Distributed Digital Rights Management

Stephen Downes
National Research Council
January 27, 2004

What is DRM?

- *Digital* – specific to digital resources, such as electronic documents and media
- *Rights* – concerned with ownership and the terms and conditions of use
- *Management* – concerned with creating mechanisms to enable or prevent use

Aspects of DRM

- *Expression* – the description of the resource, ownership of the resource, and the terms and conditions of use
- *Authentication* – verification that the person using the resource has the right to use the resource
- *Protection* – means, such as encryption, to ensure only authorized users have access

Where DRM is Applied

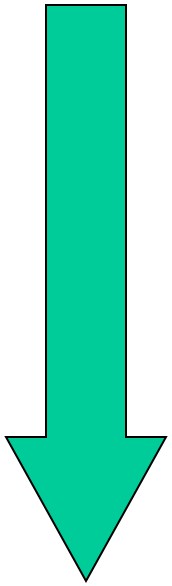
- *Resource* – a particular document or digital resource – for example, a document may be locked or encrypted
- *Access Point* – a content server, such as a website – for example, a website may require a login
- *Network* – the connections between servers – for example, ATM network

DRM Design Decision Metric

	Resource	Access	Network
Expression	Copyright notice	Terms of use notice	Rights expression language
Authentication	Password to open document	Password to access website	PIN to use ATM system
Protection	Encrypted document	Secure sockets layer	Virtual private network (VPN)

Degrees of DRM

More Pervasive



Stronger

	Resource	Access	Network
Expression			
Authentication			
Protection			

Weak DRM

- *Expression:* in the resource only
- *Authentication:* none
- *Protection:* none
- Examples: web page with a copyright notice, book with a copyright page, property with a ‘keep out’ sign

Strong DRM

- *Expression:* in the resource, access point, or network
- *Authentication:* network – single login
- *Protection:* network wide
- Example – the ATM system requires that you provide credentials to use the system, and encrypts all data and communication

Issues in DRM

- *DRM is too weak* – in networks like the web and Napster, expression alone is insufficient to ensure that rights are respected
- *DRM is too strong* – proposed DRM systems require a unique userid (eg., MS Passport) and fully secured network (eg., Rights management server, 'trusted' applications), violate privacy, fair use

The Middle Way

- *Expression* – supported at the network level through the use of a rights expression langauge
- *Authentication* – supported at the access level through the use of keys
- *Protection* – supported at the document level with locks or encryption

Critics from Both Sides…

- *It's too strong* – advocates of open content fear any DRM system will prevent people from freely sharing content
- *It's too weak* – commercial providers want stronger protection, such as authentication at the network level, to prevent file sharing

Responses

- *It's weak enough* – to use free resources, rights *must* be declared, and any further level of authentication and protection is at the discretion of the resource owner
- *It's strong enough* – a key system makes it difficult to obtain unauthorized access to content, but leaves it easier to buy content than to steal it

What Causes File Sharing?

- *When DRM is too weak* – there is no incentive to go through the extra work and cost to pay for content; commercial content is not viable
- *When DRM is too strong* – free content is not viable, and the transaction cost is too high, so it is easier to look elsewhere for the same content

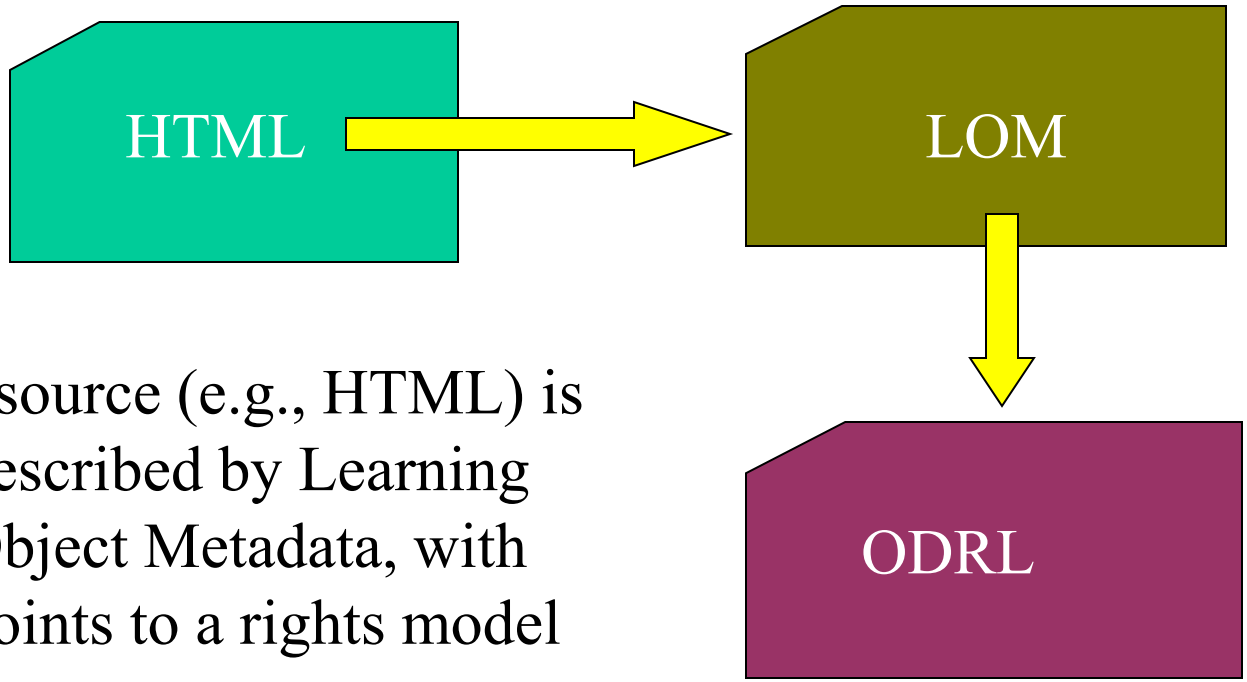
DRM Principles

- *Open Standards* – the mechanisms for expression, authentication and protection can be used by anyone
- *Open Network* – any agency or entity may provide any of the services provided by the network
- *Open Marketplace* – and agency or entity may buy or sell on the network

Rights Expression

- *Defined at the Network Level*
  - A rights expression language (REL) is used
  - Current support for ODRL because it does not create a cost – XrML, DRML are options if they are royalty free
  - A mechanism for expressing digital rights expression is supported such that these are available anywhere in the network

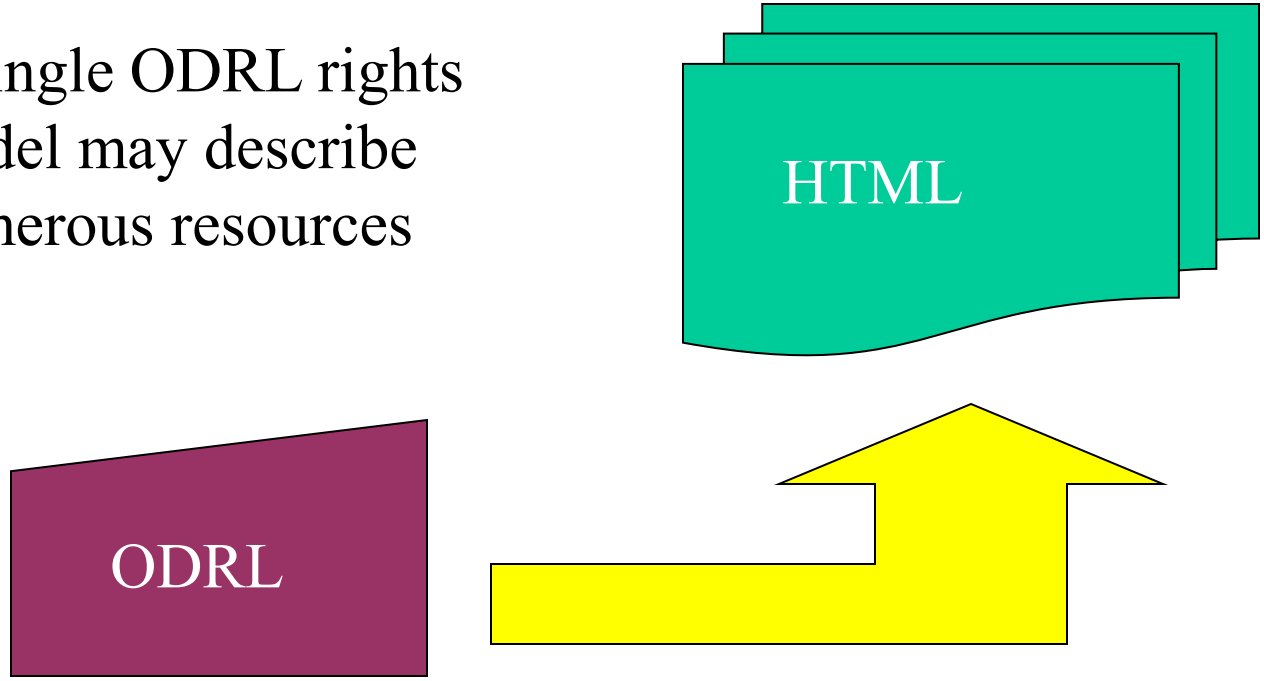
Rights Models (1)



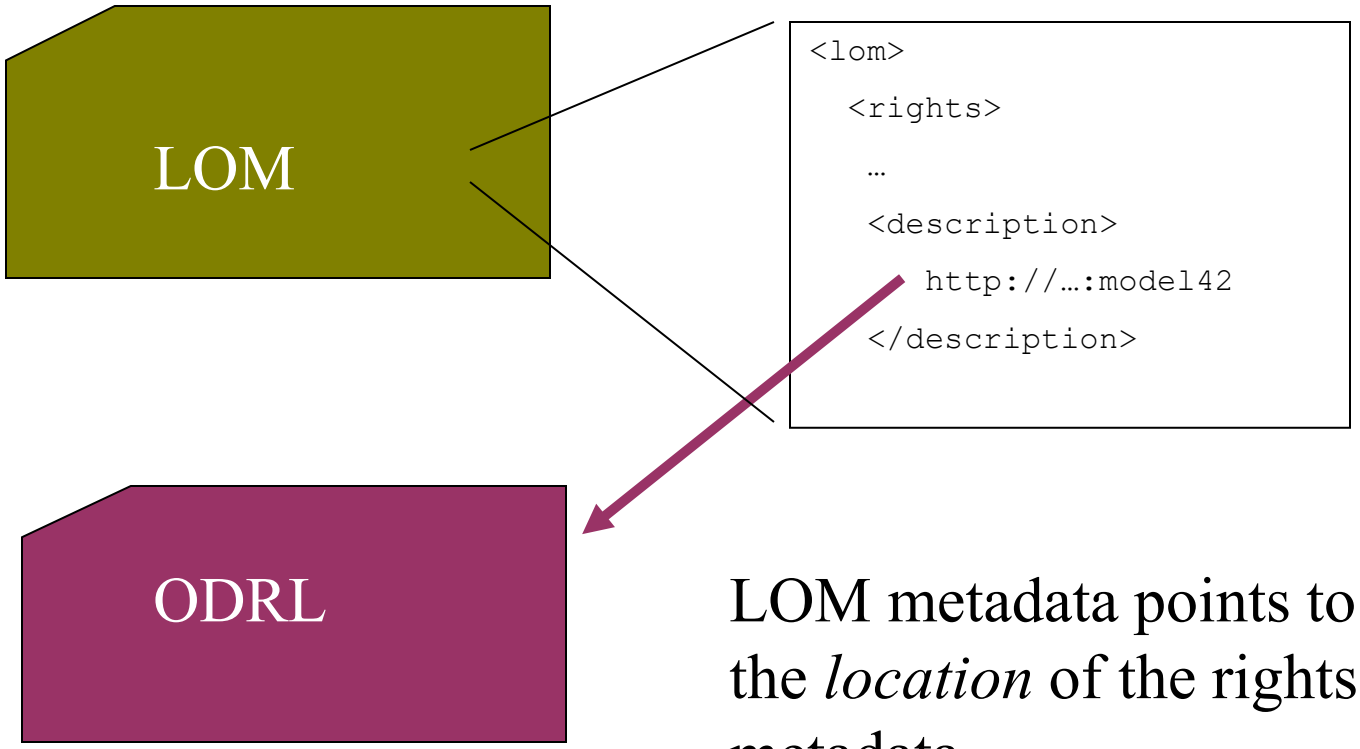
A resource (e.g., HTML) is described by Learning Object Metadata, with points to a rights model

Rights Models (2)

A single ODRL rights model may describe numerous resources



Rights Models (3)



LOM metadata points to the *location* of the rights metadata

Two Types of Right Expression

- *Offer* - this is the *proposal* that a vendor puts in front of potential customers. An offer is provided by a *vendor* who wants to sell (or give) you something
- *Agreement* – this is the offer that was accepted by the customer, and is like a contract. Agreements may be held by a third party, who acts as a *registrar* or *notary*

Pointers to Offers and Agreements

- *Pointers to Offers* – are contained in the learning object metadata for resources that are not being used yet
- *Pointers to Agreements* – may be contained if the resource is used in a package or otherwise redistributed, showing that the resource has been paid for
- Agreements are not used for free resources or one-time uses, such as viewing

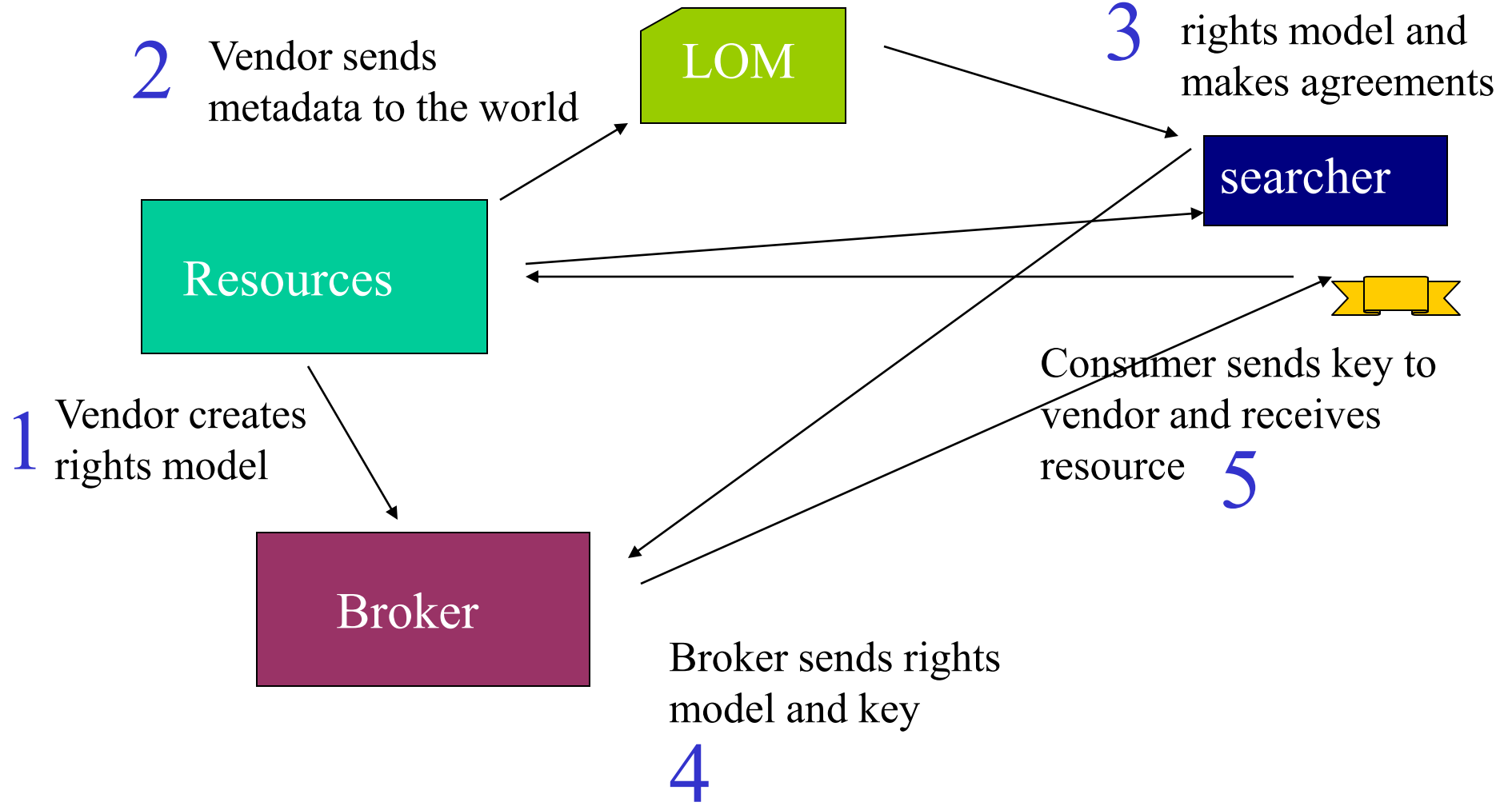
Vendor Brokers

- A *vendor broker* is a service that helps vendors create rights metadata and which stores and serves the rights model on request
- A vendor broker also conducts *transactions* on behalf of the vendor, accepting payment and providing keys for access

Vendor Broker Services

- *Create* rights metadata model
- *Send* rights models on request
- *Agree* with a purchaser who is willing to accept the terms
- *Provide key* to a purchaser who has satisfied the terms of the agreement

Vendor Repositories



About Vendor Brokers

- There may be many vendor brokers
- Large providers may be their own vendor brokers, while small provider may access a vendor broker service
- Vendor brokers receive payments and forward money in lump sums to vendors

Example

- *Creative Commons* is like a vendor broker
  - It has a set of rights models that resource providers can pick from
  - Reference to the rights models may be carried in metadata (eg., RSS CC field)
  - Customers may request to see the rights model, and know they have permission to use the resource

Example (2)

- *Amazon is like a vendor broker*
  - Vendors can use Amazon to set terms of purchase
  - Potential purchasers can obtain these terms of purchase from Amazon
  - Customers make payment to Amazon directly, which then later pays the vendor

Purchasers

- A purchaser is any person who wishes to access or use a resource
- Purchasers do the following:
  - They *locate* the resource
  - They *retrieve* rights expression
  - They *accept* the terms of conditions
  - They *make payment* if necessary
  - They *access* the resource

Locating Resources

- Resources are located via searches on metadata search service (such as eduSource)
- The searcher *may* use rights information as a parameter, depending on the search service – for example – a searcher may request ‘only free resources’ or ‘only resources that cost less than five dollars’

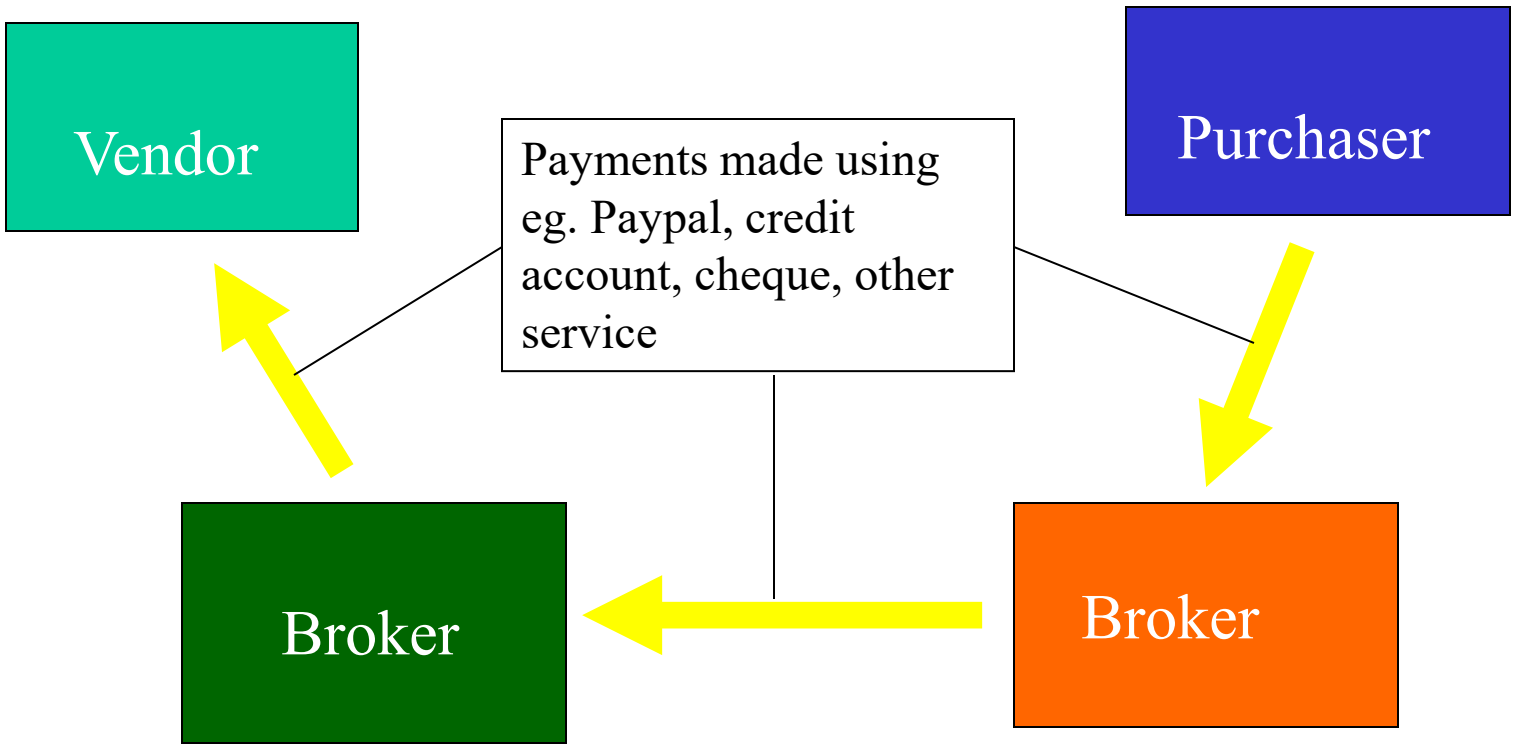
Purchaser Brokers

- This is a *new* feature unique to DDRM
- A *purchaser broker* acts as a representative for the purchaser
  - It makes requests for rights metadata
  - It pays the vendor broker for the purchaser
  - It transports the key from the vendor to the purchaser
  - It accepts bulk payments from the purchaser

Why a Purchaser Broker?

- A purchaser broker can handle many accounts on behalf of a purchaser
- A purchaser broker acts as a steward of personal information, protecting the purchaser's identity and credit information
- A purchaser may exercise transactions automatically based on rules set by the purchaser

Payment Models



Why *Two* Brokers?

- A vendor broker may accept transactions from many purchaser brokers, and a purchaser broker may make transactions with many vendor brokers
- But a vendor can deal with a *single* vendor broker, and a purchaser can deal with a *single* purchaser broker

It’s a Lot Like Your Store