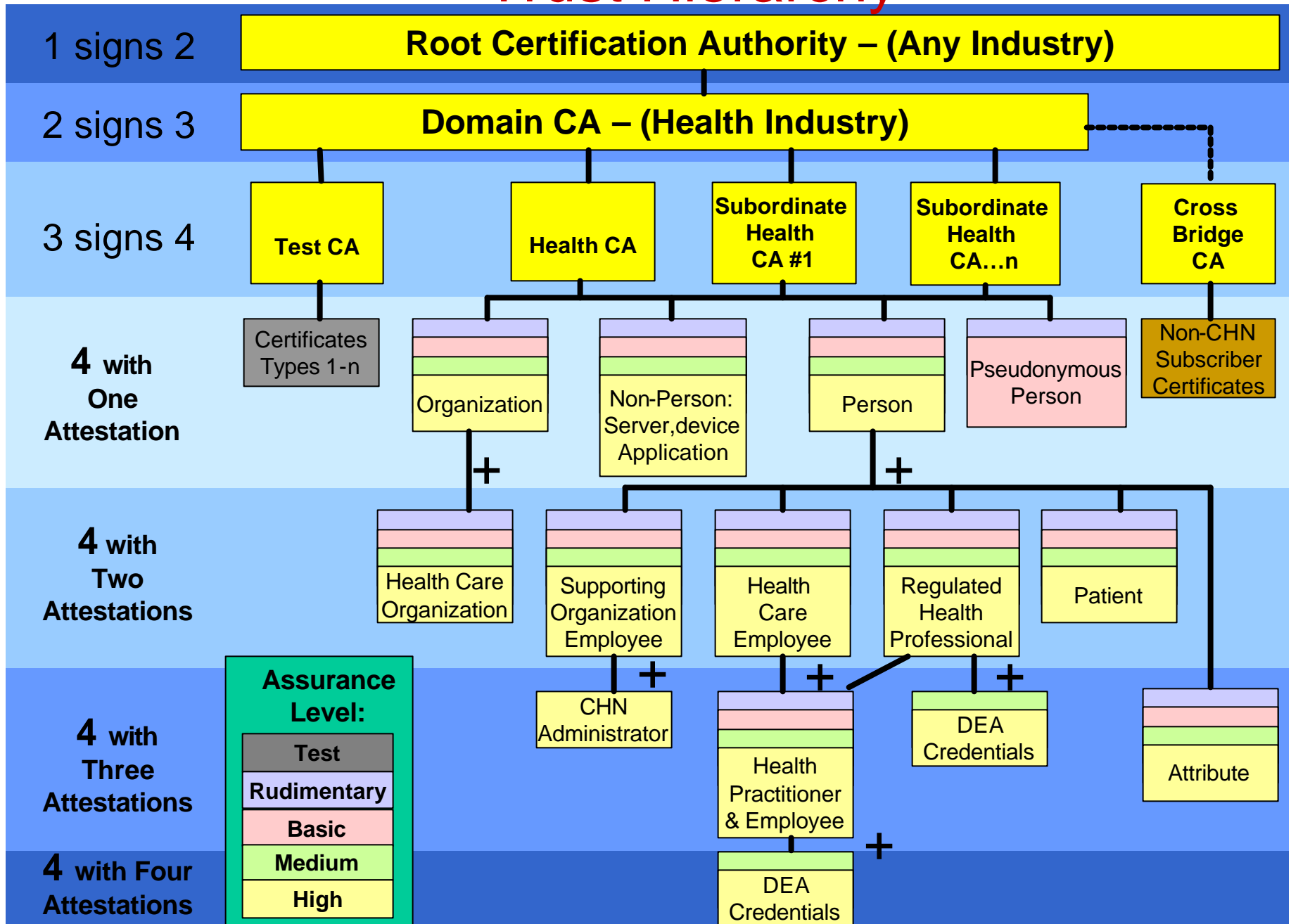
Healthcare Policy Frameworks

Type:	Rudimentary	Basic	Medium	High
Patient				
Employee				
Delegate				
Licensed Practitioner				
Server				
Group				
Device				

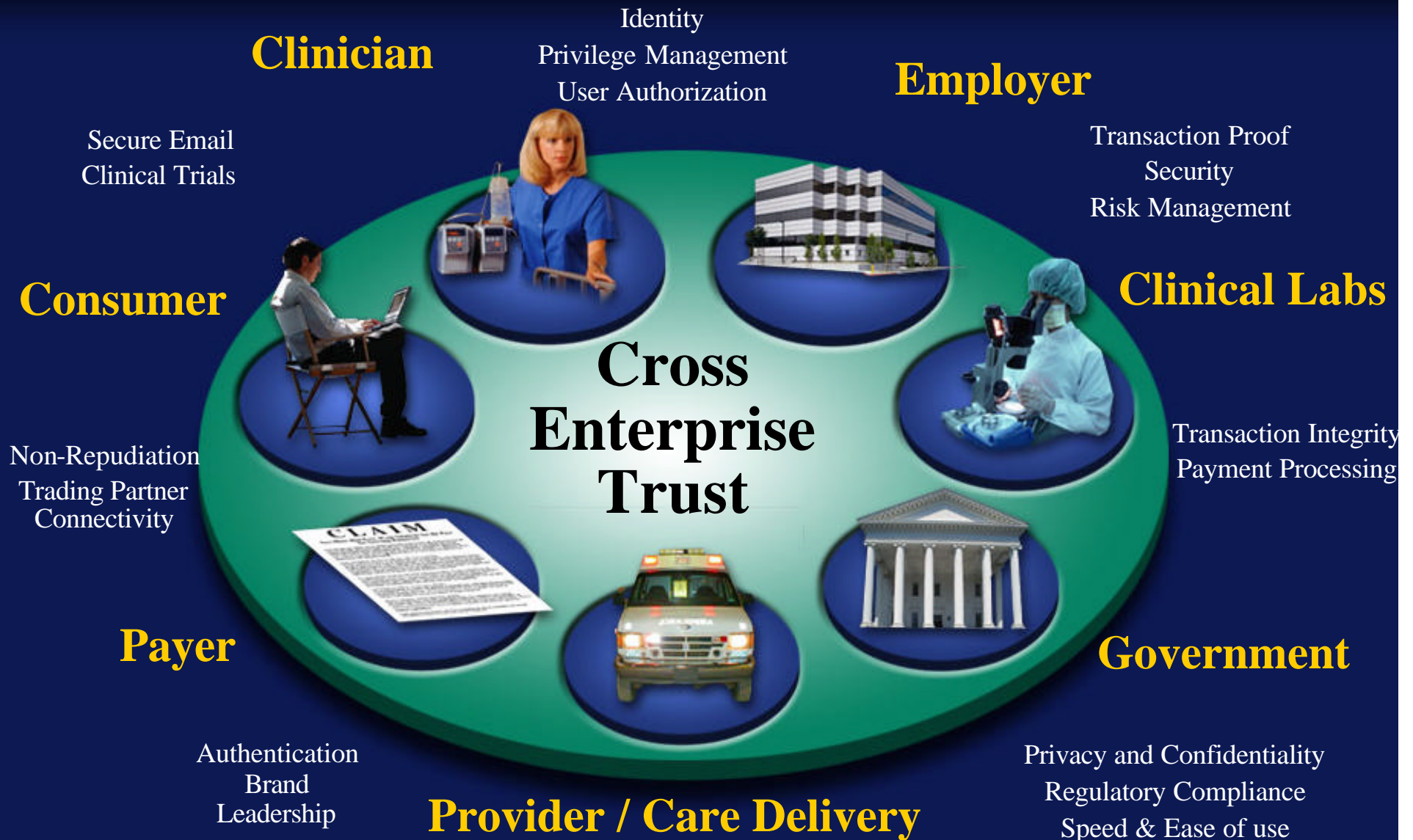


- ✓ ISO / ASTM
- ✓ Federal Bridge
- ✓ DEA
- ✓ State Licensure
- ✓ GSA

Trust Hierarchy

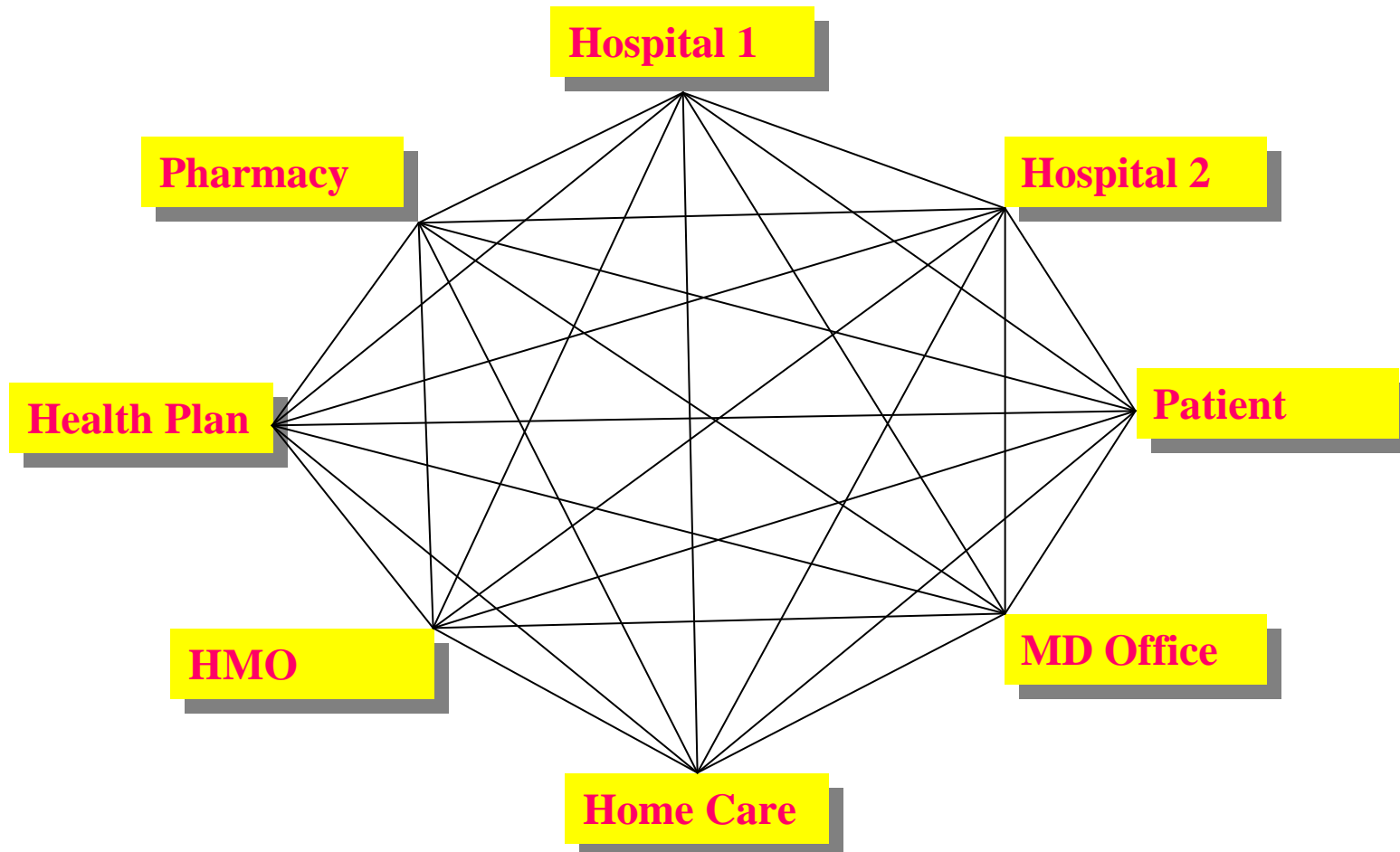


Visa Lessons Applicable to Healthcare



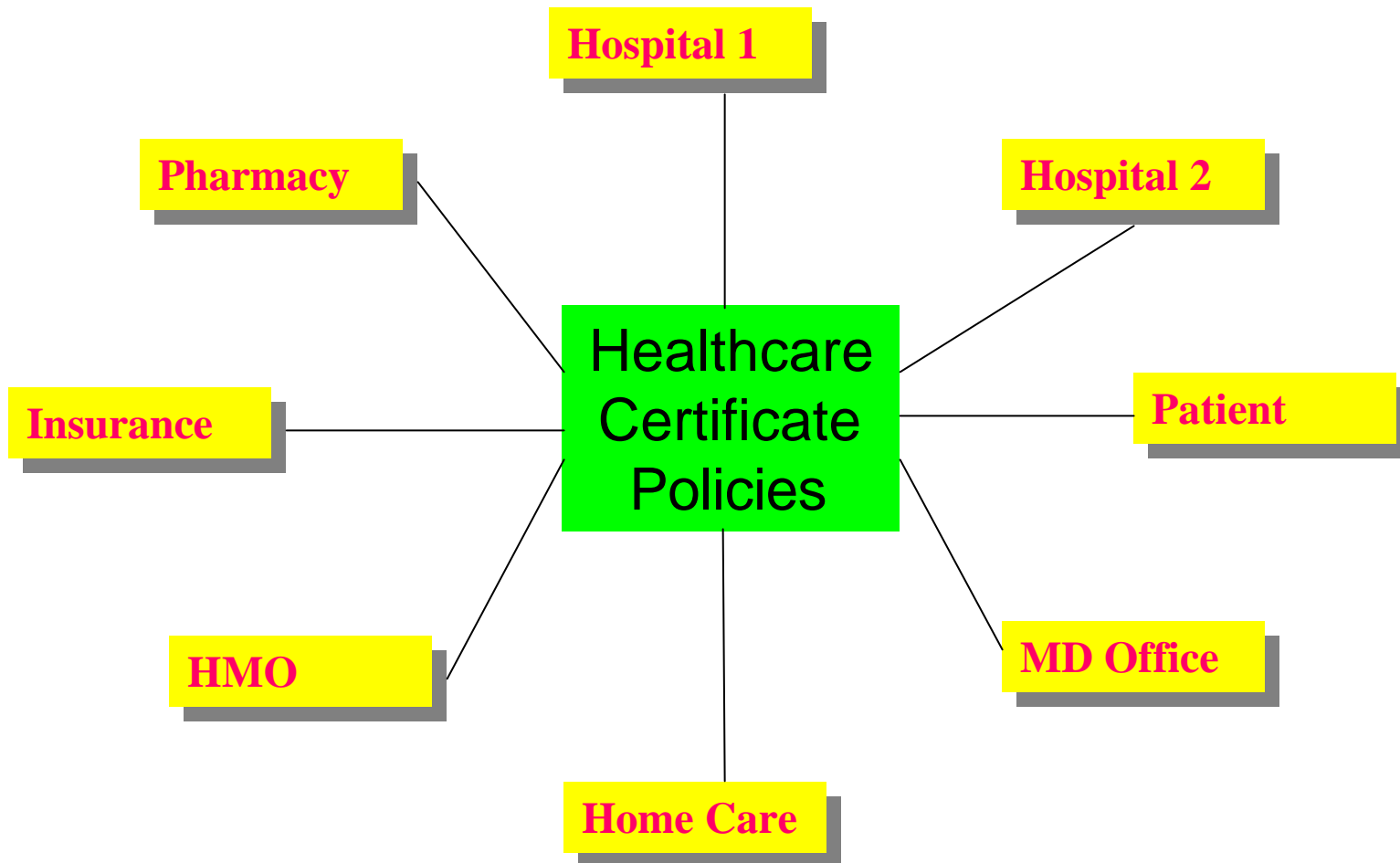


Bi-Lateral Policy Creation / Management





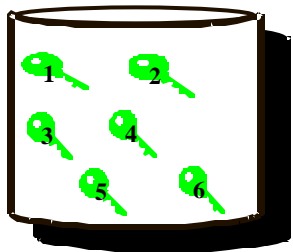
Cross-Entity Trust Model



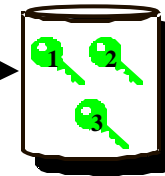


Using Public Healthcare Directories

- National Directory
 - Cross Enterprise Identities
 - Regulatory Information
 - Unique Name decipher
- Enterprise Directory
 - Enterprise Identities
 - Local Detail



National Healthcare Directory

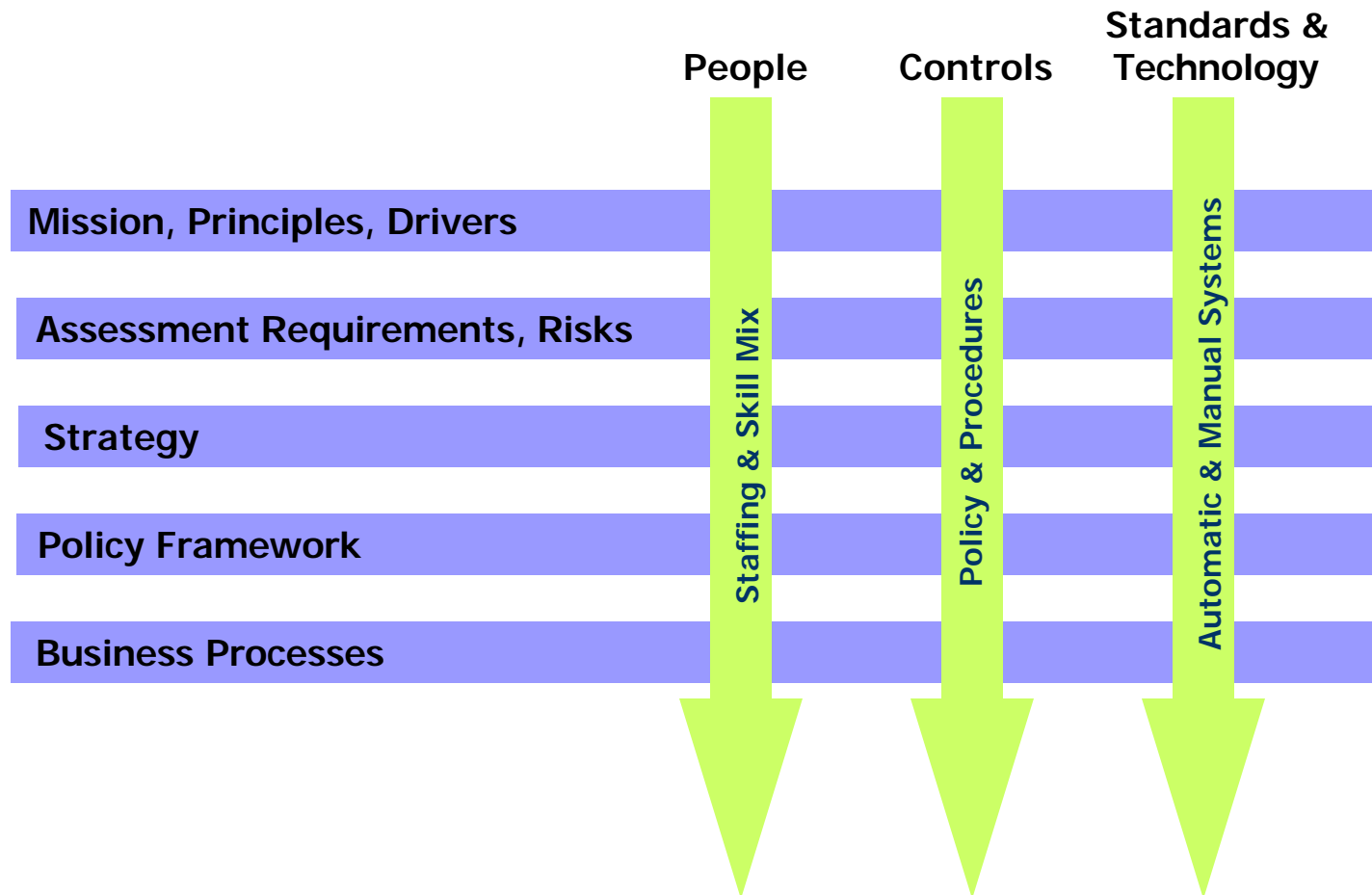


Enterprise Directory





Integrating Security with Business



Checklist

EDUCATION & AWARENESS

- ✓ Physical Access Control
- ✓ Asset Protection
- ✓ Active Environmental Monitoring

POLICY INFRASTRUCTURE

- ✓ Security Policy
- ✓ Policy Governance
- ✓ Certificate Policy
- ✓ Privacy Policy

PHYSICAL SECURITY

- ✓ Physical Access Control
- ✓ Asset Protection
- ✓ Active Environmental Monitoring

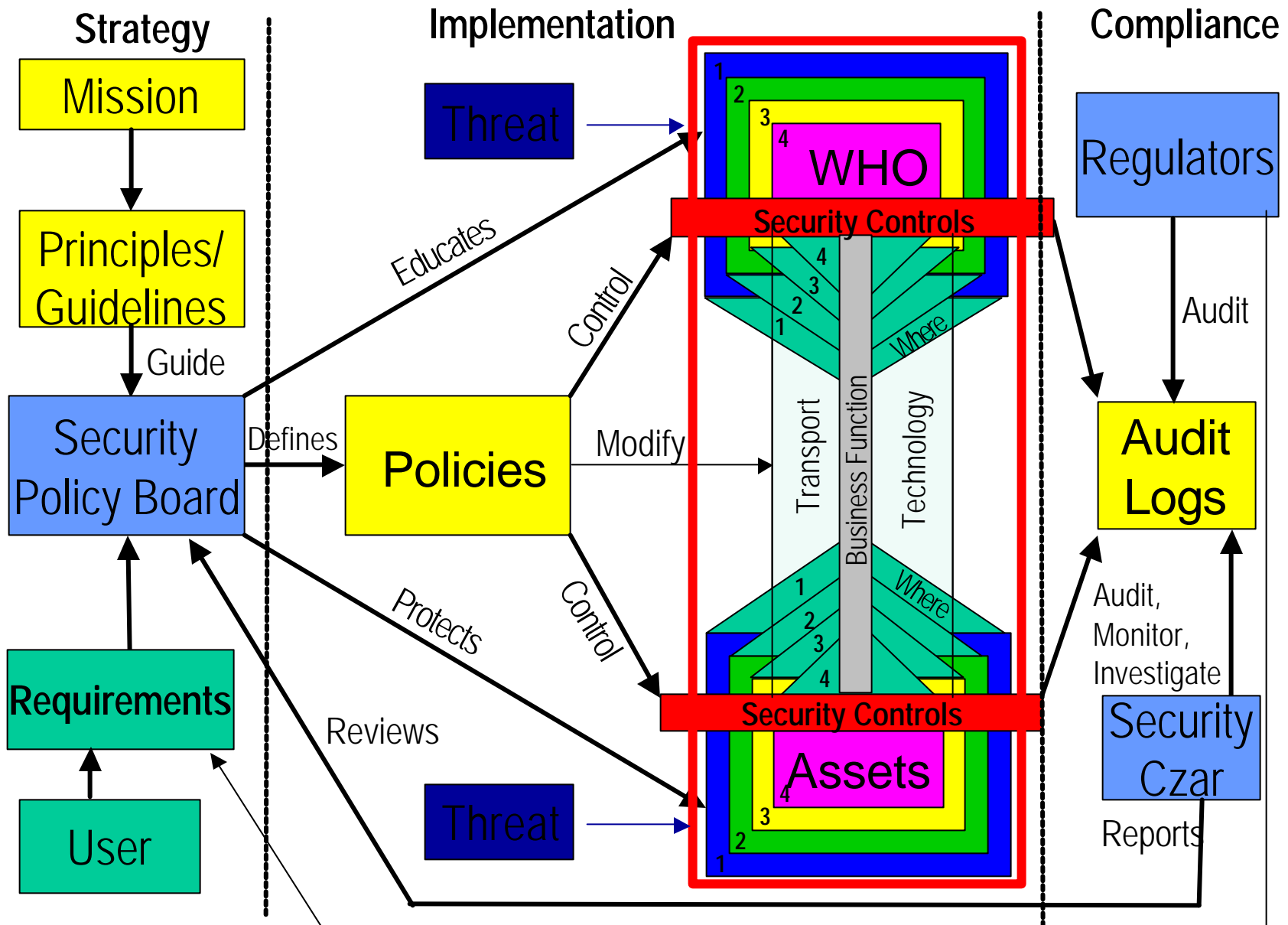
NETWORK & APPLICATION SECURITY

- ✓ DMZ
- ✓ Firewall
- ✓ VPN
- ✓ Remote Access
- ✓ SecurID™
- ✓ Directory Services
- ✓ Configuration Mgmt
- ✓ Virus Protection
- ✓ Authentication
- ✓ Access Control
- ✓ Backups
- ✓ Intrusion Detection
- ✓ VLANs
- ✓ Active Monitoring & Control

TECHNOLOGY TOOLS

- ✓ SSL
- ✓ VPN
- ✓ Smartcards
- ✓ Biometrics
- ✓ Certificates (CA)
- ✓ Registration & Revocation Service

Information Security Process Model





Which are You?

- Prophet?
- Contrarian?
- Carpetbagger?
- Other?
- All of the Above?
- Some of the Above?
- Banker



“Neither a wise man nor a brave man lies down on the tracks of history waiting for the train of the future to run over him”

-- Dwight D. Eisenhower



Health with HIPAA

Prophets, Contrarians and Carpetbaggers

Joel F. French
President and CEO
ComTrust[®], LLC
248-763-0671
Jfrench@comtrust.com
www.comtrust.com