Chapter 4. Technical Architecture

THE TECHNICAL FOUNDATION

In this chapter, we describe the technical portion of the architecture to support the functional requirements described in the previous chapters of this report. We describe the communications, data bases, and computing environment necessary for electronic commerce (EC) between the Federal government and its trading partners. Our task is to provide a foundation of information systems and telecommunications support on which to implement EC within the Federal government and to prepare this foundation as quickly as possible. Electronic commerce is not new and does not require the development of new systems. It does require a considerable amount of work to interlink existing networks and modify existing systems to make EC a reality. We begin with some background information on existing technology.

In the emerging global electronic marketplace, buyers and sellers from large and small companies will meet on equal terms, aided by a wide array of information services that allow them to target or broadcast their communications appropriately. Every aspect of the acquisition process needs to be handled seamlessly. Buyers will browse multimedia catalogs, solicit bids, and place orders. Sellers will respond to bids, schedule production, and coordinate deliveries. Third parties will facilitate the marketplace by providing such value-added services as specialized directories, brokering, referral, and vendor certification.

Many of these transactions already occur electronically but require prior arrangements and dedicated lines. The resulting costs and lead times create entry barriers to widespread participation by small business, hindering expansion of electronic data interchange (EDI) beyond large companies and their major trading partners. The new aspects of electronic transactions are interactive EDI services in addition to traditional computer-to-computer exchanges and an open marketplace in which transactions take place spontaneously on public networks in addition to proprietary ones.

The electronic marketplace is already forming. By the end of 1994, more than 10,000 companies will be offering information and services for sale over a combination of Internet and value-added networks (VANs). Their ranks are expected to swell to 100,000 in 3 years and to 1 million in 5 years when Internet connectivity approaches the ubiquity of fax. By participating actively in this marketplace and promoting a sensible mix of computer-to-computer and interactive EDI services, the government will not merely promote electronic commerce, it will stimulate the creation of a massive, competitive vendor base.

The centerpiece of the proposed technical architecture is the virtual network. The virtual network is the mechanism that agencies can use to communicate with their trading partners and provide a "single face to industry." The virtual network is a network of networks built from existing agency networks. In the past, each agency designed, installed, operated, maintained, or outsourced its own telecommunications network needs. Today, in order to take advantage of these wires, standards-based software sets up new "virtual" circuits instead of "physical wire" circuits. The virtual network is not a new network designed specifically for EC. It is the interconnection of existing networks using standards-based communications software, including the Federal Telecommunications System 2000 (FTS2000), the Internet, and other participating agency networks. Through the virtual network, agencies will be able to send transactions to trading partners as well as get required data from shared data bases.

For example, an agency request for quotes (RFQs) is created at the agency application system, passed to the gateway where it is translated into EDI format. From there it travels to the network entry point (NEP), which forwards it across the virtual network to the VANs. Each agency will not have to set up its own connections with every VAN. The VANs distribute the RFQs to interested trading partners, collect quotations, and send the quotes to the virtual network. The virtual network passes them to the appropriate gateway for translation into the agency's application format for review by the contracting activity. For example, the components of the virtual network can be used to validate quotations against the List of Parties Excluded from Procurement and Nonprocurement Programs before award and later update the Federal Procurement Data System.

AGENCY ACTIONS

To implement EC, agencies call the ECA-PMO and request technical assistance. The ECA-PMO will explain what is needed and put the requesting agency personnel in touch with one of the agency network managers participating in the virtual network. Agencies will need software that generates the transactions in X12 format or in a flat file for translation.

GOVERNMENT-WIDE ACTIONS

Because much of the electronic initiative is beyond the resources and scope of individual agencies, government-wide actions are needed. The following subsections describe those actions.

Open Systems Standards-Based Architecture

The complexity and heterogeneity of the computer and communications systems requires all participants to commit to open system standards. In their interactions with the EC technical architecture, the Federal agencies involved shall adopt open systems,

standards-based architecture as identified in the Open Systems Environment/Applications Portability Profile of NIST. FIPS Pub 161-1 (or later revision) includes guidance on the selection of ASC X12 or the United Nations EDI for Administration, Commerce, and Transport (UN/EDIFACT) standards for EDI. For the purposes of this architecture, the Federal government shall use the American National Standards Institute (ANSI) ASC X12 standard for EDI, moving with ASC X12 to EDIFACT. The benefits of open systems technology include the following:

- Connectivity among people, tools, and domains
- Mobility of information among connected people and tools
- Malleability of shared application information objects
- Avoidance of a propriety solution (which eventually must be broken at great cost).

Virtual Network Concept

The technical architecture resulted from an evaluation of networking architectural alternatives. We selected a virtual network concept because of its economy and scalability. The design and implementation will require extensive interagency coordination to establish the protocols and procedures for interagency exchange of transactions and interconnections with commercial VANs. To best meet the needs of a wide number of participants, the virtual network will incorporate a challenging combination of the following solution sets:

- Agency networks
- FTS2000
- Open system interconnectivity (OSI)
- Internet and the Internet protocol suite (IPS).

As the virtual network infrastructure is built over the next year, ECA-PMO will improve on this ad hoc process and set up a virtual network manager to build the necessary connectivity between agency networks.

Standards-Based Client-Server Data Bases

The interdisciplinary ECAT identified valuable opportunities for government improvement of procurement and financial methods. Instrumental to the accomplishment of these improvements is the design and implementation of several supporting data bases. Given the disparate responsibilities for the data elements needed by finance and contracting officers across the Federal government, these data bases should employ state-of-the-practice design and systems management for client-server technology with standardized interfaces to the data.

Security and Legal Requirements

The users of EC must have a high degree of confidence in its integrity. Participants must be assured of the authenticity of the other participants and that the messages sent and received are above reproach. Sensitive government and commercial information must be kept confidential. To balance the privacy, national defense, law enforcement, and industrial security concerns, the technical architecture supports a position of flexibility, recommending that the government use the methods preferred by the trading partner as appropriate to the transaction. Although this document incorporated security requirements in the architecture and design, Agencies will begin with small purchases (under $25,000) where the security requirements are normally minimal.

Interagency Approach/Service-Level Agreements

We believe that agencies need to look to each other, as well as to the ECA-PMO, for strategies and solutions to the challenge of EC. An interagency approach is needed because of the magnitude of resources required, the limitations on funding, and the objective of providing a "single face to industry" and the coordination that objective implies. Interagency service-level agreements for NEP services, translation services, and data base services will facilitate resource sharing.

ARCHITECTURAL PRINCIPLES

Dramatic changes in technology and economics are enabling the rapid deployment of computing and communications infrastructure across much of the world. The government and its trading partners stand to benefit substantially from the capability to process information faster and more accurately. Increasingly, the government is beginning a new "way of doing business" within the United States and abroad.

To fulfill the EC initiative, the government must keep up with the information explosion that is occurring throughout the world and be an active proponent of it. Technology is inexorably advancing, with new capabilities arising regularly. The ECA-PMO should be careful to avoid exclusive commitment to existing technology, and thereby lock the initiative into a mandatory solution, thinking that the government can pick the winning technology.

The government adopted the ANSI ASC X12 standards for EDI and will expand its use in acquisitions beginning in September 1994, with a planned transition to UN/EDIFACT in compliance with FIPS 161-1.

The ECAT technical architecture is a representation of the technical capabilities and relationships needed to implement EC in the Federal government. It describes a model for interconnecting the computer systems and applications they need for EC.

The following architectural principles provide a basis for selection of standards, implementation of technology, and modification of business practices. Principles are influenced by organizational policies, requirements, technology, trends, existing architectures, and costs.

OPEN SYSTEMS ENVIRONMENT

The government will increasingly be exchanging information and sharing information electronically with its trading partners and with the rest of the world. Such widespread connectivity and interworking among diverse computing and communications systems is dependent upon the ability to plan and coordinate implementations on a national — and even a global — scale. This can be achieved only through the use of standards. Some standards will be deployed across industries, some may be unique to each industry, and some may be defined for use within the departments and agencies of the government. In any case, a blueprint, or road map, is required within the government to understand the overall design and application of technology to achieve these diverse and far-reaching business objectives.

A major goal of implementing EC in the Federal acquisition process is to create a communication and computing infrastructure composed of standard support services, with facilities based on standards and the principles of open systems. The infrastructure must provide a means of interchanging standard transactions at a low cost with minimum impact on existing automated systems. There is a clear need to use open systems based on nonproprietary standards to support extensibility, scalability, portability, and maintainability requirements. Three primary policy variables must be monitored and nurtured: operating system environment preferences, communication protocol preferences, and data base preferences. We recommend an open systems environment including the portable operating system specification (POSIX), the Government Open Systems Interconnection Profile (GOSIP), the structured query language (SQL), and other government-approved protocol suites.

Standards-based open systems provide many benefits — such as higher levels of competition, enterprise-wide economies of scale, and the resulting lower prices — but they also convey new responsibilities to the user. With open systems, the user can mix and match system elements from a variety of vendors and is responsible for ensuring the pieces work together as intended. The utility of these decisions is found in four primary dimensions: connectivity among people, tools, and domains; mobility of information between connected people and tools; mailability of transferred application information objects; and absence of implementations that can evolve only at great expense because of their closed structure.

The ultimate goal is to migrate toward a single interconnected, interoperable standards-based internetworking environment for EC. To accomplish this goal, the ECA-PMO would promote a standards-based open systems multinetworking environment that recognizes the value of existing infrastructures. The architecture is

based on standards using a hierarchy of open international voluntary standards, national voluntary or consortia standards, and proprietary standards with multinational commercial prevalence. All communicating devices must interface to the network through a standard set of protocols and interfaces. Common services such as file transfer, E-mail, directory management, and network management will be provided through a common networking environment; services of different protocols will be completely equivalent so that a conversion can be performed from one format to the other.

Modular Components

The architecture will be modular and standardized so applications can be reusable and interoperable. Separate functions that are designed to be modular and independent of data, hardware, and the target computing platform will facilitate disaster recovery, software integration, and establishment of clear boundaries of responsibilities.

Best Commercial Practices

The goals of the National Performance Review are to search out the best commercial practices of industry and bring them into the government systems. These systems will thus avoid obsolete technology and practices. For example, maximum use of commercial off-the-shelf (COTS) software and government off-the-shelf (GOTS) software is necessary to make use of current practices in both communities. The technology and implementation techniques must be mature and proven approaches, not experimental test beds. System software, such as operating systems (DOS, UNIX, etc.) for computers and packet assembler devices, and X.25 code for communications control the allocation of resources that are independent of a particular application. All system software will be provided by reliable and financially stable vendors as determined by contracting officers' evaluation of bids and the technical and business evaluation teams. Government personnel will not modify systems software source or object code; they will contract for system software maintenance.

Single Face to Industry

A "single face to industry" means that the electronic transactions must be available to all trading partners in the same format regardless of the Federal agency originating the transaction. It means that different automated information systems employing dissimilar technologies and using different enabling technologies to package transactions can transmit through different communications networks and issue transactions in exactly the same manner to trading partners. The issue is not that every process must be identical but that the results of process (data elements) "look" the same to all of the government's trading partners. The "single face" means that standardized data elements, transaction sets, and addressing schemes are used to reach all government agencies. Providing a "single face to industry" requires the use of a government-wide set of EDI conventions. That does not mean all transactions must be sent to the same

point or processed in an identical manner but that a vendor requires connectivity to only one VAN to do business with any government department. Further, VANs only need to be connected to the government at one location to receive all transactions to and from the government.

Flexible, Scalable, and Extensible Systems

The systems developed must be flexible, scalable, and extensible to accommodate technology and functional enhancements and improvements. The modules must be capable of existing on platforms of different vendors and support alternative configurations that can be adjusted to provide an EC capability to accommodate operations of varying sizes. Additionally, as EC becomes more prevalent in government, it should allow for other functions such as logistics, personnel, health, etc., to take advantage of this information infrastructure. For the most part, government and industry information infrastructures provide a disjointed foundation utilizing diverse, nonstandard data bases with proprietary solutions that inhibit the functionality needed to support the objectives of the National Performance Review. A client-server architecture with distributed data bases, developed under national and international data standards, will provide the functionality that government and industry need to build an interoperable information infrastructure. Hence, we see the evolution of government and industry applications to shared distributed data bases and client-server architectures that will enhance the widespread migration of existing information infrastructures in support of worldwide EC.

Vendor Independence

The government must be aware of the risks associated with dependence on a single vendor. It has suffered in the past by relying on products that did not have significant market penetration or had little support. Use of products that are widely accepted and are commercially available will make it easier to get support for that product and make it easier to find qualified people who know how to use it. In addition, an existing base of users will allow the government to check the stability and performance of the product by checking with a number of customers.

Operational Management and Control

The autonomy of separate business units is vital and a required part of the operational environment. Nevertheless, the EC architecture, and its implemented systems must address the management of all forms of information (data, voice, image, etc.) in an integrated manner. Roles, responsibilities, and boundaries for all elements of the architecture must be identified. Interagency agreements will have to be created for the operation and management of common and shared facilities associated with the EC architecture.

Security Based on Need

Security and contingency planning must be based on the risk analysis performed by the respective user organizations; users should not incur or share in costs that are used to produce systems that exceed user requirements. The cost incurred in prevention should be based on potential loss. Security must be consistent with and comply with government regulations. Appropriate controls on access to the data will be based on the sensitivity and use of the data.

Standard Data Elements

Standardization of data definitions and their characteristics, implementation, access, and communication is needed across the systems to provide quality, consistency, and overall effectiveness of all implemented systems. The standard data elements for EC applications will comply with the ASC X12 or the UN/EDIFACT definitions and process. Standard implementation conventions and mapping procedures will be used to promote adherence to standard data base development rules and the use of common data dictionaries throughout the government.

Single Data Entry

Information needed by many different sources should be collected only once and then shared as needed to meet the goals of all Federal users.

Mandatory Testing

Hardware and software interoperability testing is required prior to operational use. These tests and can be performed in partnership with organizations already performing these functions; they can be performed by a contractor, provided government personnel observe and validate their results. Software interoperability is dependent on successfully completing component, integration, and system tests. The testing process requires regression testing and the use of defined scripts and scenarios.

Cost-Effective Transitions

Transition from current agency approaches to EC will be pursued aggressively to obtain the resulting benefits. Although proprietary protocols may be unavoidable for the initial transition to EC applications, the goal is to recover life-cycle cost on or before 8 years based on the maximum expected life of computerized systems. However, industrial experience by companies such as Texas Instruments and Reynolds Tobacco indicate that cost recovery may occur within 1 or 2 years. Decisions affecting cost will be on government-wide analyses performed by or for the government.

THE TARGET ARCHITECTURE

OBJECTIVES

The methods used to pass data between agencies and to more than one trading partner are driven by far reaching objectives and functional requirements. Based on the functional requirements described in Chapter 3, the objectives of the EC architecture are as follows:

- Support EC communications between agencies and all trading partners, national as well as international. The architecture must provide inter- and intra-agency communications for the Federal government and provide the enabling technology that supports the evolution of EC and its usage. The communications infrastructure must allow all Federal users access to any trading partner that conducts business with the government.
- Allow all Federal users access to data base containing trading partner profile information provided during the trading partner registration process.
- Provide a common method for trading partner registration. Because all firms participating in EDI with the government must register, the design, development, and testing of this capability will be a significant government-wide effort.
- Support security services identified for integration at Federal data centers or gateways, consistent with the requirements of the Computer Security Act of 1987. Trading partner data must be safeguarded now and as EC capabilities evolve.
- Present a "single face to industry." Supporting a "single face to industry" can be accomplished using the architectural models described in this chapter. A "single face to industry" means that quality and consistent services are provided to the business community in a standard operating environment so that no matter which agency generates the transaction and no matter where the goods or services are to be delivered, the business community will receive it one way. EDI should be implemented such that industry will have some choices but can interface to the government with the same protocols and ASC X12 transactions regardless of operating environment.

It is important to recognize that each objective requires separate and distinct consideration during formulation of the EC architecture.

AGENCY CAPABILITIES REQUIRED

To satisfy the EC architectural objectives discussed above, agencies must have, as a minimum, an automated procurement system that produces transactions that can be mapped to standard implementation conventions. Functions of the procurement system include the following:

- Accept and analyze bids from any trading partner
- Generate standard notices of contract award
- Process standard invoices and generate payments for goods and services
- Generate complete sets of technical specifications that accompany solicitations.

Even though the architecture and design of agency applications are outside the scope of this paper, it is worth looking at extending the benefits of EC between trading partners to include interactions within (and between) the business functions of an agency.

While the EC communications infrastructure and supporting data bases are essential elements in achieving the Presidential objectives, they do not stand alone. Agency applications will require some modification so that they can be linked to the EC infrastructure. This need for modification provides an opportunity for a reassessment and perhaps a reengineering of those applications. A significant portion of the benefits expected from EC are expected from the reengineering of agency processes. Since a complete acquisition cycle involves the movement of documents among many agency functions (e.g., creation and submission of request, procurement actions, finance actions, receiving, and finance again, and various reviews and approvals along the way), it is worth looking at tools and techniques that can enhance this flow of paperwork.

A number of tools are available to assist in the development of "workflow" application. These tools aid in the development of applications that "ride" on E-mail or data base systems. Some tools are specifically designed to address the flow of documents and the sharing of common data bases. Well-implemented workflow applications add considerable value when they

- include the ability to define standard forms and messages,
- establish the rules to be followed when filling them out,
- offer on-line help and training, and
- capture and store data for later analysis.

Guided forms completion, as the second point is sometimes called, can materially reduce data entry errors, as does the context-sensitive help.

The adoption of automated workflow processes within an agency can improve their operation whether or not the applications are linked to trading partners through electronic commerce. However, EC linkages add additional value and utility to both parties.

FUNCTIONAL CONCEPTS OF AN EC ARCHITECTURE

The architectures described below provide possible solutions for enabling an exchange of EDI transactions and other electronic messages between agencies and trading partners to facilitate the acquisition process. More specifically, these architectures address the problem of an agency sending EDI transactions to one, some, or many trading partners and receiving the EDI replies from those trading partners. The intent is to provide a consistent architecture that can provide the intended functionality and utilize the same suite of standards and processes. Figure 4-1 shows the conceptual functions for Federal EC from the agency through and including the trading partners. The specifics of data flows, software, hardware, and data bases are covered in subsequent sections. The functional requirements of trading partner registration and implementation agreements have been discussed in previous sections.

The following conceptual functions are needed:

- An agency process for the preparation and management of contract actions. Such a process could be fully automated, partially automated, or not automated at all.
- An EDI translation service that translates agency application data to EDI standardized formats and on receipt of EDI transactions translates the standardized data to agency application formats.
- A communications service that conveys EDI transactions and other electronic messages among agencies and between the agencies and their trading partners.

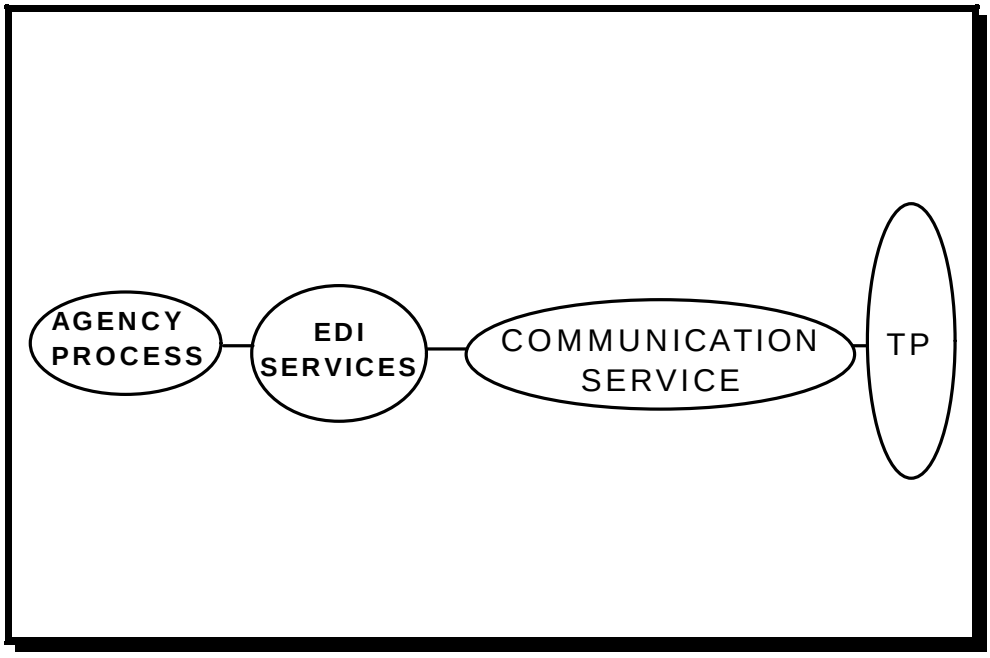

Figure 4-1. Abstract Functional Model for Electronic Commerce

TODAY'S EC ARCHITECTURAL ENVIRONMENT

Today's EC environment consists of a variety of networks that are not interconnected and are operated independently by major Federal agencies. Numerous service providers offer an array of communications and value-added capabilities to both public and private trading partners. Some networks are mature and provide a wide range of services, while others may only provide limited services. Moreover, existing networks may not satisfy agency EC requirements. Most agency networks currently have access to a limited group of VANs and trading partners. In most cases, agency applications do not have the minimum capabilities, and gateways may have insufficient translation or communication facilities. As a result of these types of differences in doing EC, even a single agency can have many faces to industry.

Figure 4-2 represents the general state of communications architecture used for EC today by the Federal agencies and the private sector environment. Many interworking and connectivity issues surface as trading partners attempt to conduct business using different VANs. While standards bodies and implementation working groups are addressing these interoperability issues, much work remains to be done.

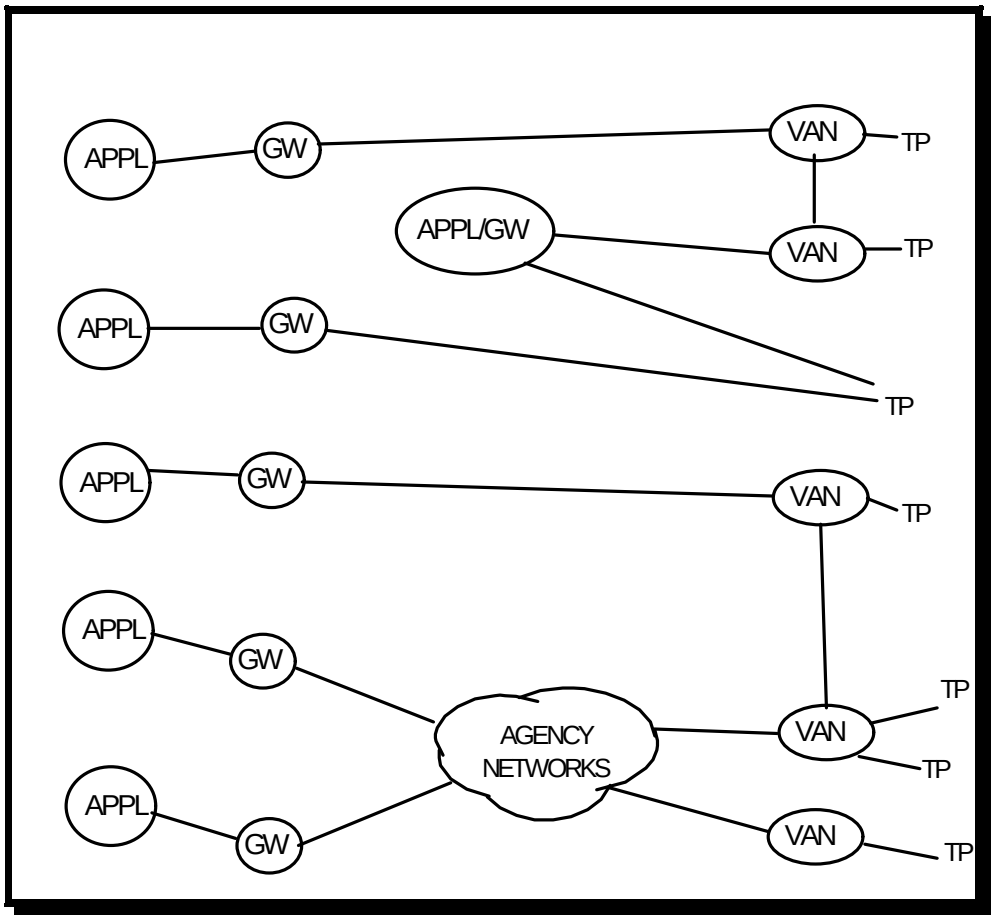

Figure 4-2. Current EC Architecture

VIRTUAL NETWORK

The virtual network is the connection of the EC target architecture. In Figure 4-3, each agency or several agencies acting as a single entity can establish an interface between government facilities and VANs. These entities may be NEPs, but they offer services other than communications and are interconnected to all other similar entities. These NEPs will provide connectivity to VANs as mutually agreed to by the VAN and the government organization responsible for the interconnection. This connectivity of entities is necessary because of the distributed processing environment in the Federal government. In this scenario, any VAN that has point-to-point connectivity to an agency today should have connectivity to at least one of these NEPs. A connected group of NEPs can be configured to provide the total communication services required, but all agencies must have access to NEP functionality. The primary benefit of the virtual network is to guarantee seamless connectivity for any user to any point.

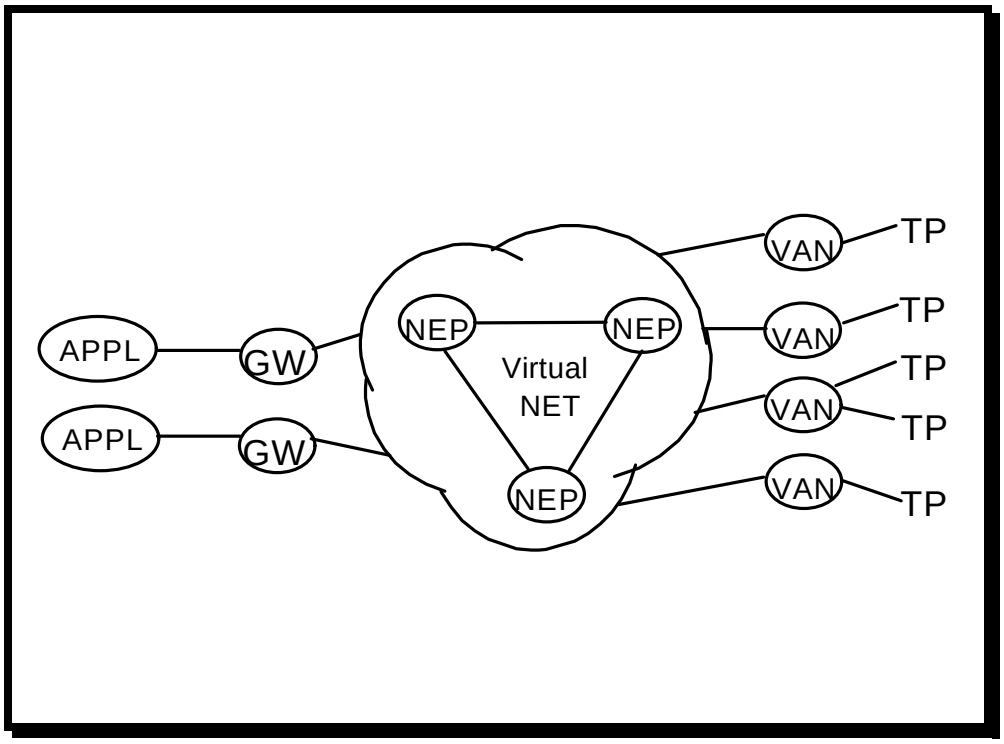

Figure 4-3. Virtual Network

The underlying makeup of the virtual network would consist of a combination of private networks linked together. For example, we consider the Internet a virtual network, or a network of networks. A possible combination would include the networks from the Department of Defense, Department of Commerce, National Aeronautics and Space Administration, other government and private industry networks such as

FTS2000, and Internet. This does not imply that a common backbone is used to connect Federal agencies with private industry.

TARGET ARCHITECTURE

The virtual network interconnects all the participants and components of the target architecture for EC. Figure 4-4 suggests several paths by which agencies can utilize the target architecture, highlighting the flexibility that the agencies can have to attain it. It also emphasizes that EC is possible without mandating use of some of the components shown in the other alternative architectures (see Appendix I). This architecture is viewed as a group of services that must be used to obtain total EC functionality. Those services can be provided to meet the demands of a specific agency, and the agency can take advantage of their availability at various locations.

The "glue" that holds the target architecture together is the virtual network described above. The architecture does not preclude the use of most of the possible scenarios shown in Figure 4-4 as long as the connectivity method does not deny transactions to any agency or trading partner that needs it. The same communications services (for example, E-mail and file transfer) can be provided with any of the paths presented in the figure above. Some minor differences may be imposed on users who are required to send messages through an NEP. Otherwise, the communications services provided do not appear to be have any significant benefits or drawbacks. In some instances, the NEP is the only centralized facility needed because all the other functions of the NEP are accomplished at the agency gateway. In some cases, the trading partner is so large and the volume of transactions is so great that the trading partner becomes accredited as a VAN as well in lieu of using a commercially operated VAN.

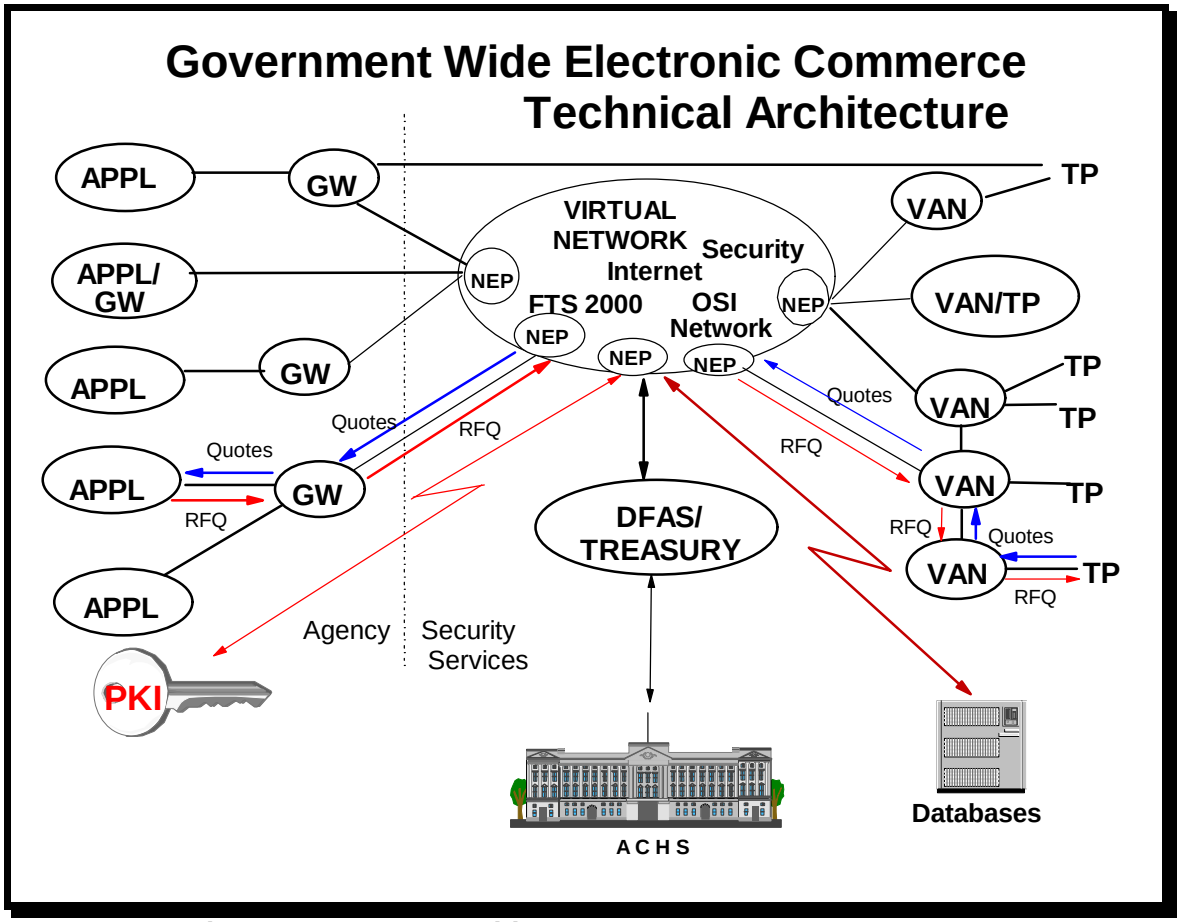

Figure 4-4. Target Architecture

The acronyms listed in Figure 4-4 are defined below:

APPL	User/agency applications
GW	Gateway
NEP	Network entry point
ACHS	Automated clearinghouse system
VAN	Value-added network
TP	Trading partner (vendor)
OSI	E-mail, X.400, X.435, X.500, FTAM
Internet	FTP, SMTP
PKI	Public key infrastructure

Each network that makes up the virtual network provides additional services such as addressing, file transfer, and security. The architecture will provide procurement offices with a means of exchanging data internally within the Federal government and with private industry trading partners with only moderate impact on installed systems. The goal is to free EC from proprietary agency systems over the long term and to

provide the capability to accommodate a wide variety of applications that meet the needs of the functional user. Acquisition-related applications and data are distributed across multiple sites. The government NEP maintains summary data, VAN agreements, and other capabilities, as well as connections to the VANs and trading partners.

This architecture is based upon existing and state-of-the-art technology that can be implemented in the next 5 years. In the future, agencies may use ASC X12 internally or at least be able to convert to ASC X12 transaction sets in the agency application systems. The evolution of this architecture, and agency migration to it, will depend upon business process changes, Federal agency cultural changes, and new enabling technologies that will facilitate the EC. Future efforts may also require the development of an architecture for EC activities that extend beyond the acquisition arena to logistics, finance, health, and other business areas that require interoperability. The target architecture is not simply a choice between a decentralized approach and a centralized one; it is a combination of the best aspects of both. Technology available today allows an EC architecture to accommodate centralized standardization of management issues and decentralized execution of processes.

COMPONENT FUNCTIONALITY

The major functions of the target EC architecture components are identified Table 4-1, which shows the functions provided by applications, gateways, NEPs, VANs, and trading partners. A number of different systems have demonstrated that the process identified in the December 1993 *EC/EDI in Contracting* report does provide the intended services. The functionality may be distributed at different locations and within different components depending on the implementation of the architecture. The order and the location that a specific function occurs is dependent on whether the transaction is initiated by the government's application or the trading partner application. Hence, the flow of transactions needs to be examined from both perspectives. The intent is to enhance the understanding of the architecture by providing an example and some supporting discussion of where specific functions of the architecture may be allocated.

Table 4-1. Transaction Flow from Government Applications to Trading Partner

Function	Agency Application	Gateway	NEP	VAN	TP
Input	Interface with internal agency management and financial systems and data bases	Flat file to provide data for ASC X12 transactions	ASC X12 transactions files	ASC X12 transactions files	ASC X12 transactions files or flat files
Process	Determine if current transaction is going to an EDI-capable trading partner	Translates flat file data into ASC X12 transactions files, transmits X12	Distributes ASC X12 transactions to VANs as required	Translate, address, and convert ASC X12 transactions to be compatible with trading partner and transmits it	Process data using trading partner application
	Generate the data elements for trading partner document/ requirement	Provide addressing information needed to route to NEP	Distribute data from departments needed to maintain single face to industry	Broadcast public documents via bulletin board	

	Prepare application data in format acceptable to translator		Provide any additional addressing needed to get to VANs	Send data to trading partner using required protocol	
	Help desk		Communications network control	Maintain help desk	
Archive	Archiving	Archiving and audit trails	Archiving and audit trails	Archiving and audit trails	Archive for audit
Security		Encryption and key management	Security boundary and time stamp	Decryption, key management, and authentication as needed	Decryption, key management, and authentication as needed
Output	Create a flat file of data elements	File of ASC X12 transactions	File of ASC X12 transactions	TP protocol	
Address: * SMTP or X.400	All transactions sent to nearest gateway	E-mail address obtained from vendor registration data base, X.500 directory, or local directory built from reply field of received transactions	E-mail address used to distribute transactions to VANs	E-mail address used to forward transactions to subscribers' mailboxes	
Address: * FTP or FTAM	All files sent to nearest gateway	ASC X12 address obtained from vendor registration data base, X.500 directory, or local directory built from reply field of received files	ASC X12 address used to distribute files to VANs	ASC X12 address used to forward files to subscribers' mailboxes	

***** With one exception, addressing is always in response to previous ASC X12 transactions and may be obtained from the reply field of the previous transaction. The one exception is broadcast transactions such as RFQs, which are always addressed from the Federal government to the bulletin board server where the trading partner accesses and retrieves the transactions.

Table 4-1 depicts the transaction flow from the agency application through the intervening components and ultimately to the trading partner. Specific transactions that are needed to update the common shared government-wide data bases have not been identified. These transactions are discussed in the business case sections which are dependent on these data bases. The table does identify different potential outputs based on implementation decisions. For example, security features are expected to impact the capabilities required at the gateway and trading partners. If the trading partner is dependent on the VAN to generate a machine-readable transaction from a fax document, then formal security mechanisms cannot be applied before the VAN. Tables 4-1 and 4-2 attempt to illustrate the flexibility in the architecture by identifying different alternative outputs.

Table 4-2. Transaction Flow and Processing from Trading Partner to Government Applications

Function	TP	VAN	NEP	Gateway	Agency Application
Input	Interface with internal business functions	Flat files or ASC X12 transactions files	ASC X12 transactions files or flat files	ASC X12 transactions or flat files	Flat files
Process	Generate flat files or ASC X12 transactions files	If required, translate to ASC X12 transactions, transmits X12	Provide required address information	Translate ASC X12 transactions files into format required by application	Use data to update government systems and data bases
	Use format compatible with VAN	Address transactions using NEP compatible protocol	Distribute transactions to internal gateway	Transmit X12	Notify personnel of action to take
		Format the data to be compatible with government applications	Distributes transactions to common data bases as required		
		Help desk.	Communications network control.		Help desk.
Archive	Archive as needed for audit	Archive as needed for restart and audit	Archiving and audit trails		
Security	Encryption, key management, and authentication as needed	Encryption or decryption and key management as needed		Decryption and key management	Decryption, key management and authentication as needed
Output	Protocol compatible with VAN	Protocol compatible with NEP	Protocol compatible with gateways	Protocol compatible with application	
Address: SMTP or X.400	E-mail address obtained from the data base built from the reply field of the transaction received	E-mail address used to forward transactions to Federal government mailbox	E-mail address used to distribute transactions to agency gateways	E-mail address used to distribute transactions to agency applications	
Address: FTP or FTAM	ASC X12 address obtained from the data base built from the reply field of the transaction received	ASC X12 address used to forward files to Federal government mailbox	ASC X12 address used to distribute files to agency gateways	ASC X12 address used to distribute files to agency applications	

Table 4-2 depicts the transaction flow from the trading partner to the government application. The functions performed by the components are somewhat different than those shown in Table 4-1 because the transaction flow is in the opposite direction. The intent is to clarify the total functional requirement by illustrating the flow of transactions in both directions.

SECURITY

The Federal government has emphasized the rapid expansion of EDI as an accepted business technology for participating in today's global market. EDI holds great promise for improving the quality and efficiency of Federal procurement. However, this technology will not be implemented in a risk-free environment. Government agencies must ensure that full consideration is given to the risk issues inherent in the use of computers and telecommunications to accomplish traditional paper-based administrative functions. Without an appropriate level of security and control, EC operation will be unreliable, and losses will be unnecessarily high. While EC systems must be protected against fraud and unauthorized disclosure of information, protection against accidents, errors, and omissions is equally important. Due to the increased processing speed of EC transactions, the cost to recover from the consequences of errors and omissions tends to be greater than with traditional business systems. Prompt, accurate, and automated detection of errors and omissions is an important requirement of EC systems.

The use of EC techniques does not necessarily increase transactional risk beyond that experienced in a paper-based environment. This is in spite of the fact that, unlike paper-based communications, electronic communications theoretically can be changed without a trace. However, relevant communications protocols such as X.400 and the evolving X12.42 and X12.58 standards themselves contain headers, password fields, and control information relevant to data protection mechanisms. These data protection characteristics, coupled with the speed of communication afforded by EDI, decreases the likelihood of successful interception of specific transaction sets. Deliberate modification implies that specific transaction sets are being targeted. In most cases, it would be quite difficult technically to locate a specific transaction set, intercept it, modify it, and then insert it back into the data stream without causing an error condition or otherwise having the modification activity detected. Viewed from the standpoint of potential threats, controls should make the cost of obtaining data greater than the potential value of obtaining or modifying the data. This is especially true within the simplified purchase process where the majority of procurement transactions (98 percent) within the Federal government fall below the $25,000 threshold. However, a small purchase order could have totals changed to exceed small purchase amounts if no check is performed. Controls available for data protection will be discussed below.

There are four requirements for the security of any process including the simplified purchase procedures. The following recommendations illustrate achieving these requirements in a paper environment:

- Confidentiality—ability to limit access to the information contained in a communication. This has generally been accomplished with some combination of security markings, envelopes, and trusted messengers (U.S. Postal Service, Federal Express, etc.).
- Message integrity—assurance that the content of a communication is complete and has not been changed prior to receipt. This is accomplished by a number of

features, the primary ones being those associated with the use of writing itself: inks that make erasure and alteration easily perceptible, salutations and closings that constrain the length of the message, and the size of the paper (form) that may limit the addition of text.

- Originator authentication—assurance that the communication originated with the named source. This is most commonly provided by the handwritten signature. The authentication purpose of the signature has two conceptual parts. First, it adds a degree of formality, increasing the likelihood of actual assent to the terms contained in the document. Second, it serves to identify the document with the originator, because signatures tend to be unique. In the simplified purchase process, these functions are served primarily by the use of preprinted forms.

- Nonrepudiation—stronger form of authentication that relates to the ability of a disinterested third party to reasonably conclude that the identified originator intended to be bound by the substance of the communication. Specifically, the originator cannot deny he sent the message, and the receiver cannot deny he received it.

The effectiveness of software security services is largely independent of the communication path selected. For example, confidentiality, nonrepudiation, authentication, and data integrity can be supported with equal facility by any of the above communication paths. Since centralized communication paths provide a common point through which all traffic must pass, they also provide a common checkpoint when maintaining an audit trail. Additionally, centralization helps to minimize the number of outside access points an agency must provide and thus reduces security threats from outside intruders. The level of security must be identified by participating Federal entities, supported by the architecture and appropriate controls put in place prior to initiating connectivity to EC. The successful adoption of any of the proposed message security measures (PEM, X.400 (1988), X.435, etc.) is dependent upon a national public key infrastructure.

Security services will need to be enhanced when other than small purchases are allowed; plans must be made for the transition to larger solicitations. NIST publication 800-9, *Good Security Practices for Electronic Commerce, Including Electronic Data Interchange,* provides guidance for developing and implementing security practices. Additionally, NIST publication FIPS 180 describes the use of a hash algorithm that does not involve encryption to verify the integrity of the message. A hash total is generated by the sender of a message and the recipient uses the same algorithm to generate a matching hash total if the message is unaltered. Intentional alteration of the message and the generation of a new hash by an intruder could defeat the purpose of the hash total. However, if the process is carried one step further with the recipient returning the hash total to the sender for verification, the risk of undetected alteration is significantly reduced.

Over the long run, if the system is expected to be economically feasible, a comprehensive security service must provide the capability for encryption with an automated key management system. The encryption capabilities should be common to all electronic transactions, not just ASC X12 transactions. The ability to use the virtual network effectively is dependent on the individual agency networks that form the virtual network providing a compatible approach to security. The specific security technology employed will be dependent on government-wide requirements and the proven technology available to those who are tasked with implementing.

There are security services that are necessary to support any user system. The principal security services can be summarized as follows: authentication, integrity, confidentiality, avoidance of service denial, and nonrepudiation. The ability to provide these services are dependent on the availability and utilization of specific mechanisms. While EC and electronic document interchange are dependent on these capabilities, many of these same capabilities are needed for any automated system. Specific requirements have been defined for sensitive systems in the Computer Security Act of 1987. Further, before any system can go operational, the designated security official must review and make recommendations to the appropriate management official regarding the system's operational readiness. Hence, if proper security is already being observed, then for most users, adequate security mechanisms exist to initiate EC application processing.

Since the system protection is dependent on passwords, passwords should be encrypted if they are passed over communications circuits. Table 4-3 shows the minimal expected mechanisms that should be implemented to achieve each of the security services.

Table 4-3. Initial and Minimum Suite of Security for EC Services

Security Service	Application	Gateway	Network Entry Point	VAN	Trading Partner	Data bases
Authentication	User ID; passwords and their encryption	User ID second passwords	Conformance with C2 level of security	User ID password		User IDs and passwords
Data integrity	Hash totals; hash total acknowledg-ment	-	Conformance with C2 level of security		Hash totals	Hash total;C2 level of security
Confidentiality	Management oversight	Management oversight	Restricted routing and address validation	Vendor agreements	Personnel practices	Read / write locks
Avoidance of service denial	Contingency plans acknowledge-ment		Contingency plans	Contingency, congestion control		Distributed data, contingency plans
Nonrepudiation (partial)		Time stamps, dedicated	Time stamps, dedicated	Time stamps, dedicated		

Security Service	Application	Gateway	Network Entry Point	VAN	Trading Partner	Data bases
		circuits	circuits	circuits		

The intent is to move toward an environment that is paperless. In such an environment, there will be the need to have digital signatures with a third party controlling certificates to validate ownership of private keys. Additionally, archiving of encrypted documents will require a public key environment. In some cases, where authentication is less of an issue, bulk encryption may be used. The intent is to avoid redundant security features. Hence, as the more robust and enhanced security features become available, the less capable features will be discontinued. Table 4-4 identifies the expected security features that will be operational in the 1997 time frame. However, advances in security technology could have a significant impact on the available security mechanisms for the future.

Table 4-4. Final Operating Security Features

Security Service	Application	Gateway	Network Entry Point	VAN	Trading Partner	Data Bases
Authentication	User ID; passwords and their encryption	Address validation	B1 level of security		User ID password	User IDs and passwords
Data integrity	Hash totals	Address validation	Conformance with B1 level of security	Hash totals	Hash totals	B1 level of security
Confidentiality	Encryption / decryption	Encryption / decryption		Encryption / decryption	Encryption / decryption	
Avoidance of service denial	Contingency plans	Contingency plans	Contingency plans	Contingency plans		Contingency plans
Nonrepudiation	Digital signature				Digital signature	

DATA BASES

Data base servers are needed to provide access to government-wide data bases. Some data may be restricted to government use only. For example, the government's EC acquisition system has two classes of data bases. The first class consists of public data that may be releasable to the general public through VANs; examples are the *Commerce Business Daily* announcements, RFQs, and contract award information. The second class consists of sensitive data that may be accessed only by the government contracting officers and staff. Examples of these data are notices of contract award, trading partner registration, response to RFQs, and private text.

Examples of government-wide data bases are the trading partner registration data base, which provides a central registration point for VANs and vendors with

appropriate access and a central repository for trading partner performance data, the wage determination data base to be maintained by the Department of Labor, and the master solicitation document, and Federal Acquisition Regulation (FAR) and FAR clauses data base to be maintained by the GSA. All of the public data may be either centralized or distributed as long as it need be updated only at one location. Most of the sensitive data will reside in the agency systems, but trading partner registration data must be accessible to all contract officers.

The use of EC for acquisition requires support of a number of data bases, as depicted in Figure 4-5. The following data bases have been identified for this purpose: trading partner registration, trading partner agreements, government-wide FARs, and agency-specific FAR supplements. In addition to these, data bases for EDI translation and for communication services are necessary. Data base services are discussed in Appendix K.

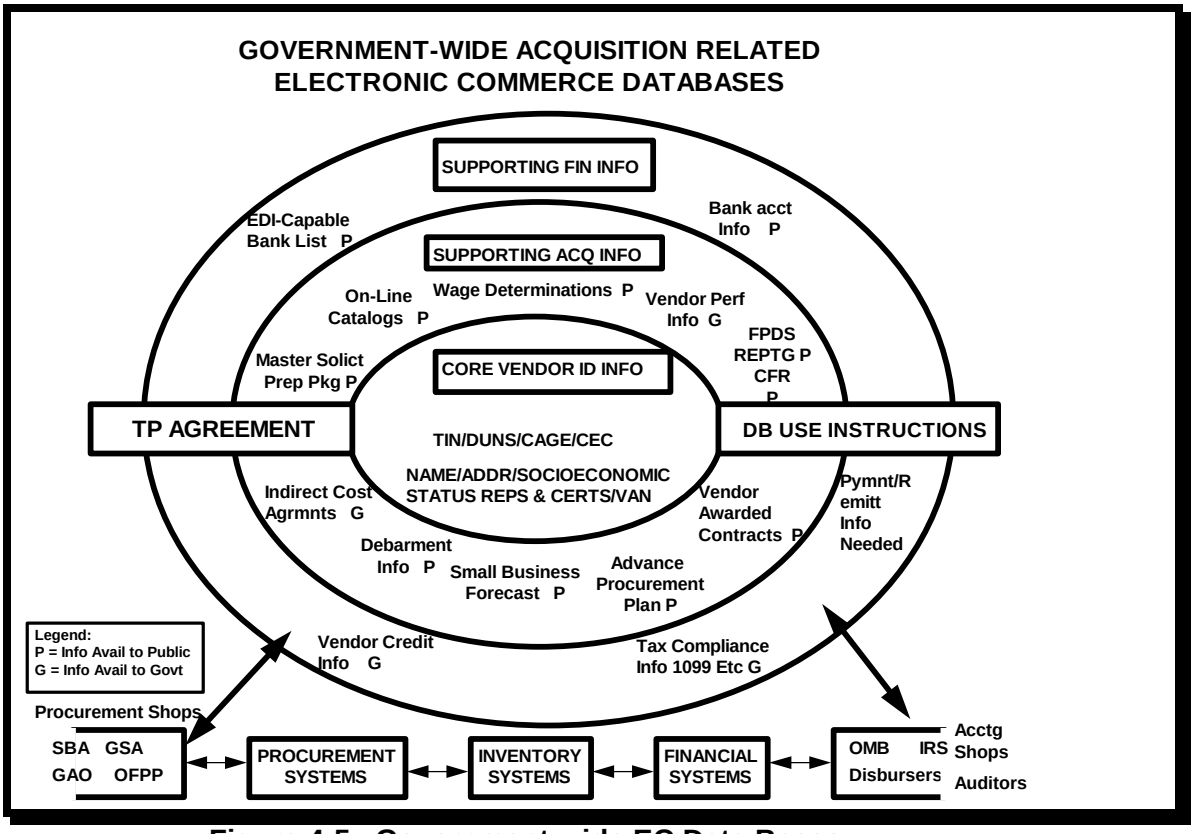

Figure 4-5. Government-wide EC Data Bases

RECOMMENDATIONS

There are a number of events and milestones that must occur before the widespread adoption of EC by the Federal government. Although several prerequisites have been or

can be met with relative ease, others depend upon the establishment of supporting infrastructure and the resolution of related policy issues.

Near-term requirements (now through 1995) include the following:

- Improvements in the support for the transport of EDI messages by interoperable E-mail systems. This is a two-part requirement: first, demonstrated interoperability of ISO X.400(88) implementations among themselves and with the Internet; second, the wider adoption of EDI message transport (X.435) over ISO and Internet transport systems. It is felt that the lack of a message store (and other shortcomings) render unacceptable X.400 implementations based on the 1984 recommendations.
- The work of the E-mail task force should be coordinated with the ECA-PMO. Both anticipate a government-wide message transport system that ties government agencies together, interfaces with industry, and provides connectivity to the public.
- Adoption of a naming and addressing structure that will ease the interoperability of the dominant message transport standards— Internet SMTP, ISO X.400(88).
- Adoption of a standard directory service capability, such as X.500, to aid in the interworking of existing E-mail systems. While existing proprietary E-mail systems (e.g., MS-Mail and Lotus cc:Mail) will remain in use for some time to come, future functional updates should include "directory user agents" that can resolve names and addresses using the distributed X.500 directory.
- Establishment of a "National Registration and Certification Authority" for use primarily by the private sector, but also for those agencies that are not large enough to have their own. In general, large agencies and those with special needs should be defining their certification policies and procedures now. It is recommended that an organization be franchised to perform this essential function and that it establish a “top-level” E-mail directory and the nucleus of the public key infrastructure.

Longer term requirements (1995 and on) include the following:

- Enhance the message transport systems to include security features (Internet privacy enhanced mail, ISO X.400/500 security entities). This includes X.435(91).
- Enhance the complex document transport capabilities in both systems to satisfy the needs of interpersonal and interprocess communications applications.
- Ensure the continuing improvement in the interoperability of various implementations. An implementation claiming conformance with a standard is not useful if it cannot interoperate with another independently developed implementation.
- Establish an internetting infrastructure to allow a seamless transport capability between established government and commercial networks.

The following solutions are for agencies implementing common shared data bases in the near and long term:

- Adopt distributed data, client-server architecture for the EC data base.
- Adopt SQL as the data base technology.
- Adopt an interagency rapid application development approach for the software development life cycle.
- Build or reengineer existing data bases to comply with NIST OSE standards. (See Appendix K.)
- Acquire DBMS SQL COTS products.
- Acquire COTS or develop interagency standardized API interfaces for front-end and back-end data bases access.
- Develop application software as a short-term technology for remote query and update.
- Establish a standard user interface and supporting procedures such that the user interface is consistent if not identical for all data bases.

SUMMARY

In summary, the technical architecture is the foundation used to support government-wide implementation of EC. The virtual network concept of linking agency networks, using existing capability, and phasing in implementation will enable the agencies to move incrementally to full EC capability as directed by the Presidential memorandum. For additional information, see Appendices H through M.