Internet Commerce Model

Recommended Technologies for Internet Commerce

Version 2.0
September 26, 2001

VICS Internet Commerce Committee

Table of Contents

Executive Summary

The vision of Internet commerce is a platform- and vendor-independent environment in which multiple parties can inter-operate using various deployment methods. It must be realized that interoperability can only be achieved through implementation using common standards.

Since the publication of the original Internet Commerce Model in October 1998, rapid advancements have occurred in business applications and in Internet technology and capability. This document, "Internet Commerce Model: Recommended Technologies for Internet Commerce, Version 2.0," is written to provide VICS members with current information about technologies that are available to help them choose technologies that will improve interoperability with multiple trading partners, reduce complexity, and reduce costs.

As companies gain experience using the Internet, it is progressing from being a means of publishing information to one of exchanging transactions and collaboration, such as product design and development, forecasting and replenishment. The emergence of exchanges or marketplaces is recognized, and the model shows several different scenarios, such as:

- Companies interacting directly with other companies,
- Companies using independent service providers to host information for their trading partners,
- Companies using one or more Marketplaces (or Exchanges) that provide value to their members by building and integrating software products and services required by their members.

Examples of these concepts are shown graphically and described in the model.

The maturity of the Internet has resulted in clearer differences between technologies that perform the business functions vs. the infrastructure technologies that provide the "electronic highway" across which the information flows. This 2001 model separates the "Application Services" components from the "Infrastructure" components, and it provides references to organizations responsible for the technologies for those seeking a more in-depth understanding of the particular technologies.

Security on the Internet is a complex issue, and increases in importance as companies' use of the Internet increases and becomes more complex. Technology for security on the Internet is typically based on encryption – and since there are many ways to encrypt data, the key to interoperability is standards. This model discusses the standards for security. However, since overall security is not better than the weakest link, the policies and procedures of your trading partners are also vitally important.

The VICS Internet Commerce Committee has selected the combination of standards and conventions that best meet the needs of general merchandise supply chain trading partners, based upon the technologies currently available. It is recognized by the committee, however, that technologies in this domain continue to develop rapidly, and these guidelines will continue to be a work in progress.

Purpose

The Charter of the VICS Internet Commerce Committee and the intention of this document are to help provide clarity, consensus and convergence around the issues of open Internet Commerce Standards for the VICS membership. Internet commerce is far broader than buying and selling. Internet Commerce encompasses all trading partner interactions that can be conducted over the Internet. The VICS Internet Commerce Committee was established to create guidelines for Internet commerce implementations. These guidelines take the form of formal recommendations of standards to deploy, as well as discussions of implementation considerations for areas where recommendations cannot be established at this time. They are intended to reduce the barriers to interoperability, accelerate the pace of adoption, and ultimately enhance the competitiveness of VICS members. They are strictly voluntary.

This document begins by describing the various ways companies use the Internet to conduct commerce. Different parties involved with electronic commerce may be organized in various deployment scenarios. The commerce model outlines the component technologies and applicable standards that are divided into application services and infrastructure. Examples are used to demonstrate how the standards recommendations and considerations apply to different business situations.

This document is the first revision to the original VICS Internet Commerce Model published in 1998. New technologies and business models continue to evolve, and thus the standards landscape will continue to evolve. There is no single solution to conducting commerce via the Internet. Multiple options are available but a comprehensive set of standards may not be available for many months. However, these recommendations are intended to provide guidance to VICS members who are pursuing Internet commerce initiatives now. They will help members select similar technologies and specifications for interacting with one another. These recommendations do not establish any new standards. They do provide a profile of existing standards, specifications, and guidelines for members' use.

An Evolving Internet Commerce Model

In 1998 in response to the rapid growth of the Internet and of commerce based on using the Internet to exchange business communications, the Voluntary Interindustry Commerce Standards organization adopted its first Internet commerce standards, described in the document *Internet Commerce Model: Recommended Technologies for Internet Commerce*, dated October 20, 1998. This model responded to the already rapidly developing use of the Internet for business, and it recommended a set of basic Internet communication standards for use in exchanging business information between companies.

Since the adoption of the VICS Internet Commerce Model in 1998 the use of, and continuing need for, cost-effective and powerful Internet technologies continues to proliferate. The Internet has become an even more fundamental component of the business communication infrastructure. The number of solutions providers and the sophistication of the technologies employed to manage data between trading environments has grown geometrically since that time. As a result, inter-operability and inter-connectivity between national and global trading partners promises to become a near term reality. Per enterprise demand, security standards have also been developed and are now included in the current model release. The VICS Internet Commerce Committee, recognized these significant developments and responded by updating its Commerce Model for 2001.

The Committee recognizes and acknowledges the important standards work being done around XML formats. It also recognizes that different business process groups such as VICS CPFR® and GCI, to name a few, are now working collaboratively in developing recommendations for the endorsement and development of standards that meet the common and diverse needs of a global community of trading partners both now and in future. Meeting the ever-expanding requirements to exchange data between trading partners through multiple standard formats and schemas will continue to be one of our most challenging goals as we begin realizing the full potential of this new technology.

Electronic Data Interchange (EDI) continues to be an industry workhorse in handling the most basic business transactions. EDI is usually transported through batch processing, the most common transactions being the purchase order (850), the invoice (810) and the advance ship notice or ASN (856). In future, EDI will more than likely migrate to EDIINT (EDI Over the Internet) so that EDI can continue to function as a viable means for moving massive amounts of basic transaction data between trading partners. It will do so over the Internet using TCP/IP and will now work together with XML to maximize value throughout the demand/supply chain as companies are now extending beyond these basic transactions by deploying more dynamic, interactive and real-time business processes.

In the 1998 Internet Commerce Model, the VICS Internet Commerce Committee recommended XML as key to unleashing the real power of global E-Commerce. Today the Global Commerce Initiative (GCI) echoes that position in stating, "XML is the next step in E-Commerce. It is the framework to be placed upon existing electronic commerce

tools. With its ease of use, compatibility with other applications and intelligence in processing information, XML promises to expand current and future business needs."

The 2001 Model envisions broad-based and complex business solutions that can now be deployed, with enhanced security, over multiple networks and processing entities by integrating multiple solutions sets from multiple Internet Use categories. Inter-operability between deployment solutions is the ultimate goal of this model. However, inter-operability will only be truly demonstrated through implementation.

Building a Baseline: Consensus Drives Direction

Because multiple organizations participate in Internet commerce initiatives, it is particularly urgent that communications be based upon common standards. Organizations such as VICS have played a significant role in establishing electronic commerce standards and practices particularly around the infrastructure model. The 2001 Model extends its standards recommendations to Applications Services. It also further refines and enhances the 1998 Infrastructure Model, particularly within the area of security.

Since this document's original publication, the VICS Board of Directors and its Internet Commerce Committee have helped build a baseline of consensus, leading towards the adoption of a globally recognized comprehensive set of standards for Internet commerce.

In January 1999 VICS Board representatives met with member representatives of EAN International, the Uniform Code Council and other international organizations to discuss the need for the establishment of a common set of electronic standards to support global trade. That meeting spawned the creation of the Global Commerce Initiative (GCI) in October 1999. One of GCI's first efforts was to announce the Global Commerce Initiative Protocol (GCIP). The GCIP was the first global and comprehensive recommendation on the management of standardized data between and among trading partners.

In February 1999 the VICS Internet Commerce Committee presented a proposal and recommendations to the Electronic Commerce Committee of the Uniform Code Council to establish a data dictionary committee for XML-based electronic commerce standards. In November 1999, the Committee formally presented additional items to the UCC for consideration. Subsequent UCC and GCI initiatives and working groups have sanctioned these recommendations.

On April 18, 2000, member representatives of the major retail and consumer goods marketplaces agreed to support the accelerated development of a "fundamental set of standards" for the exchange of data via the Internet. Those standards are being developed by EAN/UCC.

These developments give our constituents a reason to be optimistic about the pace of progress. A global set of Internet standards hold the promise of making electronic commerce a realization for all businesses including many small and medium enterprises that may have been excluded from previous electronic initiatives. This will save additional time and reduce costs from all trading partners' supply chains. It is hoped that this publication will act as a springboard toward development and deployment of more wide-scale E-commerce initiatives among the VICS membership.

Internet Use

VICS members are engaged in many Internet-based business-to-business initiatives. To ensure relevance of these recommendations to concerned members, the committee defined four general categories of Internet use:

1) *Publication:* Share specifications, advertising, and other static information with trading partners. Usually users display this data on World Wide Web (WWW) browsers, or in other associated applications, such as a spreadsheet, a document viewer, audio, or video player. This data may be subject to access control and available only to trading partners, or it may be open to the public.

2) *Interaction:* Give trading partners interactive access to product catalogs, shipment tracking, account balances, and other business information. Data gathering, such as on-line surveys and discussion, is also included in this category. This category includes person-to-system and system-to-system interactions. While the primary example of the Interact usage category currently is best described as the use of the Internet by a person to gather dynamic information, it is our belief that future interaction will increasingly occur between systems via the Internet.

3) *Transaction:* Conduct business over the Internet by taking orders, collecting payment, disbursing funds, submitting bids, or performing other business transactions. One prominent initiative, EDIINT, uses the public Internet rather than a private Value-Added Network (VAN) or direct dial-up lines to exchange Electronic Data Interchange (EDI) messages. A related initiative is Open Buying over the Internet (OBI), which combines the use of EDI, HTTP, and certification authorities to enable the purchase of materials and supplies.

4) *Collaboration:* Extend business processes beyond the scope of transactional buying and selling. Collaboration covers the spectrum of business processes, which include product design and development, joint marketing, program development, forecasting and replenishment. An example is the Collaborative Planning, Forecasting, and Replenishment (CPFR®) process, which has been developed by VICS and is being implemented by many companies.

Other forms of communication including use of such technologies as video, FAX, voice, shared whiteboards, and other ad-hoc communications are also important, but are outside the scope of this model.

The committee recognizes that for many reasons, ad-hoc solutions are sometimes employed during transitional phases of new technology adoption and deployment. Trading partners using multiple and disparate technology systems need to continue operations as they migrate to more advanced technologies. With Internet Commerce, forms and elements of electronic communications, such as both structured and unstructured flat files and ftp without a security component have been utilized to move data through the pipeline. The Committee suggests that the importance of these ad-hoc approaches will diminish over time as companies begin to adopt the standards

recommendations delineated in this document. Such standards should maximize value and ROI for all parties by reducing development and deployment costs while encouraging and maximizing solution benefits on a global scale.

Deployment Scenarios

Companies can utilize the Internet in any combination of the previously described use categories. Businesses may also involve multiple parties in their business processes. The following scenarios describe the ways companies deploy electronic commerce between themselves and their partners:

- *Extranet:* A company can deploy an application solution as an extranet application, offering client-level access to its trading partners.

- *Application Service Provider (ASP):* A company can choose a third-party service provider to host a solution on its behalf, providing client-level access to its trading partners.

- *Marketplace:* A company can join a net marketplace, and use the application services that it offers a client.

- *Company-to-Company:* A company can deploy an application solution locally, and exchange data with other companies' similar application solutions.

- *Company-to-Marketplace:* A company can deploy an application solution locally, and exchange data with one or more marketplace-hosting the same application solutions.

- *Marketplace-to-Marketplace:* Two or more net Marketplaces can exchange data for use by their respective member companies.

Figure 1 illustrates all of these scenarios, which can be grouped into two types: shared deployment and peer-to-peer deployment. All of these scenarios are (or will soon be) in general use. A company may need to deploy more than one approach to collaborate with its full set of trading partners.
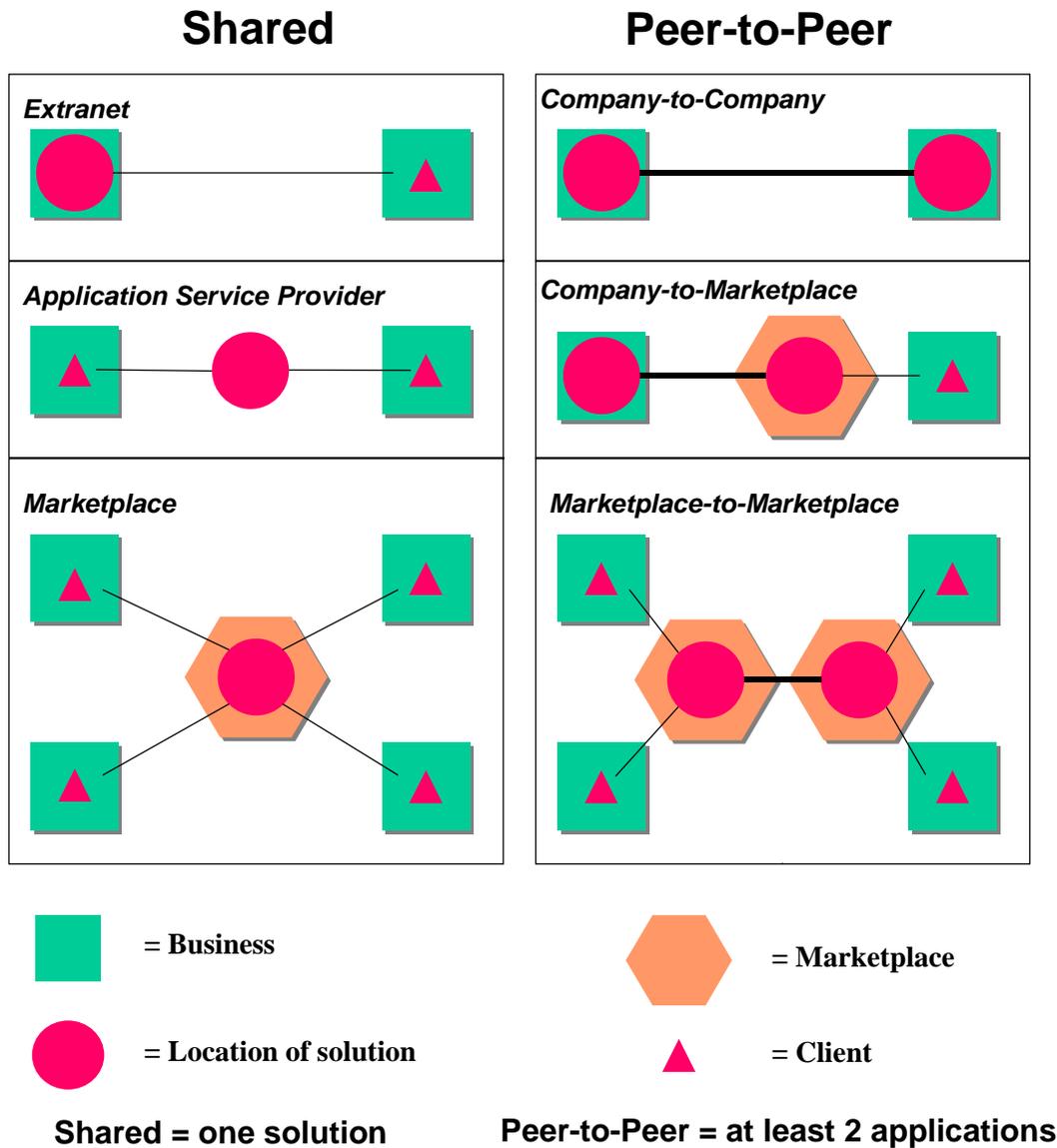
Figure 1: Deployment Scenarios

It is important to distinguish the communication requirements of these deployment scenarios. In the first three (shared deployment), buyers and sellers share an application solution that resides at the retailer, supplier or marketplace. In the last three (peer-to-peer deployments), buyers and sellers exchange messages between their respective application solutions to coordinate their activities. Peer-to-peer deployments depend upon common message formats, message selection, message transport, and security standards. Shared implementations use whatever means the selected application vendor provides.

Interactive Example: Check Order Status

Our 1998 example addressed one of the most common business process activities, a retailer wanting to query a particular vendor on the status of a purchase order or group of purchase orders in the production/distribution pipeline. In 2001 new XML technology can be utilized to automatically pull and post such data to internal legacy systems, Exchange servers, and/or browser based extranets, so the data can be viewed or system processed on demand and managed interactively as changes to the order status occur.

It is now even possible to push and pull this data in a many-to-many-environment so that one retailer can view order status across multiple trading partners. Trading partners could use queries to search orders not just by vendor, Product ID or P.O. number, but by multiple product characteristics like color, style type, lifestyle category, price value and/or even delivery window within or across vendors. This capability opens a whole new dimension to the world of order management, replenishment, and business intelligence and response.

The following two scenarios illustrate how business process requirements could be managed more efficiently and effectively over the Internet. These examples represent just two of the many ways that Internet technology can be used to streamline and automate essential business processes between trading partners. For the purposes of this document, "Exchange", "Trading Exchange", "eMarketplace" and "eMarket" are all represented by the term "Marketplace". Although they may currently represent different functional versions of a "Marketplace", standards support and adoption remains essential to facilitate and assure cross-model inter-operability.

Scenario 1: Peer-to-Peer
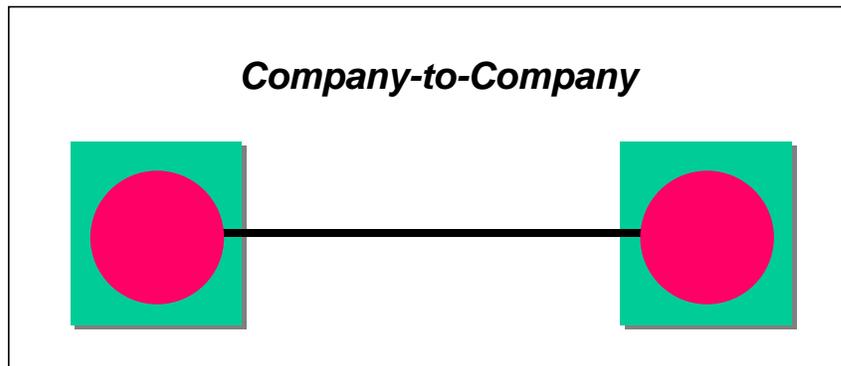
Figure 2: Peer-to-Peer Scenario

Figure 2 depicts the Peer-to-Peer scenario, with one retailer using the Internet to query one vendor on its order status. The query can be initiated by an individual or be a system query. It assumes both a simple EDIINT option and/or combined with an XML component. These standard formats can be generated directly from backend systems or translated from other flat-file formats as data pass from one corporate peer to another.

| System Components	Model Process
Retailer Legacy System	Legacy system maintains original and updated data. Retailer may rely on third-party providers to maintain all or part of data repository, security and/or network infrastructure.
Retailer Extranet	Logs onto Internet through TCP/IP network protocol. Selects data transport protocol (HTTP; FTP; SMTP/MIME) Pulls data from either retailer, exchange, vendor system environment or third-party data repositories or solution providers, utilizing any of the 2001 data formats and security keys.
Public Internet	Uses one of the transport standards with or without browser using standard security protocols as required to access vendor extranet or IP gateway through unique URL (Internet address).
Vendor Extranet	Retrieves updated data from legacy system. Makes data available to trading partners using a browser with applied security. Any of the recommended standards components may be employed in the building of the vendor's extranet.
Vendor Legacy System	Legacy system maintains updated data from supply-chain using standard input, EDI, EANCON or XML standards. XML based application pulls and translates data into XML schemas and transmits data over TCP/IP to retailer legacy system where it is read via XML translators and sent on to query source according to agreed upon business rules

Scenario 2: Marketplace-to-Marketplace
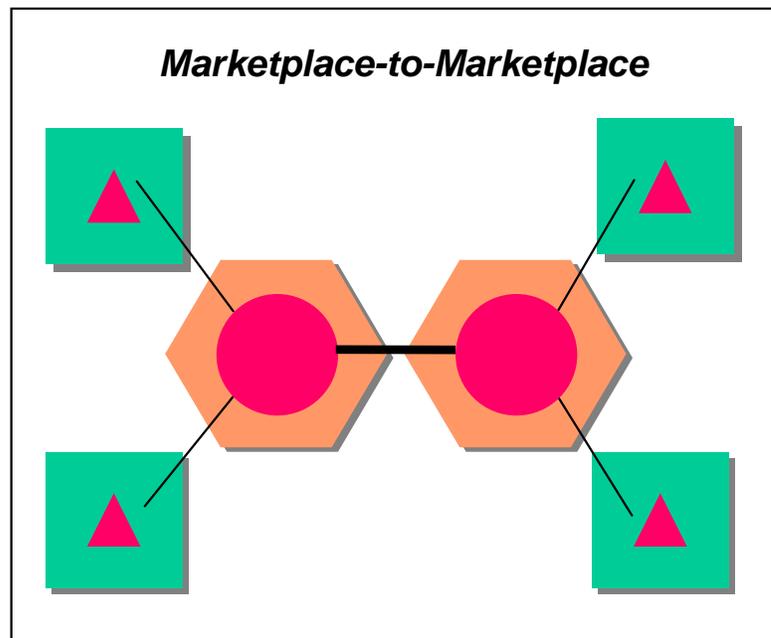
Figure 3: Marketplace Scenario

Figure 3 depicts the Marketplace scenario. These marketplaces provide specific value to their members by building and integrating products and services required by trading partner members to execute their business transactions. Thus, the second scenario will review one retailer querying a marketplace, which then passes all or part of the query on to another marketplace, which then processes the request and sends it on to a vendor. The query is answered in the backend of the peer vendor and returned to the retailer's extranet or backend system, depending on whether or not the query was initiated by an individual or a system. An example might be a retailer participating in a large consortium marketplace with other retailers. The consortium marketplace finds it useful to use an alliance marketplace that might better handle certain product verticals, so it makes a choice to integrate with that alliance marketplace to pass data back and forth between them. Such a scenario will become more common as both peers and marketplaces realize that by working together through common standard inter-connections they can reach critical mass more quickly. This scenario echoes the way phone companies work together.

Note: It is projected that, in the future, many more combinations of new types of interacting parties will link up to effect a final business process transaction by utilizing these new standard specifications. An idea for next generation service might be the possibility for purchase orders to be analyzed by a "weather marketplace" that compared local weather and climatic forecasts to product attributes and distribution models in each particular P.O. so recommended adjustments could be made prior to release. Price and delivery optimizations are other types of marketplace services that could come online in the next few years.

System Components	Model Process
Retailer Legacy System	Legacy system maintains original and updated data. Retailer relies on one or more third-party providers to maintain all or part of data repository, security and/or network infrastructure.
Retailer Extranet	Logs onto Internet through TCP/IP network protocol. Selects data transport protocol (HTTP; FTP; SMTP/MIME) Pulls data from either their own system environment, Marketplace, vendor system environment or third-party data repositories or solution providers, utilizing any of the 2001 data formats and/or security formats and keys.
Public Internet	Uses one of the transport standards with or without browser using standard security protocols as required to access Marketplace through unique URL (Internet address).
Marketplace 1	Uses one of the transport standards with or without browser using standard security protocols as required to access second marketplace through unique URL (Internet address).
Marketplace 2	Uses one of the transport standards with or without browser using standard security protocols as required to access vendor extranet or legacy IP gateway through unique URL (Internet address).
Vendor Extranet	Retrieves updated data from vendors legacy system using XML and makes data available to Marketplace using XML schemas. Any of the recommended 2001 standards components may be employed in the building of the vendor's extranet.
	And/or
Vendor Legacy System	Legacy system maintains updated order status data from supply-chain using standard inputs: Flat-file, EDI, EDIFACT, or XML. Marketplace query pulls updated data via XML then transforms and transmits data over TC/IP to second marketplace's servers where it's read via XML translators and sent on to query source according to agreed upon business rules.

Principles

The vision of Internet commerce is a platform- and vendor-independent environment in which multiple parties can inter-operate using various deployment scenarios. However it should be understood that inter-operability is achieved through choices made during implementation. Partners of different sizes and technical levels can collaborate through technologies that are accessible to them. This communication is supported by formal standards, which evolve through an open process. The VICS Internet Commerce Committee has used the following principles to develop these guidelines:

1) *Standards:* The model should use existing standards wherever possible. Where *de jure* standards have not been established, the committee has selected *de facto* standards that have an open process, that are managed by a non-profit organization, and are supported by multiple technology vendors. If these criteria have not been met in an area, the committee has declined to make a recommendation.

2) *Scalability:* The system must be able to scale to large implementations in terms of number of transactions, trading partners, collaborative relationships, users, and collaboration interactions.

3) *Security:* Trust and privacy are major issues in a collaborative environment. As the exchange of information between organizations becomes increasingly electronic, the risk for misuse and theft intensifies significantly. For obvious reasons, sensitive information should be accessible only to those who have permission to view it. Internet commerce solutions must ensure data is secure when exchanged via public networks. The VICS Internet Commerce Committee strongly recommends that companies develop policy statements regarding privacy and the protection of information. Businesses should develop policy statements outlining their efforts to safeguard information. These policies will be instrumental in facilitating the trust necessary to successfully accomplish electronic business. A security policy should outline the steps companies take to protect business information as it is exchanged across the public Internet. A privacy policy statement describes the ownership and usage of this information once exchanged.

4) *Openness:* Solutions that require a single vendor's application are not acceptable in collaborative relationships. Each trading partner must independently consider all of its customer/supplier relationships. It is unlikely that all of them would choose the same implementation approach. By using open and published standards, new trading partners can come online quickly, and the systems can evolve. In addition, an open solution must be based on mature technologies, because the rapid pace of development and market acceptance can take evolving technologies in diverging directions-including extinction. Openness is a base criterion for selection as a standard.

5) *Manageability:* An Internet commerce solution must be easily maintainable by all parties.

These principles provide a basis upon which to establish mutual expectations between parties involved in electronic business (ebusiness).

The revised VICS Internet Commerce Committee's Internet Commerce Model is structured as two sets of recommended standards: the application services standards and the infrastructure standards. The application services standards allow business applications to identify the location and capabilities of partners' systems, come to agreement with a partner to transact business, format messages that partners' applications can interpret, and reliably send and receive those messages. The infrastructure standards determine *how* to provide these application services securely on the global Internet. Figure 4 illustrates the categories of standards in the model.
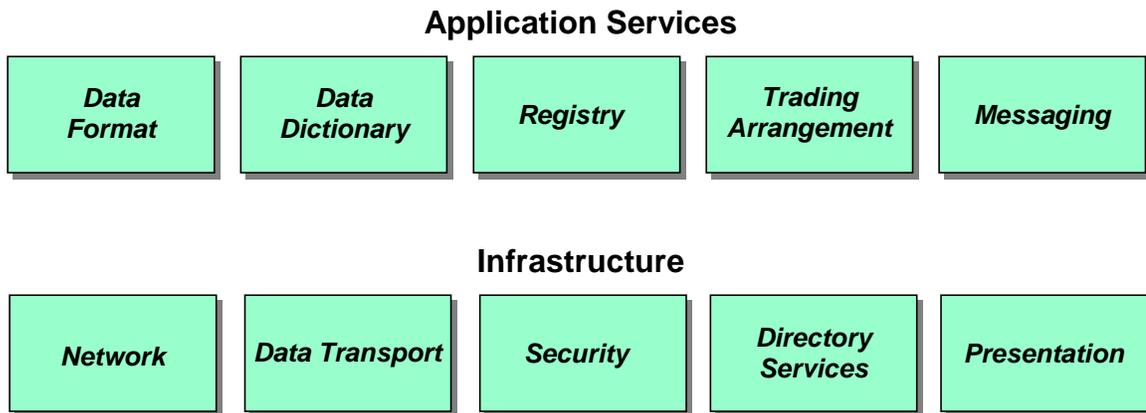
Application Services

Data Format	Data Dictionary	Registry	Trading Arrangement	Messaging

Infrastructure

Network	Data Transport	Security	Directory Services	Presentation

Figure 4: Internet Standards for Electronic Business: Overview

For example, two businesses may use the ebXML messaging service (an application services standard) to send purchase requests. The transport used to send the ebXML messages may be HTTPS (an infrastructure standard). The Internet Commerce Model includes infrastructure standards that are visible to users of application services.

Application Services Standards

Table 1 describes the categories for application services standards. Applications typically utilize these standards directly to conduct business electronically.

Table 1: Application Services Standards

Component	Description
Data Format	Standards and conventions for structuring data content.
Data Dictionary	Standard semantics (content and meaning) for messages exchanged within a given data format.

	Standards for storing data and service specifications, such as API's, as well as registering the locations of applications that are capable of handling data and service requests using those specifications.
Registry	Standards for storing data and service specifications, such as API's, as well as registering the locations of applications that are capable of handling data and service requests using those specifications.
Trading Arrangement	Standards for publishing the range of electronic business scenarios that an organization can support, and for negotiating the specific scenario to be used between two trading partners.
Messaging	Standards for the bundling of data and service requests into a message, determining the options for routing the message to one or more destinations, and then transporting the data over the network.

Figure 5 illustrates the committee's selection of standards for applications services in the Internet Commerce Model. Most areas present alternatives, which are appropriate for different scenarios.

Data Format	Data Dictionary	Registry	Trading Arrangement	Messaging
W3C XML Schema	EAN•UCC GDD	(See "Future Development – Registry Services")	ebXML Collaboration Protocol	ebXML Messaging
VICS EDI	ASC X 12			SOAP
EANCOM®	EDIFACT		(manual)	IETF EDIINT

Figure 5: Internet Standards for Electronic Business: Application Services

Conceptually, the application services standards are closely modeled on the ebXML technical architecture. As it is envisioned, ebXML will provide a comprehensive data processing environment for electronic business. Unfortunately, at present the ebXML specifications are still in draft form, and software that implements ebXML is still at a prototype stage. The Internet Commerce Model retains many of the same categories of standards as ebXML, but offers existing alternatives where they are available for immediate use in Internet business initiatives.

Data Format

Before two applications can exchange data and service requests, they must agree upon the syntax of the messages to be sent and received. Internet business initiatives employ one of three data formatting specifications (based upon the data dictionary used) to send and receive data.

1) *W3C XML Schema:* XML-based message exchange makes use of the W3C XML Schema definition (XSD) language to describe the format of messages. XSD is greatly superior to XML Document Type Definitions (DTDs) for electronic business messages, because XSD includes many built-in data types (date, time, language, and numeric), supports better data validation, and offers safe ways to incorporate variants and enhancements through extensions (subtypes).

2) *VICS EDI:* The Voluntary Interindustry Commerce Standard for EDI (VICS EDI) is published and maintained by the Uniform Code Council, Inc. (UCC). These guidelines are used by the general merchandise industry, including department and specialty retail stores, mass merchandisers and their suppliers, to exchange business information electronically. The VICS EDI Guideline is a fully compliant subset of the Accredited Standards Committee (ASC X12).

   ASC X12 was chartered by the American National Standards Institute (ANSI) to develop uniform standards for inter-industry electronic interchange of business transactions – electronic data interchange (EDI). It is comprised of government and industry members meeting for the purpose of creating national EDI standards for submission to ANSI for subsequent approval and dissemination.

3) *EANCOM®:* EAN International, a not-for-profit international association, developed EANCOM®, a detailed implementation guideline of the UN/EDIFACT standard messages. UN/EDIFACT messages are often complex; thus a subset, called EANCOM®, was established to provides clear definitions and explanations that allow trading partners to exchange commercial documents in a simple, accurate, and cost effective manner.

Data Dictionary

Beyond the structure or syntax of messages, companies must agree on the semantics (meaning or content) of each data element. Data dictionaries can establish a precise meaning for the shared information, allowing for a meaningful sharing. Electronic business data dictionaries are generally syntax-dependent, and adapted to specific industries.

1) *EAN•UCC Global Data Dictionary (GDD):* For XML-based electronic business in the retail industry, EAN International and the UCC have developed a new data dictionary. The GDD currently includes party (company) and product item master data alignment, purchase orders, despatch advice (ASNs) and invoices. The output of VICS committee work, such as Collaborative Planning, Forecasting and Replenishment (CPFR®) is being integrated into the GDD to expand its scope to a larger proportion of manufacturer/distributor/ retail interactions.

2) *ASC X12 EDI:* The ASC X12 Data Element Dictionary represents the collection of basic building blocks on which all Electronic Data Interchange transaction sets are constructed. The dictionary listing (in data element number order) defines each data element and its cross-reference to EDI segments and transaction sets in which it is used, including all available codes and attributes. The VICS EDI Guidelines use the ASC X12 Data Element Dictionary for the complete specification of all data elements.

3) *EDIFACT*: The UN/EDIFACT Data Dictionary defines each data element and its cross-reference to all UN/EDIFACT messages in which it is used, including all available codes and attributes.

Registry

Once application messages are defined, companies need a common point of reference for them. They also need to know which organizations support business processes that use those messages. Registry and Repository standards provide a distributed, categorized information base of service offerings. Companies consult the repository for the details of the business transactions, and use the registry to find partners, or register their own business process offerings. There is currently a great deal of activity in this important area. However, this activity has not yet led to the development of standards that are appropriate for inclusion in the VICS Internet Commerce Model. There is additional discussion of this area in a later section of this document, "Future Development – Registry Services."

Trading Arrangement

Once services can be defined and registered, organizations need to identify which combination they wish to use. There are many optional or alternative components in most business services; there are also a variety of security schemes, message transport mechanisms, and service level requirements. Historically, organizations would work out these details manually – selecting a value-added network (VAN) for their EDI transmissions, adjusting their EDI translator software to account for any variants in EDI transaction mapping, and documenting service requirements in a Trading Partner Agreement (TPA). As the number of trading relationships grows, however, the burden of configuring all of these trading arrangements becomes too difficult to manage.

The ebXML Collaboration Protocol provides interfaces that can help an organization automate the negotiation of trading arrangements. It is divided into two parts: the Collaboration Protocol Profile (CPP) and Collaboration Protocol Agreement (CPA). Companies register CPPs that contain all of the options for each service that they are prepared to support. When two companies prepare to transact business, they select among the intersection of options that their companies have available, and capture the chosen set of options as a CPA. The CPA is the service contract between the parties.

ebXML Collaboration Protocol is still a draft specification, and software that makes use of it is not yet available.

It is important to note that electronic business initiatives can begin without an automated trading arrangement in place. The Internet Commerce Model encourages but does not require the use of online trading arrangements.

Messaging

The final step is requesting application services and transmitting data among organizations. Messaging is a broad topic that describes services in this area.

Many standard, Internet-based data transport mechanisms are in use today, including HTTP for hypertext (web-based) content, SMTP for e-mail and FTP for file transfer. None of these transports by themselves offers the services that applications require for messaging. To conduct Internet commerce, organizations require a messaging system that can process both synchronous and asynchronous service requests, can transfer very large data volumes in multiple messages, can guarantee delivery, and incorporates security. Previously, messaging systems with these attributes have been proprietary, so standards-based initiatives had to rely on more primitive transports. The Internet Commerce Model prescribes three new standards-based specifications that address broader messaging requirements:

1) *ebXML Messaging Service:* Currently at its .98 release level, the ebXML Messaging Service incorporates most of the requirements for XML-based application-to-application messaging over the Internet. ebXML Messaging uses a MIME multipart/related envelope to carry a header container and a payload. The header is formatted according to the SOAP V1.1 specification. It describes the sender, receiver, routing details, and contents of the message. The payload may contain application or other data formatted according to SOAP V1.1 with attachments. Typically this data is XML-based, but ebXML Messaging does not place any constraints on its format. ebXML Messaging includes synchronous and asynchronous messaging, guaranteed and secure delivery. The specification is transport-independent; both HTTP and SMTP can be used to physically transfer the data.

2) *SOAP:* The Simple Object Access Protocol is a specification for accessing XML-based services over HTTP. Jointly developed by technology vendors, SOAP has been submitted to the Worldwide Web Coalition (W3C) as a note published on their web site. SOAP is designed more as a remote procedure call (RPC) mechanism rather than a data transfer mechanism.

3) *EDIINT:* EDIINT AS2 is an Internet Engineering Task Force (IETF) specification developed explicitly for transmitting EDI messages over the Internet. However, it can be used for XML communications as well. It has a narrower set of features than ebXML Messaging, but is already being used by some organizations. Software that supports EDIINT has begun to appear on the marketplace, and some packages have demonstrated interoperability. Like ebXML, EDIINT uses a MIME multipart/related envelope, though the header details differ. Both HTTP and SMTP transports may be used.

In summary, companies will likely use a variety of application services standards over the next two years. For different kinds of initiatives, a specific profile of services standards

probably makes the most sense. For example, organizations wishing to transmit VICS EDI over the Internet will most likely use EDIINT and manually configure their trading arrangements. XML efforts may use SOAP until ebXML Messaging implementations are available.

Infrastructure Standards

Table 2 lists and describes the five components identified for infrastructure standards.

Table 2: Infrastructure Standards

Component	Description
Network	The fundamental underlying standards that define the network.
Data Transport	Standards for propagating files, messages, transactions, and other data content over the network.
Security	Standards for security.
Directory Services	Standards for identifying and locating resources on the network.
Presentation	Standards for the markup or graphical display of data to a user.

The committee has organized these areas into the model illustrated in Figure 6, Internet Standards for Electronic Business: Infrastructure. Each component area of the model includes the recommended specifications for that area. Some areas present alternatives that are appropriate for different scenarios.
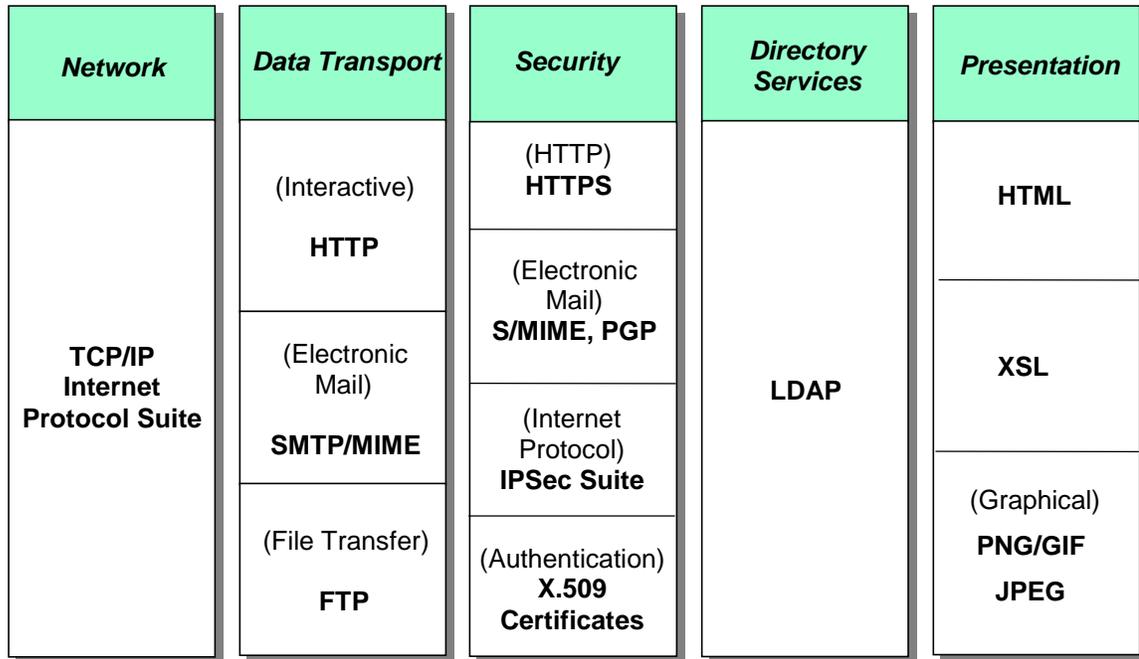
Network	Data Transport	Security	Directory Services	Presentation
TCP/IP Internet Protocol Suite	(Interactive) **HTTP** (Electronic Mail) **SMTP/MIME** (File Transfer) **FTP**	(HTTP) **HTTPS** (Electronic Mail) **S/MIME, PGP** (Internet Protocol) **IPSec Suite** (Authentication) **X.509 Certificates**	**LDAP**	**HTML** **XSL** (Graphical) **PNG/GIF** **JPEG**

Figure 6: Internet Standards for Electronic Business: Infrastructure

While there are some dependencies among the model components, the objectives of each are functionally distinct. The order of the components is not intended to imply layering or dependency.

The following sections describe these components of the VICS Internet Commerce Infrastructure Model in more detail.

Network

A suite of protocols, known formally as the TCP/IP Internet Protocol Suite, and more commonly as TCP/IP, is used across a globally distributed set of interconnected networks and computers. This set of networks and computers is, in fact, the Internet. (Other standards define the media and electrical signals that allow the physical interconnection of these networks and computers.) In essence, selecting the TCP/IP Internet Protocol Suite for the VICS Commerce Model means the global Internet has been selected as the backbone for electronic commerce.

The fundamental protocol of this suite is the Internet Protocol (IP). One of the components of the Internet Protocol is a naming system, which gives each computer or device attached to the Internet an address, simply referred to as its IP address. Computers and devices communicate with each other by using this IP address.

The Transmission Control Protocol (TCP) defines rules for data transmission over the Internet Protocol. Most of the other Internet protocols then layer upon both TCP and IP.

In addition to these two fundamental protocols, the full TCP/IP Internet Protocol Suite includes a number of other protocols that facilitate the operation of the network. These protocols are included as part of this component of the VICS Commerce Model.

Today, TCP/IP is the most broadly implemented network protocol set in the world. It is delivered with a wide range of computers, from the desktop to supercomputers. It is this near ubiquity that makes the Internet today's *de facto* global information infrastructure.

Data Transport

The transport component deals with moving an entire useful set of information from one system to another over a network protocol. A relatively small set of protocols has been developed for moving information. These are the HyperText Transfer Protocol (HTTP), the Simple Mail Transfer Protocol (SMTP), and the File Transfer Protocol (FTP). (New applications sometimes are developed on top of these three widely implemented protocols. For example, the current generation of Internet fax machines moves a fax image inside of an SMTP message.)

The three recommended specifications in this area are:

1) *HTTP:* HyperText Transfer Protocol is the protocol underlying the World Wide Web. HTTP provides the capability for moving content and exchanging data in real time using the Internet. HTTP is most commonly associated with moving content formatted with the HyperText Markup Language (HTML) from a server to a browser – and thus supports a user's interaction with a server. More recently, Extensible Markup Language (XML) was developed to move information from system to system using HTTP as the underlying protocol.

   HTTPS – the secure version of HTTP – uses a particular application of public key cryptography, Secure Sockets Layer (SSL) for encryption and decryption of the data being carried by HTTP. HTTPS can provide privacy as well as authentication. (See the section on Security below for a more detailed discussion.)

2) *SMTP/MIME:* SMTP is the Simple Mail Transfer Protocol, originally designed to send plain text messages over the Internet (i.e., over Internet Protocol, IP). SMTP has been enhanced with the Multipurpose Internet Mail Extensions (MIME), to allow it to carry more than just plain text. SMTP/MIME allows electronic mail (email) to carry other types of messages, including attachments (enclosures) that are a popular part of most current email systems. Real time synchronous exchange of data/information is not supported directly via Simple Mail Transfer Protocol (SMTP). Files may be transferred using SMTP. Though SMTP places no constraints on the sizes of the files, many companies implement size maximums on SMTP messages. In these cases, large messages cannot be sent or received.

   Most email originates on a human user's email client software and is manually composed, with the destination being a recipient's email client software. However, email both can be composed by an application and can be sent to an application.

Security for SMTP is not as standardized as security for HTTP. (See the section on Security below for a more detailed discussion.)

3) *FTP:* The File Transfer Protocol allows for the transfer of entire files from one computer system to another. Either a person or a process can control the transfer. Moving files from one system to another requires that a user has an account on both systems or that an account on one machine be open to all users (an anonymous FTP account) The need to give an account to an "outside" user, the effort to manage/maintain FTP accounts, and the fact that logins cross the network in clear text are all disadvantages of this protocol. However, it can be a useful protocol in some situations, for example, 1) when files are extremely large, and 2) one wants to make a file available to a large number of people, many of whom may not be known (anonymous FTP). Some corporations restrict the use of the File Transfer Protocol because of concerns about security.

There are a number of security enhancements that are employed to make this protocol more secure. However, broad scale standardization has been slow in developing. (See the section on Security below for a more detailed discussion.)

Security

Security on the Internet is a complex and multi-faceted issue. Technology for security on the Internet is typically based on encryption – and since there are many ways to encrypt data, the key to interoperability is standards. In this section, we discuss the recommended standards for security. Additional facets of security are discussed in Appendix 2. Note that technologies and standards play a significant part in making it possible to construct elements of the electronic commerce environment with increased security. However, since overall security is no better than the weakest link, the policies and procedures of the companies involved are also vitally important

There are a number of techniques for adding security features to the Internet. Three significant ones are:

a) Directly adding security features to a single application: This is the technique being undertaken for electronic mail, but no formal standard has yet been adopted nor has a single *de facto* standard emerged.

b) Developing a general security mechanism that can be incorporated into a number of different applications: The principle example of this is Secure Sockets Layer (SSL), which has been incorporated into the software of the World Wide Web to produce a secure use of HyperText Transfer Protocol, HTTPS. SSL has also been used in implementations of a secure file transfer protocol and numerous proprietary systems.

c) Adding security to a lower level protocol, allowing all applications that run on top of that protocol to benefit from the underlying security features: This approach is exemplified by IP Security, normally abbreviated as IPSec. IPSec adds security features to the Internet Protocol layer. All protocols running upon IP automatically benefit from the security features provided by IPSec.

The VICS Internet Commerce Model incorporates four security standards:

1) *Secure use of HTTP (HTTPS):* This provides: 1) authentication of the HTTP server ("the web server") to the client (typically, the desktop browser) and 2) encryption of the data stream between the two, providing privacy and integrity checks. This is the standard security mechanism implemented by all secure web servers and supported by all modern web browsers. HTTPS is built upon Secure Sockets Layer (SSL), a protocol that can be used in a variety of applications.

2) *S/MIME and PGP:* Security standards for electronic mail have not developed as formally or fully as is desirable. Hence, there is no "standard" way to interchange electronic mail that fulfills the typical requirements of confidentiality, integrity, and authentication/non-repudiation. Nevertheless, two technologies are in use: S/MIME and PGP. Proposals based on these technologies are in the formal standards development process, and commercial products support each. To exchange secure email, the involved parties must all agree to use one of these two technologies or the other. Both can provide the desired security features but the implementations differ significantly.

3) *IPSec:* The IPSec protocol is a set of standards that provide IP network-layer security. These standards ensure privacy, integrity, and authentication. IPSec allows for the implementation of Virtual Private Networks (VPNs) over the public Internet between the firewalls of the entities at each end. In this scenario, an encrypted tunnel is created that is then used by all applications. The IPSec protocol suite provides: 1) an authentication header, 2) an encapsulating security payload format, and 3) a protocol negotiation and key exchange protocol, Internet key Exchange (IKE).

   Once a Virtual Private Network is established between two (or more) points, all traffic – from any application – benefits from the security provided by the VPN.

4) *X.509 Certificates:* X.509 certificates are a key piece in providing scalable authentication systems, such as those required to make HTTPS or IPSec work on a large-scale basis. These certificates can provide the association of a public key with a particular person, entity, or system. (For small systems, a manual process might be used.)

Security extensions for FTP have been proposed within the Internet Engineering Task Force (IETF), which is the cognizant standards body. However, commercial implementation of the extensions does not seem to be widespread. Typically, two issues may need to be addressed: 1) providing a mechanism for logging into an FTP server without sending a password in the clear, and 2) protecting the confidentiality of the data during transmission. One mechanism that is sometimes used to protect the password is to employ a secure shell mechanism (e.g., SSH from SSH Secure Communications). To encrypt the data transmission, a product employing SSL is sometimes used.

Directory Services

A variety of applications require or could use directory services, analogous to a telephone directory. The Lightweight Directory Access Protocol (LDAP) provides a standard way

to access directories while allowing a variety of ways of implementing the underlying directories.

(Note that X.500 is no longer listed as a part of the VICS Internet Commerce Model. The further development of LDAP-compliant products and the interfacing of LDAP to a variety of directories have made the specification of a particular directory structure no longer important.)

Presentation

In many applications, data need only be shared between computer-based applications. In these cases, there is no direct presentation layer (though the result of the computer application may ultimately be presented to a person in some form). Other applications present information to a user.

1) *HyperText Markup Language (HTML):* HyperText Markup Language is the "language" used to describe what a World Wide Web page should look like. Browsers interpret this language to make the final presentation of this information to the user. HTML is still evolving, as users of the Web find the need for improved control over the specific layout of information sent to the browser as well as the need to simplify the generation and maintenance of Web pages. Applications such as those based on the World Wide Web (which uses HTTP to transmit data), typically expect a user to view the information that has been transported. Today's browsers typically support viewing data that has been created using HyperText Markup Language (HTML) 3.0, Java, and JavaScript.

   (This paragraph needs work. What should we say about active content?) Limitations in what can be accomplished within HTML have spurred great interest in other technologies that would allow more dynamic presentations at the user's computer. For example, Java and JavaScript provide for less static web pages. This is still a rapidly shifting area, with the standards battle still underway.)

2) *Extensible Style Language (XSL):* XSL, the standard for style sheets created to support the display of XML information on a screen, is a new recommendation within the VICS Internet Commerce Model. Using this standard, web browsers will be able to graphically depict any XML-encoded document.

3) *Graphical presentations:* Much of the use of the World Wide Web includes the transmission of images, or pictures. A variety of standards exist for images of various sorts. Many of the most common image formats are supported directly by the web browsers. Other formats require additional software to be viewed. Today, the major graphic image formats typically supported by the browser are:

   a) *PNG/GIF:* There are now two major alternatives for the presentation of lossless graphics on the Web. The newer standard is Portable Network Graphics (PNG, pronounced "ping"). PNG is technically superior to the older format, Graphic Image Format (GIF), and can be used instead of GIF for most applications. Among its benefits are: 1) it is freely available and not encumbered by patents, and 2) its compression algorithm generates smaller files. Most major browsers

now support the basic PNG format, though support is still incomplete for some PNG features. Many software products for generating Web content now support generating lossless images in PNG format.

GIF remains the dominant format for lossless images. However, it is based on a patented compression algorithm, which makes GIF undesirable as an Internet standard. Nevertheless, GIF remains a major *de facto* standard for the Web.

The VICS Internet Commerce Model recognizes the use of both PNG and GIF for lossless images on the Web. However, given the increased support for PNG in browsers and content creation software, usage of PNG is encouraged for newly developed content.

b) *JPEG:* (pronounced "jay-peg") is a standardized image compression mechanism. (JPEG stands for Joint Photographic Experts Group, the original name of the committee that wrote the standard.) JPEG is designed for compressing either full-color or gray-scale images of natural, real-world scenes. It works well on photographs, naturalistic artwork, and similar material. It does not work as well on lettering, simple cartoons, or line drawings, for which PNG is a better alternative. The JPEG compression algorithm is lossy. That is, the exact image cannot be reconstructed from the compressed image. This allows for significant compression of images while still allowing a reconstruction that is adequate for viewing by a person. The degree of compression is variable, allowing trade-offs between compressed image size and image fidelity when presented to a viewer. JPEG handles only still images, but there is a related standard called MPEG for motion pictures.

The registry concept is one of the newest emerging technologies in e-commerce. While standards in this area are immature, it is important to include registry services in e-commerce strategies. The next revision of this model will include more details on the registry standards as they continue to evolve.

Registry Services Defined

Companies need a common point of reference for e-commerce messages as they are defined. They also need to know which organizations support business processes that use those messages. Registry standards provide a distributed, categorized information base of service offerings. Companies consult the repository for the details of the business transactions, and use the registry to find partners, or register their own business process offerings.

Registry Services Specifications

As of September 2001, there are no *de jure* registry services standards in place. The leading candidate is the ebXML Registry Services specification, still in draft form. ebXML Registry Services defines how organizations can advertise their service capabilities in a distributed registry. The registry has a flexible categorization scheme to assist other organizations in locating the registry entries. ebXML defines mechanisms for federating content among registries, rather than replicating the entire contents.

Meanwhile, there are other organizations that are building registries, and have published specifications for accessing them. The two most prominent efforts are *Universal Description, Discovery and Integration (UDDI)* and *UCCnet*.

1) The UDDI specification is a joint development effort of technology vendors to create an XML business services registry. Although it is not a *de jure* standard, the specification is publicly maintained at the uddi.org web site, and implementations of the registry are already in use. UDDI at present has a somewhat narrower focus than ebXML Registry Services, because 1) the services represented there are all defined in terms of SOAP (an XML transport mechanism for service requests described below), 2) when multiple repositories are used, they simply replicate their content to remain consistent, and 3) there is no built-in mechanism for managing trading arrangements.

2) *UCCnet:* UCCnet is a wholly-owned, not-for-profit subsidiary of the Uniform Code Council that seeks to provide registry and repository services for the synchronization of item (product) and party (organization) data between partners in an e-commerce environment. UCCnet has submitted its specifications for interfacing to EAN International and the Uniform Code Council for inclusion in the EAN•UCC Business Messaging Standard.

The UDDI and UCCnet specifications may influence (or like SOAP, become a part of) future public standards. Aspects of these services complement and/or compete with others; it is impossible to say today what the final form of a registry standard will take.

Conclusion

These Internet guidelines are a work in progress. The VICS Internet Commerce Committee has selected the combination of standards and conventions that best meet the needs of general merchandise supply chain trading partners, based upon the technologies currently available. Technologies in this domain continue to evolve rapidly. In order to validate the technology selection and continue to develop the technical recommendations for Internet commerce, the committee will encourage members to conduct reference pilots. Through the piloting process, the technologies outlined in this document will be tested further in real business situations and field conditions. The committee then hopes to publish subsequent revisions to this document that will enhance these guidelines and standards selections as they emerge.

Acknowledgements

Appendix 1: Security and Encryption

Security

Every Internet commerce implementation will need to consider both the threats to and the risks of doing business over the public Internet, where important messages are exchanged over a public network. Today's Internet satisfies a key requirement for broad scale electronic commerce – that of being nearly ubiquitous – and, with each passing month, it becomes even more pervasive. However, the threats and the risks associated with the Internet also continue to evolve. Organizations using the Internet need to explicitly consider these threats and risks by conducting appropriate assessments. Moreover, these assessments need to be repeated periodically.

These completed assessments can provide significant input to forming the security requirements for the system. If the threats and risks are high, additional effort and cost is justified in creating a more secure environment. But, creating highly secure environments for electronic commerce, which may involve many companies that are broadly distributed geographically, is not a straightforward task.

Because security considerations were not an important part of the initial research activity that created the Internet, the technologies and techniques for improving security on the Internet are still being developed.

Some of the major areas that need to be considered in developing security requirements are:

a) *Privacy:* knowing that nobody can read the information that is being transmitted – except the intended recipient

b) *Integrity:* the assurance that the message content cannot be changed (intentionally or accidentally) or, if it is changed, that the change will be detected.

c) *Authentication:* verifying the identity of a user or source of a transaction.

d) *Nonrepudiation:* being able to guarantee that a message or data can be proven to have originated from or received by a specific person.

Encryption

The technologies and standards for security on the Internet are based on encryption. The encryption technologies include both "secret key encryption" in which a single secret key is used both to encrypt and decrypt a message and "public key encryption" in which a pair of keys is used. One key is the public key, which is openly shared. The other is the private key, which must be kept secret.

The major advantage of secret key systems is that data can be encrypted and decrypted with modest computer resources. The disadvantage is that both the sender and receiver of an encrypted message must possess the same secret key. Distributing the secret key to both sender and receiver is a very difficult problem, particularly when the secret key is changed frequently.

Public key systems solve the distribution problem, since by definition the public key must be made public. However, the computational resources for encrypting a message with public key cryptography are significantly larger. Therefore, systems suitable for widespread application in electronic commerce are constructed as hybrids, using both secret key and public key cryptography.

There are a variety of algorithms in use in each of these two classes. Typically the end user is not aware of which specific encryption algorithm is being used, and in fact most modern software supports a number of different algorithms. Systems using cryptography typically negotiate which specific algorithms will be used.

The software may also support a number of different lengths of keys. This aspect is of great concern to the end user. Keys used in secret key encryption are typically, 40, 56, or 128 bits long. Keys of 40 bits can be trivially broken on desktop computers in less than 5 minutes, simply by performing an exhaustive search. Key lengths of 56 bits can now be cracked with specialized hardware or significant computing power in 1-2 days. Today, only keys of 128 or more bits are deemed to be cryptographically strong.

Thus, to achieve any real measure of security, it is necessary to assure that a system is operating with secret key lengths that are cryptographically strong. This is not the default state for most software. For example, when a normal Web browser negotiates with a Web server to determine the key length and specific algorithm to use in an SSL connection, the negotiation, by default, starts at 40 bits. If the systems believe that this is the greatest length of key that they both support, the interchange will proceed with this key length. To assure that the interchange does not proceed unless the key length is, for example, 128 bits, either the server or the browser must be manually configured to insist upon this greater key length.

(An older version of a popular web browser was shipped with a problem in the software that caused all attempts to negotiate up to 56 bits to fail. Thus, that browser could only connect with a 40-bit key – unless the browser was manually configured.)

To achieve comparable security, keys used in public key cryptography must be significantly longer than those used in secret key cryptography.

Application of Encryption to Achieve Security

Privacy

Conceptually, privacy of a document or a communications channel is achieved by encrypting it. The details of how this is done differ with specific mechanism that is used. Privacy is implemented in a variety of ways for different applications on the Internet.

The World Wide Web uses the services of Secure Sockets Layer to achieve privacy. The browser and server negotiate a key length and algorithms, generate a random secret key, share the secret key using public key cryptography, and then exchange information that is encrypted with the secret key.

Currently, for electronic mail, there is no Internet standard for privacy. Two proposals are currently under review and further refinement for the Internet Engineering Task Force:

Secure MIME (S/MIME) and Pretty Good Privacy (PGP). Key lengths are prescribed in advance by the user. The algorithms used must be selected from a pre-agreed upon set.

Integrity

Data integrity is achieved by computing a function based on the data content. This function generates a small additional data item, a "hash", and is such that changing the data content will change the hash. The hash is then sent encrypted so that it is private. The receiving software can validate that the message, which is not encrypted, has not been modified by independently calculating the hash and comparing it with the one that has been sent.

Frequently, the message part will also be encrypted so that it is also sent privately, thus assuring both privacy and integrity. However, they are conceptually separate capabilities.

Authentication

There are a variety of application areas and techniques for authentication - "proving" that an entity (a person or a process) is who it claims to be. Typically, highly reliable methods for authentication cost more than methods that provide less assurance. For example, a user is authenticated when he/she logs onto a computer system:

a) At the simplest level, a "user name/password" is used to authenticate someone when logging in to a computer system.

b) Security tokens provide an additional level of assurance. In addition to knowing something (user name/password), the user must also possess something (the token). There are a variety of systems that utilize different types of tokens (both hardware tokens such as security cards and software tokens). Systems that require "something you know" plus "something you have" provide better authentication/security than those that require only one of these do.

In exchanging information, there also is frequently a need for authentication. For example, is electronic mail really from the person that claims to be sending it? Or, am I really talking to the Web server of the company that I think I am talking to? Techniques that assist in authenticating include:

a) Digital signatures: A digital signature "proves" that a specific document came from a specific person. One of the most obvious application areas is in electronic mail. To generate a digital signature, the integrity hash is first computed as discussed above. This hash is then encrypted with the sender's private key. The recipient can decrypt the encrypted hash with the sender's public key, which "proves" that it came from the sender. Moreover, if a newly computed hash on the received message matches the hash that was sent, then that is precisely the message that the sender "signed."

Note that signed messages do not need to be private. The signature is tied to the integrity of the message, not the privacy.

b) Certificates: Digital certificates are employed with public key cryptography - and in general require some form of directory services - to provide even more information.

For example, the encrypting of a document with a person's private key guarantees that it came from that person. A directory system that contains a certificate associated with that person, accessible using that person's public key, could show other information, such as his/her corporate authority. These extra details could facilitate electronic business. The current standard for certificates is X509.3.

Nonrepudiation

Nonrepudiation has two components: nonrepudiation of origin (i.e., authentication) and nonrepudiation of receipt (i.e., a signed receipt). Nonrepudiation of origin is provided by authenticating the sender, as described in the previous section. Nonrepudiation of receipt of a message (which can be accomplished in the US mail system by using Certified, Return Receipt Requested mail) is accomplished by the recipient of a message sending back a digitally signed receipt. Typically, the body of this message is the integrity "hash" of the original message described above, which proves that the message was received.

Digitally signed receipts are necessary to prove nonrepudiation of receipt. A digitally signed receipt proves that the message was truly received, the sender was authenticated and the integrity of the message was verified. When the sender receives the digitally signed receipt and verifies the identity of the signature in the receipt, nonrepudiation of receipt has been established. A signed receipt can be used for tracking, logging, and reconciliation purposes.

Without nonrepudiation, the sender cannot be assured that the recipient actually received the message that was sent. Also, if the message acknowledging receipt cannot be authenticated, it is possible that the receiver might assert that the message acknowledging receipt was not from him.

Appendix 2: Internet Commerce Model Standards

Standard	Organization	Web Reference
ASC X12	American National Standards Institute (ANSI)	www.ansi.org/
ebXML Collaboration Protocol	UN/CEFACT and OASIS	www.ebxml.org/
ebXML Messaging	UN/CEFACT and OASIS	www.ebxml.org/
ebXML Registry Services	UN/CEFACT and OASIS	www.ebxml.org/
EDIFACT	International Standards Organization (ISO)	www.iso.ch/
FTP	Internet Engineering Task Force (IETF)	www.ietf.org/
EANCOM®	EAN International	www.ean-int.org/
EAN•UCC GDD	Uniform Code Council	www.uc-council.org/
GIF	Unisys	www.unisys.com/
HTML	World-Wide Web Consortium (W3C)	www.w3.org/
HTTP	Internet Engineering Task Force (IETF)	www.ietf.org/
HTTPS	Internet Engineering Task Force (IETF)	www.ietf.org/
IETF EDIINT	Internet Engineering Task Force (IETF)	www.ietf.org/
IPSec Suite	Internet Engineering Task Force (IETF)	www.ietf.org/
JPEG	Joint Photographic Expert Group (JPEG)	www.jpeg.org/
LDAP	Internet Engineering Task Force (IETF)	www.ietf.org/
PGP	PGP Security	www.pgp.com/
PNG	World Wide Web Consortium	www.w3.org/
S/MIME	RSA Security	www.rsasecurity.com/standards
SMTP/MIME	Internet Engineering Task Force (IETF)	www.ietf.org/
SOAP	See http://www.w3.org/TR/2000/NOTE-SOAP-20000508/	www.w3c.org/
TCP/IP Internet Protocol Suite	Internet Engineering Task Force (IETF)	www.ietf.org/
UDDI	The Universal Description, Discovery and Integration (UDDI) project	www.uddi.org/
VICS EDI	Uniform Code Council (UCC)	www.uc-council.org/
W3C XML Schema	World Wide Web Consortium (W3C)	www.w3c.org/
X.509 Certificates	International Telecommunication Union	www.itu.int/
XSL	World-Wide Web Consortium (W3C)	www.w3.org/

© Voluntary Interindustry Commerce Standards

Appendix 3: Acronyms

ANSI	American National Standards Institute
API	Application Program Interface
ASC X12	Accredited Standards Committee X12 EDI
ASP	Application Service Provider
CPA (TPA)	Collaboration Protocol Agreement (Trading Partner Agreement)
EDIINT	EDI (or XML) over the Internet
GCI	Global Commerce Initiative
GCIP	Global Commerce Initiative Protocol
GIF	Graphic Interchange Format
ICC	Internet Commerce Committee
IKE	Internet Key Exchange
IPSEC	Internet Protocol Security
MIME	Multipurpose Internet Mail Extension
OBI	Open Buying over the Internet
PGP	Pretty Good Privacy
PNG	Portable Network Graphics
S/MIME	Secure MIME
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
UCC	Uniform Code Council
UDDI	Universal Description, Discovery and Integration
VAN	Value Added Network
VICS	Voluntary Interindustry Commerce Standards
VPN	Virtual Private Network
XML	Extensible Markup Language