

PROJECT
DR**M**

The word "PROJECT" is in a blue, sans-serif font. Below it, "DR" and "M" are in large, blue, 3D block letters. The "ea" is contained within a white wireframe globe with a blue grid.

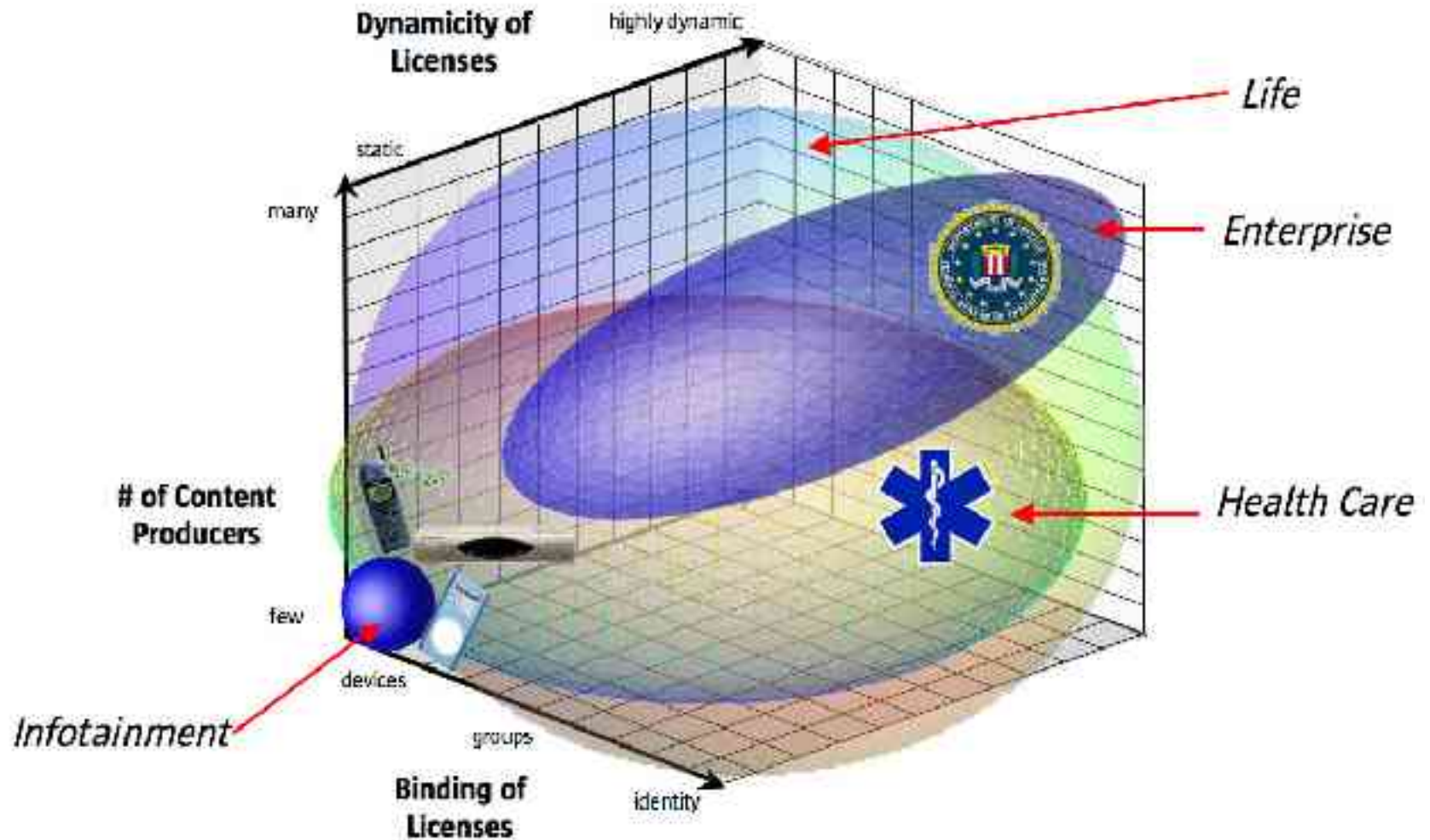
Introduction to DReaM

Gerard Fernando

Santa Clara, California

March 15-16, 2006

DRM Requirements

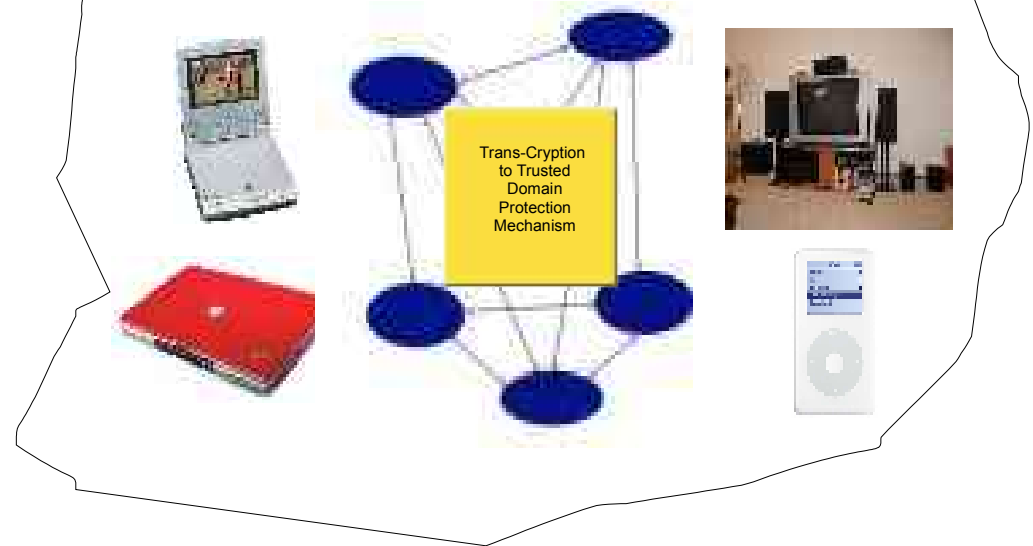


Infotainment/Content Model

Trusted Client Devices



Trusted P2P Networks



Business Applications

Healthcare & Medical



Military



Business & Education

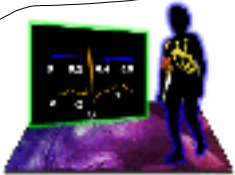


Finance



Life Model

Personal Information



Personally Identifiable Info



Personally Generated Information/Content



Open Media Commons

- Specify open, ***royalty-free*** digital rights management standards
- Collaborate with like-minded open-source communities
- Influence standards organizations
- Promote the creation, duplication and distribution of digital content and ensure that creators and owners get compensated

OMC's Project DReaM

- Supports Open Media Commons (OMC) vision of open source and royalty-free intellectual property
- Leverage Liberty Alliance to promote Identity & Role based licensing models, rather than device based licensing only
- Addresses both Conditional Access (CA) and Digital Rights Management (DRM) system models
- Addresses customer requirements for multi-system interoperability
- Independent of any specific content type
- A horizontal solution platform capable of supporting: Business, Content and Life vertical markets
- Exploration of RMS policy options beyond encryption (watermarking & tracking)

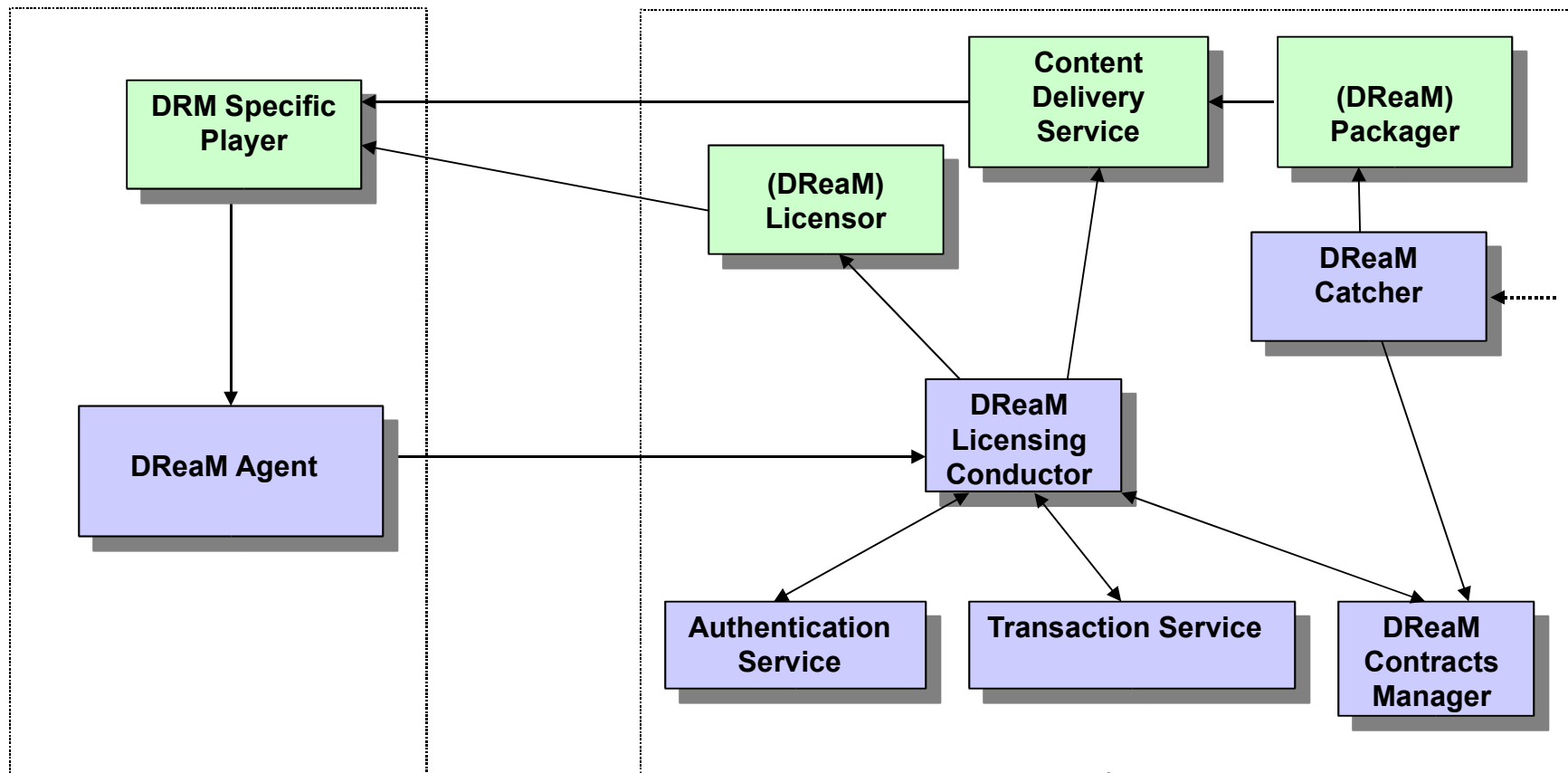
DReaM project - Two Goals

- Disintermediation (D15N)
 - Separation of back-office services from content protection functions.
 - Can support many content protection technologies (including proprietary)
- Content protection functions based on open, royalty free technologies
 - CAS (Conditional access system) - intended to handle limited content access scenarios where the consumption is immediate.
 - DRM (digital rights management) - management and protection of content during its entire lifetime.

Main Technical Mechanisms

- Encryption of Content and keys
 - > Symmetric (content): 3DES, AES
 - > Asymmetric (keys): RSA, ECC
- Issuance of Certificates
- Revocation
- Back-channel of communication
- Secure Device
 - > ID, Clock, Storage, Execution
 - > TCG (trusted Computing Group)
 - > SOC (System-on-a-chip)

Architectural overview



DReaM Client Side

DReaM Service Side

Content protection components

Disintermediation components

Components of DReaM - Disintermediation

- DReaM Licensing Conductor - Primary point of contact for client (with Disintermediation system)
- DReaM Contracts Manager) - Content Rights Server/Repository
- DReaM Catcher - Content Catcher/Ingest
- DReaM Agent
 - Ability to negotiate for licenses
 - Supports CA and DRM models

Components of DReaM - Disintermediation

Continued:

- Authentication Service - to enable identity and role based licensing
- Transaction Service - Payment & Fulfillment (e-Commerce)

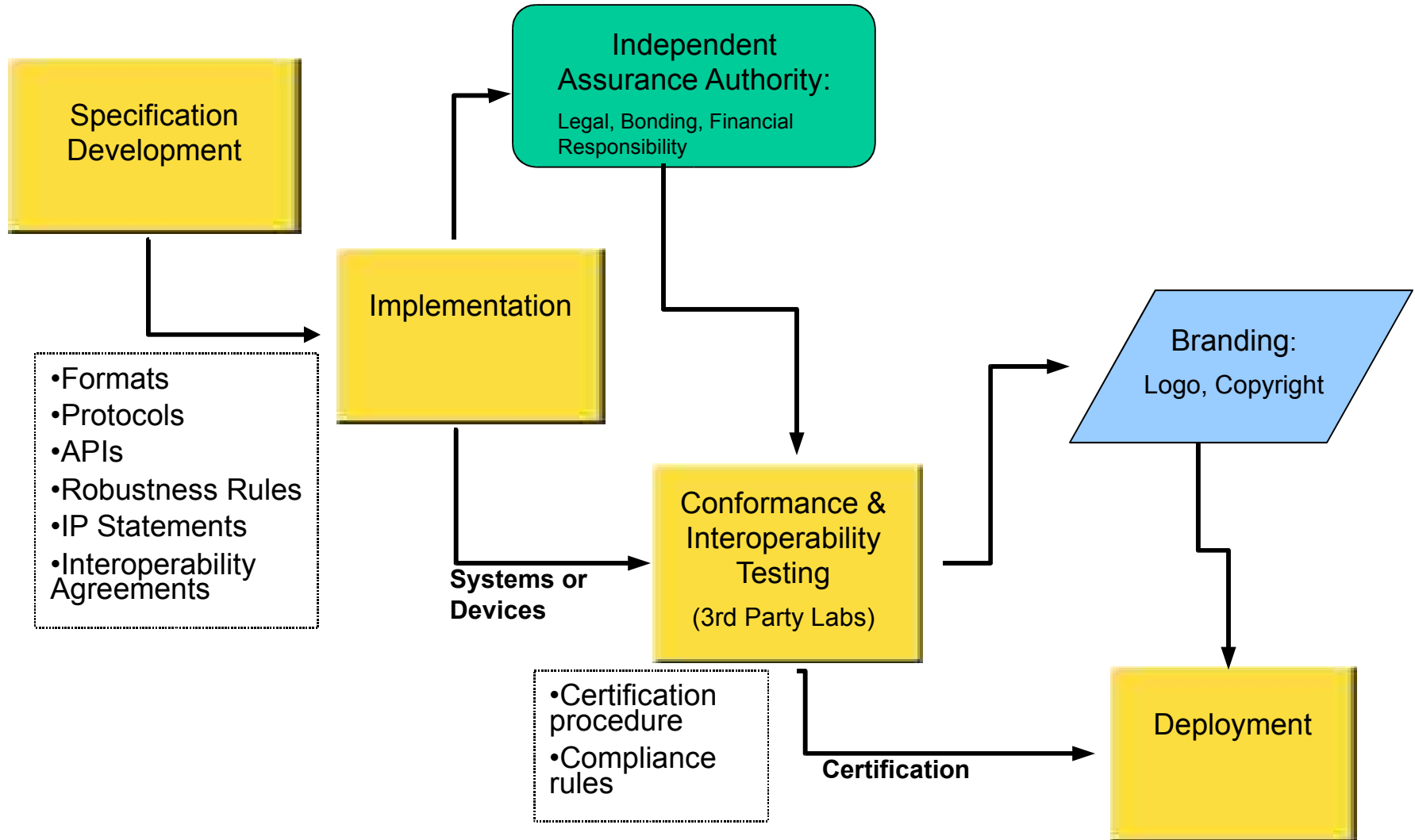
Components of DReaM - Content Protection

- DReaM Packager - Content Packaging, encryption
- (DReaM) Licensor - Generation and delivery of licenses (rights and keys)
- DRM specific player
 - Set-top-box, Mobile phone, CE devices, PC
 - Secure Device
 - ID, Clock, Storage, Execution
- Content delivery server

Rights Management

- Rights management will be applicable to broad spectrum of content, devices, users and industry types
- Open Source & RM is not an oxymoron!
 - > PKI, C&C, SOC, etc.
- Failed standards process
 - > When RAND is not Reasonable
- Open Source + Royalty-Free = Better
 - > Open Media Commons (OMC)

The Process Ahead



What is Required to Implement a DReaM Based Solution?

- Specifications & API's
 - > Content encryption
 - > Key management
 - > License/rights expression
 - > Service API's for configuration and upgradeability
- Robustness rules
 - > Client, network, service
 - > These will differ for application domains

DReaM Based Solution for CAS

- MPEG-2 TS content (including AVC, VC1)
 - > CAS (Conditional Access System) defined & code available
- Specifications & API's
 - > Content encryption - defined by DReaM-CAS spec
 - > Key management - defined by DReaM-CAS spec
 - > License/rights expression - *Not necessary for CAS*
 - > Service API's for configuration and upgradeability - TBD
- Robustness rules - TBD

DReaM Based Solution for DRM

- For MPEG-2 TS content
- Specifications & API's required (to extend from CAS to DRM)
 - > Key management - defined by DReaM-MMI
 - > License/rights delivery - defined by DReaM-MMI
 - > Service API's for configuration and upgradeability - TBD
- Robustness rules - TBD

DReaM Based Solution for DRM

- Formats other than MPEG-2 TS
 - > Content encryption - TBD (for both CAS and DRM)
 - > Possibly, use ISMACryp for RTP based content?
 - > Key management TBD

Elements of DReaM presented at this workshop

- Digital Rights Management Service (DReaM-MMI)
 - > Ability to manage rights for any type of content in various usage models
- Conditional Access (DReaM-CAS)
 - > Ability to deliver timeline dependent content to multiple consumers (IPTV, telemetry, surveillance)
 - > Includes content protection and distribution technologies
- Disintermediation (DReaM-D15N)
 - > Intraoperability Framework
 - > Separation of back-office services from players/consumption
 - > Authentication, Billing, Entitlement, Rights Management, Subscriber Services, Portal, Content Delivery
 - > Interoperability with existing content protection technologies
 - > Client-side Player/Consumption, Licensing, Packaging
 - > Emphasis on Identity based licensing over device licensing

Other DReaM topics presented at this workshop

Continued:

- Usage scenarios & business requirements
- Technical requirements

PROJECT
DREAM

Introduction to DReaM



<http://OpenMediaCommons.org>