authentica

Managing the Risk:

Information Security Technologies

Bryce Griswold
System Engineer
Authentica, Inc.

Kevin Barry
Director Eastern Sales
Authentica, Inc.

The Issue:

Need to share information both internally and externally – with employees, contractors and other agencies

- Intra-organizational dissemination
- COI (Communities of Interest)
- Coalitions
- SBU data
- Need to know information
- RFP/RFQ content to many vendors
- Agency to Agency
- Homeland Security information

The Opportunity:

- More efficient organization
- Improved control of Intellectual property
- Delivery of up to date need to know data
- More accurate data
- Auditing
- Digitally shred sensitive data
- More effective decisions due to having access to the most current data

The Risk

- **Partnership one day, competition the next**
- **Contactors who serve your competitors as well as your company**
- **Careless or malicious users**
- **High employee turnover, increased use of contractors**
- **Lost/stolen computing devices**
- **Indiscriminate e-mail discussions**
- **Digital information scattered over a distributed workforce and partner network**

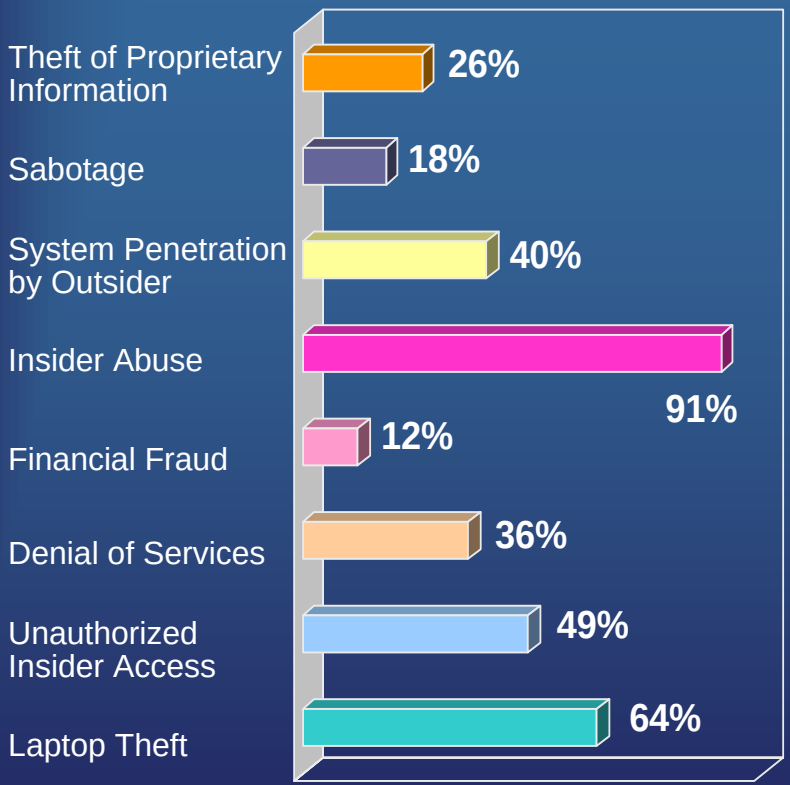
➢ **Leak or unintended redistribution of mission-critical information**

➢ **Persistence of outdated information**

Loss of control over sensitive information

Lock the windows too?

$377 Billion in annual losses to US companies



How information is lost

- Not defensible with traditional access-based security solutions
- There needs to be a solution that protects the information itself

Source: **2001 CSI/FBI Computer Crime and Security Survey**

Case Study

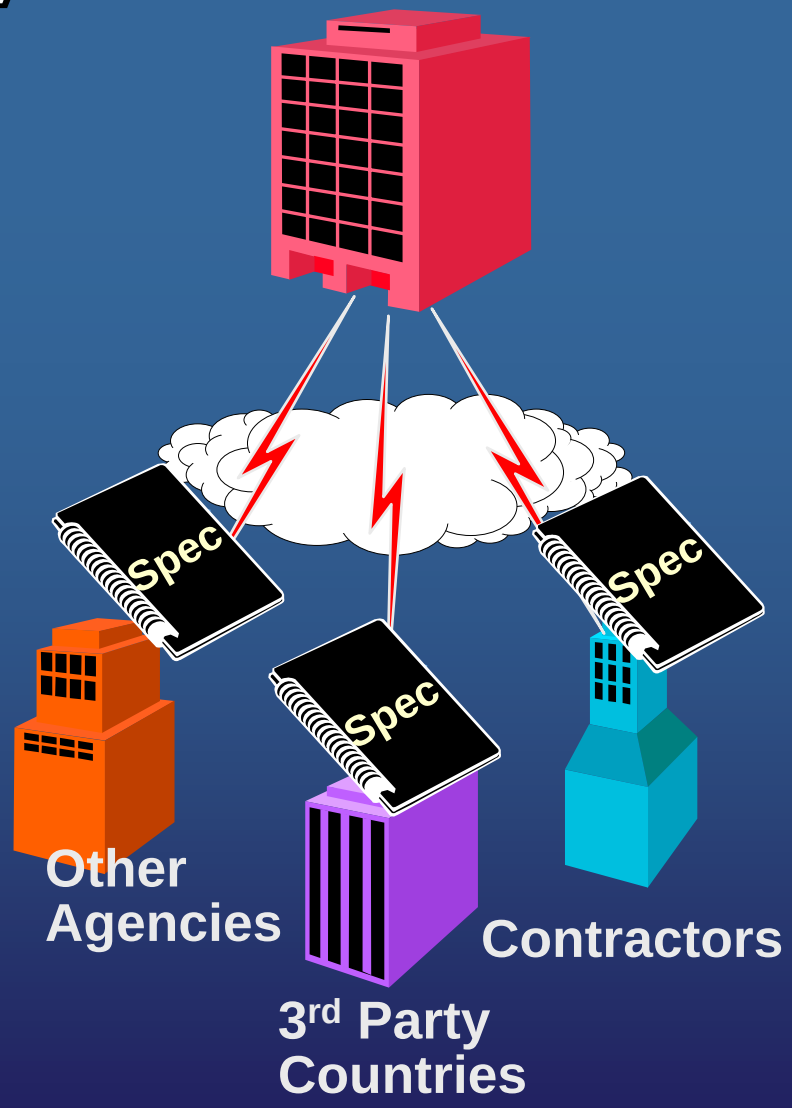
Dissemination of Intelligence Reports

Problem:

Need easier way share confidential information with analysts and decision makers

Issues:

- Tracking the number of paper copies in circulation
- Authorization (PKI, secure id, etc. not enough
- No protection from copying, difficult to retrieve
- Multiple levels of sensitivity within a document

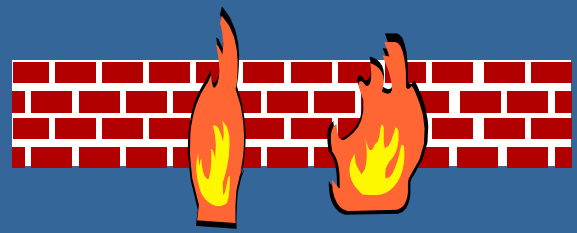


Securing the Information

Traditional tools

- Firewalls
- Symmetric file encryption
- Asymmetric encryption
  - S/MIME, PGP, etc
- Web access control

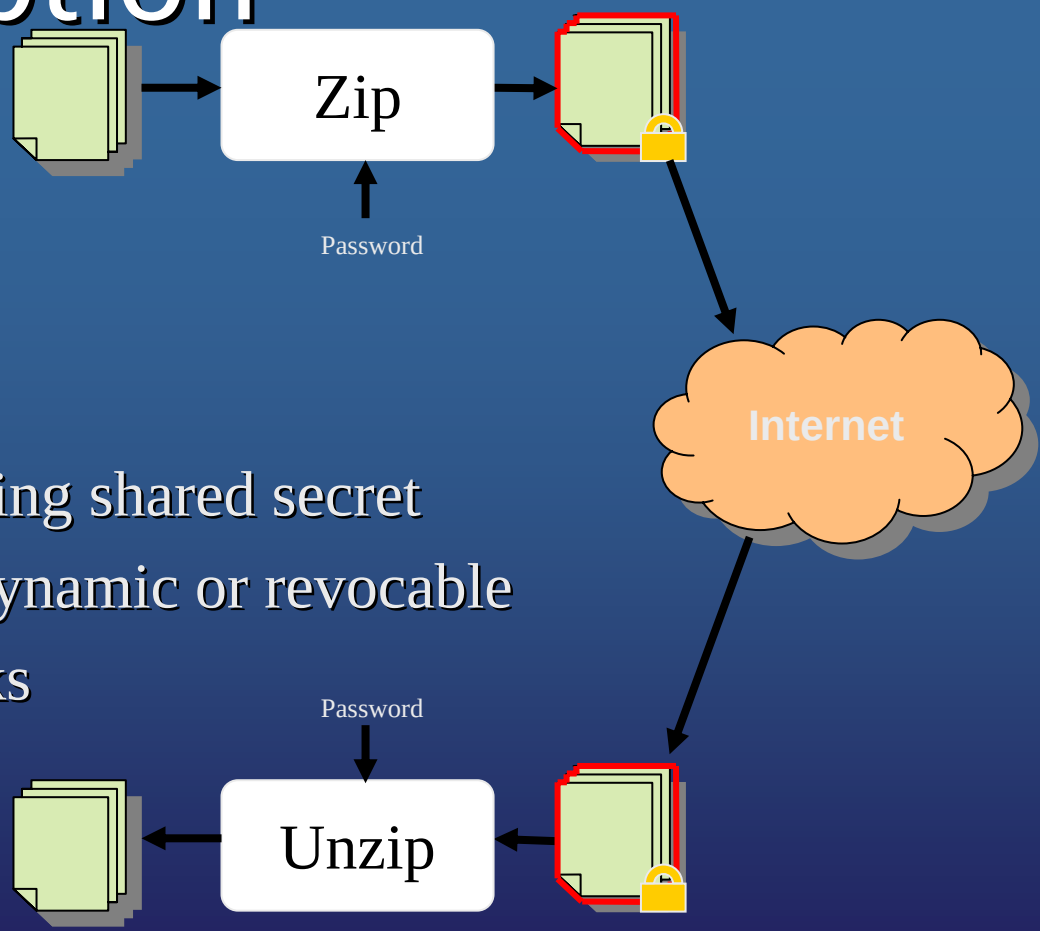
Firewalls



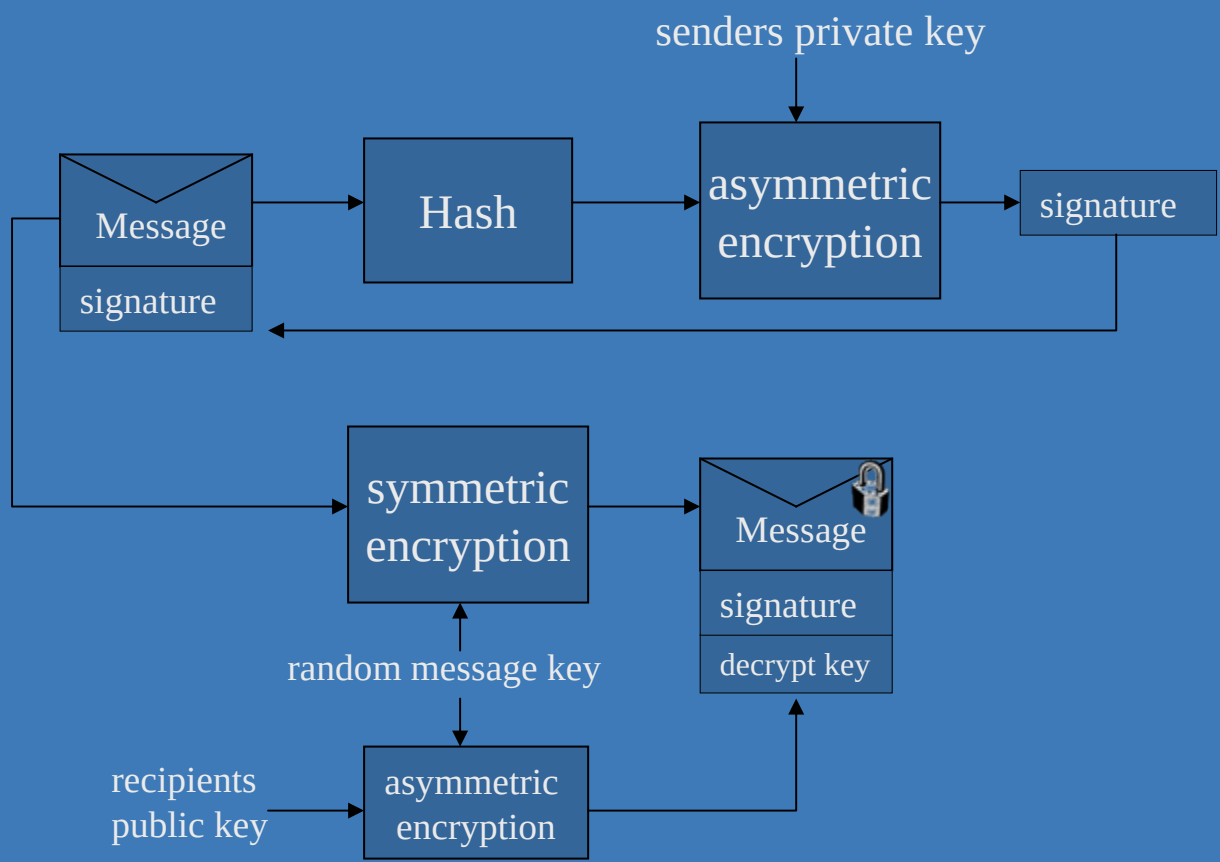
- Pros:
  - Protects the perimeter from “hackers”
  - Central administration
  - Mature technology
- Cons:
  - Complex Configuration
  - Provides no privacy or non-repudiation
  - Doesn’t protect information from insiders
  - No persistency of control
  - Limited Auditing
  - Perimeter control

Symmetric File Encryption

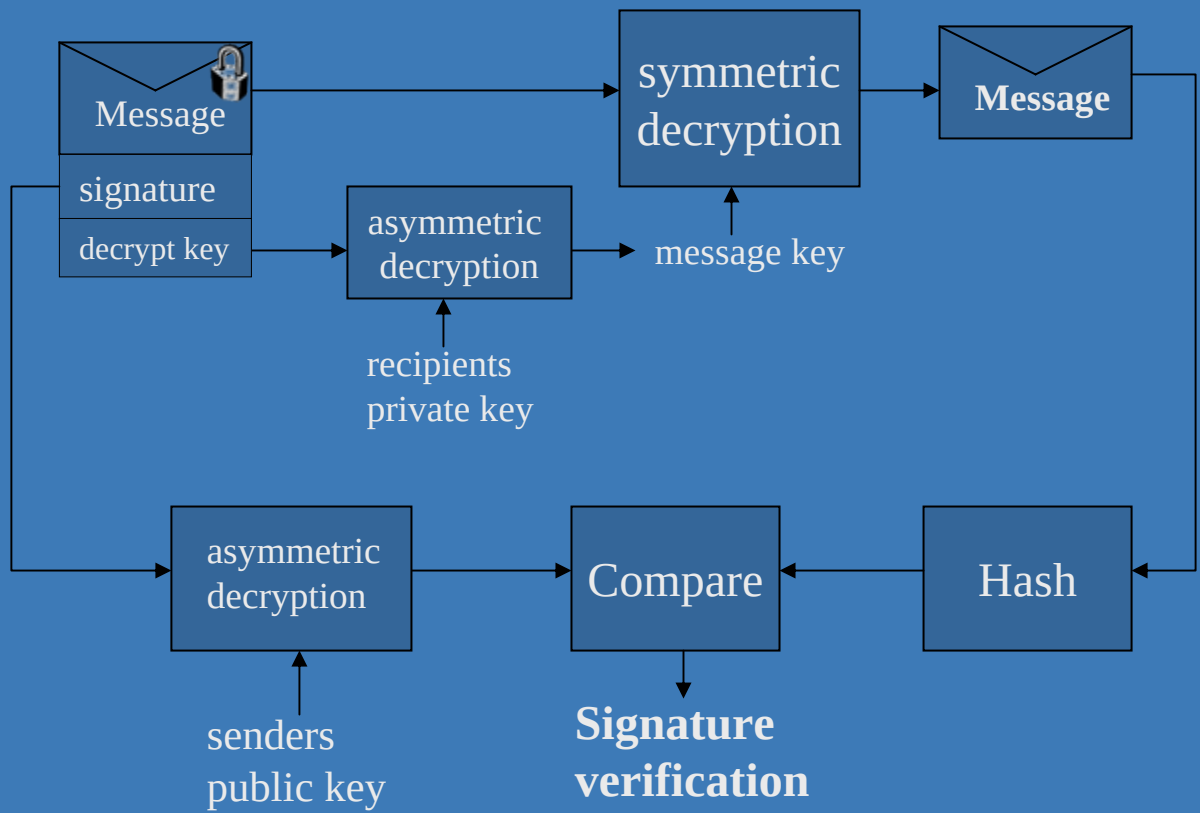
- Pros:
  - Cheap and simple
  - Provides privacy
- Cons:
  - Issues with communicating shared secret
  - Control not persistent, dynamic or revocable
  - Subject to off-line attacks
  - No auditing
  - Transferable



Asymmetric Encryption Overview (Sender)



Asymmetric Encryption Overview (Recipient)



Asymmetric Encryption

- Pros:
  - Reliable user-specific encryption
  - Sender non-repudiation
  - Strong authentication
  - Native to mail application
  - More than mail
- Cons:
  - PKI issues
    - key distribution
    - trust
    - certificate revocation
  - Control not persistent, dynamic or revocable
  - No auditing
  - Transferable

Web Access Control

- Pros:
  - No client component required
  - Simple user experience
  - Can be integrated into existing apps
  - Highly customizable
  - Encrypted during transmission (ssl)
- Cons:
  - Weak authentication
  - Control not really persistent, dynamic or revocable
  - Limited auditing
  - Transferable
  - Single point of vulnerability

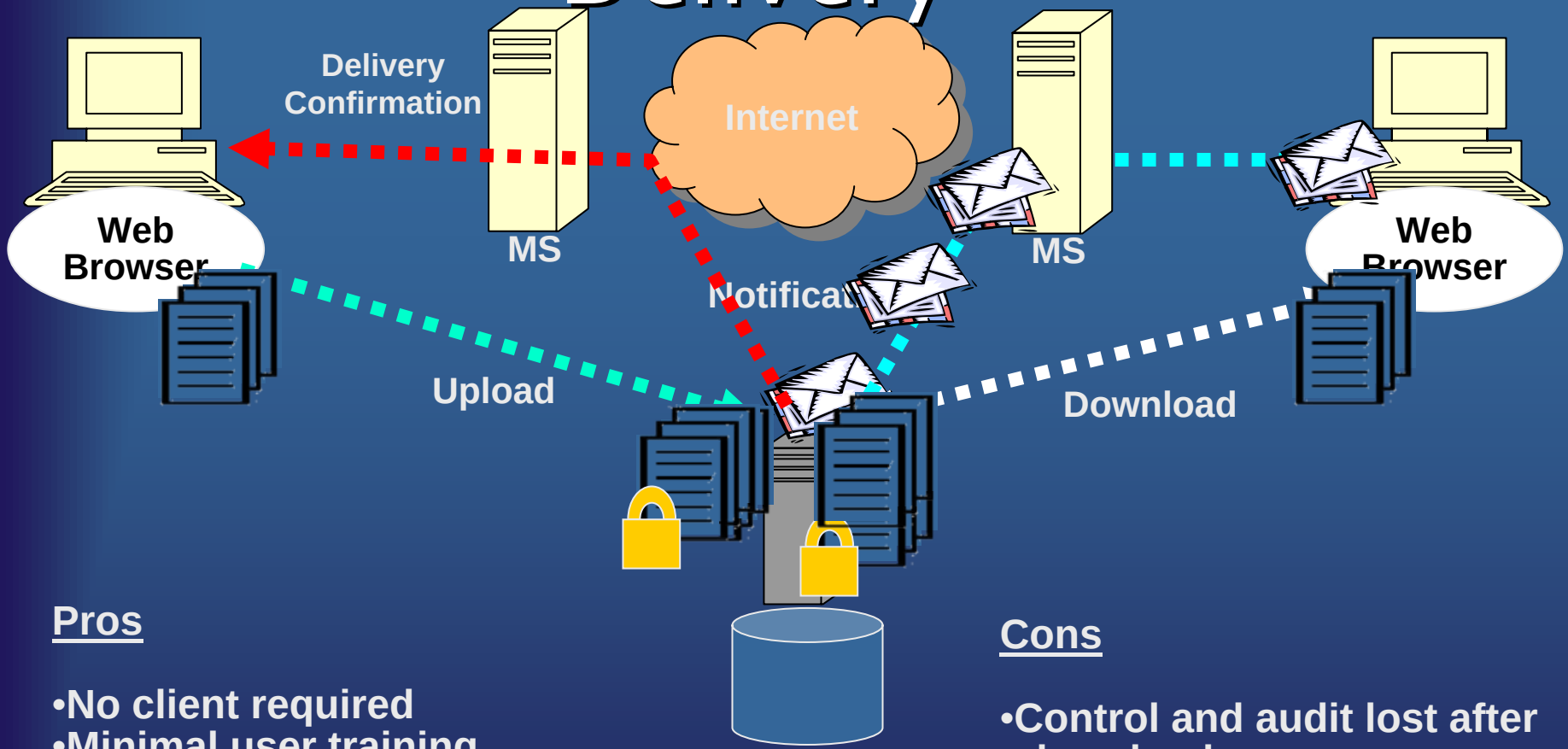
What's Missing?

- The ability to control and protect the information after its delivered
  - Change access rules after it is delivered
  - Expire access and restrict forwarding
  - Restrict print and copy rights
  - Continual audit trail
  - Protection independent of delivery

Some New Alternatives

- Secure delivery services
  - Secure Web document delivery
  - E-mail notification and server encryption
- Traditional Digital Rights Management (DRM)
  - Secure wrappers for digital media
- Dynamic DRM (Active Rights Management)
  - Information encrypted and key and policy managed centrally

Secure Document Delivery



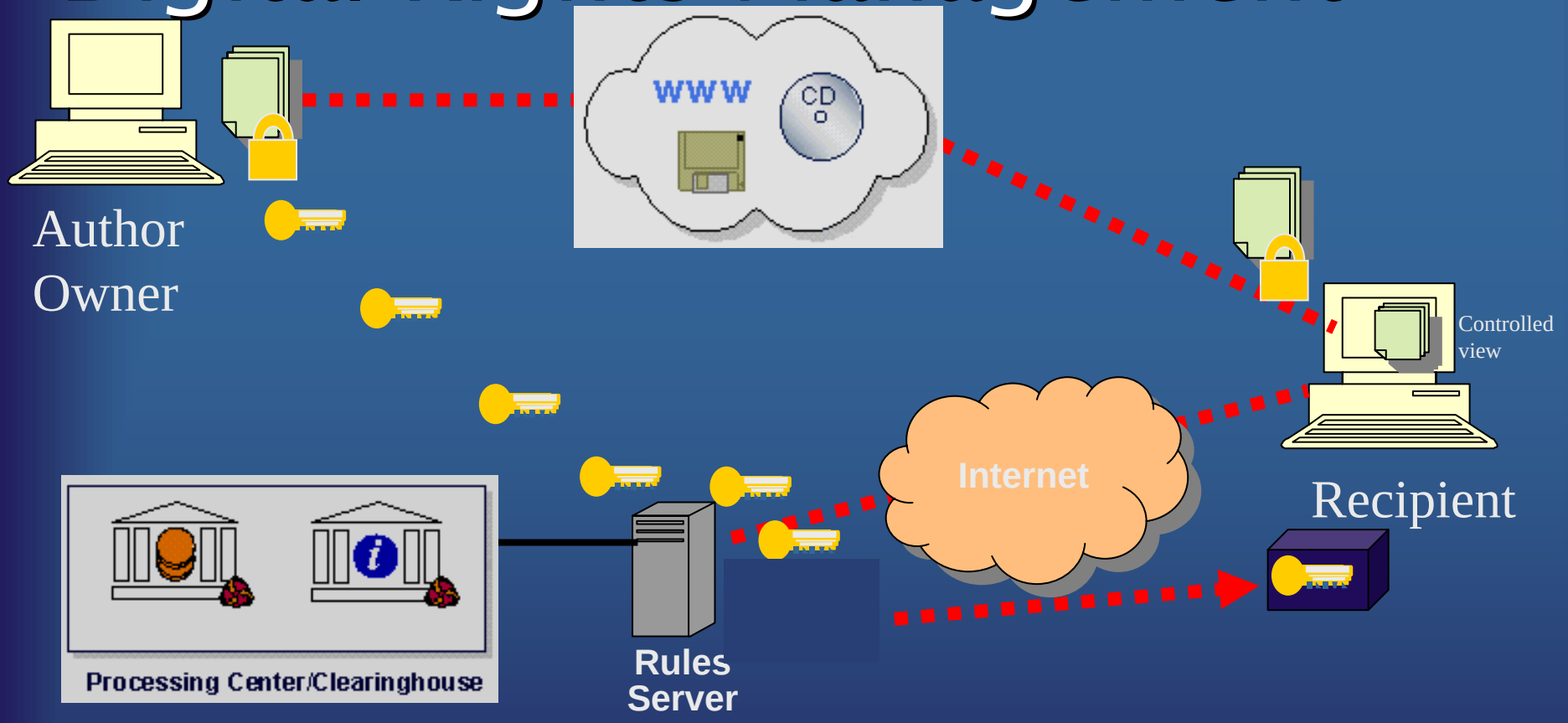
Pros

- No client required
- Minimal user training
- Encrypted during transmission
- Revocable until download and save
- Limited audit

Cons

- Control and audit lost after download
- No use control
- Transferable
- Single point of vulnerability

Digital Rights Management



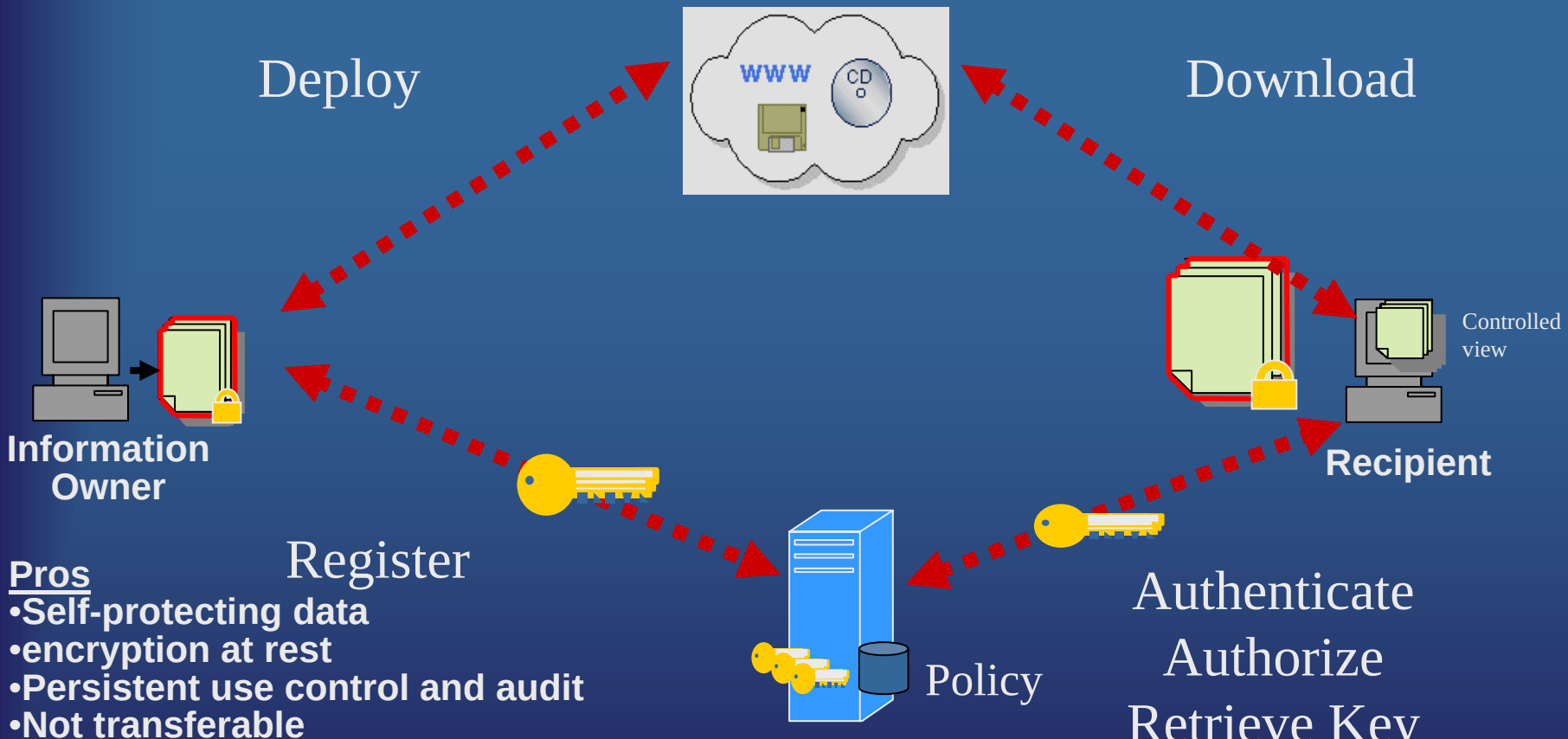
Pros

- Always encrypted
- Enforces use control
- Not transferable
- Limited audit

Cons

- Requires client to view
- Not revocable
- Audit initial access only
- Subject to offline attack
- Geared toward e-commerce apps

Active Rights Management



Pros
- Self-protecting data
- encryption at rest
- Persistent use control and audit
- Not transferable
- Revocable
- Dynamic policy control
- Permanent audit

Cons
- Requires client
- Requires connectivity to view

Ultimate Goal: Information Control

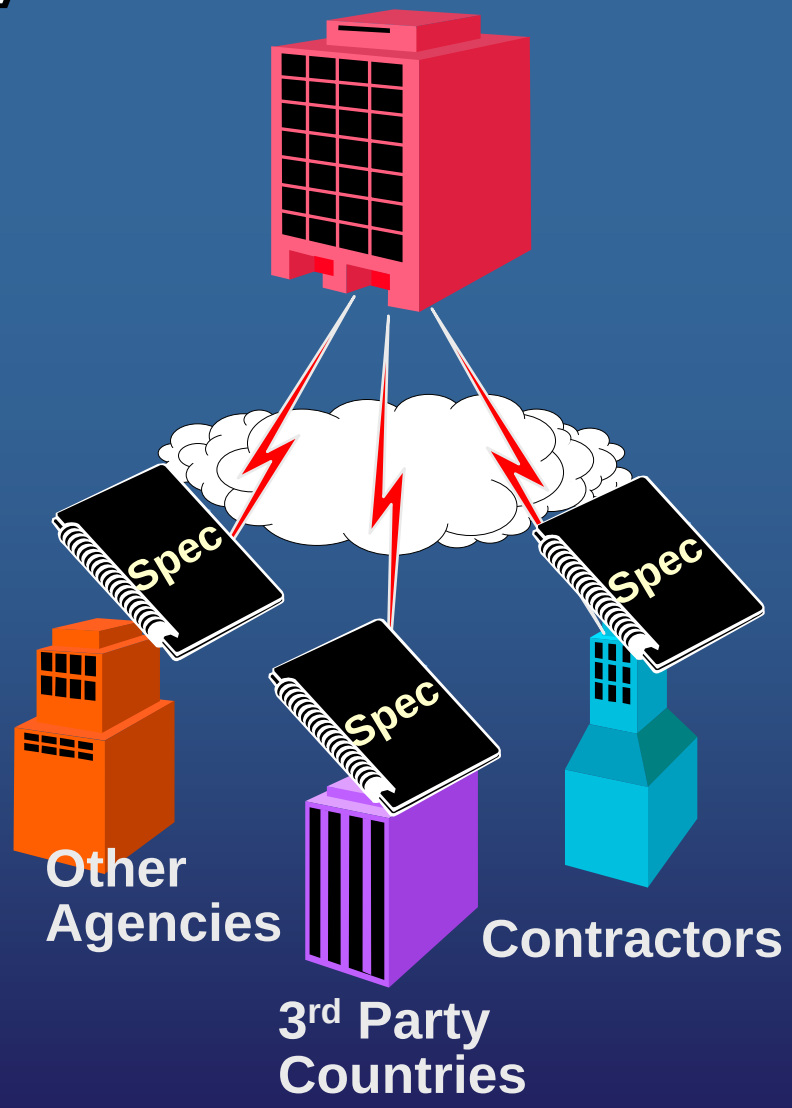
- Easy to use
  - Simple model
  - Native environment
- Dependable Security
- Dependable Authentication
- Persistent and Dynamic Control when applicable
- Use control (copy and print)
- Comprehensive Auditing
- Supports breadth of content types
- Scalable and deployable

Case Study

Dissemination of Intelligence Reports

Solution:

- Persistent control of sensitive reports – even after delivery
- Dynamically control access on need to know basis
- Revoke and/or change access when relationship changes or need expires
- Integrate authentication and authorization decisions into existing application
- Monitor activity on docs/web/email
- Expire old content when new revisions become available



Technology Direction

- Encryption at the object level – document, message, audio/video clip, image, etc.
- Integrated authentication and authorization engines (LDAP, SAML, etc.)
- Use control – view/play, print, copy, forward
- User-accessible audit
- Revocable and/or expire-able

authentica