

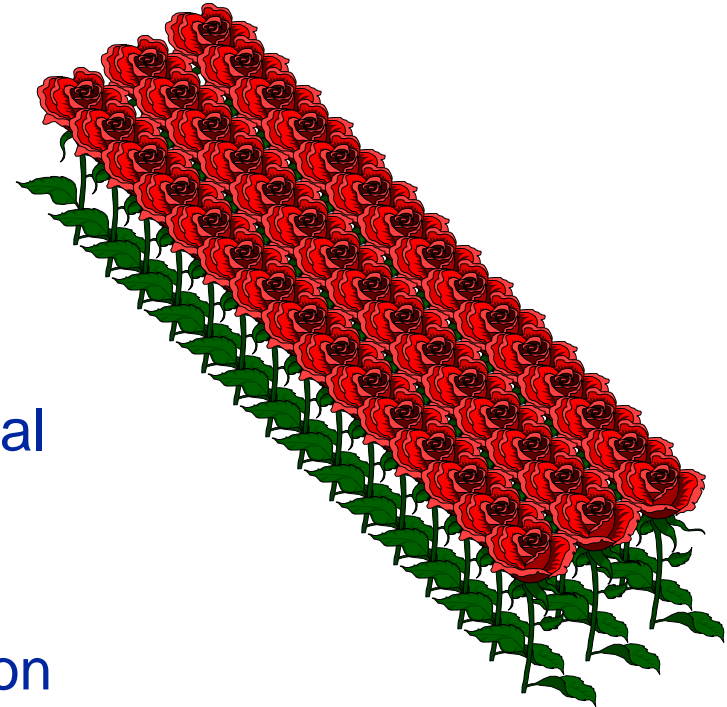
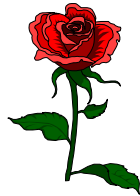
## Outline



# Secure transfer of digital originals



# Secure Transfer of Digital Originals



- u **Owner / seller**

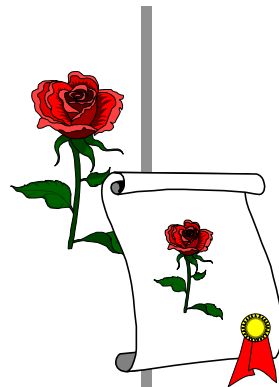
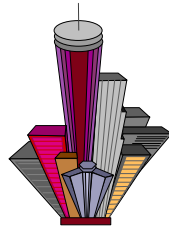
- u Protection of Intellectual Property Rights (IPR)
- u Prevent *mass-fraud*
- u Cost-effective protection

- u **Buyer**

- u Secure against wrong accusations by sellers
- u Authenticity of copies bought
- u No negative impact on quality, performance

# Authenticity of a Copy

Creator



RA/CA



- u Registration of creators
  - u by whom?
  - u semantics of certificate?
- u Achieves “accountability”
- u No guarantee for correctness
- u No guarantee for honesty
- u Several “code signing” proposals



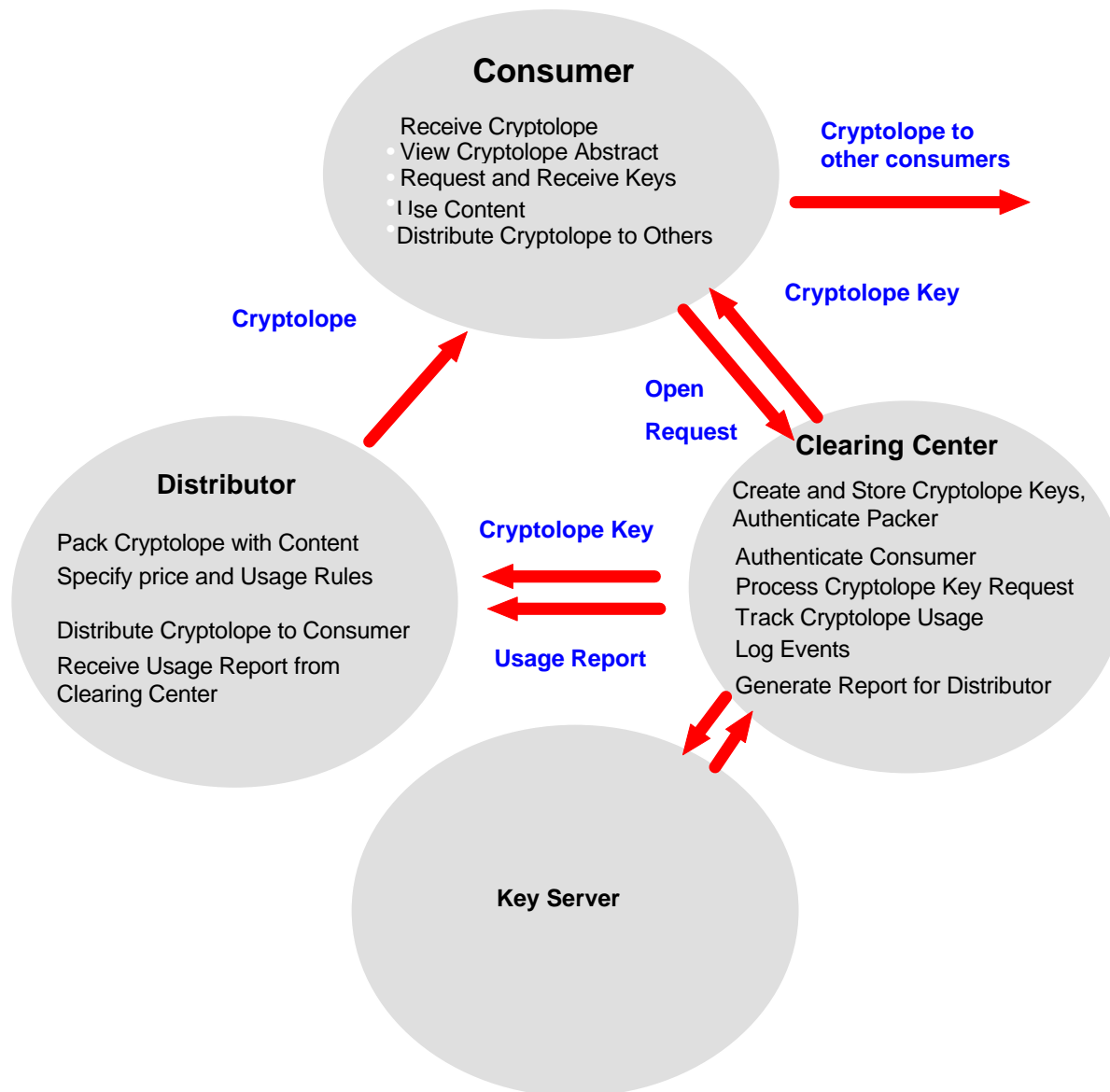
# Copy Control

---

- u **Decrease incentive of making illegal copies**
  - u Customization: specific info, interactive presentation
  - u Short lifetime of information
  - u Cheap access to information
- u **Increase risk of distributing illegal copies**
  - u Individualized authentication, watermarking
  - u **Fingerprinting**
- u **Prevent illegal copies**
  - u Low-tech attackers: **super distribution**
  - u High-tech attackers: tamper-resistant hardware



# Superdistribution

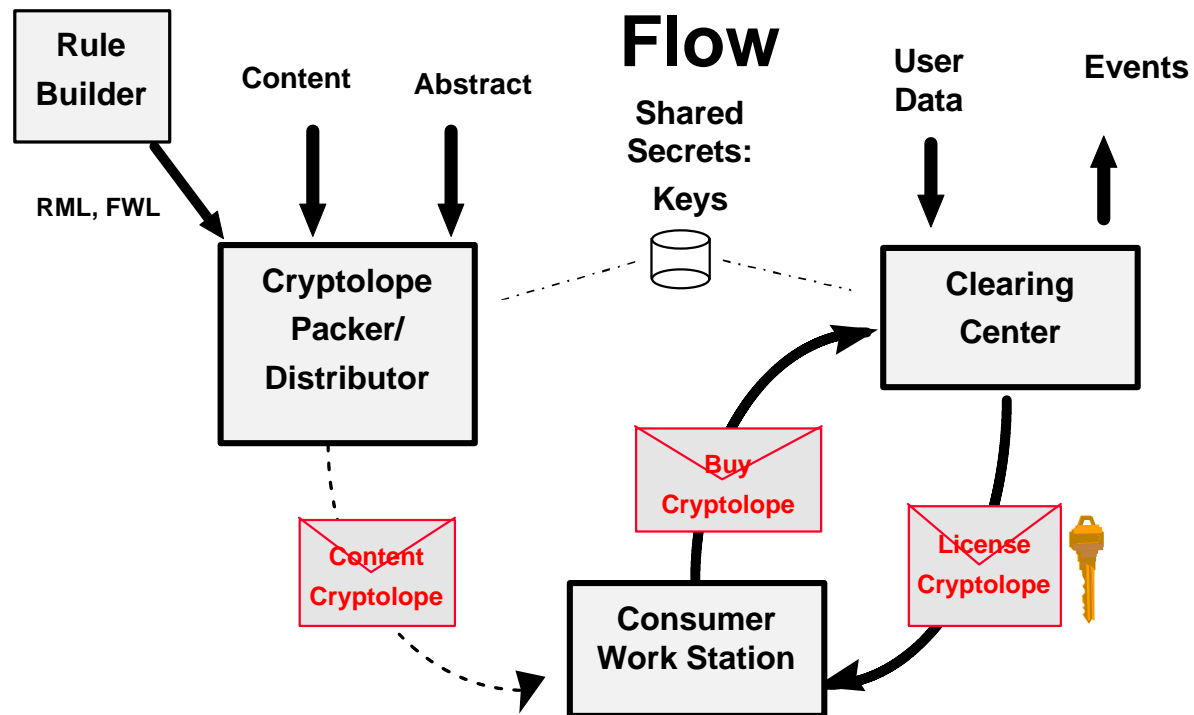




# Superdistribution



## Cryptolope Transaction



# Superdistribution



## u Content cryptolope

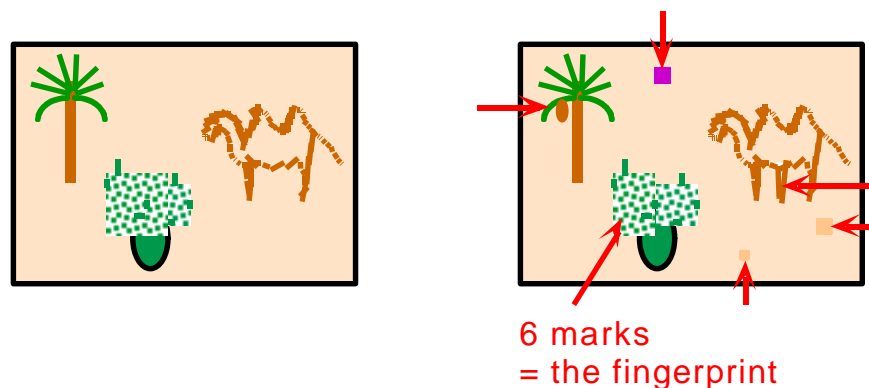
- u Bill of materials
- u Abstract, metadata
- u Encrypted files + key records
- u Rights management language
- u Fingerprinting / watermarking
- u Digital certificates

## u Cryptolope types

- u Content
- u Buy = spec's + consumer environment info
- u License = keys + F/W details



# Fingerprinting



- u **Different in each sold "copy"**
- u **No significant change to data**
  - u Usefulness for buyer
  - u Marks hard to find for traitors
- u **More tolerant against transformations than data**
- u **Collusion tolerance**
- u **Asymmetric fingerprinting**
- u **Anonymous fingerprinting**



# Fingerprinting

