

Personal Identity, Trust, and Internet Digital Rights Management

Gordon Lyon, Manager

Distributed Systems Technologies Group
Convergent Information Systems Division
NIST

lyon@nist.gov



1

Purpose...

**Informally Explore
a bit of...**

***Next Generation*
Digital Rights Management
(DRM)**



2

Highlights DRM need for ...

- *balanced concerns*
 - Technical
 - Business
 - Legal
- *open, user-acceptable* features
- *interoperable* contents and systems

Capsule

- Many DRM problems as yet unclear
- Field is complex, immature
- Digital Intellectual Property will leak
 - Web can amplify loss
 - DRM will reduce leakage
- Recommendation—Design realistically:
 - Understand business model*
 - Do worst-case analyses*
 - Incorporate technology that helps*

Outline

- Introduction and setting
- DRM
- Catch 22 of 1st Generation DRM
- Designing around the problem....
better integrity via biometrics
- Summary, Conclusions

Digital Rights Management..

Uses IT mechanisms (e.g., Internet)



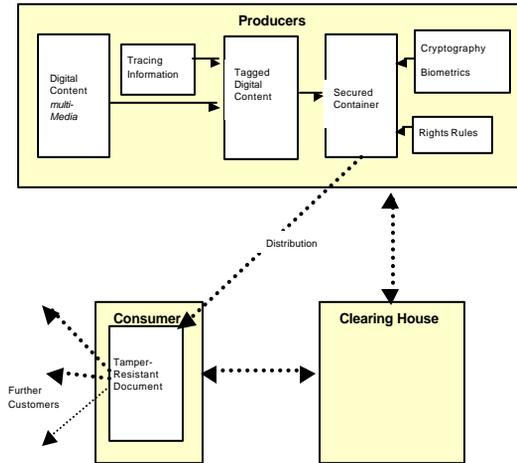
Digital content = intellectual property (IP)



IP attributes

- Ownership
- Access, Control
- Use, Payment
- Warranty, Authenticity
- Privacy, Risk

DRM Stylized Flow



End of the 1st Generation: DRM's Dilemma

Physical control of receiving device:

- **Without:** **Cannot guarantee** product security
- **With:** **Spoils business model** of open Web market.

INTERNET—The Digital Autostrada/ Motorway/ Autoroute/ Interstate/ Autobahn

- Open
- Ubiquitous
- Digital
- Automated

Business attractions...

- lower cost
- more functionality
- enhanced current market
- **large**, lively *new* markets

Some DRM Challenges

■ Usability

- Open access
- Ease-of-use

■ Interoperability

- Rights expression language(s)
- Digital object formats, container(s)

■ Integrity

- keep “leakage” low
- enforce agreements

today

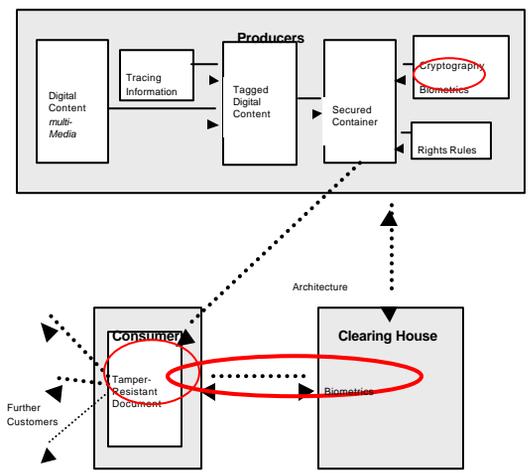
Better Integrity I: Biometric Identification

“Automated methods of recognition via physiological or behavioral features”

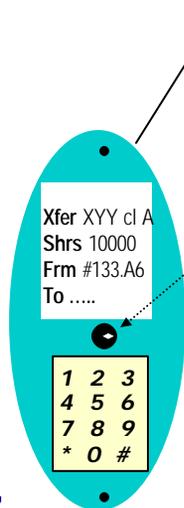
- Biometric should:
 - Eliminate passwords, PINs
 - Bind to **one and only one** person
 - Have high acceptance rate (hits)
 - Have low false alarm rate (misses)
 - Be cheap



Examples in DRM System



Web Appliance: Convenient, Open, Secure via Biometrics?



Example: Appliance Scan Lens

- hold at arm's length
- see *active* face on screen
 - => to start
 - => during check points

Get physical context from appliance—higher dimensional identity not so easily faked.

Better Integrity II: Web Trust Should...

- **Dispel participants' wariness**
(even if never actually meet)
- **Promote business**
(through assurance)
- **Be affordable**
(scalable cost)

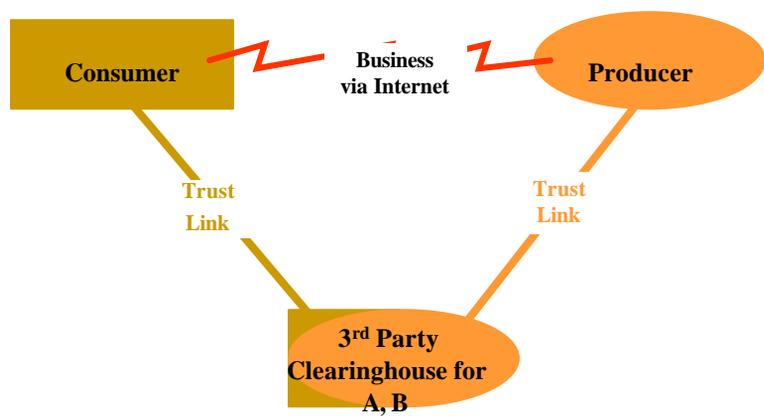
State of E-Trust

- Authentication is inadequate on Web for
 - **Unknown** e-commerce parties
 - Known parties with **no common credential authority**
 - Available solutions expensive (e.g., **PKI**)

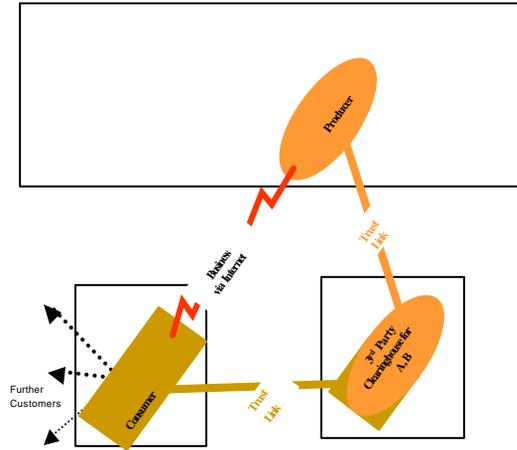
FSTC: "Trust is a **crucial inhibitor** of e-commerce.."



As DRM Clearinghouse



In Earlier DRM Diagram Terms...



3/7/2002
NIST

17

Suggestion for NextGen-DRM

Avoid physical control that inhibits, but....

- Much stronger identity binding
 - biometric inputs
 - remote evaluations?
- 3rd parties for trust
 - assurance, reputation services
 - sharing of risk
- Keep inexpensive, convenient

3/7/2002
NIST

18

Summary, Conclusion

■ 1st gen. DRM

- over-emphasized conventional security
- narrow, restrictive implementations

■ Next Generation(s) of DRM

- Balanced--technology, business, legal
- Popular--usable, interoperable, widespread

Will evolve own methods

- Biometrics + assurance can play a significant role