Issues in Rights Managed Content Interoperability

Presentation to DMDA

April 4, 2002

Applied Value Inc
Lexington, Ma 02421

Tel +1.781.778.1800
eMail slipoff@appliedvalue.com

Outline

The objective of this presentation is share my work-in-process thinking from the perspective of the the several *hats* that I wear

Consumer
Electronics
Society

- My hats
  - Chair IEEE CE Standards Committee
  - Employee in "OurGroup" of Media and Telecom Companies
  - Consultant to industry
- My perspectives
  - DMDA Playing field
  - Key Issues
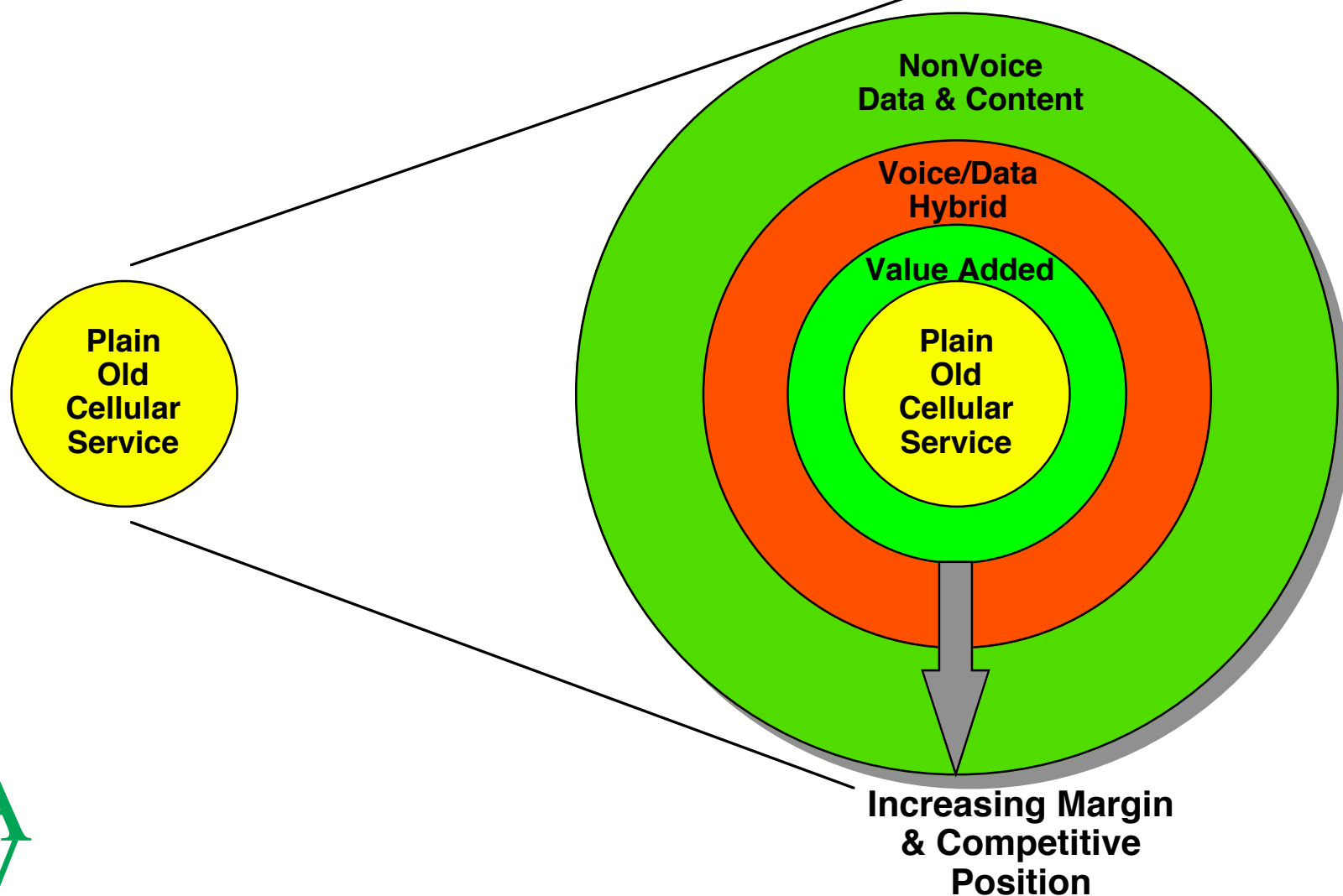 - Recommended Solution Architecture

OurGroup

My Hats

In the interest of disclosing any bias, as well as my vantage point here is a little about *who I am* and *who I work for*

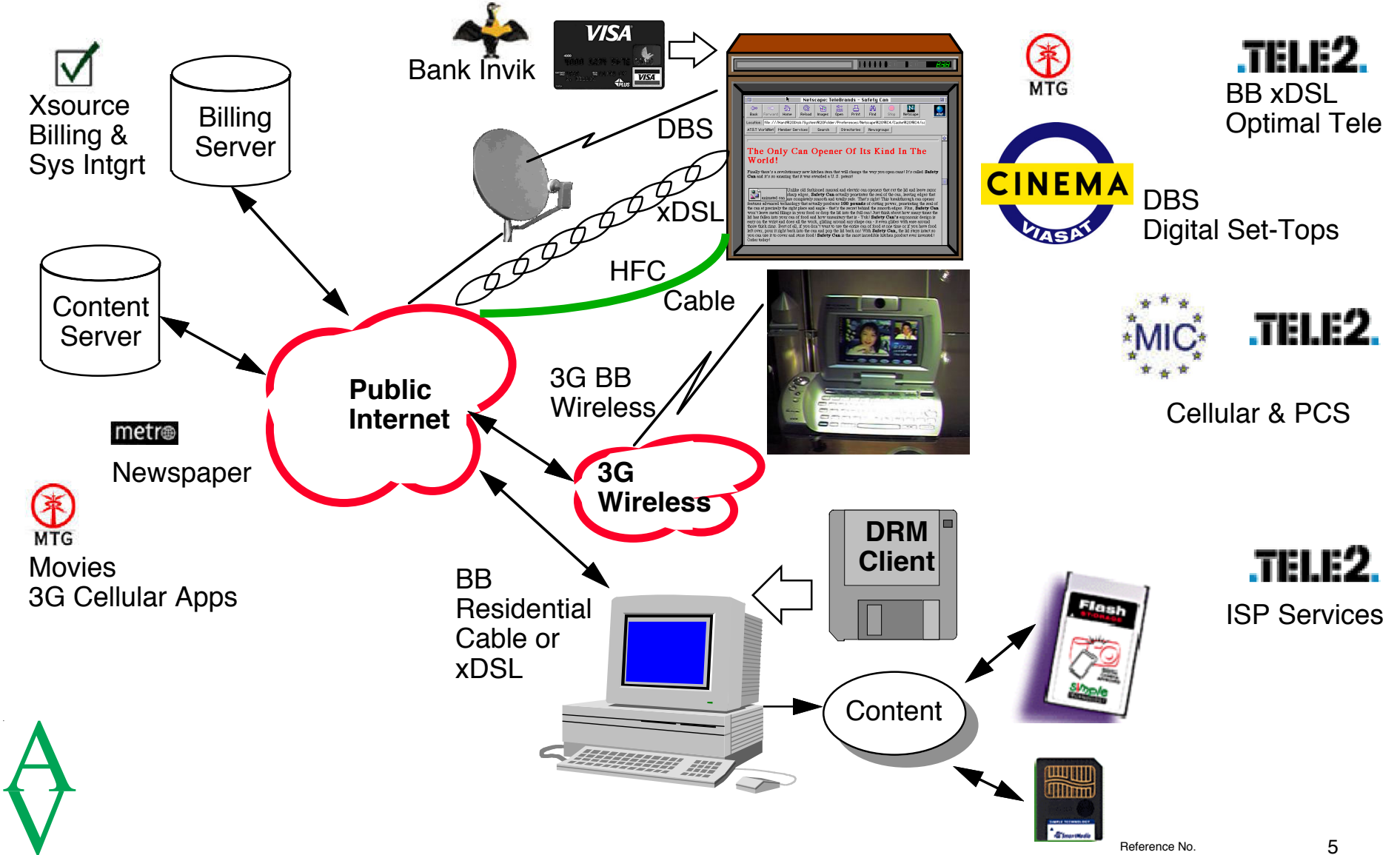| Stu Lipoff	IEEE & CE Society	OurGroup	Applied Value

• 30 years experience
  —5yrs portable RF
  —25yrs Consultant @ ADL
• Education
  —BSEE/BSEP
  —MSEE
  —MBA
• IEEE
  —Institute fellow
  —Past pres CE Soc
  —Chair CE Stds
• Practice
  —TIME[4]
  —Svc Providers
  —Suppliers
  —Top Line Rev
• Related Experience
  —MCNS cablemodem
  —RIAA/IFPI Next Gen CD
  —DataPlay DRM
	• IEEE is World's largest technical organization and publisher
	• Transnational non-profit professional organization
	• CE Society is one group under Tech Activities Board
	• Standards board has cross society responsibilities, e.g:
	  —Ethernet 802.3
	  —WiFi 802.11
	  —ATSC TV
	• CE Society standards chair has liasion responsibility to the Standards Board
		• A mainly European based cluster of public and private firms linked by common ownership
		• Public cluster of firms have market caps >$US10b
		• Both *new* and *old* economy ops
		  —Old: pulp/paper and financial services
		  —New: telecom and media
		• Private Companies
		  —Professional services such as Applied Value
		  —Incubator startup operations
			• Boston based tech & mgt consultants
			  —About 50 staff
			  —15 in Boston
			  —30 in R.O.W.
			• Founded about 4 years ago as ADL spin-off
			• Captive work for OurGroup ranges from 25-50% of total hours billed
			• Works jointly with other professional service family members
			  —Netcom
			  —Secure Value
			  —Shard Value
			  —Bassett

We have several operating companies with an interest in increasing revenue and margin by adding enhanced services and engaging in transactions involving rights managed content.

**NonVoice
Data & Content**

**Voice/Data
Hybrid**

Value Added

**Plain
Old
Cellular
Service**

**Plain
Old
Cellular
Service**

**Increasing Margin
& Competitive
Position**

OurGroup companies have telecom and media interests

Xsource
Billing &
Sys Intgrt

Billing
Server

Bank Invik

DBS

xDSL

HFC
Cable

3G BB
Wireless

Content
Server

**Public
Internet**

metro
Newspaper

MTG
Movies
3G Cellular Apps

**3G
Wireless**

BB
Residential
Cable or
xDSL

**DRM
Client**

Content

MTG

TELE2
BB xDSL
Optimal Tele

CINEMA
VIASAT

DBS
Digital Set-Tops

MIC TELE2

Cellular & PCS

TELE2
ISP Services

Key Issues for Rights Managed Content Electronic Distribution

Because there are a variety of stakeholders any solution will likely have to balance benefits and implementation timing against various kinds of *costs, drivers, and inhibitors,* e.g:

Music Companies	**Media Manufacturers**	**Consumer Electronics Manufacturers**
• Meet customer needs • Manage piracy • Provide compatible media • Manage, control, and/or meter distribution and usage • Reduce costs	• Recoupe capital investment • Maintain throughput • Minimize variations • Minimize license fees • Satisfy record company needs	• Meet consumer needs • Introduce new, high margin, products • Maintain sale of CD copiers • Reduce license fees
Computing/ IT Manufacturers	**Software/IT Publishers**	**Communications Service Providers & Broadcasters**
•Meet customer needs •Provide multimedia systems •Maintain backward compatibility •Facilitate new applications and software	•Accelerate upgrade sales •Wide platform compatibility •Control piracy •Tap into recurring revenue stream	• Facilitate consumer broadband services • Move upstream in value chain toward content management
Consumer Groups	**Regulator/Lawmakers**	**Technology Provider Intellectual Property Holders**
• Argue for broader fair use • Minimize consumer costs • Maximize life of legacy device investments	•Search for political solutions •Serve the public interest •Favor simple short term actions	•Seek to keep technology proprietary • Maximize favorable license terms

Today's DRM space has a limited set of choices in each dimension

- Content
- DRM Function
- Synergistic Functions
- Delivery Platform
- Business Models
- Content Container
- Communications Channel
- Key Technologies
- User Experience

Key Issues for Rights Managed Content Electronic Distribution Segment Dimensions

	Yesterday	Future
Content	•Publications •Music •Images •Video/Movies •Software •Games	**Same +** •Interactive multimedia •Virtual reality •Agents & tools •Feature upgrades •??New ideas to come??
Function	•Anti-piracy	**Same +** •Privacy •Revenue Accounting •Audience measurement •Forensic watermarking
Synergy	•None	•Messaging/Email •Transaction processing

Key Issues for Rights Managed Content Electronic Distribution Segment Dimensions

	Yesterday	Future
Delivery Platform	•Wintel PC	**Same+** •Non-windows O/S on PC •Network appliances •PDAs •Cellphones •Personal Multimedia Devices •Games & toys •Automobile onboard computers •Smart white goods appliances •Home servers/PVRs •Agent software and tools
Business Models	•Pay to own	**Same +** •Pay per play •Pay to upgrade •Rent to own •Pay less per copy •Reverse pay (I.e. advertising) •Super-distribution •Pay to use •Pay to distribute •Pay for convenience

Key Issues for Rights Managed Content Electronic Distribution Segment Dimensions

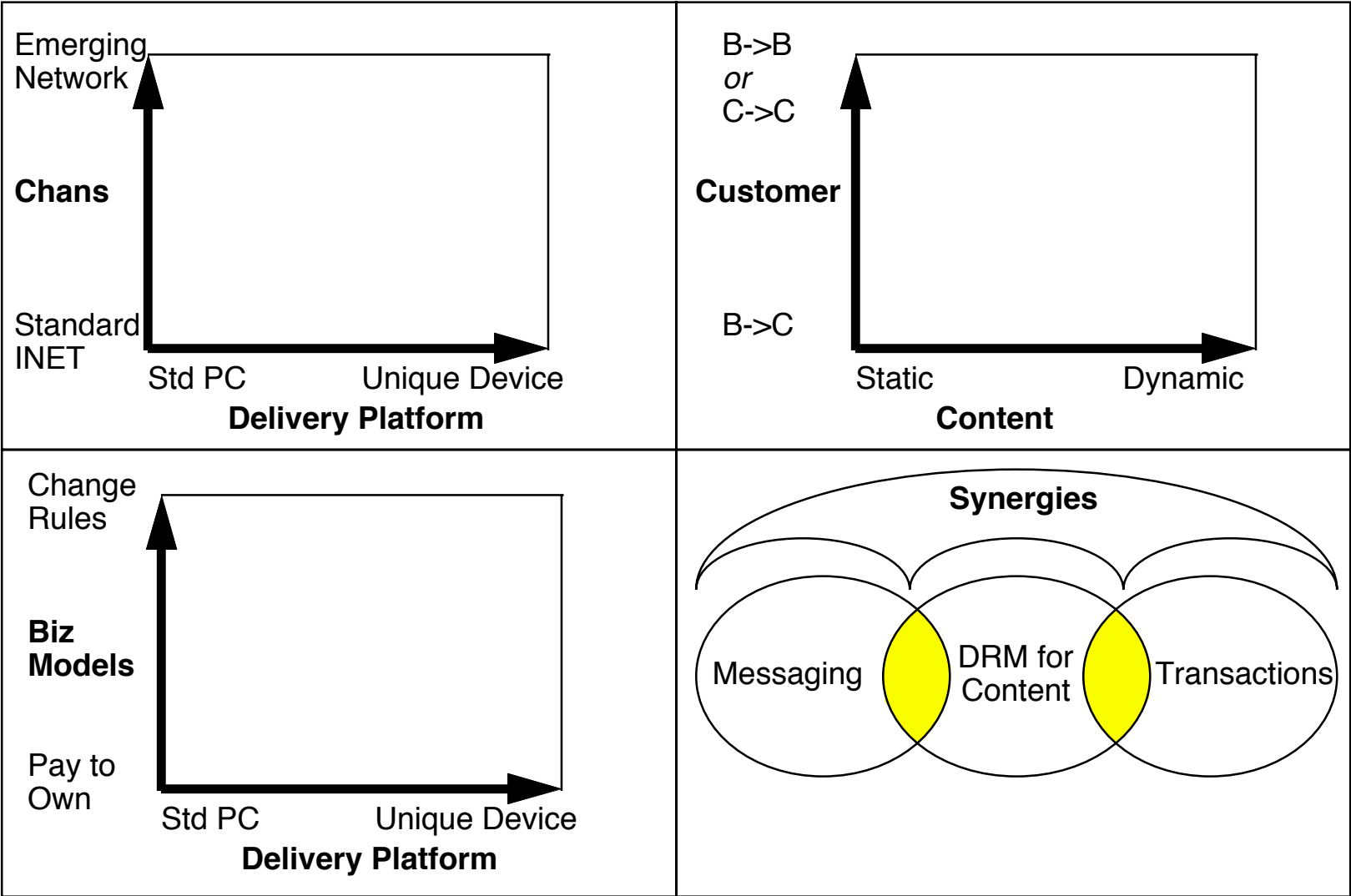|	Yesterday	Future
Content Container	•HardDrive on Foreign Remote Server	**Same+** •Harddrive on local customer provided server •Harddrive on local operator maintain server •Physical media (CD, flash, DataPlay, etc) •Peer to Peer from Harddrive of peer computer
Comm Channel	•Public Internet	**Same+** •Private and virtual private networks •Wireless public networks •Wireless private networks •Physical distribution (I.e. stores)

Key Issues for Rights Managed Content Electronic Distribution Segment Dimensions

	Yesterday	Future
Tech-nology	•Private key encryption •Public key encryption	Same Same+ •Smart cards •Quantum computing •Highly parallel processing •Biometric access control •Watermarking •Fingerprinting •Security kernals •Software Defined Products
User Exper-ience	•Complex •Bound to single delivery platform	**Same** **Same+** •Portable across platforms (bound to user) •Bound to media •Bound to portable "key"

Some possible maps include

Chans

Emerging Network

Standard INET

Std PC   Unique Device

Delivery Platform

Customer

B->B
or
C->C

B->C

Static   Dynamic

Content

Biz Models

Change Rules

Pay to Own

Std PC   Unique Device

Delivery Platform

Synergies

Messaging   DRM for Content   Transactions

Possible categories include

- Financial

- Technology

- Market Segments, e.g.
  - Customer
  - Business Model

- Risk levels

- Need for partners

- Barriers to entry (e.g. patents)

which need to be mapped into
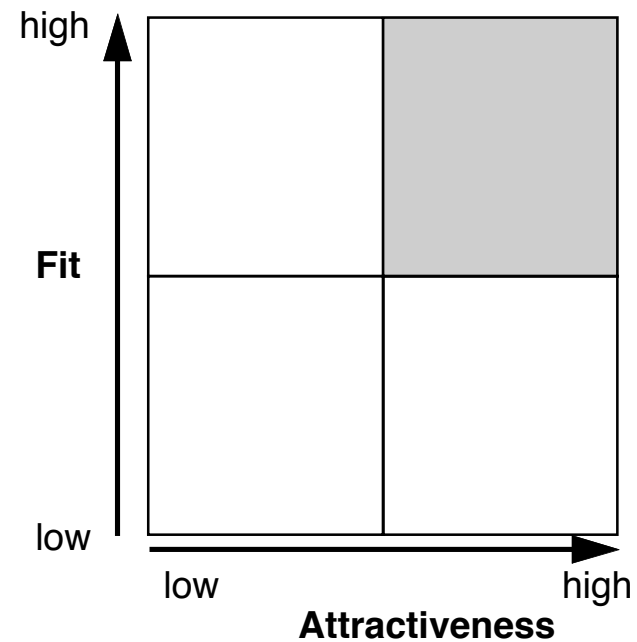
Are risks within reason and does it meet security/threats and other performance requirements?

- Security Issues
    - Protection against piracy by cryptoanalysis (strength of algorithm)
    - Protection against piracy by tampering/cloning
    - Containment (i.e. global secrets)
    - Data integrity
    - Audit and accountability

- Other Performance Issues
    - Storage capacity overhead for protection
    - Computational complexity->delays/throughput reduction due to en/de-cryption overheads or key-exchange overheads
    - Access time delays due to key-exchange overheads or other validation process overheads
    - Costs
        - Of authoring systems
        - Of drive hardware
        - Delta impact on media

Does it have the required features and the flexibility to accommodate new needs?

- Security Related
  - Renewability
  - Revocation
  - Transfer of rights
  - Watermarking
  - Serial numbering (e.g: by title, by production run, by instance)

- Flexibility
  - Ability to support wide variety of business models including: free, limited rights trials, pay to play, pay to own, serial copy management, etc
  - Open architecture aspects
  - Compatibility with other media DRMs
  - Compatibility with communications based DRMs

- Convenience
  - Requirements for extra steps by consumer
  - Negative impacts on navigation features

Does it support the business models and concerns for each of the stakeholders?

- Required division of roles and responsibilities along value chain

- Required division of revenues/costs along value chain

- Compliance with US Government ITAR regulations

- Operating costs implications

- Compliance with well known industry standards (e.g. SDMI)

- Requirements for licensing and/or intellectual property risks

We believe the main DRM related issues of interest would group into the following categories

- **Technology**

  Are risks within reason and does it meet security and other performance requirements?

- **Functional capabilities & features**

 *Does it have the required features and the flexibility to accommodate new needs?*

- **Business issues**

  Does it support the business models and concerns for each of the stakeholders?
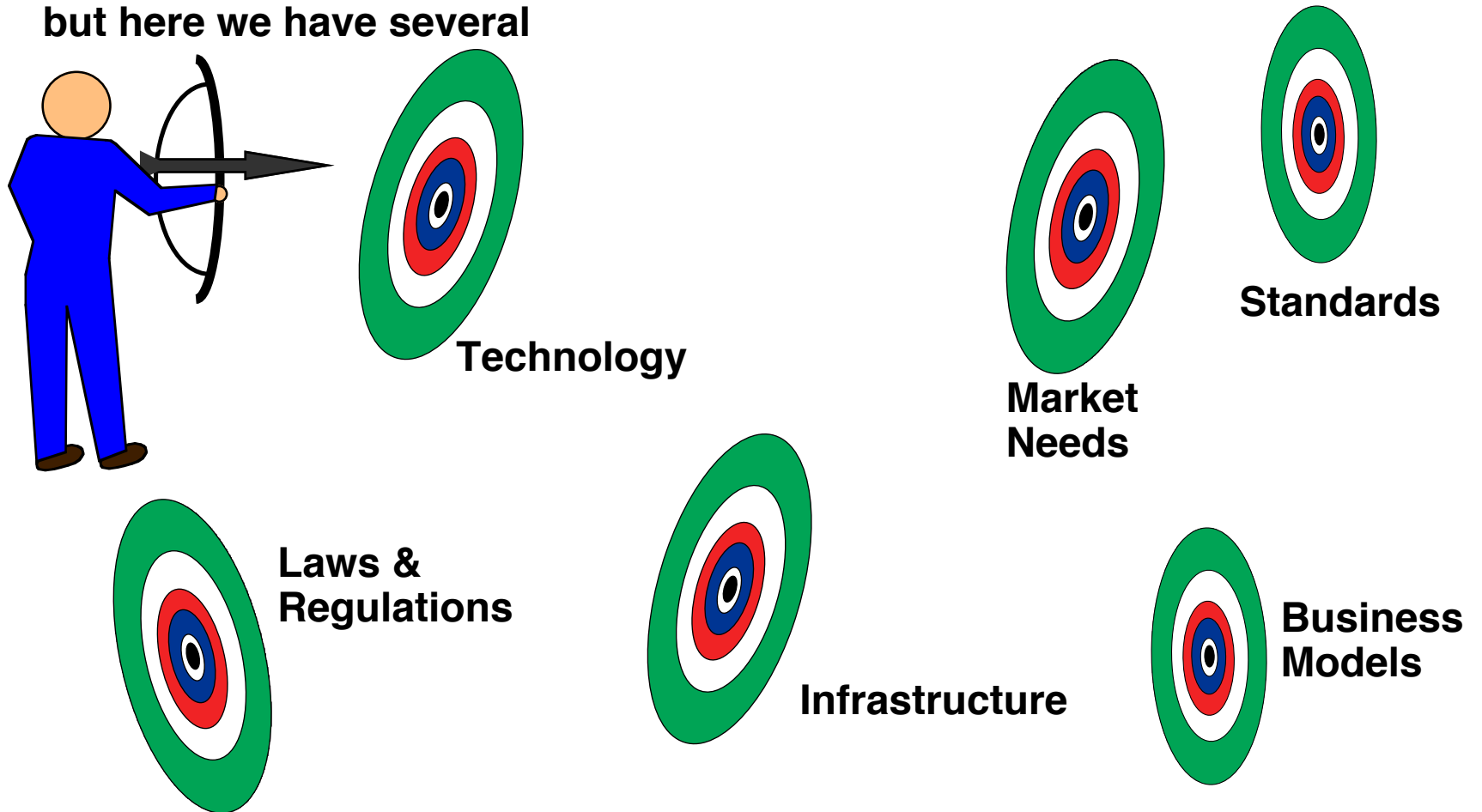
Developing a solution with one moving target would be hard enough but here we have several

Laws & Regulations

Business Models

Technology

Market Needs

Standards

Infrastructure

Developing a solution with one moving target would be hard enough but here we have several

Technology

Standards

Market
Needs

Laws &
Regulations

Infrastructure

Business
Models
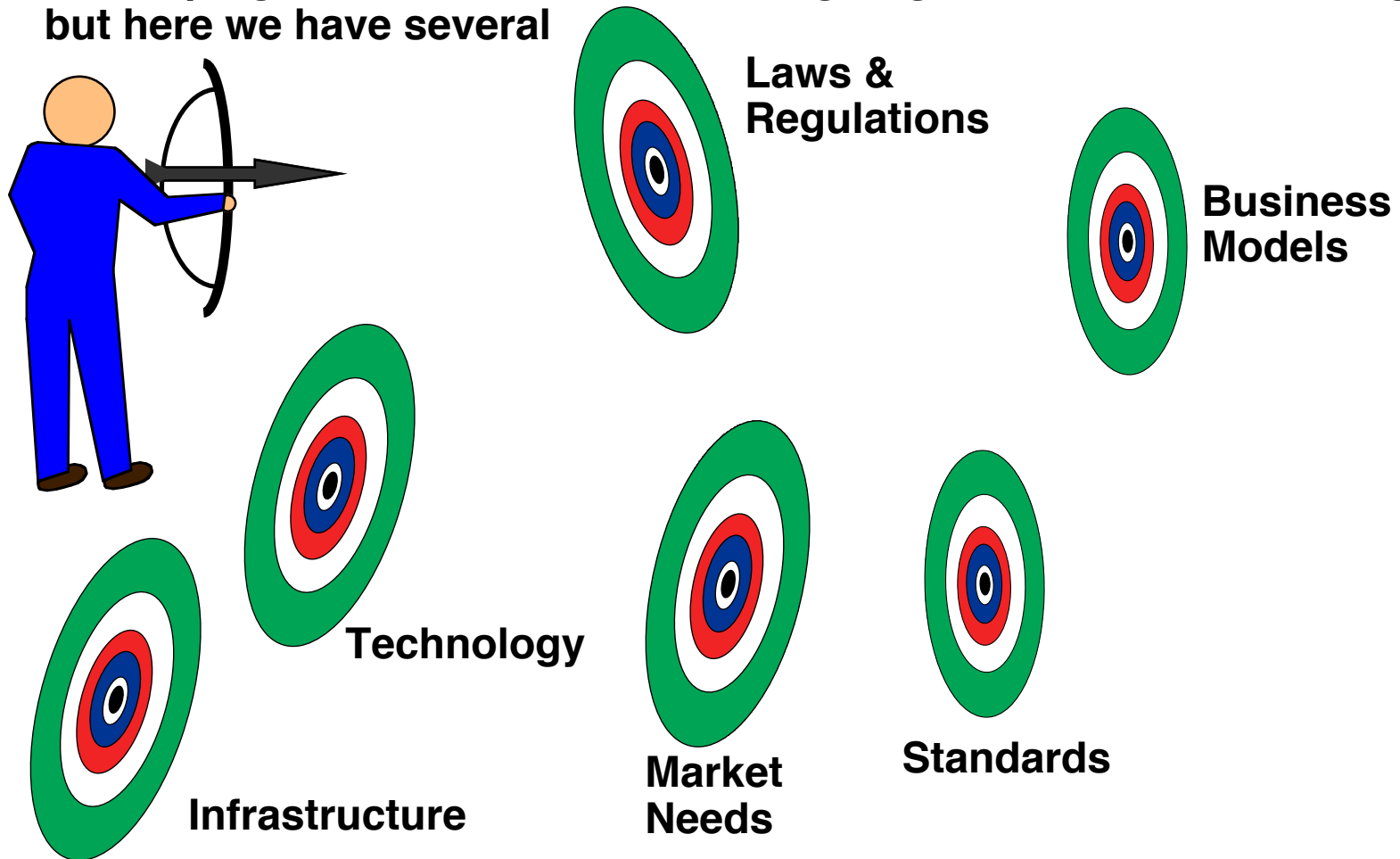
The only thing we know for sure is that *what we believe to be true today* **is likely to be very different from** *what we will know to be true in the future*

I believe finding the *right answer* involves keeping the following guiding princibles in mind

- Continuously test and score the solutions against the criteria likely to be used by each stakeholder, separating the two different kinds of criteria
    - Type 1: knock out criteria (e.g. no means for revocation/renewal)
    - Type 2: comparative criteria (e.g. access time delay)

- Try to reach consensus at high layers of abstraction   prior to attacking the next layer down

- Layer your standards from physical to applications layer trying to avoid any cross layer dependencies

- Draw as much as possible on well known, tested, and accepted industry standards

- Build into the
    - architecture, file formats, protocols, and processes
  an evolutionary means for
    - flexibility, growth, and an upgrade path

Because of a major paradigm shift to software defined CE products one can think about an ideal architecture based on *platforms* rather than *hard coded products*
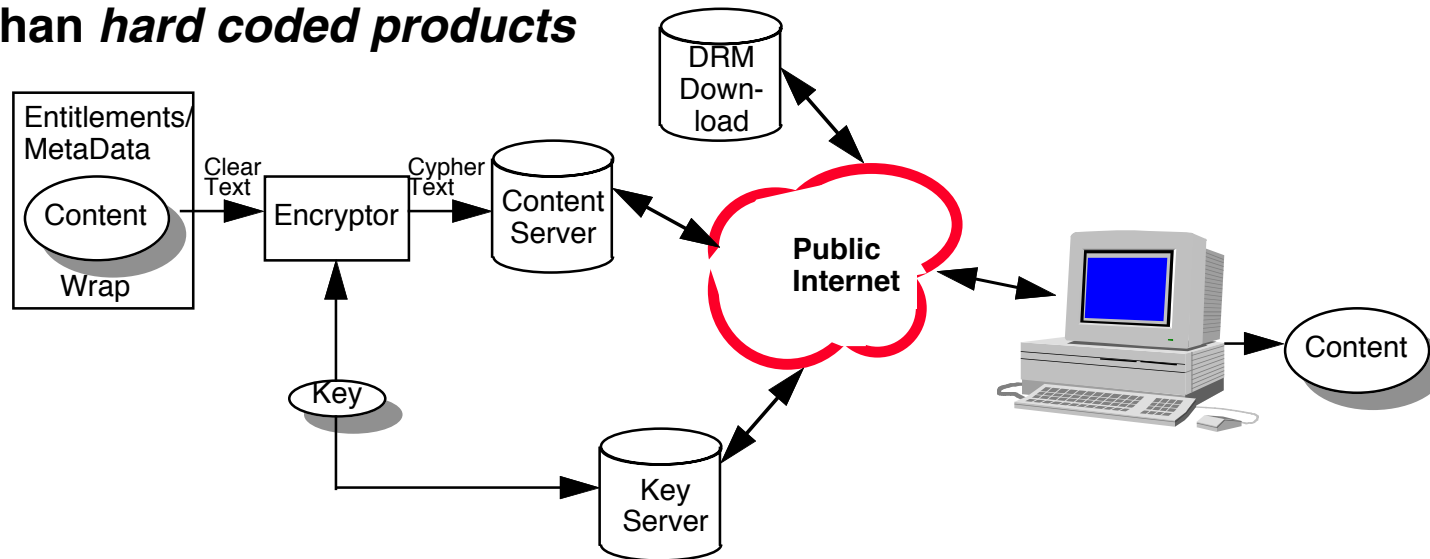
- Since the PC is has well defined protocols and software architectures it is possible to design an interoperability standard from a platform perspective
- In such a case one need only assume level 1 through 3 communications protocols and an IP transparent pipe between servers and the PC
- The software architecture can be assumed to be a choice from a small set of well known O/S and presentation level peripherals and protocols
- To be useful the standard should be concerned only about a minimal level of topics
  - On the client end identify the minimum set of hardware and software requirements and options
  - On the server end one must specify
    - A revision 0 protocol for session establishment
    - A format for a data dictionary for the meta data and revision 0 transaction set
    - A revision 0 session protocol that includes the means to negotiate for highest common denominator revision support above revision 0

A example of the session flow would be

Server ◀—————————— **IP Transparent Link** —————————▶ Content

◀— **Communicate to server to establish account and identify platform** —

————————— **Download to platform a compatible DRM client** ——▶

◀———— **Use designated transaction set to request transaction** ————

———— **Download DRM protected Content with Standard MetaData** —▶

◀———— **Use designated transaction set to confirm transaction** ————

If the CE Device Supports an IP Stack and a Programing Language then it can be treated as a platform same as a PC

Server ← **IP Transparent Link** → Content

examples

Content Rendering Engine	MP3
Programing Language	J2ME
Download Protocol	TFTP
IP Stack	UMTS

← **Communicate to server to establish account and identify platform** —

Download to platform a compatible DRM client →

← **Use designated transaction set to request transaction** —

Download DRM protected Content with Standard MetaData →

← **Use designated transaction set to confirm transaction** —

Since current generation CE devices may lack programmability a small number of specific DRMs can be identified as a transition to future software defined devices

Server

IP Transparent Link

Content

PreLoaded DRM

Communicate to server to establish account and identify platform

Download to platform a compatible DRM client

Use designated transaction set to request transaction

Download DRM protected Content with Standard MetaData

Use designated transaction set to confirm transaction