

Report on Reuters Response to MPEG-21 CfR
Report to XACML Committee Face-to-Face Meeting

David Parrott
Reuters/Chief Technology Office
18 July 2001

The Permissioning Problem

Reuters Today

- Private networks give tight access control
- Reuters client-site components allow fine-grained permissions
- Control is reduced on satellite feeds
- Many data types, all with different permissioning models and implementations
- Heavyweight subscription contracts.

Digital Rights Management (DRM)

- Managing:
 - Rights (IPRs, Permissions, Access Controls, Usage, etc)...
 - Obligations...
 - Audit trails...
 - ... across the *entire* value chain (of IPR creators, publishers, distributors, consumers...)
- Electronic, machine-readable contracts
- In equal measures:
 - Legal Infrastructure
 - Business Infrastructure
 - Technology Infrastructure.

Many Approaches to DRM

- Standardised Markup for Expressing Rights and Obligations
- Detection of IPR Infringement
 - Watermarking
 - Fingerprinting/Traitor Tracing
 - Tracking/Searching
- Rights and Obligations Enforcement
 - *Permissioning and Access Control (encryption technologies if appropriate)*
 - *Licensing and contracts*
 - *Sandboxes (protected environments).*

Why are we Interested in Digital Rights Management?

Reuters needs to permission its data and protect its IPR...

- Data is inherently valuable
- Unified approach across “Slice and dice” service offerings
- Unified approach across flexible and varied distribution channels
 - e.g., proprietary networks, satellite broadcast, public Internet
- Broadcast mode delivery is required in many cases for scalability
 - permissioning restricts access to just those parts paid for
- Third party content comes with complex and exacting distribution rules
 - plus regulatory requirements
- Data flows are multi-directional and include contribution rights.

What Digital Rights Management is *NOT*

(i) It is *not just* enforcement by locking up content in a layer of encryption

Restricted Actions:

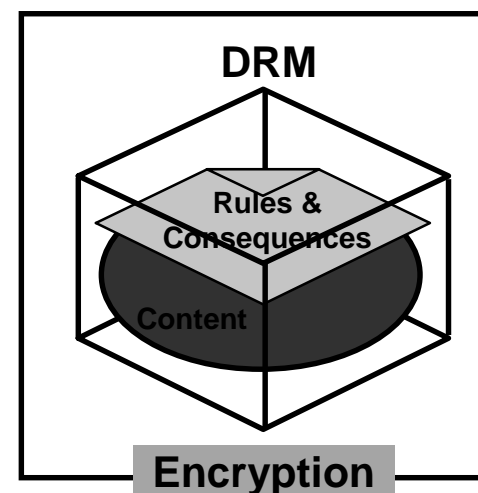
- View, Print, Save, ...
- No “fair use”
- B2C dominated

Security/Trust Problems:

- Software inherently unsafe
- Trusted applications restrictive
- Vulnerable to systematic attack

Proprietary Implementations:

- Lacking interoperability
- Closed user-base
- Risk backing the wrong player

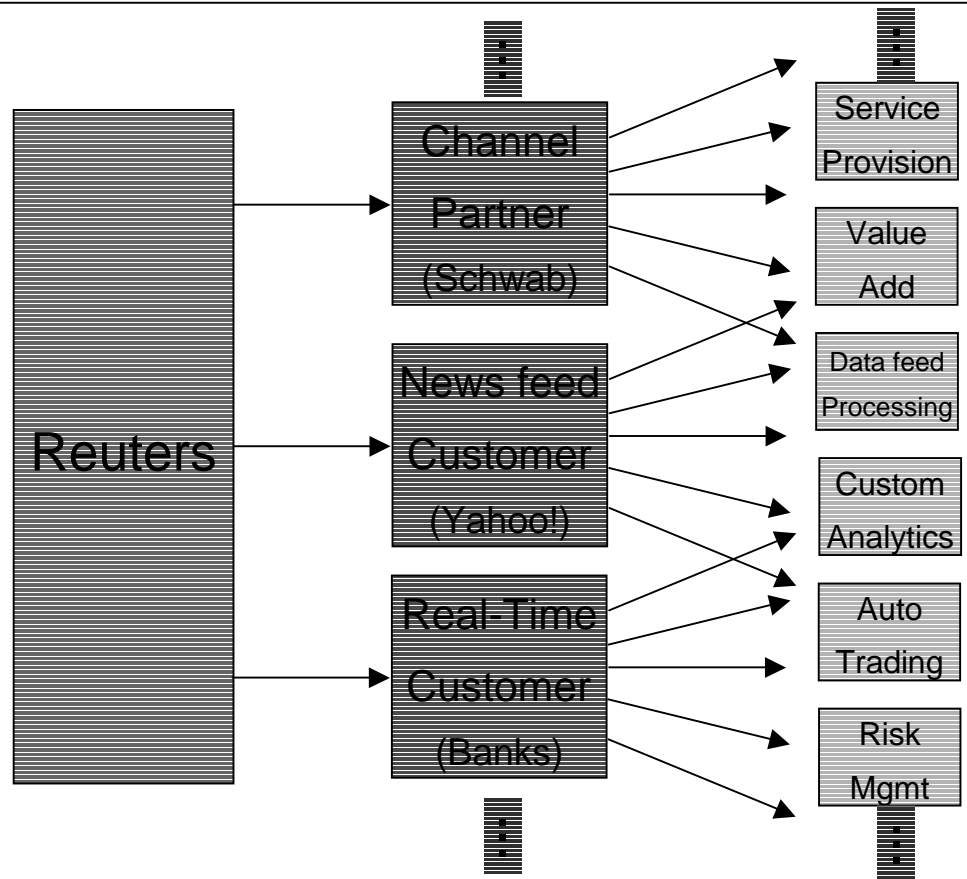


What Digital Rights Management is *NOT*

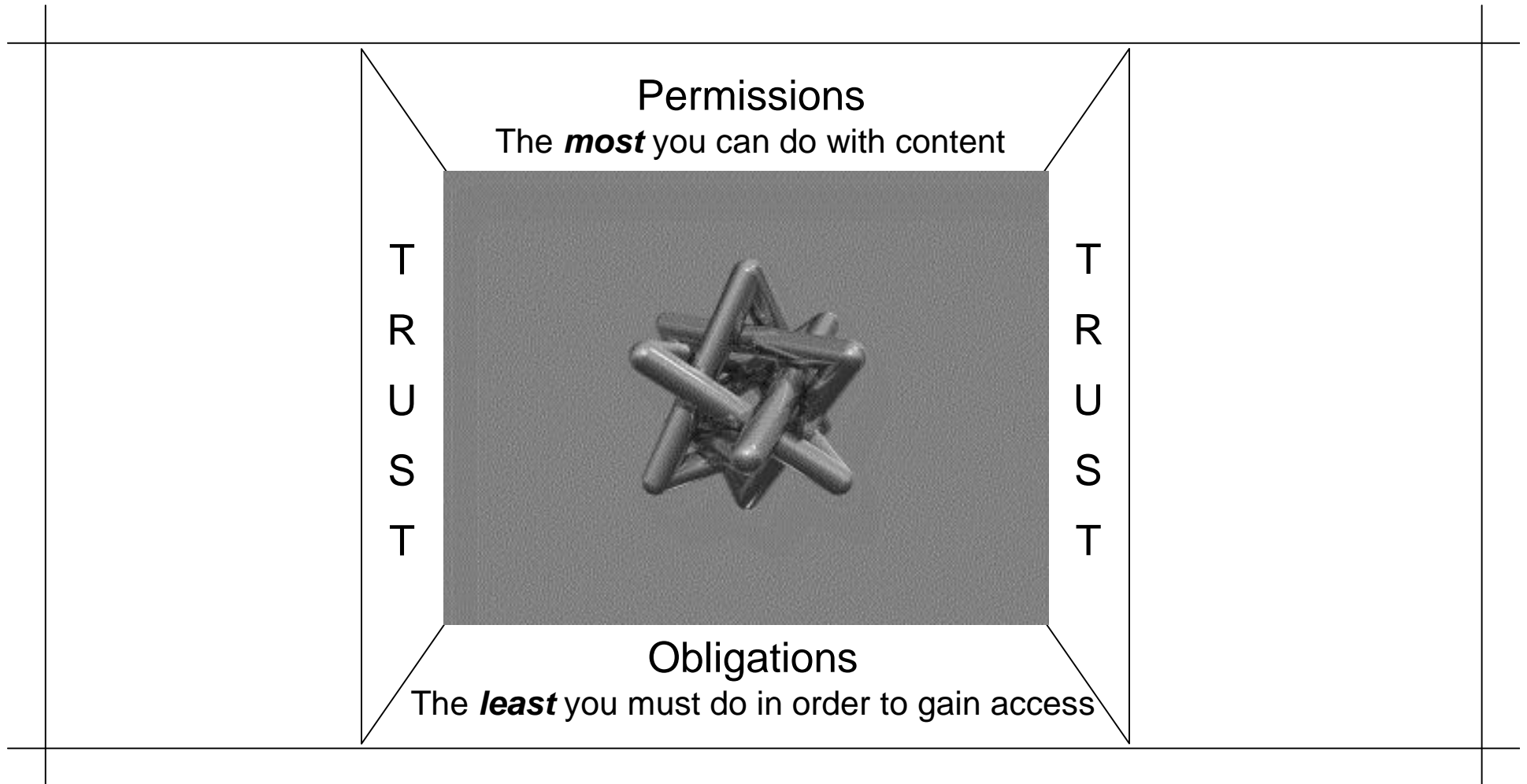
(ii) It is *NOT* the exclusive domain of “Eyes and Ears” B2C data delivery



Vs



Content, Permissions, Obligations, and Trust



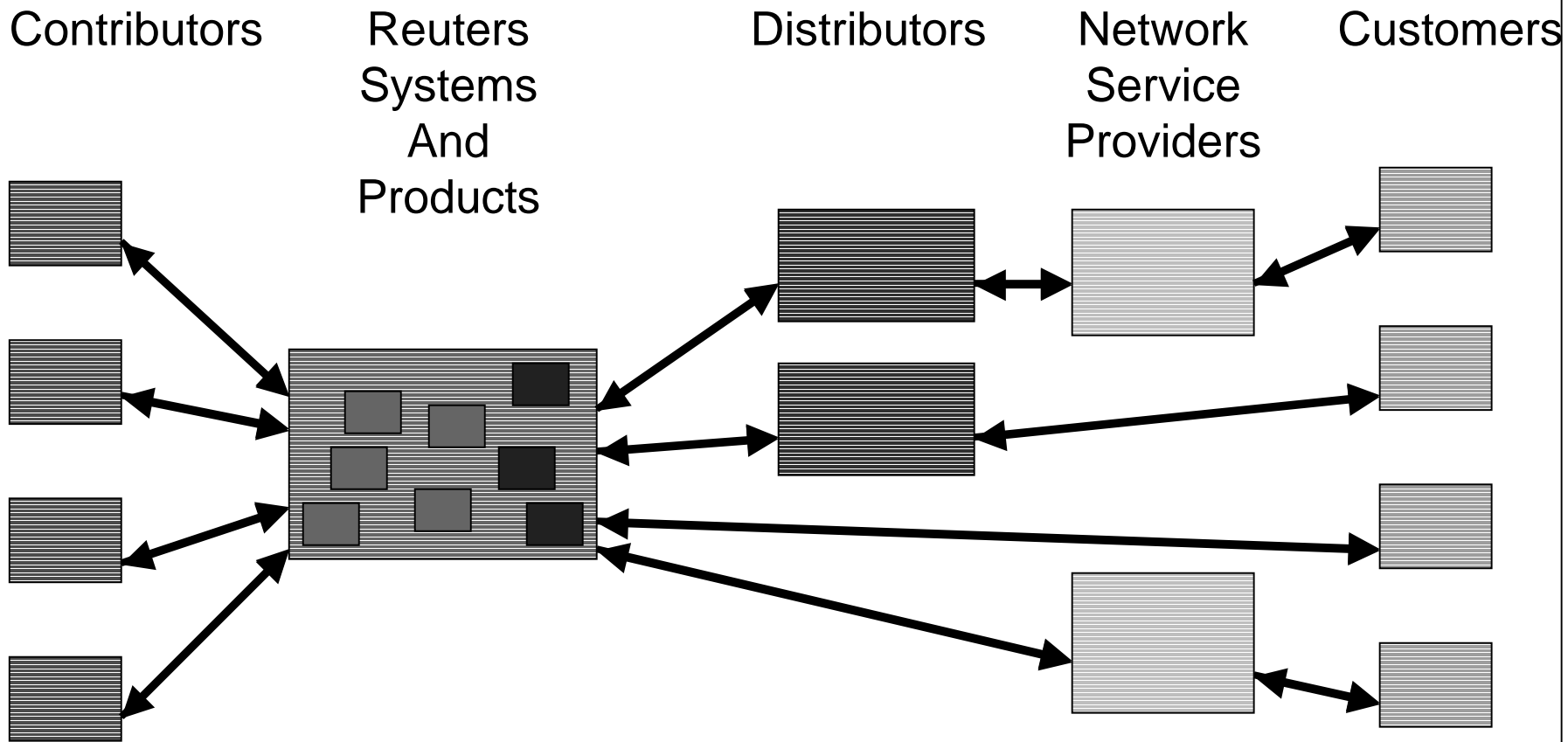
MPEG-21

- Content

- *Creation and Production*
- *Distribution*
- *Consumption and Usage*
- *Packaging*
- *Identification and Description*
- *Representation*

- Intellectual Property Management and Protection
- Financial Management
- User Privacy
- Resource Abstraction
- Event Reporting

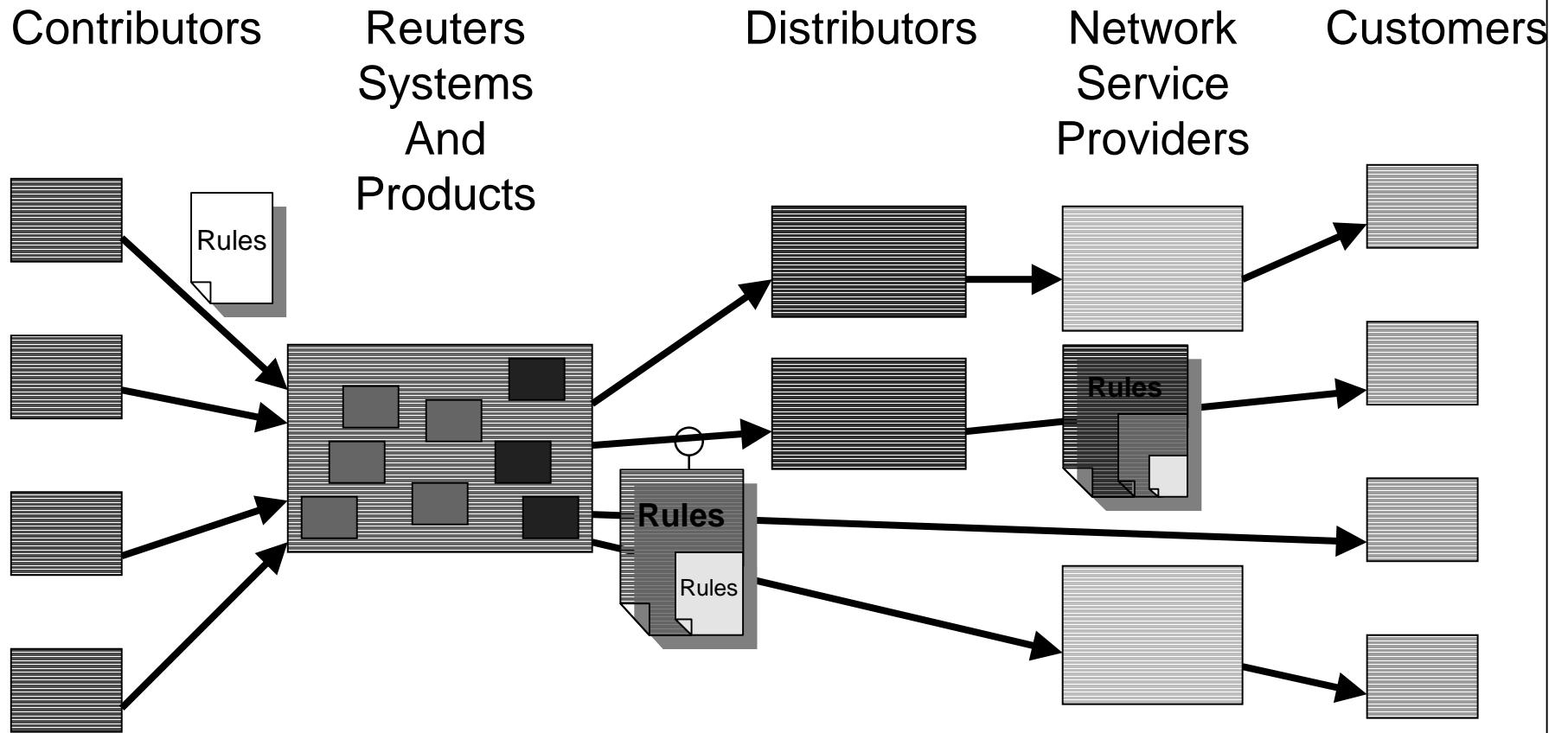
Rights Expressions Everywhere



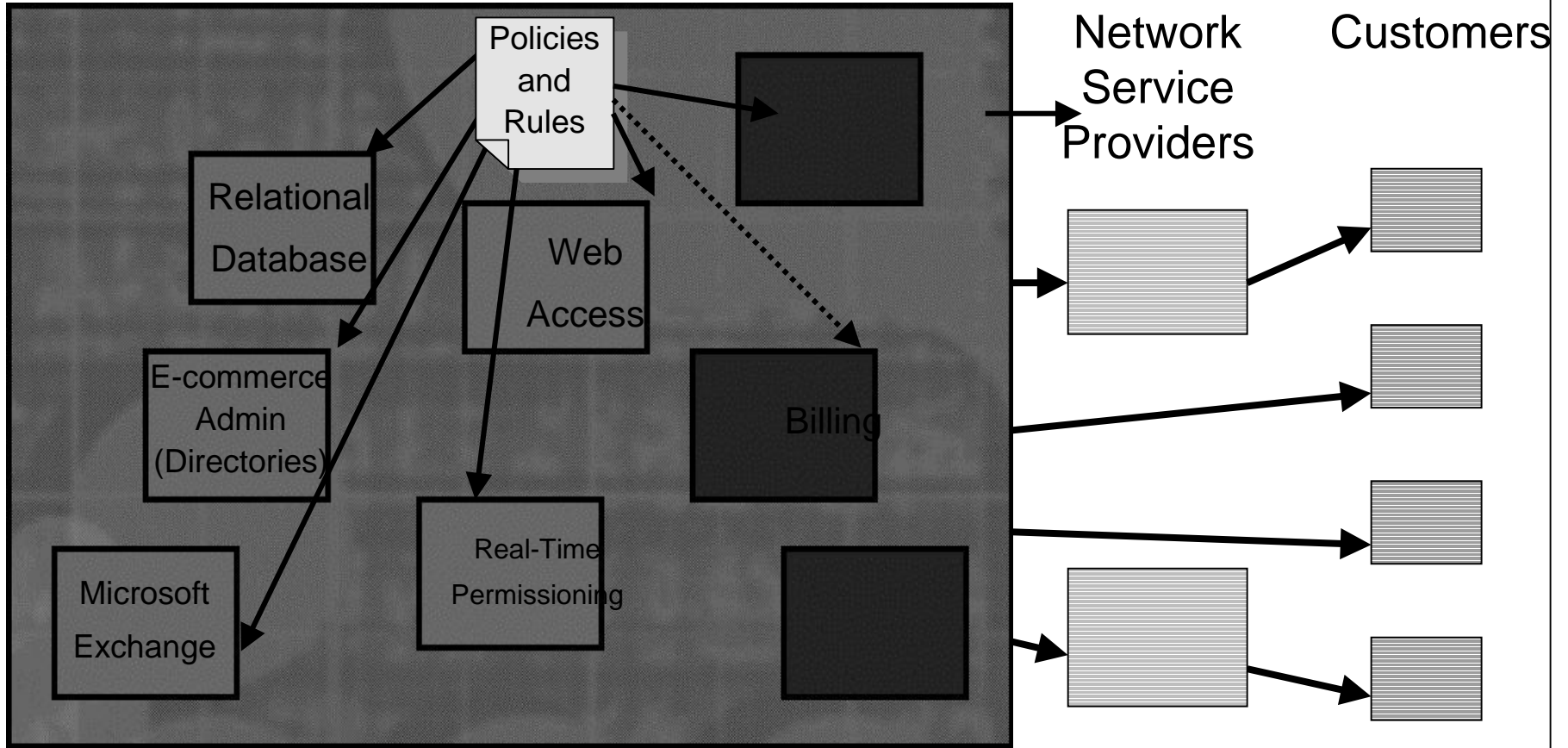
REUTERS 150 YEARS



“Straight-Through” Rules Processing



Unified Rules Definitions



Requirements for Rights Data Dictionary & Rights Expression Language

3.1 REQUIREMENTS FOR THE STRUCTURE OF THE STANDARD

3.1.1 Division of the Standard into an Extensible Core and Standard Prelude

3.1.2 Inclusivity

Requirements for Rights Data Dictionary & Rights Expression Language

3.2 REQUIREMENTS FOR RIGHTS STRUCTURE AND MANAGEMENT

- 3.2.1 The Relationships between Rights and Obligations
- 3.2.2 Rights and Obligations Transfer (Inheritance)
- 3.2.3 Rights and Content Independence
- 3.2.4 The Types of Content over which Rights and Obligations Apply
- 3.2.5 Matching Rights and Obligations to Digital Objects
- 3.2.6 Matching Rights to Contexts
- 3.2.7 Location, Form, and Access Control of Data Dictionaries
- 3.2.8 Management of Issued Rights and Obligations
- 3.2.9 Fail-Over and Behaviour Modification
- 3.2.10 Privacy of Terms Expressed in the Language and Data Dictionary
- 3.2.11 Expression Evaluation

Requirements for Rights Data Dictionary & Rights Expression Language

3.3 REQUIREMENTS FOR RIGHTS AND OBLIGATIONS DEFINITIONS

- 3.3.1 Operational Specifications
- 3.3.2 Reporting
- 3.3.3 Acknowledgement of Source
- 3.3.4 Rights and Obligations for Real-Time Data
- 3.3.5 Rights and Obligations for a Stream of Digital Objects
- 3.3.6 Rights and Obligations for Transactional Data
- 3.3.7 Rights and Obligations for Database or Server Access
- 3.3.8 Usage Rights
- 3.3.9 Managing Communities
- 3.3.10 Contract Management
- 3.3.11 Business Models

Requirements for Rights Data Dictionary & Rights Expression Language

3.4 ATTRIBUTES ON WHICH RIGHTS AND OBLIGATIONS ARE PREDICATED

3.4.1 Temporal

3.4.2 Geographic

3.4.3 Environmental

Requirements for Rights Data Dictionary & Rights Expression Language

3.5 REQUIREMENTS PERTAINING TO TRUST

- 3.5.1 Identification of Trusted Entities
- 3.5.2 Trusted Time Services
- 3.5.3 Trusted Applications and Environments
- 3.5.4 Certifiable Audit Trails
- 3.5.5 Agent Authentication
- 3.5.6 Data Integrity
- 3.5.7 Agent Mandated Privacy
- 3.5.8 Confidentiality

Requirements for Rights Data Dictionary & Rights Expression Language

3.6 ADDITIONAL FUNCTIONAL REQUIREMENTS

3.6.1 Specialised Support for Business to Business (B2B) Commerce

3.6.2 Machine Processing of Digital Objects

Requirements for Rights Data Dictionary & Rights Expression Language

4 OTHER AREAS FOR CONSIDERATION IN BUILDING THE STANDARD

4.1 CHANNEL DEFINITION

4.2 OBJECT MODELS

4.3 WORKFLOW