Federal Electronic Commerce System

Proposed by:
National Aeronautics and Space Administration

Draft Version: 1.09

March 31, 1994

Preface

White papers have been requested by the Office of Management and Budget which propose how Federal Government Departments and Agencies might deploy a common Electronic Commerce System as a means to streamline Federal Government procurement processes. In response, a telecommunication system's policy, a functional architecture, and an operational deployment plan are identified and discussed.

The system design is founded upon an open architecture which is standardized and scalable, and for which mature and established implementation technology exists from many sources. The architecture harmonizes electronic messaging, directory and electronic data interchange services with NII networking and security facilities.

The roles and resposibilities of various Federal Agencies are outlined and justified, and outstanding operational policy issues are identified for later detailed consideration. The USPS is proposed as operator of a massive National Certification Authority. A system profiling telecommunciations protocols and procedures to provide a workable solution to the problem of secure messaging which meets National Security is suggested.

Contents

Chapter 1

Introduction

In order to plan the development of the National Information Infrastructure (NII), executive Departments and Agencies have been requested to prepare White Papers which describe strategic and technical issues pertinent to important economic application areas. Responding to the recommendations of the National Performance Review, specific proposals for automated systems (and operational and deployment plans) have been requested for the Executive's own use of the information and network infrastructure for the purpose of Federal Government procurement.

The Clinton Executive Memorandum on "Streamlining Procurement Through Electronic Commerce", of October 26 1993, specifies the goals of an Electronic Commerce initiative and a timetable for the introduction of appropriate technology into Federal Government procurement systems. A management framework is laid out in which the President's Management Council, and the Office of Federal Procurement, will oversee the deployment and operation of a single, harmonized Electronic Commerce System (ECS) which exploits the emerging NII.

Heads of Agencies have been charged with producing concrete system and technology deployment proposals. These shall indicate how the ECS will be harmonized across all agencies by defining the capabilities, roles of each cooperating agency. They shall state the technical requirements which deployment of specific NII telematic services shall satisfy in order to provide an ECS, and give timescales associated with attaining given levels of service and coverage.

1.1 Executive Summary

The introduction of a trusted electronic mail infrastructure usable by society as a replacement for paper mail requires the solution of a number of technical telecommunications, security and legal problems. This draft White Paper responds to the Electronic Commerce (EC) initiative by proposing a set of requirements and a specific system design which exploits electronic messaging and Electronic Data Interchange (EDI) technology. Technical policy and standards for telematic service provision are stated, along with the analysis of the operational features of the appropriate National Information Infrastructure (NII) communications and security infrastructures.

The deployment of the NIIis a element of the Executive's program for the incorporation of advanced telematic services into the day to day activities of American business activities. The telecommunications policy formulated to direct and control the program aims to apply mature, standard, telematic services technology as a means, firstly, to reduce the cost of administering government and, secondly, to increase the competitiveness of American companies by increasing information flow – while lowering communication costs.

The EDI solution for mixed secure organizational and individual messaging assumes a national policy on implementing secure messaging over common carriers. The policy requires the establishment of an "Electronic Commerce Environment (ECE)." This messaging-application independent information sharing environment combines the infrastructure of the ECS with the commercial services of electronic messaging carriers. The result is a public secure messaging infrastructure in which connectivity between all players is ensured, whilst distributing operational management.

The secure messaging framework in the national ECE establishes a set of services and procedures which form a secure telematic association between arbitary electronic messaging users (voice, inter-personal, and EDI messaging applications). These associations are achieved through maintaining a well-managed security infrastructure (in which all the security and communication characteristics of the parties are described), rather than "on-line" interactions. The result is the electronic exchange of legally-admissable commercial documents.

The profile of requirements for specific telematic services used to fashion the interworking environment have been formulated having considered the need for: national coverage of the message handling environment, the body

of legislation and structures for regulation, national security and cryptography policy, the anticipated categories of messaging users, and the desire to institute a competition policy in the provider market place. In the area of controlling and empowering individual information privacy, the requirements respect the need for legally-empowered law enforcement authorities to intercept otherwise confidential information tranmission.

In the operational arena, it is proposed that the USPS provide public third-party service to the electronic messaging users who require public key certification, and identity management services. The USPS proposes to operate a massive database representing a national Certification Authority, in which authenticity of users will be guaranteed through utilization of the network of post offices and postal employees. A logical scheme for distributing authority is defined whereby internal communciation of Agencies need not use USPS facilities. Similarly a role for GSA is proposed. For certification involving State government and large corporations, where criticality is very high indeed, GSA procedures are expected to serve the more special purpose environments of high risk (but low sensitivity) messaging.

1.2 Scope and Intended Method of Use

The analysis addresses an open EDI-oriented messaging service, global management infrastructure, and operational concept upon which to found an open National Electronic Commerce Environment (ECE), combining eletronic messaging, and an Electronic Commerce System (ECS) providing value-added security services to uses of EDI messaging applications.

The purpose of the ECS is to enable the interchange of legally-recognised, revisable, commercial documents, between Departments and Agencies of the Federal Government, commercial Trading partners and individuals. The telematic, messaging and administrative infrastructure upon which it is based shall be a high-quality portion of the NII in which specific levels of service, protocol conformance, algorithms and procedures will be mandated.

The operational concept distinguishes between official, commercial and private messaging environments. The ECS addresses only the needs of official information exchange; detailed national policy for generalized commercial and mail-order electronic commerce services is not addressed. The presentation of issues shows, however, how the ECS is designed to develop into a

national EC infrastructure.

1.3 Paper Organization

The paper is organized to present two complementary perspectives on the architecture and operational concept of the proposed ECS: a top-down identification and justification of the policy issues used to constrain design choices, and a bottom-up presentation of how Agency responsibilities are categorized when operating or procuring the various technical and management procedures and processes.

Chapter 2

Overview

To deploy an effective National Electronic Mail infrastructure in which the statements transported and handled by electronic messaging procedures are legally recognized, a set of social, legal, political and telecommunications issues must be addressed. Accordingly, technical interchange recommendations and standards must be profiled for the specific information-processing environments which comprehensive messaging systems automate.

2.1 Service and Management Infrastructures

Three highly-distributed and deeply intertwined functional infrastructures are required in order to enable scalable, private, legally-viable, and confidential, and otherwise trustworthy, electronic message interchange:

Business EDI-message handling of origin-authenticated, official data, within government administration, commercial trading partners, and in the homes of individuals;

Messaging A reliable and predictable Message Handling and Transfer System, switching and transporting uninterpreted, private electronic messages between well-named official, organizational and residential service subscribers;

Assurances A regulated, legally-respected, set of large Trusted Third Parties (TTPs) providing value-added messaging security services to Federal government Departments and Agencies, organizational trading partners and

residential individuals: registration of official, commercial and personal names and identities, and non-repudiation of the acts and intents of the origination of message-based communication before a civil, criminal, or military court.

The requirements upon these infrastructures are characterized by a set of issues for which specific policy decisions are required. The discussion of each issue represents a major design decision point which shall govern how the Federal Government (NII) telecommunications and automated information-processing infrastructure will be organized in order to support the interchange of official messages required by Electronic Commerce.

Within the official messaging environment, it is anticipated that Federal Agencies will be engaged in providing or using the infrastructures identified above. A short presentation is made of the constraints faced by Federal Agencies with respect to OMB requirements on cost recovery, competitive practices, and upholding rights to individual privacy, when operating or delivering services. The purpose of this analysis is to highlight how the model ensures that the strategic framework can develop into a national, market-oriented scheme.

2.2 Operational Reponsibilities

Prepare an overview of how each of GSA, DoD/NSA, and USPS shall share responsibility; describe how the IRS, SS and FAA consume the service immediately. Show how commercial and private forces integrate to form a market.

Chapter 3

Electronic Commerce System Architecture

The ECS design is constrained by a set of requirements placed over each of the functional infrastructures. These represent prototype policy decisions on issues relevant to the creation of an ECS which would develop into a National infrastructure. The underlying competition, regulation, and security issues are legitimate subject for public review and comment.

3.1 Infrastructure Requirements

3.1.1 Business Issues

Commerce operates on the basis of a set of protocols enacted between players in the relevant market including offer, acceptance, delivery, payment and receipt. Each action is accompanied usually by the exchange of a message.

The vast majority of commercial markets do not require assurances that the protocols, or the messages interchanged, are especially secure, beyond the assurances which headed notepaper and regulated, public messaging services – such as the USPS currently provides. Systems of dispute resolution exist whereby recourse to law can be made when one party makes a contractual or tort claim against another.

Though specialized electronic transactions and precautions are necessary in some high-risk circumstances, the vast majority of transactions performed

using paper-based message exchange, may be catered for by open (secured) electronic messaging technology. (Open electronic messaging assumes that there is no particular, bilateral or "a priori" agreement between the parties to do business by electronic means.)

The issues for business practices are concerned therefore with integrating electronic messaging and security procedures into business adminstration procedures, as an enhancement to EDI practices already in wide-spread use. Whereas EDI interconnects business systems according to established commercial protocols, most current implementations perform transport of data using Value-Added-Networks (VANs). By careful integration, and use of security protocols, the added-value bilateral services of the VAN can be slowly replaced by secured, open messaging, when supported by a national third-party trust and identity registration infrastructure.

1. Environments

   The ECS shall operate in a number of messaging environments which classify message interchange according to the purpose for which it is used: official, commercial and private-individual.

2. Naming

   The transfer of official procurement information shall be conducted between officially-named Agencies and Departments, individuals and commercial organizations, using the services of electronic messaging common carriers. The naming architecture used in the official messaging environment shall be founded upon the existing civil naming and registration infrastructure, and official names shall be made unique in order to serve as personal and organizational identifiers.

3. EDI Messaging

   Official messages shall represent mixed inter-personal and EDI messages according to the requirements of CCITT F.435, as profiled for EDI transactions handlers and protocols in use today. The interchange of EDI Messages by electronic messaging shall be massively scalable (in the number of subscribers who may be addressed) and extensible (in the forms, types and encodings of commercial documents which may be reliably exchanged). The exchange of messages shall exploit robust

store-and-forward messaging, between multiple originators and recipients who may or may not have agreed previously to trade based on electronic message communication.

3.1.2 Security Issues

National Security is concerned with issues that characterise the appropriate use of cryptography for assuring privacy and authentication of official, commercial, and private information during transfer. For electronic commerce, existing cryptography policy requires extension. Policy must be drawn up to accommodate the distribution of authority amongst social groups to operate cryptosystems. Distribution must support the objectives and technical constraints of a trusted, electronic messaging environment, and be appropriate to the various purposes for which secured messaging is used.

1. Classification

   EC in the Federal government shall be conducted using telematic services and solutions available commercially, in order to achieve the goals of streamlining administration, and acheiving operational cost-reduction. This implies that procurement information transferred through the system shall be limited to "unclassified but restricted" sensitivity, and that NSA-defined "Class II" cryptodevices shall be applied to protect against fraud and loss of confidentiality. There is no requirement for the ECS to be "multi-level secure."

2. Algorithms

   The risks associated with the transfer and handling of the lower sensitivity levels associated with general-purpose procurement information shall be mitigated by protecting the information and the system using FIPS-based escrowed-encryption, digital signature and key distribution algorithms. The expertise of the NSA shall be exploited to reinforce public confidence in security protocols, and cryptosystem technology which shall ensure that the official messaging environment is protected against attempts at masquerade and authorized information disclosure.

3. Security

   The EC system shall ensure that all official messages faciliate the non-repudiation of message origination, based on a standardized security service provided by the electronic messaging environment. Official Trusted Third Parties shall provide services to Agencies and Departments, commercial organizations and residential individuals who opt to engage in official messaging. The procedures used shall assure communciation parties that digital signatures can establish the origin of messages in a non-repudiable manner, when presented to a judicial party.

4. Trust

   An official security infrastructure shall be deployed in the form of Official TTPs operated by Federal Agencies who have jurisdiction over assurance and naming services for the official activities of non-military Federal Government Departments and Agencies, government commercial trading partners, and residential individuals.

5. Security Domains

   The technical nature and operation of cryptographic keying and assurance procedures upon which public confidence in the security of cipher-protected information transfer depends requires that competent parties are regulating, administering these facets of the ECS. Within a given domain, certified and conformant technology and procedures will be mandated, and regulated to ensure that all due care and attention is paid to the management of crypographic material and technology.

6. Authentication Domains

   The ECS design is founded upon adoption of a risk-based segmentation of the messaging environment. The care and approaches used to assure that risks of security compromise are mitigated to expected levels depend upon the purposes for which messaging is used. The ECS calls for sharing of responsibility for operating economic sectors and subsector. For military information systems, the DoD and NSA shall operate the Defense Messaging System (DMS) domain, in which is located a national registry of all domains. For official messaging and information

systems, the USPS and GSA shall serve Federal Government Agencies and Departments, commercial organizations and residential individuals, according to the level of risk faced, where USPS shall orientate to serve the public and speciality markets, whilst GSA serves the larger "corporate" needs occuring between Federal Agencies, State governments, and large commercial organizations.

3.1.3 Messaging Issues

Messaging always occurs with a purpose. The risks associated with the communication reflect the importance of the information transfer, and the impact failure to communicate would probably have.

The switching of Electronic Mail between providers has developed into an industry, using a mixture of mature and experimental protocols and switching techniques, and wide variety of quality of services and tariffs charged in a competitive marketplace. To date, however, only three categories of wide-area electronic, switched, message handling service have been in evidence: Inter-personal memo exchange using RFC 822 or X.400 message switching networks, VAN based point-to-point messaging exchange between trading partners, and military versions of the SMTP mail protocols using secure, closed and managed IP networks.

1. Communication

   The official electronic message handling environment shall enable any (reasonable) number of individuals to communicate legally-binding information without the parties having ever previously inter-communicated, and without the messaging user being concerned with specifying routing paths through interconnected messaging networks.

2. Addressing

   The addressing and routing of mail transfer by carriers is to be handled separately from naming of parties, and many different addressing schemes are anticipated. All carriers of official mail shall have the capability to switch, represent and transport X.400 addresses, and handle RFC 822 (internet) Domain Defined Attributes.

3. Capabilities

The capability of a recipient to handle security is signalled by registering in the Directory entry for the named recipient a security certificate. Similiarly, attributes may describe the type of processing which the station is capable of performing in the area of bodypart handling, or word-processor transfer formats. Just as an OSI stack advertises to the world the services it is willing to offer, so then messaging UAs must advertise their capabilities. This includes statements as to the EDI transactions which a given UA is willing to handle, and the responsibilities which the automated processing is willing to assume.

3.2 Policy on ANSI X12 EDI

The NII shall be required provide a robust and reliable open electronic messaging service. This message transport service shall be provided by many different telecommunications carriers who shall operate interoperating Management Domains, and they shall use any appropriate network services. The mail service shall enable the tranport of different messages content types: for the purposes of EC within the Federal government and for use in official messaging, it shall convey X.435 messages. In order to exploit the installed EDI base in companies, the X12 format for representing information and transaction handling shall be used. Only the mandatory Kernel elements of service of the EDI Messaging Service are permitted, and the EDI protocol (P.edi) is not required.

1. Bilateral/Multilateral Communication

   The handling of EDI messages by the ECS assumes an open messaging infrastructure; the interchange of messages may occur between users who may not have engaged in prior acts of inter-communication. A trustworthy national scheme for naming organizations and individuals is mandated in order to facilitate the communication assurances formally provided for by bilateral agreements.

2. EDI Naming

   This shall promote simple and flexible naming of both organizational, individual and EDI Recipients. The registration and listing of names

shall exploit competitively-organized registration and directory services. EDI names shall exploit existing industry structures for assigning and distributing EDI identifiers; these shall be optionally represented in the directory as alias entries, though these identifiers shall not be used to directly address or name EDI recipients, and will not be certified by the ECS.

Chapter 4

Operations and Responsibilities

The following text has not been agreed by the USPS.

As a part of the deployment of a *National* Information Infrastructure, the USPS is proposing to operate a Public Key Infrastructure (PKI) which enables the secure interchange of inter-personal and EDI messages between organizational and individual messaging users. The ECS provides the value-added messaging "administration" services which enable subscribers to apply the security capabilities.

The PKI provides security and confidentiality for low-sensitivity, organizational and individual messages originating from a number of economic sectors: federal (or "official"), commercial, private, and military. The PKI does not address secure messaging requirements for handling information of secret (or higher) sensitivity; nor for life-critical applications.

The USPS proposes to operate the "official" messaging environment, and also to ensure the interoperability of secured messaging services across authentication domains. These include the Department of Defense, suported by the National Security Agency, which will manage the low-sensitivity miltary branch of the official infrastructure.

The ECS is the security administration component of the ECE. The EDI Messaging System combines the capabilities of a number of telematic service agents which facilitate the interchange of eletronic commercial documents via

the provision of services of mixed public and private management domains. The ECS is public, generic Information Technology solution which combines the EDI MS with a set of public-oriented security and assurance management procedures which reflect National telecommunications and security policy and NII deployment goals.

4.1 Scope of Agreement

In the area of national policy over low-sensitivity security in public telecommunications services, a split of operational responsibilities is required. There are existing Agencies who manage and control overall national security issues, policy and standardization. With the uptake of electronic messaging, there are also now administrative agencies who aim to deliver or use the envisaged national coverage of secured technology and services as part of their response to the National Productivity Review.

It is not the business of NASA, USPS, SSA, IRS, or FAA to be particularly involved in the higher elements of national policy on security. However, it is their responsibility, however, to demonstrate that they are commited to acheiving management and administrative change within their respective delivery of government services to the public as required by the Clinton Executive Memorandum..

Thus:

> The agencies agree that using joint means to demonstrate common commitment to applying secure messaging shall be the primary objective of an inter-agency collaboration. That, joint activities shall take the form of formulating common green paper and budgetary recommendations on using and deploying common-elements of telematic technology, and that proof of concept activities will be mounted to generate an actual inter-agency secure messaging infrastructure. The proof of concepts shall be designed as pilots which seek to introduce EC services into normal agency operations, and thus establish the viability and utility of the concept.

4.2 Agency Roles and Responsibilities

The following points delineate the roles and responsibilities each agency will pursue as a contribution to the joint programme.

1. NASA Space Act

   NASA shall transfer its experience in operating agency-wide, national and international telematic services to all operational agencies. It shall make available or otherwise introduce mature and appropriate commercial technology solutions which it has deployed within in own distributed centers, or assist with the evaluation of alternative proposed solutions from industrial sources. NASA shall not be a technology provider. However, it will provide limited specialization of existing mature technology which it uses for its own networked operations. Mainstream technology development, deployment and operations shall come from operational agencies.

2. USPS Operations

   USPS shall operate a Federal Certificate Management Domain and offer the ECS to register and otherwise manage the public keys of the each agency and its public trading partners, or members of the public. USPS shall be responsible thereby for operating the "official" messaging domain, whereby public organizations and individuals may transact business with Federal agencies.

3. USPS Federal Partnership

   The USPS shall operate as a Federal Adminstrative Directory Data Management Domain (ADDMD) – a common Directory management domain in which Federal certificates for officially-registered organizations and individuals from multiple (federal) Trusted Third Parties will be stored. USPS shall operate a TTP serving the public, and commercial organizations. USPS shall operate as the Federal X.500 ADDMD for publicly-available certificate listings. It shall use a combination of naming architectures, specified in accordance with the NADF SD-5 principles, in which it will exploit the existing database of residences, and the civil naming infrastructure. The Federal entries in the directory shall provide listings in which only certificates (and other minimal

search-oriented identification information) is stored. USPS shall not offer a public white pages directory service, though its X.500 Directory and Certificate Database shall be publicly available. USPS shall operate the "NADF CAN" as a public service. in order to guarantee the integrity and accuracy of the utilisation of the civil naming infrastructure by public X.500 Directory service providers.

4. USPS Non-repudiation Service

   USPS shall operate a Federal Trusted Timestamping Service, for any subscriber whose certificate resides within the Federal Directory Management Domain, and whose provider uses USPS Certificate Management Procedures for revocation. This service may be used to officially stamp messages, representing a non-repudiationnon-repudiation of origin statement assuring recpients that at the moment of official signing, there was no reason to believe that a fraud had been committed.

5. Agency-managed Certificate Domains

   USPS shall make available to any Agency its Federal certificate management technology in order that said agency may operate an agency-specific TTP (constituting a separate security and authentication domain) for internal individual communication purposes.

   Should the policies of the USPS official TTP and the Agency be in accordance, agency certificates may also listed in the Official Directory ADDMD. Such certificates shall be deemed to have been issued under the same Federal policies and offer the same assurances, enabling the USPS to offer the Federal Trusted Timestamping Service for agency-managed certificates.

6. IRS EDI mailbox

   The IRS shall specialise EDI technology which applies the ECS enviornment. This shall facilitate the exchange of ANSI X12 EDI messages via X.435 services operating over a variety of messaging and network transport providers including X.400. The IRS shall operate an organizational mailbox to which individal megssaing users may officially communicate Tax Return data with the IRS.

7. FAA SocialSec PatentOffice

Chapter 5

OMB Operating Requirements

The following sections discuss aspects of detailed policy of operations which have yet to be finalized. Each section responds to key parts of the OMB Circular No. A-130, which interprets statutory law governing the activities of the Federal Government, issues policy statements in each of the relevant areas, and requires agencies to follow procedures which ensure compliance with legal requirements.

As each of these areas have impact upon the documentation of the open architecture for electronic commerce, and upon the design and distribution of processes for implementing the system, further work is required to detail how the design requirements and how the operational concept all explicitely cater for each class of OMB requirements.

5.1 Security and Assurance

Under Computer Security Act 1987, NIST is empowered to set the technical standards, advise upon operatational aspects of training, propose regulations for, and perform evaluation of, the effectiveness of the system. Following recommendation that the concept and architecture proposed in this paper be advanced, refinement and details of the issues addressed shall need to be made to address the security and quality policy issues governed by NIST.

Furthermore, the set of controls established in Appendex III to OMB Circular No. A-130 over the deployment of Automated Information Systems, require the specification and documentation of the safeguards implemented

to assure that risks to the assets managed by information systems shall be quantified, and that known vulnerabilities to the security of systems and information be stated.

(NASA is already acting in collaboration with NIST to define its own procedures and technology for its internal individual messaging certificate management solution.)

5.2 Privacy Act Requirements

The Privacy Act of 1974, as interpreted for use by Federal Agencies in OMB Circular No. A-130 and appendices, requires that Federal Agencies recording or otherwise maintaining information about individuals shall undertake procedures and programs which demonstrate that the provisions of the Act are being met. In addition, agencies shall report to the Director OMB their activities covered by the reporting requirements of the Act.

In the deployment of the ECS, each agency, for whom responsibilities for recording activities are established in the context of the ECS, shall file an initial report on the nature and purpose of the recording activity, and also report annually on the detailed operational usage of processes which disclose information to the public about individuals.

Given the purpose of the recording and dissemination of information about indivuals in the context of facilitating electronic commerce using an open architecture, it may be seen as appropriate to obtain a waiver to the requirements of the Privacy Act. However, though a relaxation on the detailed requirements for monitoring coverage and use of such recording might be waived, it will still be necessary to demonstrate that safeguards are in place to prevent abuse of the facility.

5.3 Cost Accounting, and Cost Recovery

The nature of the ECS proposal is such that agencies will cooperate in the provision and use of the underlying telematic services, and will share responsibility for funding, resourcing and managing vital processes which shall ensure a single infrastructure is maintained.

Consequently, in line with the requirements of OMB Circular No. A-130,

a detailed business model shall be created which details how costs will be accounted for, and recovered. Arguments shall be made to demonstrate that cross-subsidy claims can be countered.

The expectation is that the ECS shall be operated as an independent cost and revenue center. The users of the service include both Federal and non-Federal groups. Accordingly, full costs of operation shall be recovered from Federal groups, and cost shall be recovered from non- federal groups in a manner consistent with OMB Circular No. A-25.

5.4 Competition and Monopoly

The ECS is required to demonstrate that the underlying concept promotes competition and does not entail a monopoly position. To the contrary, it has been demonstrated that the classifications of messaging domains, the structures relating Trusted Third Party certificate issuing authorities, and the separation of value-added infrastructure providers from carriers of electronic mail, represents a clear commitement to openness and a competitive market for a varaiety of value-added trust services.

Chapter 6

Conclusions

An architecture has been presented which exploits well-understood, scalable, enabling systems technology in order to provide a National infrastructure for Electronic Commerce. Practical management structures have been proposed, and management domains and information-processing environments defined to address real-world situations which require the combination of messaging, security, assurance, and interchange of business or EDI documents.

An operational concept has been elaborated which identified how various economic players can combine their activities to provide an integrated national service, whilst allowing a competitive marketplace, and a high degree of functional distribution and autonomous management.

In order to ensure that the specific needs of the Federal government are met, including the interchange of EDI between members of the public, and agencies, specific arrangements were made for the interchange of official EDI messages.

The model of harmonizing secured messaging and security management in the official, commercial and private-individual messaging environments, assurance-based trust infrastructure was contrasted against military models of security domain and integrity management. A two layer framework of Trusted Third parties was proposed, in which responsibility for identity registration is dispersed on the basis of the risks which each community is subjected.

In the absence of hierarchical jurisdictional authentication domain management, and in order to provide messaging users with a single, comprehensive, secured e-mail service, messaging users may exchange secure mail by

using the message origin notarization services provided by the Trusted Third Parties. This faciliates availability to all of authoritative non-repudiation of origin security services – required by judges when resolving business disputes.

The recognition of a very small number of national authentication domains provides for the connectivity of secure mail services, at various levels of assurance. Inter-domain secure messaging and legal- quality non-repudiation of origin security services are obtained through the notarization services of National Trusted Third Parties.

The proposal is justified by reference to the ease with which it may be introduced into existing social systems and mechanisms. Through maintenance of the roles of traditional players, automation and technology have been shown to upgrade the commercial messaging environment to faciliate legally-respected electronic commerce communicated through secured, electronic mail, without fundamentally altering social structures, yet expanding opportunity by meeting the challenges presented.

Index

ADDMD, 16
architecture, 4
assurance, 7, 10, 12
authentication, 9

bilateral, 8, 12

civil naming, 8
competition, 3, 7
conformance, 10
crypography, 10
cryptography, 9, 10
cryptography policy, 3

digital signature, 9, 10
DMS, 11
DoD, 6, 10
Domain Defined Attributes, 11

EC, 2, 4, 9, 10, 12, 15, 23
ECE, 2, 14, 23
ECS, 1, 2, 3, 4, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 19, 20, 23
EDI, 7
EDI, 2, 8, 12, 13, 14, 15, 17, 21, 23
Electronic Commerce, 1, 6
Electronic Commerce System, i
Executive Memorandum, 1, 15

F.435, 8
FAA, 6, 15

GSA, 3, 6, 11

infrastructures, 5
IP, 11
IRS, 6, 15, 17

judiciary, 10
jurisdiction, 10

key distribution, 9

law enforcement, 3
legislation, 3

market, 6

NADF CAN, 17
NADF SD-5, 16
Naming Architecture, 8
NASA, 15, 16
National Performance Review, 1
National Security, 9
NII, i, 1, 2, 3, 6, 12, 15, 23
non-repudiation, 10, 17
NSA, 6, 9, 10

Office of Federal Procurement, 1
Office of Management and Budget, i
official, 3, 8, 9, 10
OMB, 6, 24
open architecture, 3

operational concept, 4

P.edi, 12
PKI, 14, 24
policy decisions, 6
President's Management Council, 1
privacy, 3, 9
public confidence, 9, 10
public key, 3
public review, 7

registration, 8
regulation, 7, 10
RFC 822, 11
risk, 7, 9, 10, 11

sensitivity, 9
SMTP, 11
SS, 6
SSA, 15
streamlining, 9
Streamlining Procurement Through Electronic Commerce, 1

tort, 7
TTP, 5, 10, 16, 17, 24

user authenticity, 3
USPS, 3, 6, 11, 14, 15, 16, 17

VAN, 8, 11, 24

X12, 12
X.400, 11
X.500, 12, 17
X.500 ADDMD, 16
X.435, 12, 17, 24