An INTERNATIONAL STANDARD for the LABELING of DIGITAL OBJECTS

(A proposal for a Consumer Protection Act of Digital Products)

Viktor E. Hampel
Technical Advisor on Data Protection to Government and Industry
HAMPEL CONSULTING
1515 Jefferson Davis Hwy., Crystal Square Suite # 913
Arlington, VA, 22202-3312, (703) 413-8836
E-Mail: vhampel@attmail.com

Executive Summary

This report proposes collaboration toward an international standard for the commerce of digital objects. In the United States, it should derive its authority from a ***"Consumer Protection Act for Digital Products"*** patterned after the ***"Food and Drug Act of 1906 (21 USC)."*** This would bring under control the lack of accountability on the information highways with the help of an agency, similar to the Food and Drug Administration (FDA), mandated *"to develop administrative policy for the safety, effectiveness, and labeling of digital products, and to review and evaluate new applications of such products."*

It is now technically and economically feasible, and the enabling standards are in place for data authentication, protection, labeling, and safe conduct over open channels: *Digital* product labels in the structured header of a standard envelope would define the rights and powers of copyrights' holders, equivalent to the *visual* copyright notices on title pages of bound literary works and movies. Descriptive *digital* product labels would advertise their source and content, equivalent to the *visual* content labels on food containers mandated by the FDA. Certified digital signatures would bind this information in the header to the body of the object to assure its integrity, ownership, and use.

Registered Digital Product linked to the header with certified digital signatures	**Digital Signatures**	**Header Information** with digital labels

Missing is an agreement on the packaging and description of digital objects based on contents to assure their safe storage, retrieval, transport and use. This forces present electronic mail systems to encapsulate each object either as `unknown,' or to deliver distinct service for security and processing. Current work underway toward *enveloping and modularity in CALS*, a preferred *Cryptographic Application Program Interface (CAPI)* for cryptographic service API, and a standard *Message Security Protocol (MSP)* should be extended to digital objects in general, mindful of their legal implications for global electronic commerce.

President Clinton challenges us *to move in a New Direction and build Economic growth for America with Technology.[1]* Nonpartisan legislation toward this goal would harmonize the related efforts worldwide. Norms for global electronic trade would strengthen the interests of vendors and the rights of consumers. Agreement on a minimum, necessary and sufficient liability and accountability would deter counterfeiting, piracy, and increase trust among business partners. A ***"Consumer Protection Act for Digital Products"*** would also help to resolve the controversy over the constitutionality of legislation to reduce violence and indecency shown on television, Cable and Internet. Standards for labeling would allow consumers to make better informed decisions, to ***reject*** or to ***retrieve*** multimedia objects based on contents. *This retains our right to free expression, but gives us the means to hear and to see only what we want to know.*

Keywords: Digital products, enveloping, labeling, copyright, authentication, communication, decency, legislation.

Preface

It has taken 16 years, beginning in 1906, before the quality of **food and drugs** came under federal regulation with standards for their safe packaging and labeling to protect our *physical health*.

The protection of electronic commerce started with the Computer Security Act in 1987. But information technology is evolving so rapidly that we still do not know what we get when we pay for **digital products**, and find it difficult to help our children reap the benefits of audiovisual education without damage to their *mental health.*

1. Problems and Partial Solutions [2,3]

Work toward the national information infrastructure (NII) is progressing.[2] But the still uncontrolled growth of goods and services on public information highways like Internet, brings into doubt their suitability for business and profit. As television, computers, and communications merge, and compete for buyers of advertized goods, the lack of accountability and safety leads to large-scale illegal copying, fraud, a plethora of proprietary `secure' payment schemes, and concerns about the unbridled access by minors to adult material. Industrial espionage and the threat of information wars suggest the need for a fundamental solution.[3] The narrative below is meant to point to the root of the problem.

1.1 A Lack of Accountability on Public Information Highways

Some welcome the unregulated growth of information technology and credit it with the spectacular rise of a new industry. The entertainment industry stretches its limits, and computer products get sold without liability for their end-use. Software is still not `recognized' as a commercial product by the Uniform Commercial Code (UCC). Warranties promise *only* replacement when found to be defective, or not conforming with documentation upon receipt. All license agreements substantially include the following language:

> "... To the maximum extent permitted by applicable law, originators or suppliers of products disclaim all other warranties, either expressed or implied, including but not limited to implied warranties of merchantability and fitness of the software and its documentation for a particular purpose ...
>
> ... originators and suppliers are not liable for any damages whatsoever (including without limitation, indirect damages, consequential damages, and damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use or inability to use this product, even if originators or its dealers have been advised of the possibility of such damages."

Even security products to protect assets are being sold this way. Costs for product maintenance and loss of business are difficult to assess. Some estimate that the diminishing security of financial transactions by traditional means alone costs taxpayers more than $10 billion each year, in part due to skillful counterfeiting of financial instruments, the fraudulent reproduction of bank checks with magnetic toners on laser printers, net scams, and the compromise of credit cards or cellular phones. For 1995, the GAO reports some 250,000 unauthorized penetrations of unclassified Pentagon networks.

In the absence of federal guidance for a safe and interoperable electronic payment system, ingenious proprietary schemes promise safe traffic and payments over unsecured lines. [4] Developers of the future joint multi-function smart-cards for VISA, Master Card, and EuroPay, plan to keep their method secret.[5] Stored-value cash cards already competed successfully during the Summer Olympics in Atlanta. But anonymous sales with electronic-purse cards worry vendors of copyrighted material that is restricted for sale in the United States and Canada, because unknown buyers may be overseas and pose as fronts for illegal copying.[6] The Treasury Department is concerned about loss of revenues from sales in cyberspace, and about large-scale *anonymous* trans-border flows of funds.

In Europe, smart-cards are already used to carry personal insurance and medical information. But in the United States, the application of authentication tokens with memory is driven by incompatible domestic products and an invasion of foreign technology. For military service, the much needed replacement of the `dog tag' with a smart Personal Information Carrier (PIC), containing not only the name, rank, and serial number, but also training records, MOUs, security clearances, medical emergency data, etc., is stymied by the absence of a trusted cryptographic chip.[7]

1.2 Infringement and Piracy of Intellectual Property [8]

Intellectual property has always been difficult to protect. Under the law, copyright protection is afforded all producers and assignees for original art. But the transition of their representations from paper, to analog and digital notations has made possible indistinguishable replication.

Printed books and literary works are registered with the Library of Congress with the issue of a unique ISBN number that is dated and quoted on each title page. International copyright agreements serve the industrialized nations, but do not deter large-scale illegal copying of books in developing countries.

Analog audiovisual products now bring more royalties to the entertainment industry with protective marks on their audio and video tracks to prevent illegal copying on replay equipment equipped with the `Sierra Chip.' Predictably, clever minds found ways to circumvent this filter and numerous decoders get advertised by mail order for their use in the privacy of homes. Reports by the British Copyright Council to the Commission of European Communities, show alarming statistics of piracy. [9]

Digital products still get mass-produced as identical copies on cassettes and CDS for music, movies, interactive games, entire operating systems, and software like *Windows-95*. Microsoft Corporation has tried to reduce losses by holographic emblems on the *outside* of each package sold. But these external visual marks appeal to the integrity of buyers and do not interdict their illegal use. For each genuine copy sold, at least one copy is said to be made illegally. Recent surveys reported at last year's NISS conference, implied that 40% of software in U.S. businesses is pirated, and nearly 90% of all software used elsewhere.[10]

These losses of revenues from electronic publishing can be avoided, as was demonstrated already in 1990 by the U.S. Veterans Administration when it delivered the 2.3 million medical records of veterans to its field offices, encrypted and compressed, on one CD. The now patented technology packages the data together with its controlling application and boot records on identical disks. Distributors can unlock any of the data elements and processing commands when authorized or paid by the consumer. The technology utilizes entity-to-entity authentication with multiple keys over dial-up lines or Internet. [11] This type of electronic publishing eliminates the tedium of transferring large files by wire.

Derivative technology on high-speed networks, like ISDN, makes the sale of digital objects by wire practical and retains proof of ownership at the time of sale, by sealing into the medium the transaction parameters: Object name, Serial number, Seller-ID, Buyer-ID, time-stamp, etc. But, in the absence of a standard for enveloping and description, each digital product sold by demand online must be used with its distinct proprietary control program. ORACLE Corporation is using this approach.

1.3 Dissimilar Approaches for the Registry of Intellectual Property

To keep up with the number and complexity of digital objects, agencies responsible for the registry of intellectual property are switching to electronic filing and collaborate with contractors, industry and academia to develop disparate tools for object identification in support of their mission:

- Copyright Office Electronic Registration, Recordation & Deposit System (CORDS)
- Patent and Trademark Office (DOC/PTO)

CORDS is a recent initiative to automate the **C**opyright **O**ffice Electronic **R**egistration, Recordation & **D**eposit **S**ystem of the Library of Congress.[12] Started in 1993, it is planned to automate the registration of literary works and future hypermedia objects. Despite the practical applications of the standard general markup language, SGML, and its subset for hypertext, a new, more powerful meta language is envisioned with the help of academia. The future CORDS language is to be capable of locating compound objects stored on a distributed network by reference to their registered unique `handle' which defines its compound properties. No presumptions need to be made about the object or their location. The CORDS approach intentionally avoids issues of content. This is intended to make it flexible and extendible for registration and should permit the assembly and retrieval of very large and complex mosaics of registered hypermedia works for research and education. As to content, users will be expected to scan the retrieved objects with data analysis tools, or use additional meta constructs, similar to those for surfing on the World Wide Web. The Corporation for National Research Initiatives (CNRI) and the Interactive Media Association (IMA) provide support.[13] Applicants will use *Privacy Enhanced Mail (PEM).* www.cnri.reston.va.usa & www.ima.org

The Patent and Trademark Office (PRO) plans to speed up the processing time of patents from more than two years to one year, in order to cope with a 6% increase per year and 236,679 patents in 1995. After experimenting with a *proprietary* system developed in Visual Basic by the European and Japanese patent offices, the PTO is now converging on SGML. This will facilitate the effective use of Internet, because 40% of all patents in the United States are filed by foreign companies, and because 35% of patents are filed by 50 large companies and firms that already use SGML and the preferred *standard* markup language for the description of intellectual property.[14]

In the absence of an agreement how best to describe hypermedia objects, agencies spend their limited resources on their immediate needs, deferring to deal with the complexity of a unifying standard at later time.

1.4 `Indecent' Programming and Multimedia Technology [15]

Audiovisual programming with interactive feedback is an effective tool for instruction. First developed for military training and concurrent engineering, visualization in three dimensions leads to faster understanding and better designs. In schools, academia and industry, video instruction with feedback is complementing personal interaction with teachers and experts. Individual, computer-aided instruction is revolutionizing the historic education in classes.

The entertainment industry commercialized virtual realty in video games with spectacular effects. Some defend that vicarious experience relieves stress and is beneficial. But following the bombing in Oklahoma City, the FBI found detailed illustrated instructions how to assemble and trigger the type of explosive used. It had been freely circulated on Internet for some time. This prompted strong concern about the availability of antisocial and subversive literature, violent depiction of crime, and adult audiovisual material on Internet, cable, and television.

Minors are known to spend hours watching TV and playing interactive computer games each day. Parents find it difficult to stop their children from learning time and time again how to hurt, maim, rape, kill, and use drugs or alcohol to resolve conflict. Confronted with similar situations in real life, they react by reflex. This seems to be confirmed by the recent *"UCLA Television Monitoring Report." [16]* To date, all imitation crimes are said to have been settled out of court. Self-regulation by the Motion Picture Association of American (MPAA) has helped [17], but civic-minded observers point to a slide toward greater gore and progressively base and promiscuous programming by producers to retain their clientele. This is dispassionately documented by the movie critic Michael Medved as a war on traditional values in ***"Hollywood vs. America"***. [18]

For an objective assessment, the government contracted for an impartial, comprehensive study documenting the increase in violent crime during the last decade, and found: Arrests of juveniles are disproportionately greater for murder, rape, robbery and aggravated assault than ever before.[19] Attorney General Janet Reno responded by stating:

> *"What you see here is a road map to the next generation of crime. Unless we act now to stop young people from choosing a life of violence and crime, the beginning of the 21st century could bring levels of violent crime to our community that far exceeds what we have experienced thus far."[20]*

Congress included in its recent overhaul of the Communications Act the V-Chip and enacted provisions to restrict `indecent' exposure of minors to graphic depiction of violence, crime, and porn on television, cable and Internet. But courts upheld free speech as a guaranteed right,[21,22] further confounding the confrontation between Administrative policy and the needs of industry and consumers to benefit from electronic trade. [Table-1]

1.5 World Wide Concerns

Leading educators and law enforcement officials attribute the growth of frivolous crime worldwide to violent TV programming, extravagant interactive shoot-and-kill games, and comics which hold the attention of children and teach them how to inflict harm and kill with a laugh: *"Just point and click - Bang!"*

In the United States, sexually explicit movies can not be shown on television and Cable. US Code 18P 1462 and subsequent legislation prohibits interstate transportation of obscene material, with lesser intrastate restrictions. Violent and spectacular videos are consequently offered for sale or rent in local stores and get sold for broadcast overseas. Our country *is* the leading information society, but the entertainment industry is perceived as an inadvertent promoter of crime:

- Canadian regulators debated last year the adoption of a screening system against TV-Violence that would include `blacking out and filtering' offensive U.S. Cable channels in Canada during prime time.[23]

- President Mitterrand is quoted as not minding so much his young French generation to be infatuated with English-speaking videos, but being abhorred by the pollution of their minds, and the learning of reflex behavior that may lead to violent crime, torture, sex and drug addiction.[24]

- German prosecutors investigated this year whether CompuServe was violating pornography laws in Germany by making `indecent' resources on Internet available through its online service.

- The People's Republic of China announced earlier this year the intent to filter `perverse,' violent, and pornographic material from Internet at national interconnecting gateways.

- Islamic countries are attracted by western technology, but they are appalled by our uninhibited culture and its freedom of violent expression. They worry about the ill effects of uncontrollable MTV and rock music with anarchistic lyrics and seductive imagery upon their children.

- Russia and former adversaries are embracing democracy as a new and better way of life, but are critical of our permissiveness and corollary export of violent crime, allegedly as an unavoidable penalty of a people blessed with the constitutional guarantee *"of free expression to say and to show as they please."*

- General Agreements on Tariffs and Trade (GATT) came to a halt in Geneva during the recent deliberations when countries could not agree on uncontrolled export of U.S. broadcasts and videos. The issue was tabled.

Trying to explain these accusations, observers point to recent adds by foreign firms that advertise still greater doom and gore in their latest video games. They question whether losers of WW-II may have bought controlling interests in the U.S. entertainment industry to corrupt our youth, and thus to defeat us at home, if not in battle. If true -it is unlikely to work as planned: *The genie left the bottle and is taking global flight.*

1.6 Threats of Industrial Espionage and Information Wars [25]

Most commercial software is still being sold as a collection of dated files, named in a packing-list. Buyers have little assurance about their completeness and integrity. Once installed, the application depends upon other components, like the operating system, and perhaps firewalls. Even when object-oriented design constructs are applied, the attention of developers is likely to focus on interfacing and operability - not on integrity and security. This practice for software carries over into the design and fabrication of integrated circuits, components, and functional assemblies.

The United States is the world's largest consumer of electronic equipment and audiovisual products, of which 70% get manufactured in the Far East.[26] U.S. business and U.S. weapons depend on them. But dormant, known faults and embedded hostile algorithms in software, hardware, and integrated circuits can be triggered by remote controls to cause havoc and denial of service.[27] It will take time before critical ICs get equipped with unique identities to permit assured links to other components with certified entity-to-entity authentication that is no longer *bit*-sensitive.[28] For mission-critical applications, a new class of trusted, resilient systems will have to be invented. [29]

CIA Director, John M. Deutch, expressed these concerns in his recent public testimony to a Senate subcommittee, in June, when he urged Government and industry to prepare for cyber-warfare attacks on U.S. computers. Noting that military and civilian systems are highly vulnerable to such attacks, the Senate Governmental Permanent Subcommittee on Investigation was told *"we have evidence that several countries are developing the doctrine, strategies and tools to conduct information attacks. These warfare techniques could disrupt such critical services as utilities, air traffic, and finance, with very large onslaughts likely within a decade." [30]*

The recommendation of *The President's Commission on National Infrastructure Protection* is still awaiting approval. According to recent reports, President Clinton is expected to issue the executive order for a multi-agency commission, to plan a defense against cyber-wars by foreign governments and terrorists, later this year.

2. Emerging Standards point to the Feasibility of a General Solution

The ***Computer Security Act*** of 1987 was meant to correct some of these problems. In 1989, following the tests of public-key algorithms by DoD/OSD's PLUS program for the Protection of Logistics Unclassified Systems, we expected public-key standards and products to follow and serve some myriad needs. In 1990, we asked the *Computer Security Systems and Privacy Advisory Board* to hasten the process with a `comprehensive mapping' of *technical* and *legal* issues, e.g., those that are characteristic of *handwritten* signatures and *digital* signatures, to learn what must be done, and what can be done better. But it took four years of debate for the DSA to get confirmed, and a draft of legal issues for *"Digital Signature Guidelines"* can be ordered this year from the American Bar Association (ABA).[31]

Standards are a basic requirement of electronic commerce. All committees are at work to combine data authentication and encryption into an enabling technology system for simple and complex tasks. It is an arduous undertaking. The national and economic welfare of each country is at stake - and evil knows no bounds. New and simple solutions *will* rise, but for the problems of today, we have to use what we have. For the purpose of this report, we note the accomplishments, and recent recommendations of **CALS**, **NIST**, and **NSA** committees to **ISO** and **EDIFACT** for encapsulating, labeling, registering, and specifying a standard *Security service API* for *`Digital Objects.'*

2.1 CALS Standards for Enveloping, Description, and Authentication

CALS is a strategic approach for standardization, known worldwide as the standard for **C**ontinuous **A**cquisition and **L**ife-cycle **S**upport. It was initiated by OSD in 1984 at LLNL, in collaboration with 120 contractors, to prepare for the delivery of modern weapon systems.[32] Today, concurrent engineering and automated manufacture are the new goals. The requisite pooling of talent makes product integrity and communications security a necessity, and can no longer be pursued in isolation. In 1994, the Secretary of Defense directed the Department to save costs by releasing ***all*** U.S. *military* specifications to industry for the procurement of less expensive, *commercial* products with state-of-the-art technology.[33] The family of military specifications, embodied in Mil-Std-1840, now serves a global industry as the preferred system of standards.[34] (www.acq.osd.mil/cals/cals.html) [Table-2]

Enveloping, and universal classification of digital objects is the key to Phase-2 of CALS. The requirements stem from the early understanding that an integrated weapon systems data base would have to carry in digital form an object through its entire life cycle of design, analysis, manufacturing processing & planning, the ordering of spares, and online provisioning. These requirements are complemented by the need for technical and training manuals, maintenance instructions, automated manufacture, logistics, and support analysis. Objects get created only once, but are available to

hundreds of collaborators from government, contractors, and military components - with selective and time-dependent authorizations for access and use. Presentations of objects are unique collections of product data, enveloped and described by their preferred constructs. This approach may serve as the universal framework, for today's overlapping standards, to converge toward a common object architecture. http://arioch.gsfc.nasa.gov/wwwvl/de.html.[35]

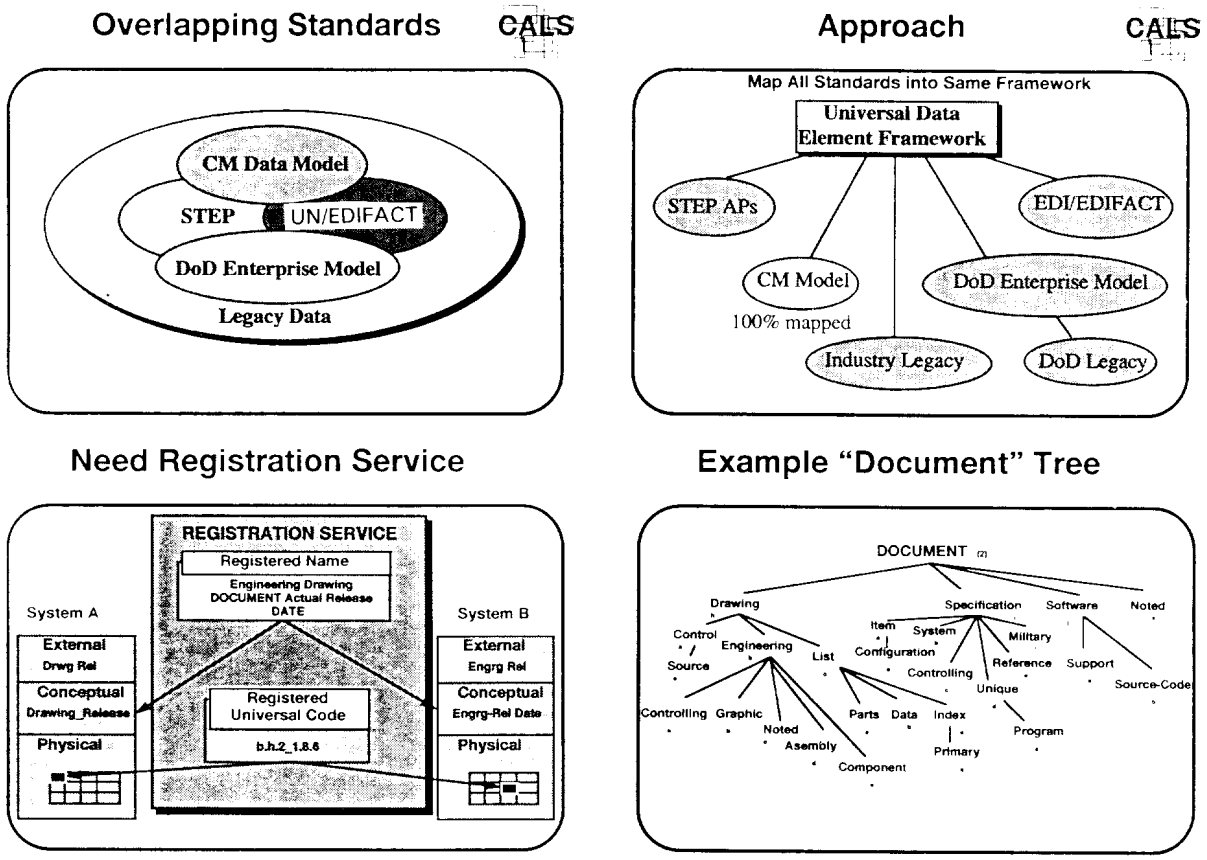


Fig.1 CALS Universal Framework for *`description and registration'* of Digital Objects

Description of data is critical. The CALS enterprise requires classification of objects, universal data dictionaries, translators, and interpreters for control procedures, capable of recognizing and removing inaccurate, untimely, and inadequate data, and equipped to add, revise, explain, and authenticate correct data. If one is unable to categorize data, one is unable to establish their complete unambiguous meaning.

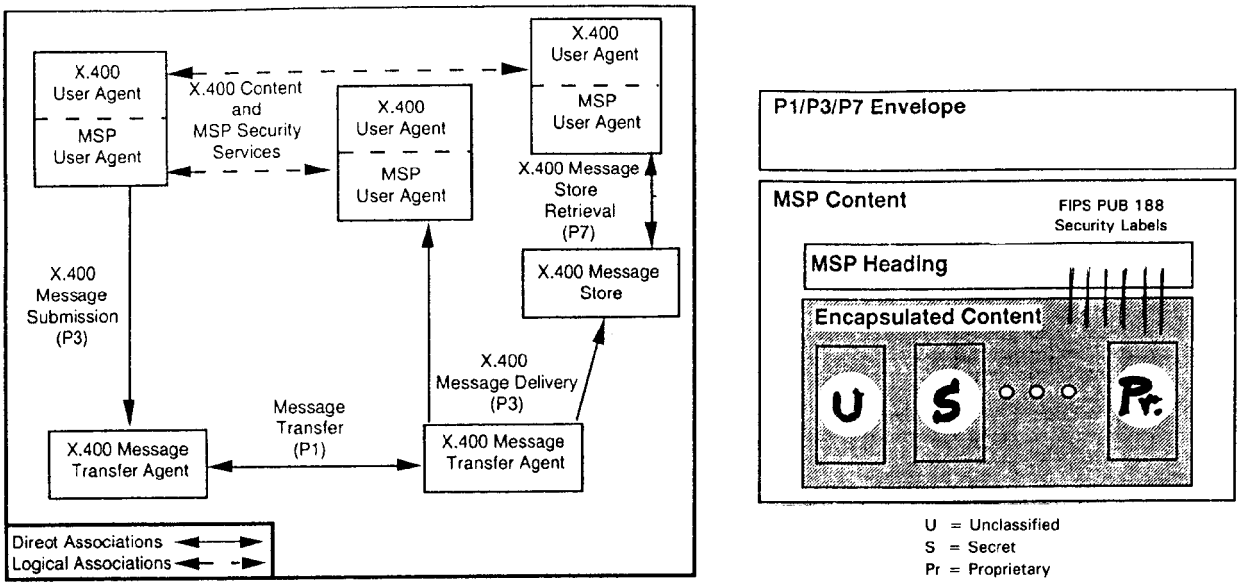
The results are impressive. The *PDES* product definitions exchange specifications are the cornerstone of CALS. *SGML*, the powerful CALS standard general markup language, led to the popular subset for hypertext markup, *HTML*, and *JAVA*, which permit cross-platform portability. Earlier this year, *JAVA* has been selected to give near-universal portability for the next generation of *WordPerfect*. The fusion of text, graphics, video, and audio now extends in CALS to the standards for photography and motion pictures, *JPEG & MPEG*.

Authentication has been added to Mil-Std-1840 in Version-3. It now includes digital signatures with ITU X.509 key certification, and was submitted by the DISA Standards Office to ISO for review.[36] Results of the modernization and standardization enterprise are being tested continuously on the CALS Test Network (CTN), headquartered at LLNL, and get reported at international CALS conferences and in committee work. The CALS enterprise and its approach to data manipulation have universal appeal, and enjoy global endorsement. In the United States, the OSD CALS office, NSIA, and CALS Resource Centers, transfer CALS technology to industry and vice versa. CSC and SRA corporations work with other contractors on security and pilot projects for DoD's joint CALS program, *JCALS*. **CSC**: Bob Hurwitz (609) 983-4400; **SRA**: Gene Cartier (703) 803-1734 (ftp://ftp.fedworld.gov/pub/cals-std/cals-std.htm) [34,36,37]

2.2 Message Security Protocols (MSP) for the Transport of Digital Objects [38]

The early availability of federal and commercial E-mail may explain in part why the need for a generic, universal packaging and description standard for digital objects did not arise earlier. Most E-mail products can attach or encapsulate digital objects and communicate cross-platform when compliant with CCITT X.400 protocols. But few provide inherent message security, and when they do, are *not interoperable.* (An exception are mail services empowered by *AT&T's SecretAgent* crypto system, which provides not only cross-platform inter-operability, but also multi-algorithm cryptographic operations in software (including the EA2 exportable algorithm), is substantially MSP compliant, adapted for SMTP secure mail transfer, and has transparent interfaces to a growing number of crypto-boards and authentication tokens, including Datakey's *SignaSure*, Spyrus' *Lynx*, Fisher's *SmartDisk* and *Watchdog*, Cordant's *NetAssure & PCAssure*, iPower's *Persona Card*, IRE's *Crypto-card*, or NSA's *Fortezza*, and can be embedded in applications with linkable object libraries and command-line interfaces.[39])

The need for writer-to-writer, secure and interoperable E-mail service over public networks, and the requirement to treat each encapsulated object with distinct levels of attention, led NSA to develop the *Message Security Protocol (MSP)* as the recommended standard for interfacing with the international *CCITT X.400 Message Handling System*. MSP is an integral part of the Secure Data Network System (SDNS) and is documented in SDN.701. Recent revisions of Version-4 permit any type of message to be sent and received securely, including the ITU defined X.400 Message Transfer System conventions for electronic data interchange (EDI), ITU X.12.58. Of particular interest for this report is MSP's capability for the secure **encapsulation** of *any* digital object as shown below:



Encapsulation of Digital Objects in the MSP Protocol

Until a universal, secure object description standard is developed, *secure encapsulation* is a viable alternative. We quote from SDN.701: The MSP user agent resides between the X.400 user agent and the X.400 message transfer agent, and X.400 user agents may be either distinctly or tightly coupled protocol entities. MSP is independent of the message content being protected and the user's message preparation system. The new content type, MSP, is submitted to the X.400 message transfer system. For message delivery, the recipient user agent may either form a direct association with the message security agent, or use a message store. This message store provides the information on delivered messages to support selective processing, including: connectionless confidentiality, authentication, integrity, access, control, and non-repudiation with proof of origin and delivery. The NIST Standard Security Label for Information Transfer, FIPS PUB 188, can be used to convey this information from the encapsulated object to MSP and X.400, as part of the *Minimum Interoperability Specifications for PKI Components.* The SDN.701 (V4) recommendations have been forwarded to ISO for review.[38,40]

2.3 CAPI, Security Service API, and Recommendation for their Extension to Digital Objects [41]

NSA's Cryptographic Application Program Interface (CAPI) recommendations go one step further. They express the urgent need for a general, unifying approach not only to the Message Security Protocol, but also to the prevailing cryptographic modules of commercial secure-mail products, and their integration with applications. Developed by NSA's Cross Organization CAPI team since last year for *Application Programs*, NSA's recommendations should be generalized to *Digital Objects*. The justification would read nearly verbatim like that given by NSA for CAPIs:

"Until recently, the integration of cryptographic functionality into digital Object Descriptions has required that developers tightly couple the *Object* to the cryptographic module. This approach forces each new combination of *Object* and cryptography to be treated as a distinct development effort, and does not provide for the modularity and maintainability expected of commercial products. An approach that can provide flexibility and cost savings is the use of a standardized *Cryptographic Object Description Interface (CODI)* suite. The compelling case for a modular cryptographic interface has given rise to the development of proprietary CODI proposals. An NSA cross-organizational team should be formed to assess the ability of these proposals to meet anticipated needs. A review of the CAPI criteria should be made as to their applicability to *Digital Objects* in general, leading to a detailed analysis and recommendation.

Rather than recommending a single *CODI*, the NSA team may find it appropriate to recommend several that could handle simple and complex classes of *compound objects* with needs for distinct cryptographic service of their subsets, similar to the proposal for the CAPI standards, GSS-API (Internet Engineering Task Force), the GCS-API (X-Open), CryptoAPI (Microsoft) and PKCS #11 Cryptoki (RSA), because these CAPIs had been designed to support significantly different levels of cryptographic awareness, ranging from minimal security needs to extensive requirements for the underlying cryptography. Criteria to be considered by the team to assess each of the predominant CODIs should also include: algorithm independence, object independence, cryptographic module independence, modular design and auxiliary services, MISSI cryptographic support, safe programming, and security perimeter designs."

Even though a CODI *suite* should address the needs of a wide variety of digital objects, it is anticipated that most digital objects and products will require minimal knowledge of the underlying cryptography. Therefore, to serve present and future needs, ***one*** high-level Generic Security Services *(GSS-ODI)*, and the extensions for independent data unit protection ***(IDUP**-GSS-ODI)* should be selected, just as ***one*** *IDUP-GSS-API* was chosen because it does not assume real-time communications between sender and recipient, and because it protects each object unit independently of all others in store-and-forward applications.[41] The NIST/PKI Project Teams generalize this approach in the initial outline of June 7, 1996, for the *Minimum Interoperability Specifications for PKI Components*, which includes identification and registration of objects for the *Federal PKI Trust Models*, that are independent of the mode of object transport.

2.4 ISO and UN/EDIFACT extensions to "Associated Objects"

In the meantime, this summer, UN/EDIFACT subcommittees have been authorized to update their syntax for "associated" data in Part-8 of the standard. This update is to provide a framework for more general data sets, capable of accepting unspecified digital objects, for which some allowance is made already in ISO 9735. This includes encapsulation of EDI standard transaction sets, with the X.12.58 data security structures. www.R3.ch/sjwg

Communications with committee members suggest that updates of standards ***react*** to market pressures. A ***proactive*** approach is needed for the proposed system of standards for the encapsulation of digital objects, their structures, content, need(s) for protection, and binding. Security and data labels could serve to transfer requirements for cryptographic service, and to the object transport service, similar to the approach taken by NSA for the recommended standardization of the *Security Service APIs*.[38,41]

Good electronic mail systems replicate and exceed the services of postal mail. Digital signatures can do more than handwritten marks. In retrospect, these implementations came about by trial and error. A deliberate proactive approach should be undertaken to map societal conventions for the delivery of goods and services to those expected from electronic commerce.[42,43] A Congressional initiative would encourage collaboration.

Summary Statement

Legislation for electronic commerce of digital products and their communications is inevitable because *digital objects* have to be bound and protected by *digital* means.

Standard digital labels in a structured header would protect producers, and give consumers the means to select, use, and pay only for products they need at work, approve for their families, or desire to see as adults.

A ***Protection Act for Digital Products*** would encourage collaboration. It should cover all aspects of electronic commerce and extend to communications, television, cable, and public networks. Consumers should be able to ascertain by recourse to the ITU x.509 public-key directory that an acquired object was genuine as advertised.

When *President Bush* was first briefed on this proposal in 1989, it was too early. Today, it is technically and economically feasible.[Table-3]

Supreme Court Justice Clarence Thomas, when he heard of this approach during an informal meeting, stated emphatically:

"This technology retains our right to say and to show - as we wish,
but it gives us also the means to hear and to see - only what we want to know!"

Postscript

The proposal for collaboration toward an international standard for the commerce of digital products was submitted in July to the *U.S. CALS Industry Steering Group (ISG)* and to the *CALS International Board of Directors [44]:*

- ISG Chair and CEO: *Lt.Gen. USAF (Ret) James A. Abrahamson* (202) 824-6015

- ISG/IPID Chair, Information & Process Integration Division: *Robert Kidwell* (304) 367-1699/135.

Table-1: Precedents for the Labeling of Consumer Products

All legislative powers to establish justice, insure domestic tranquility, provide for the common defense, promote the general welfare, and secure the blessings of liberty to ourselves and our posterity is vested in the United States Congress. The list below highlights some legislation, its implementation, and industry's response to public concerns about what we *eat, hear, and see*.

1906: The Food and Drug Act (21 USC 1-15), and its implementations by the Food and Drug Administration (FDA), now requires content labeling for foods, drugs, and cosmetics.

1922: Movie Production Codes are distributed with films made by the Motion Picture Association of America (MPAA) in a voluntary program to describe their content for the benefit of the viewing audience.

1968: Movie Ratings G, M, R, and X are introduced by the MPAA as better definitions to replace the rudimentary `production codes', as self-regulation in response to criticism by the public that some codes were unfit for children: R prohibits attendance of children *below* 16, and X *below* the age of 17. M soon changes to GP, and then to PG.

1984: The PG-Rating, requiring Parental Guidance, gets split into PG and a new PG-13, which suggests stronger Parental Guidance and recommends no admittance under the age of 13 years.

1990: The X-Rating gets upgraded by one year into NC-17: No Children 17 and under admitted. This is in response to the U.S. Supreme Court decision because of greater violence and crime in X-movies. States and cities receive some local controlling power. MPAA ratings get printed *externally* on video containers (of different colors), and are shown at the start, not during, movies containing indecent material unfit for children.

1992: Cable Television Consumer Protection and Competition Act of 1992, restricts indecency on Cable.

1994: The White House announces *Clipper* and *Skipjack* to protect voice and data, including key-escrow.

1996: The V-Chip to filter Violence gets added to the revised Public Communications Bill by request of President Clinton. MPAA representatives promise implementation in TVS and desktops within a year.

The Communication Decency Act (CDA), restricting indecency on Internet, was ruled in June by a three-judge federal court in Philadelphia to be unconstitutional, because *technology* of Internet did not allow people who post information, to control who may receive it. The Justice Department is appealing.

The Cable Television Consumer Protection and Competition Act of 1992, restricting indecent programming on Cable, was ruled in June by the U.S. Supreme Court as unconstitutional in part: Cable providers may refuse indecent programming (*sexually explicit or patently offensive*) on leased channels paid for by independent programmers, but may *not* refuse to air indecent programming on public access channels, when requested by local governments and educational organizations. (E.g.: Information on AIDS, Abortion, etc.)

FM-side band labeling and control get started as a voluntary technology to label different radio broadcasts, and their associated advertisements, tailored to different `classes' of listeners with perceived needs and means.

The Platform for Internet Content Selection (PICS) is a control product by MIT's WWW-Consortium (AO, CS, Prodigy, etc.) for providers to label resources so that parents can exclude them with PICS products. www.w3.org/pub/WWW/PICS/. Some sites require credit card numbers or `adult' PINs.

A draft standard for Key-escrow of stronger exportable encryption is promised by NIST/CSL to help resolve the debate between federal agencies and industry on *"Cryptography's Role in Securing the Information Society."[3]*

As television and telephony migrate to ***digital*** *broadcasting*, ***digital*** *controls* should become technically and economically feasible, utilizing technology developed for the communication and control of ***digital*** data.