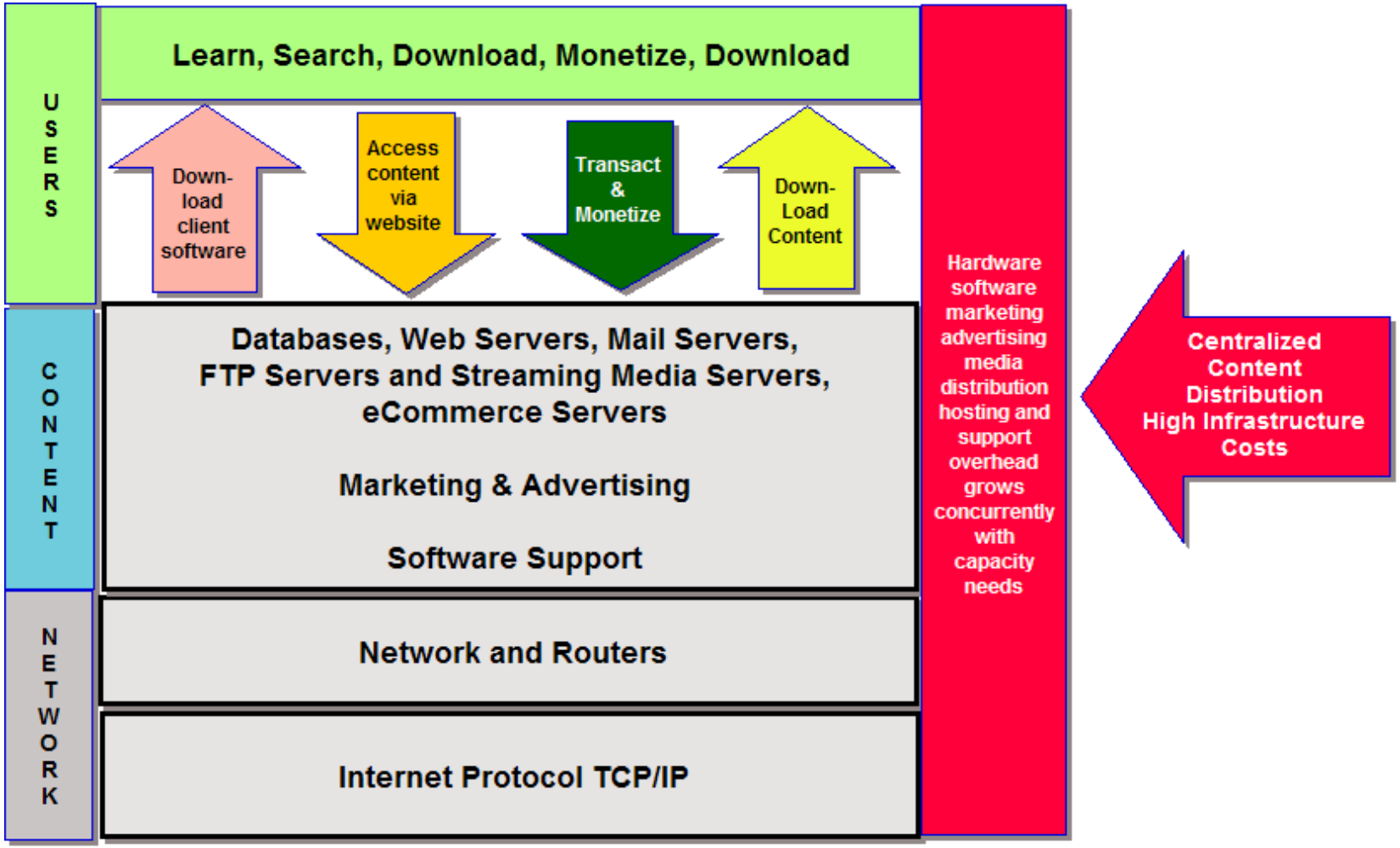
Patented Object Level DRM, e-Commerce, Content Security and Tracking

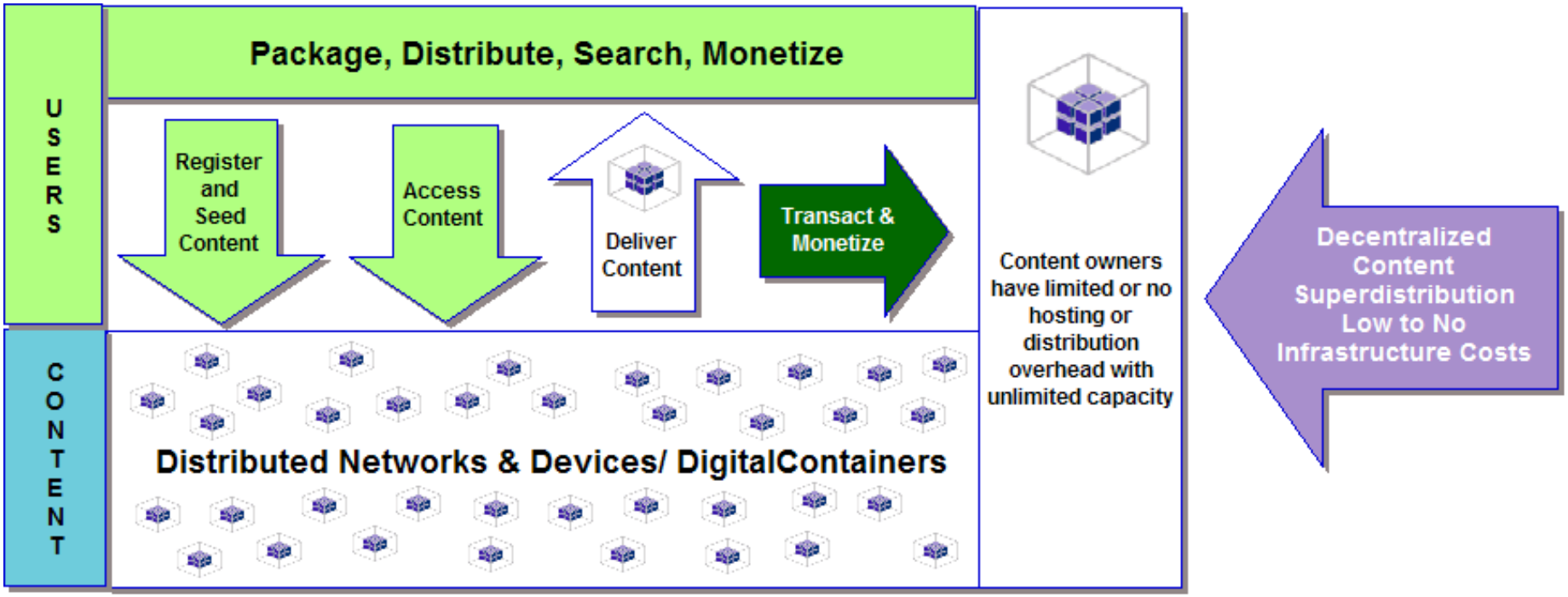
Centralized Content Infrastructure

High overhead, marketing and support costs



The New Content Infrastructure

Decentralized, Low to No Overhead



The Business Model for Content Owners

A new economic model for digital content distribution and sales

Content is easily packaged, labeled, registered, distributed, marketed and monetized with protective DRM and on-board payment system in distributed network environments

All Intellectual Property Has a Profitable Business Model

Market Trends

"More organizations need to realize that DRM solutions have the potential over the next three to five years to aid compliance with maturing privacy legislation — for example, implementing the role-based access that HIPAA requires. As this happens, DRM will emerge as an infrastructural element rather than a standalone technology solution."

- David Thompson, META Group

March, 2004

Market Trends

Significant trends in the DRM market include:

- Litigation over patent infringement in the DRM industry heats up
- Increased consumer acceptance of protected content
- Dominant digital download business models emerge
- Tethered files in enterprise class DRM are the rule

- Jarad Carleton, Frost & Sullivan

Enterprise Uses of DRM

Financial Services

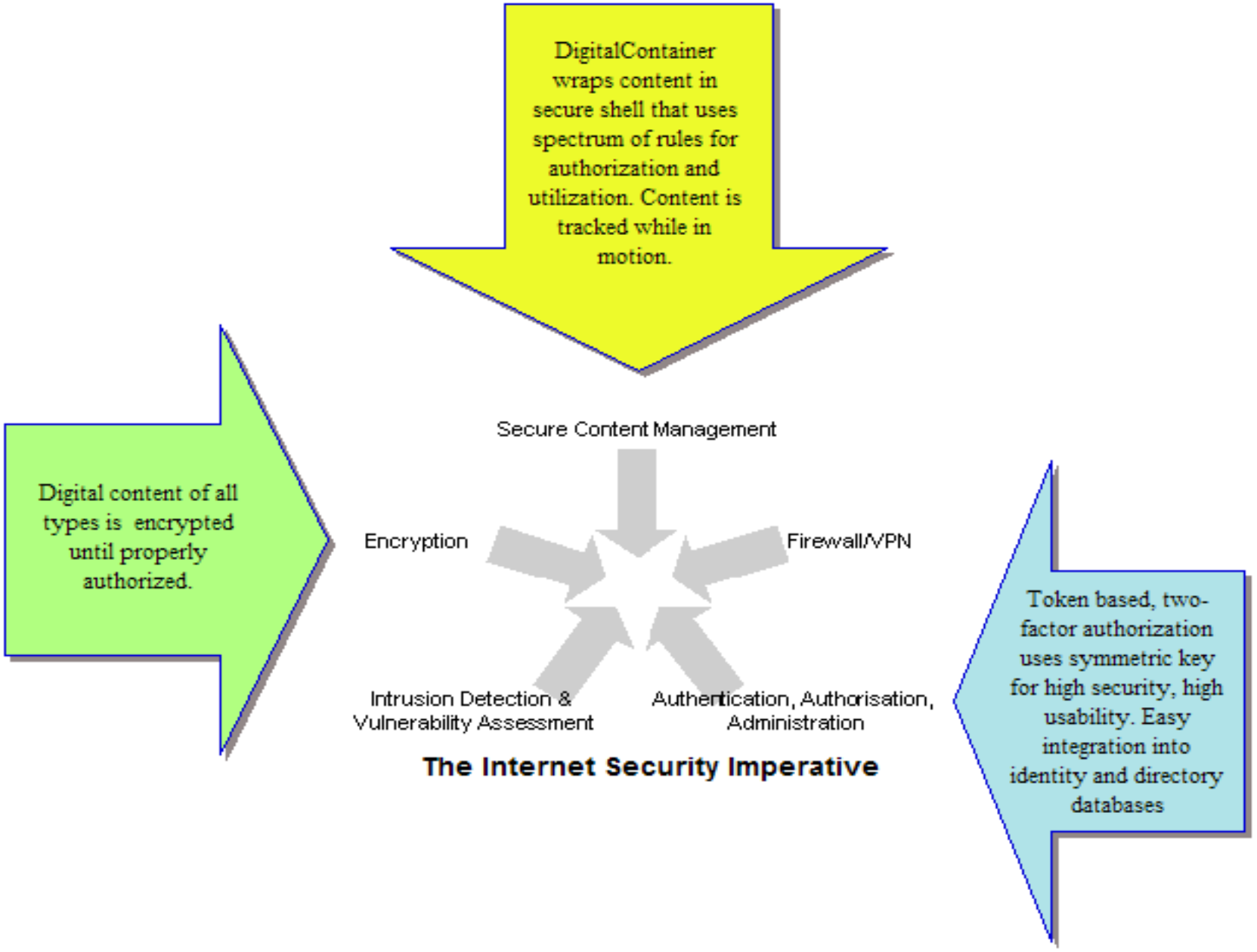
- Graham-Leach-Bliley Title V - privacy of banking customer info
- Sarbanes-Oxley - integrity of accounting info
- Investment banking “virtual deal rooms”

Healthcare

- HIPAA - confidentiality of patient records
- FDA21 CFR Part 11 - integrity of drug clinical research info

Other

- California SB 1386 - privacy of personal information
- ISO 17799 - best practices for enterprise information security
- R&D and new product information
- Confidential documents in hands of employees who leave

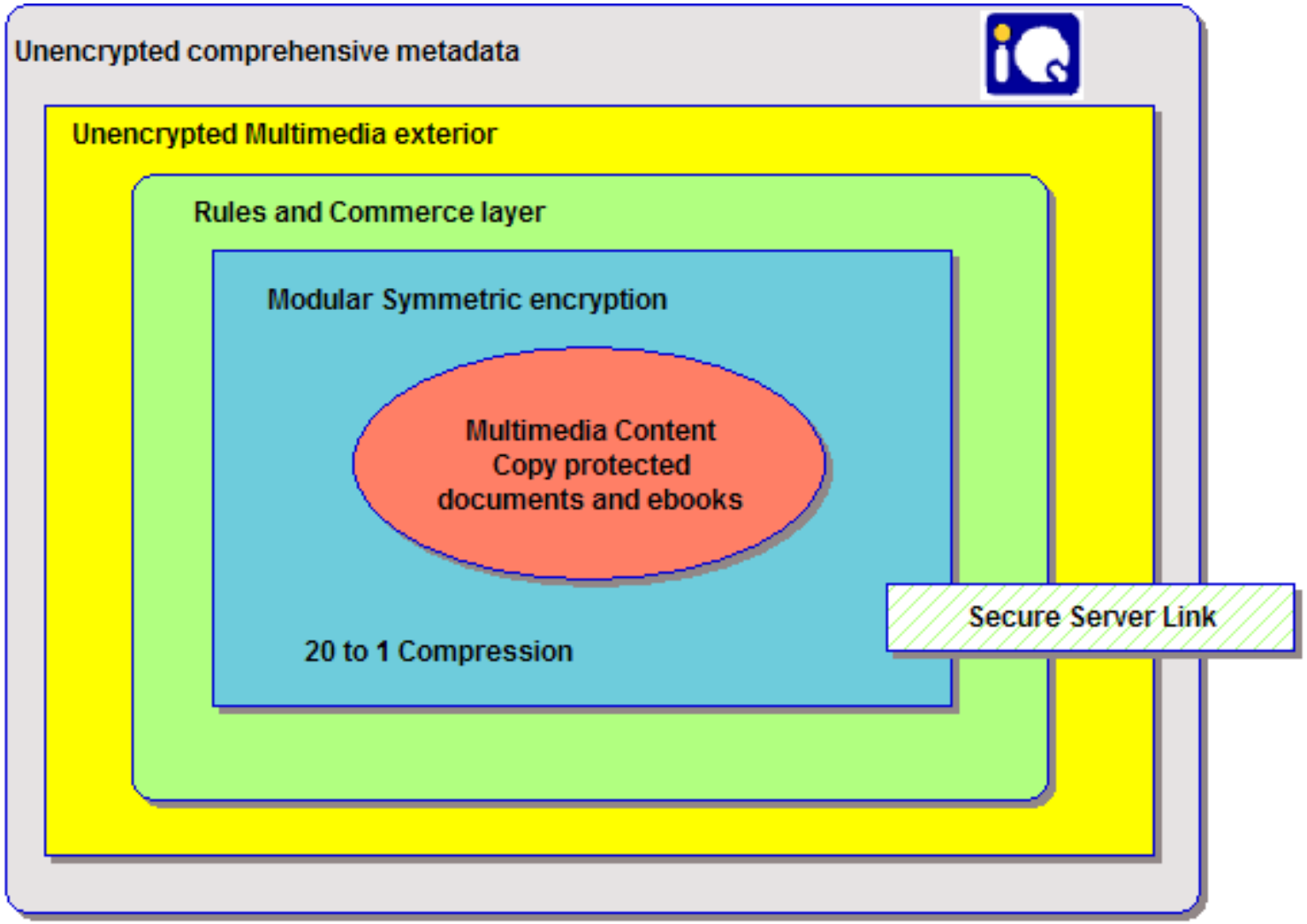

DigitalContainer wraps content in secure shell that uses spectrum of rules for authorization and utilization. Content is tracked while in motion.
Digital content of all types is encrypted until properly authorized.
Secure Content Management
Encryption
Firewall/VPN
Intrusion Detection & Vulnerability Assessment
Authentication, Authorisation, Administration
Token based, two-factor authorization uses symmetric key for high security, high usability. Easy integration into identity and directory databases
The Internet Security Imperative

Relevant Applications

Patented Object Level File Security and E-Commerce for Competitive Advantage

- General content security for ECM
- Digital Asset management
- Monetization of content: e-commerce
- Secure digital distribution
- P2P hybrid collaboration
- Data mining/tracking/market research
- Targeted marketing programs
- Compliance, healthcare, Homeland Security

Digital Container Architecture

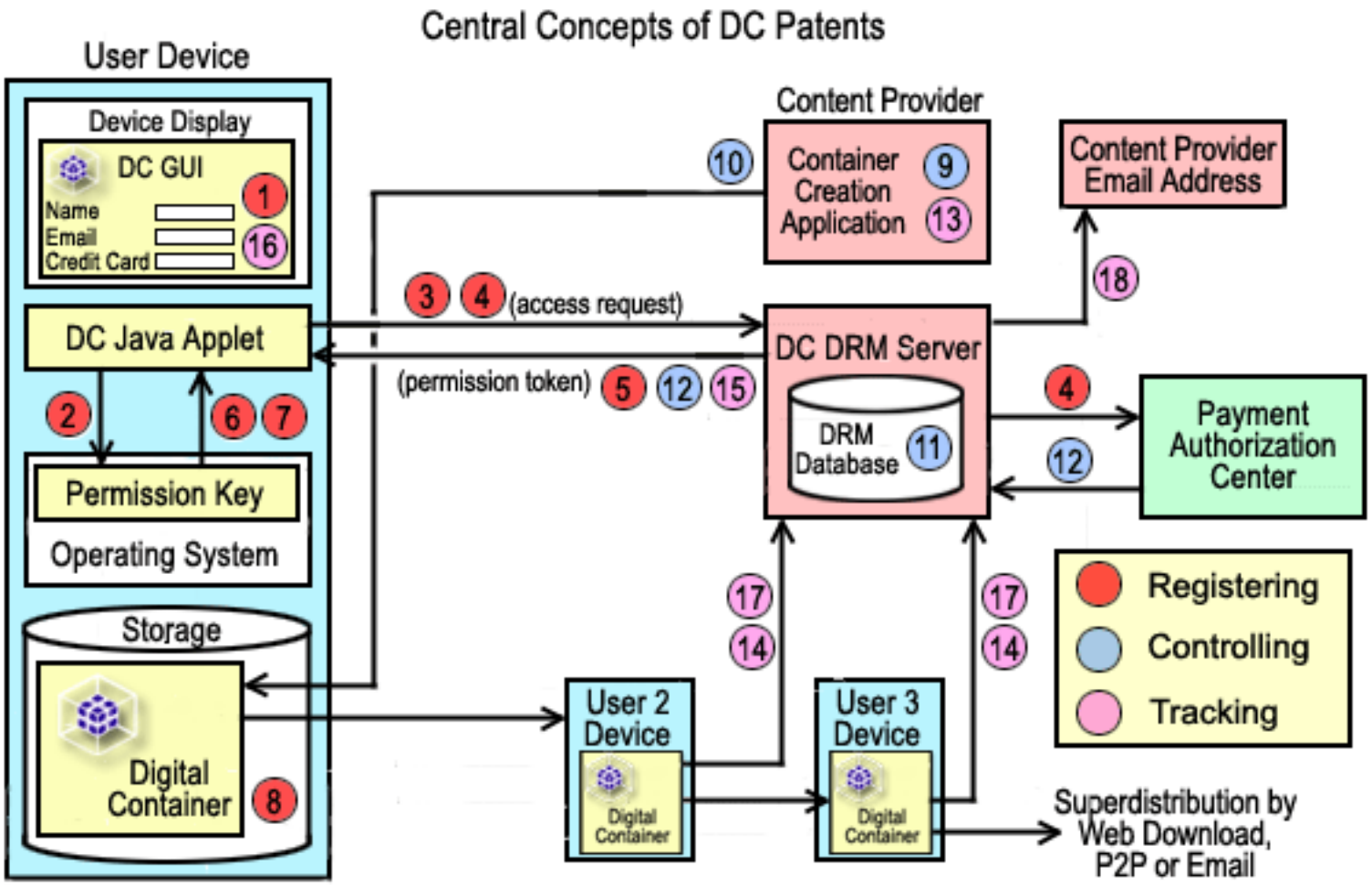


The DigitalContainers' patent family consists of:

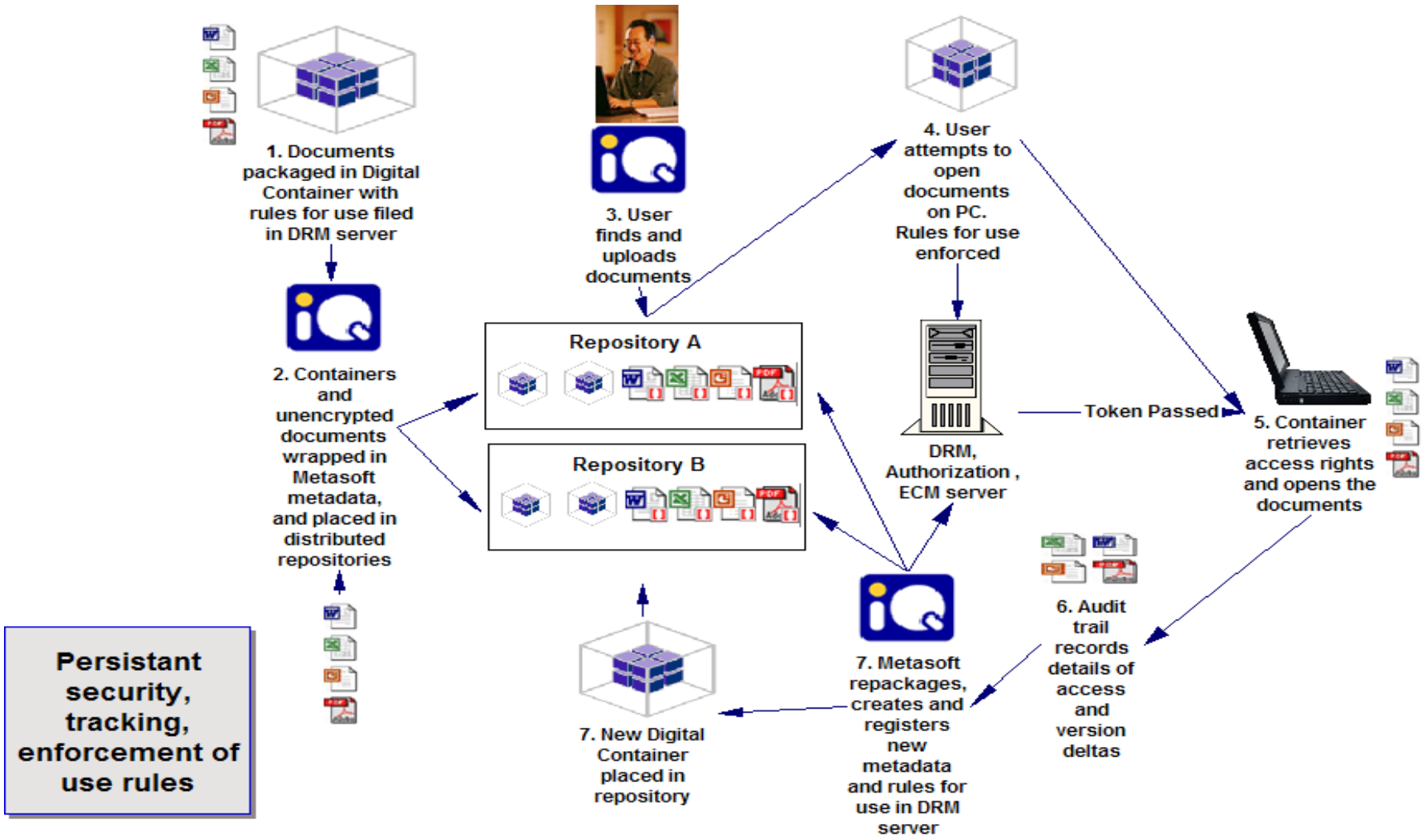
- Regulating Access to Digital Content
  (US Patent 6,389,541)
- Tracking Electronic Content
  (US Patent 6,751,670)
- Delivering Electronic Content
  (U.S. Patent No. 7,127,515)
- Secure Streaming Container
  (U.S. Patent No. 7,251,832)
- Securing Digital Content System and Method
  (Notice of Allowance, June 2008)
- Controlling Access to Electronic Content
  (In Process)

Analyst Coverage

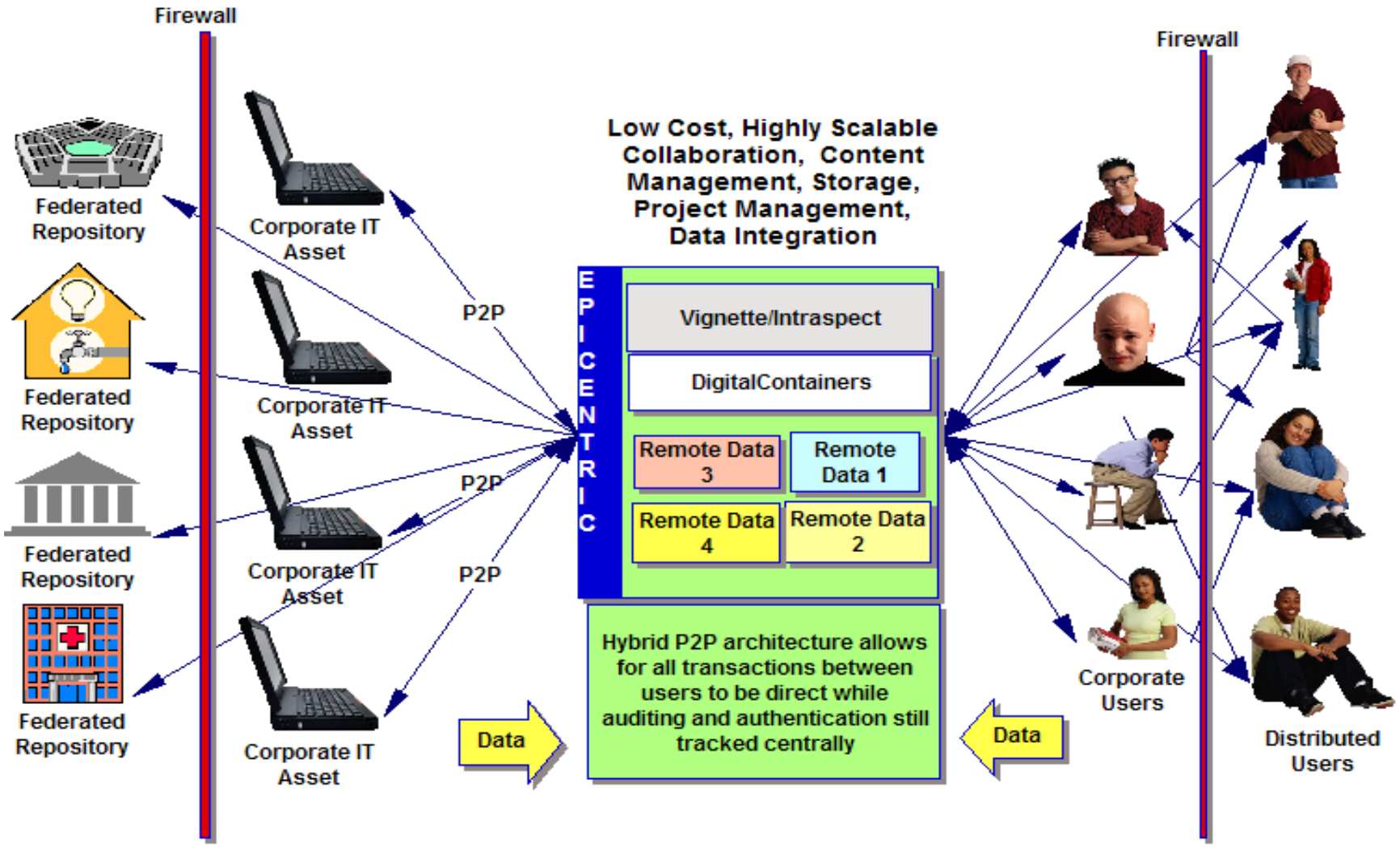
PatentMetrix, independent analyst firm,
designated DigitalContainers' patent,
U.S. Patent 6,389,541,
Regulating Access to Digital Content,
"a critical patent for the future of DRM."


Central Concepts of DC Patents
User Device
Device Display
DC GUI
Name
Email
Credit Card
1
16
DC Java Applet
2
6
7
Permission Key
Operating System
Storage
Digital Container
8
Content Provider
10
Container Creation Application
9
13
Content Provider Email Address
18
3
4
(access request)
(permission token)
5
12
15
DC DRM Server
DRM Database
11
4
12
Payment Authorization Center
17
14
17
14
User 2 Device
Digital Container
User 3 Device
Digital Container
Registering
Controlling
Tracking
Superdistribution by Web Download, P2P or Email

Secure Content Workflow



Secure ECM using distributed networks



Distributed Networking Vertical Markets: MetaGroup

- Financial
  - M&A
  - outward facing client distribution
- Pharmaceutical
  - clinical trials
  - drug discovery
- Insurance - circulation of materials to captive and non-captive agents
- Medical
- Niches within the government

Distributed Network Markets: Ovum Research

- Media production
  - Film
  - TV
  - Audio
  - Multimedia
- Health Care-Secure collaboration with large files
  - X-Rays
  - MRI
  - Sonograms
  - Echocardiograms
  - Video
- Secure Enterprise Media Distribution
  - Training and Product Videos
  - Corporate addresses
  - Presentation storage and retrieval

Patent Claims

Process and Architecture

Central Concepts of DC Patents - Legend

Regulating Access to Digital Content - Red:

1. User receives DC container and attempts to access content
2. DC Java applet checks for pre-existing permission key
3. If none found, applet opens encrypted communication session with DRM server and requests permission token
4. Permission request can include user payment data processed by payment authorization center
5. If request approved, permission token received that starts installation process
6. During installation process, encrypted permission key written to device OS
7. Permission key ties container to device

- Content is decrypted and decompressed and made available for use

Controlling Access to Electronic Content - Blue:

9. Content provider creates a Digital Container that includes electronic content and instructions for:
   - collecting payment information or other user data
   - transmitting a message including the payment information to a DRM server
   - receiving a reply to the transmitted message
   - selectively providing access to the electronic content based on the reply to the transmitted message
10. Content provider compresses and encrypts the content and transmits the container to the user over the Internet

- Information, including payment information, received from user while attempting to access content is transmitted to a DRM server and is stored in a database
- Based on analysis of this user and payment information, the server transmits a message controlling access to the electronic content

Tracking Electronic Content - Purple:

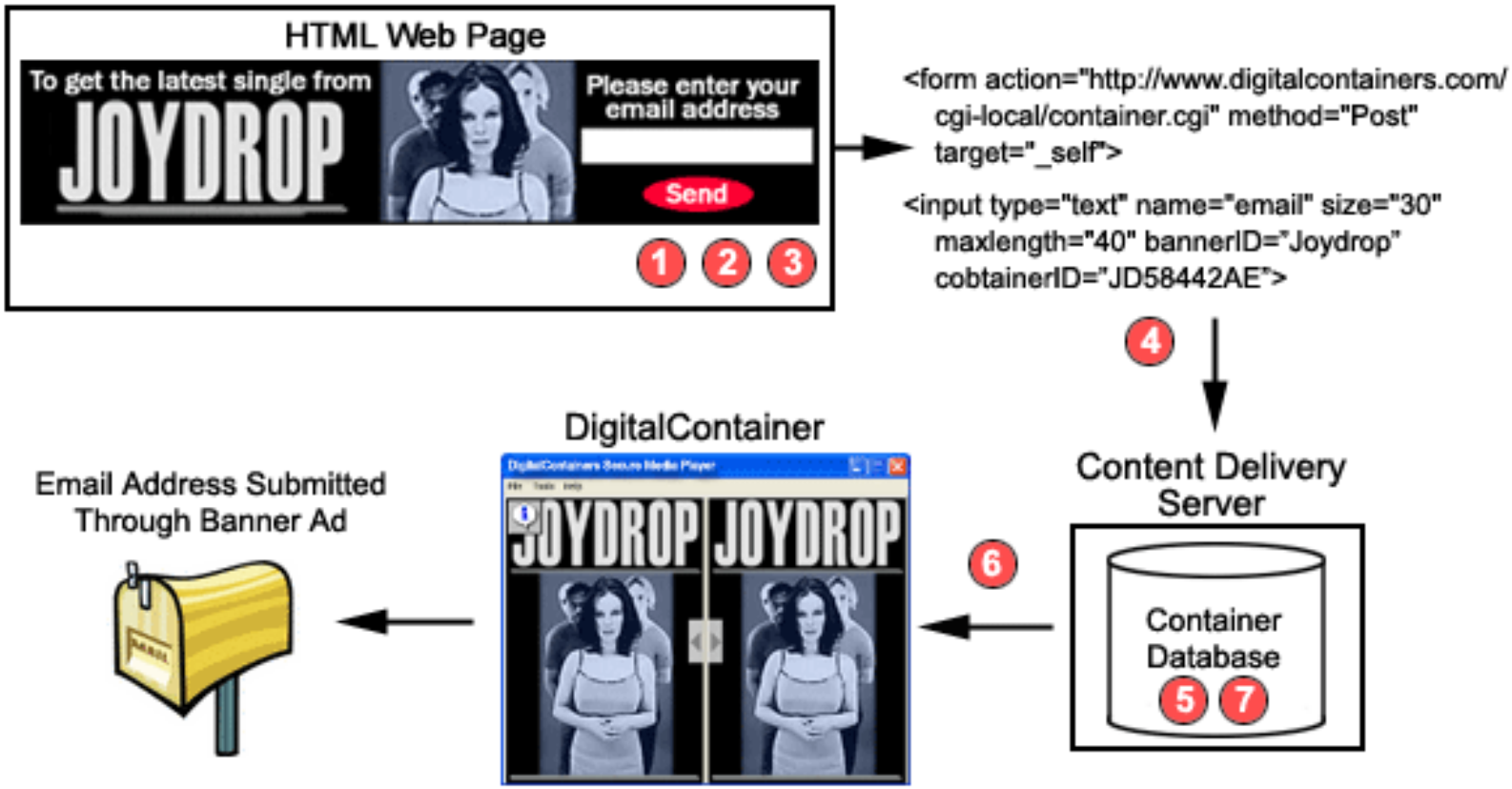
13. Content provider produces a container that includes:
    - electronic content that is encrypted and compressed
    - an email address or IP address that will be used to collect the notification information
    - instructions that collect notification information and attempt to transmit notification information to the address when a user attempts to access the content
    - instructions that decompress and decrypt the content when access is granted
14. As each successive recipient of the container attempts to access the content on a different machine, notification information is transmitted to the address.
15. Access to the electronic content is denied until the notification information is successfully transmitted and an access granting message is received in response

- If the notification information is collected and transmitted successfully, access is granted to the electronic content without re-collecting or re-transmitting notification until the container is sent to a new recipient

13. The notification information can include demographic or payment information interactively collected from each successive user or system identification information derived from the user's computer or network.

- The originator of the container is notified each time a successive recipient accesses or attempts to access the contents

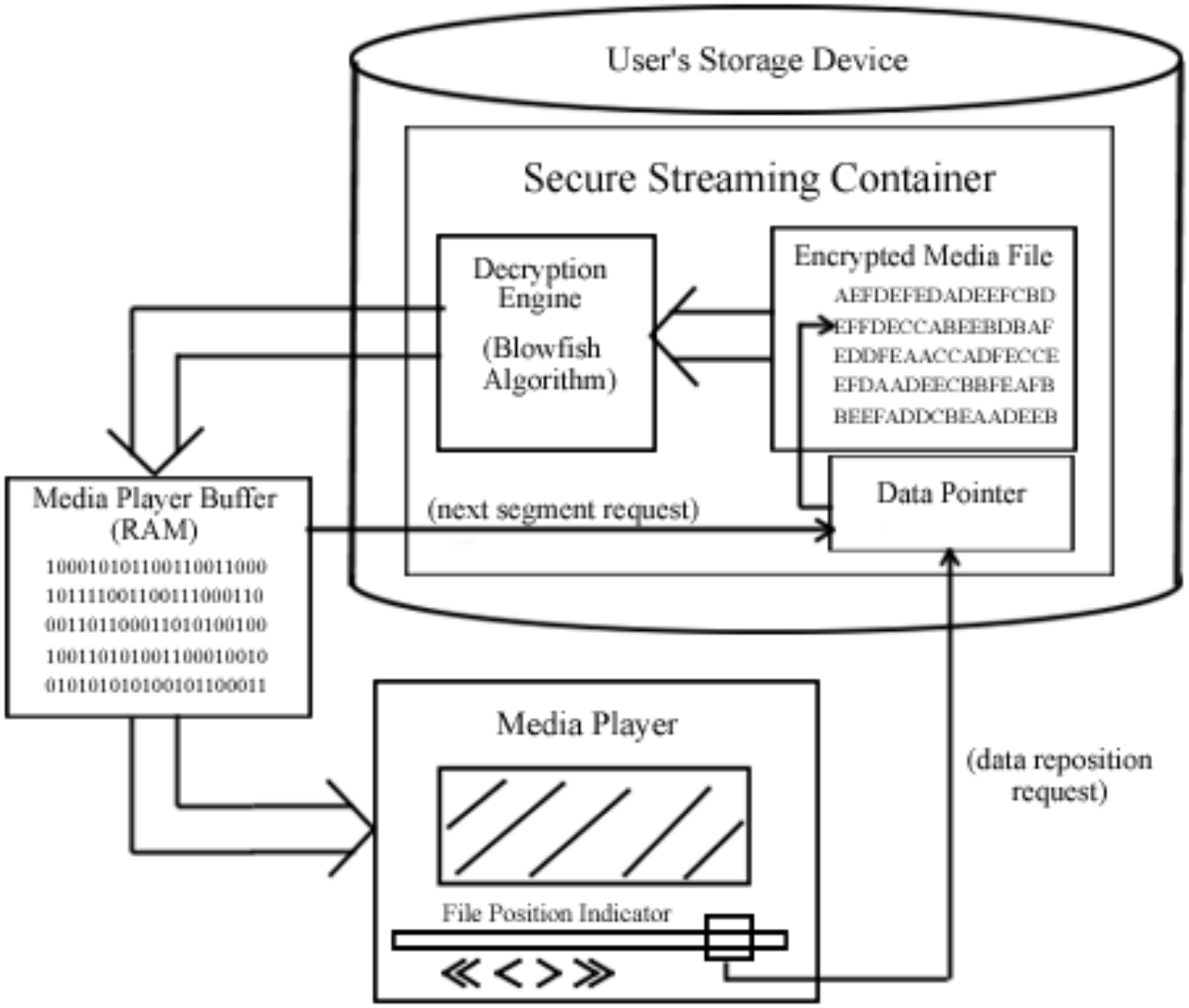
Delivering Electronic Content



Delivering Electronic Content - Legend

1. A user views a web banner ad that asks him to enter his e-mail address into an HTML form in the banner in order to receive more information about the subject of the banner ad.
2. This HTML form may also request additional demographic information. The instruction residing in this HTML form may also obtain system information from the user's computer.
3. This process may also take the form of the user selecting a link corresponding to the subject of the web page. This link will open a separate window that requests the email address and other demographic information without modifying the page currently displayed in the browser.
4. The instructions residing in this HTML form execute a script, such as a CGI script, that transmits the collected information to a second computer.
5. The instructions residing in this HTML form execute a script, such as a CGI script, that transmits the collected information to a second computer.
6. The second computer then transmits the selected electronic content to the address originally submitted by the user.
7. The second computer can use the information received from the first computer to identify the specific banner ad and computer where the request originated.

Secure Streaming Container

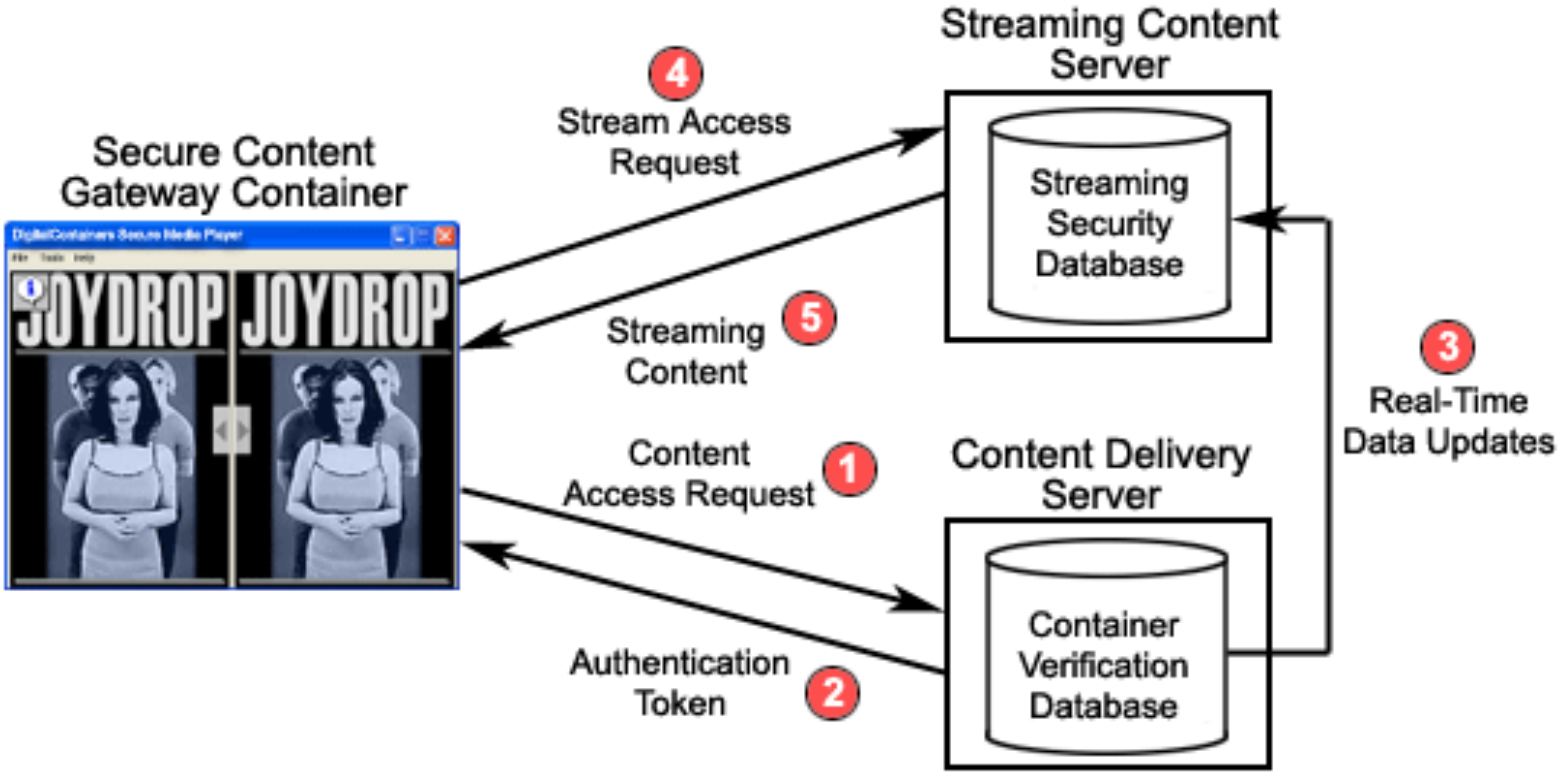


Secure Streaming Container (SSC) Function

1. An SSC is created that contains:
   - An encrypted “main” media file such as a user normally streams from an Internet streaming server. Any audio or video file type can be used that can be played on the user’s media player or on the internal SSC media player
   - Secondary promotional and media files such as graphics, promotional html and image pages and preview clips
   - A set of operational modules that control the decryption and playing of the media file
   - The usual payment or demographic data gathering instructions
2. The user is authorized to access the contents of the SSC as per normal container operation.
3. Once opened, the SSC “control” module evaluates the user’s device and deploys the secondary operational modules to decrypt the content file in the most secure manner possible
4. The SSC can utilize the user’s resident media player or the media player included in the SSC if no player is detected that is registered to play the main media file type.
5. The SSC decrypts the media file “on the fly” and sends it to the media player in decrypted chunks.

- In this manner the media file is never copied to the user’s device in it’s entirety in either encrypted or unencrypted form and is therefore extremely difficult to hack and make unauthorized copies.

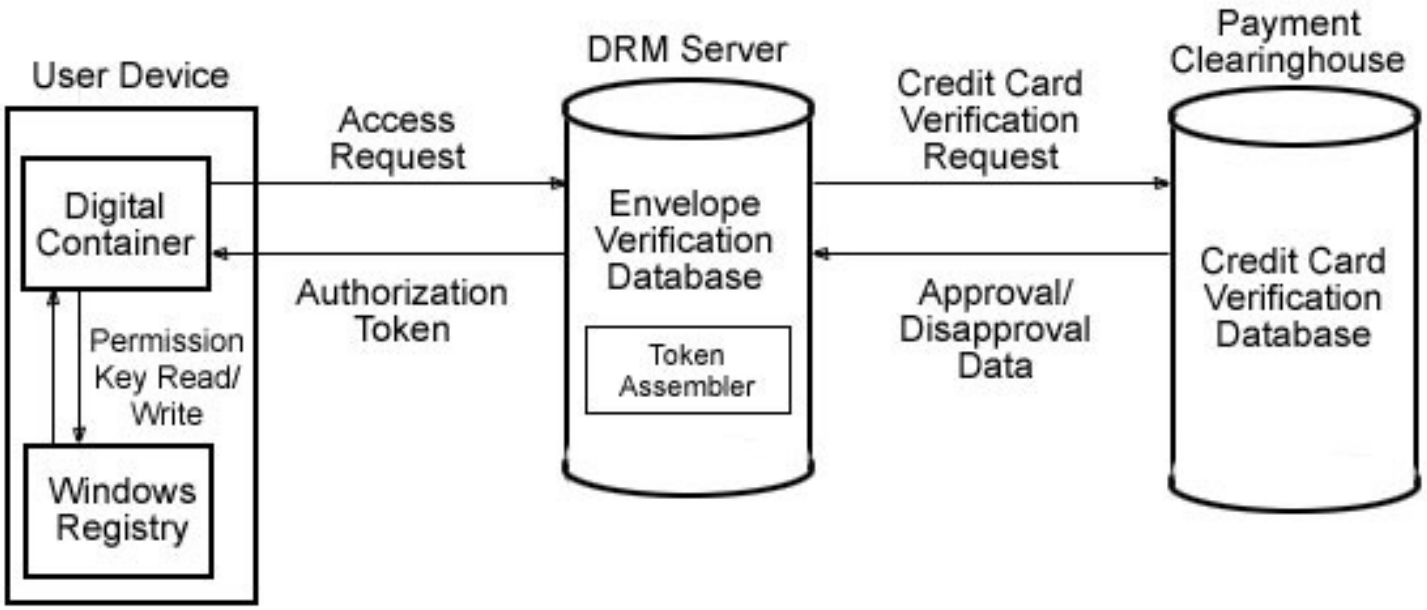
Secure Streaming Content Gateway (SSCG) Container



1. An SSCG is created that contains:
   - An encrypted, hidden URL that points to a secure media streaming source
   - Secondary promotional and media files such as graphics, promotional html and image pages and advertising which can be updated
   - The usual payment or demographic data gathering instructions
2. The user request access to the container contents as per normal container operation.
3. When the container verification database approves access to the container, certain ID and security data is written to the streaming server security database in real-time.
4. The authorization token is returned to the container and the user gains access to the hidden streaming URL.
5. The SSCG passes certain ID and security data to the streaming server security database when user accesses streaming URL .
6. The streaming server checks the security database for the appropriate ID and security data and, if correct data is found, authorizes access to the streaming content file.

Authentication – Current System

An overview of the current DCI system covered by Regulating Access to Digital Content is displayed below.

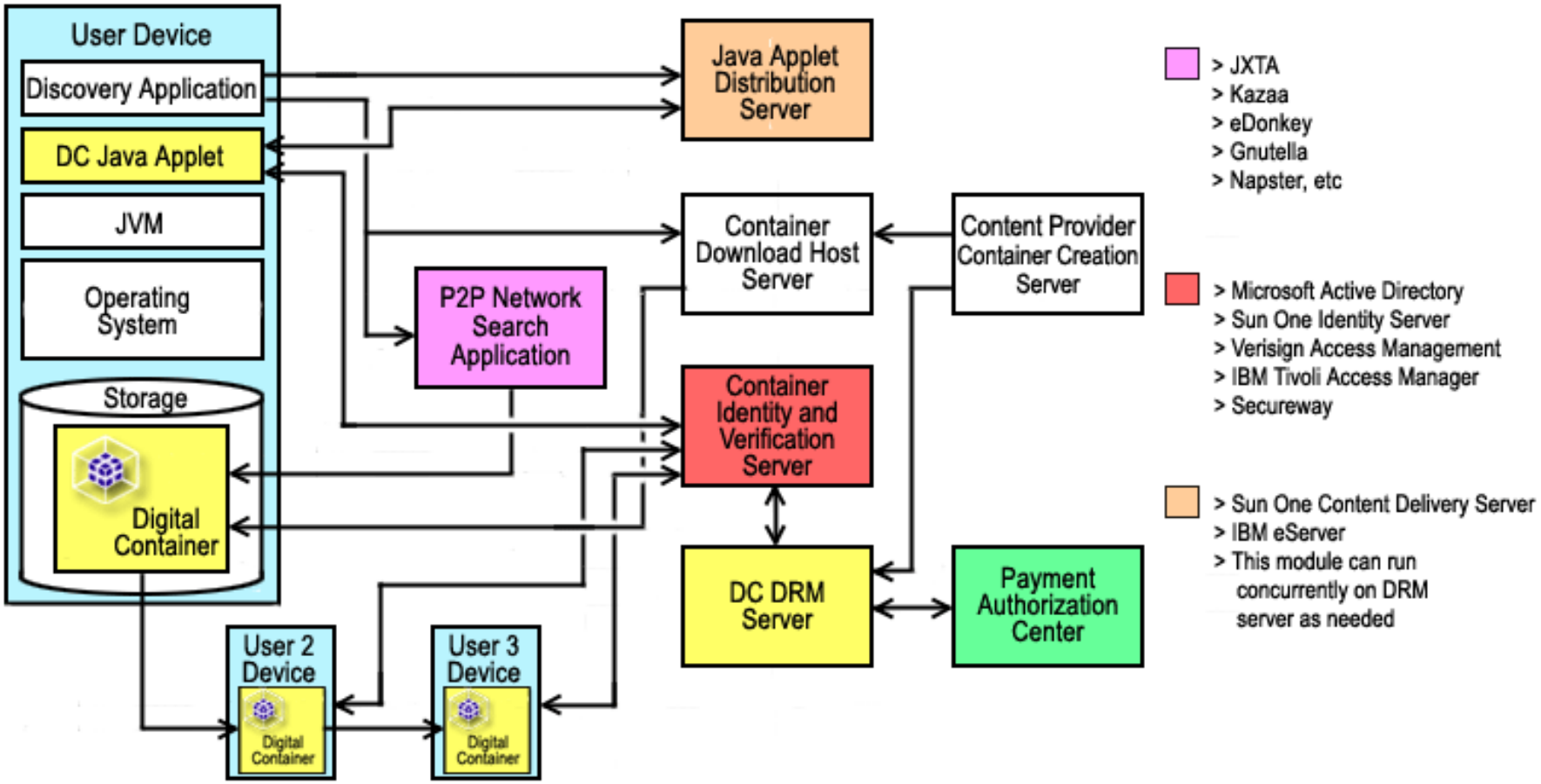


Sequence of events in the current system are:

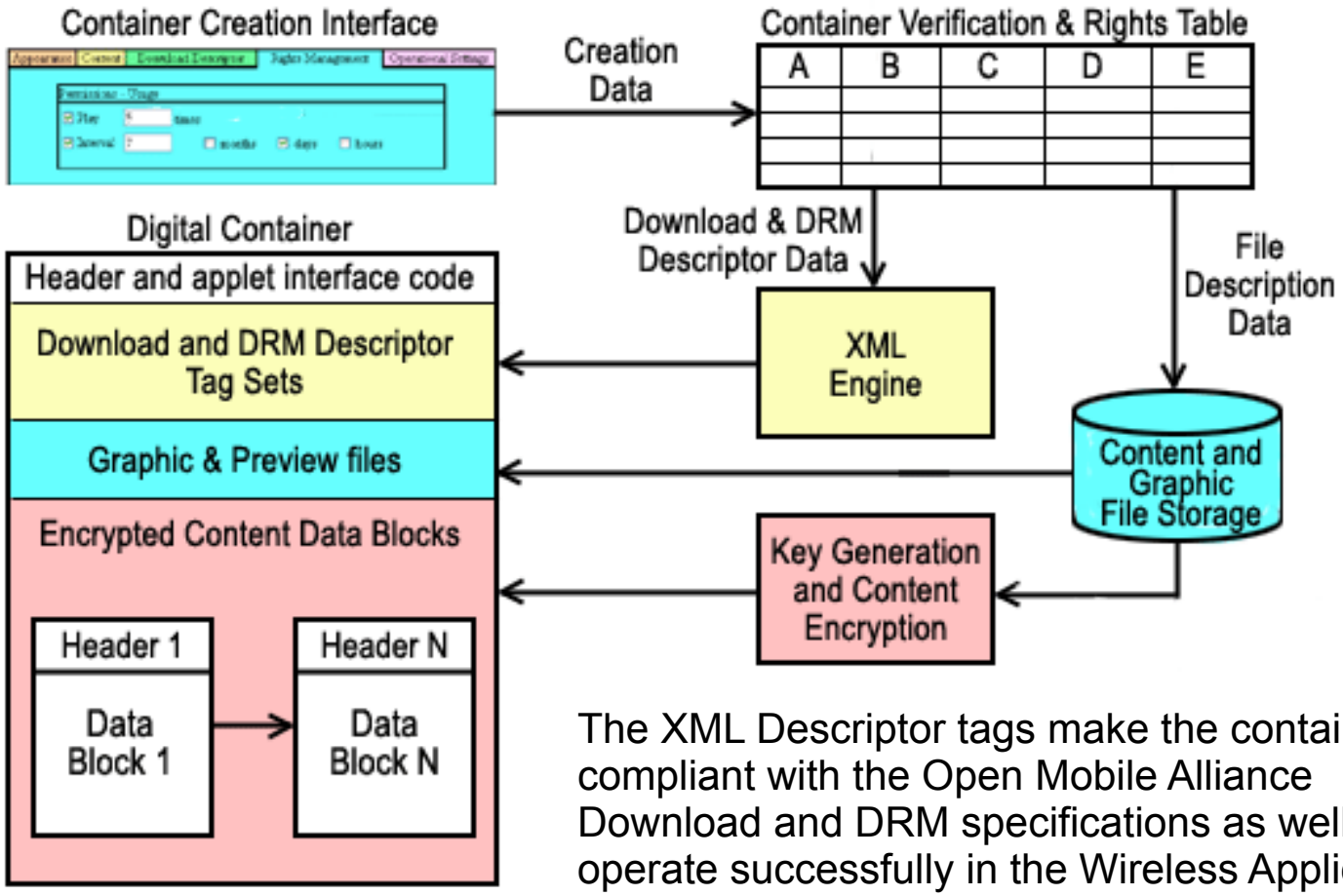
- When user attempts to open container, secure com link is opened to container DRM server to pass access request
- Container ID and user data, such as credit info, is passed to server
- Server validates container and passes credit data to Payment Clearinghouse
- Payment approval data is returned to DRM server and authorization token is assembled and transmitted to user device
- Authorization token includes first generation DRM/rights data
- Container code reads token and combines unique container ID data and data unique to user system to create permission key
- Permission key is encrypted and written to Windows Registry
- When container is accessed again, container code finds permission key and opens without need to repeat authorization procedure

Next Generation System

This system will utilize the JVM and java applet to create a cross-platform container.



Next Generation Container Assembly



The XML Descriptor tags make the container compliant with the Open Mobile Alliance Download and DRM specifications as well as operate successfully in the Wireless Application Protocol environment.

Other Applications

Other Markets

Market Size

	Market (in billions)
Business Process Outsourcing (BPO)	$122
Digital Rights Management (DRM)	100
Customer Relationship Management (CRM)	76
Enterprise Resource Planning (ERP)	66
Electronic Bill Presentment and Payment (EBPP)	32
Secure/Certified Document Delivery (SCDD)	10
Knowledge Management (KM)	9
Content Security	9
E-Commerce Software	8
Authentication	6
Peer-to-Peer networking (P2P)	5
Hosted Authentication	4
	$447

Sample Applications and Verticals

- Legal Peer-to-Peer Commercial & Business Networks
- eCommerce Infrastructure Providers
- Corporate portal development
- Information quality initiatives
- Secure community-based content and knowledge exchange networks
- Semantic Web application development
- Knowledge Management, Training & eLearning
- Legacy revitalization
- Custom application development

Sample Applications and Verticals

- Web Services deployment
- Data warehouse or data mart development (supporting ETL and BI)
- Executive information systems and key performance indicators
- System end-of-life and data migration.
- Emergency Response
- Intelligence, CRM, BI, BPC, Network
- Operations Support
- Clearing Houses and Brokerages

Sample Applications and Verticals

- Electronic Performance Support Systems (EPSS)
- Mergers & acquisitions
- Business reorganization
- Business process management
- Outsourcing
- Application deployment and upgrades
- Application integration (supporting EAI or remote procedure calls)