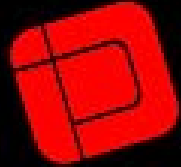




**ID**CERTIFY

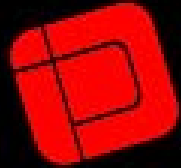


IDCERTIFY

- 
- **Digital Signatures and  
E-Commerce**
- 

**Presented by: Linda Mackintosh to  
Wyoming Chapter of ARMA International**

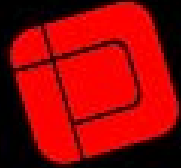
- 
- February 10, 2000**



ID CERTIFY

## Agenda

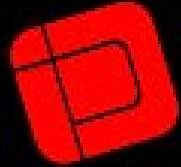
- |                           |   |
|---------------------------|---|
| <i>8:00 – 8:25 a.m.</i>   | <i>Registration</i>                                 |
| <i>8:30 – 10:00 a.m.</i>  | <i>Electronic Commerce – Where Are We Going?</i>    |
| <i>10:00 – 10:30 a.m.</i> | <i>Break and Vendor Exhibit</i>                     |
| <i>10:30 – 11:45 a.m.</i> | <i>The World of PKI</i>                             |
| <i>11:45 – 12:55 p.m.</i> | <i>Lunch</i>  |
| <i>1:00 – 2:30 p.m.</i>   | <i>Creating a Digital Signature and Certificate</i> |
| <i>2:30 – 3:00 p.m.</i>   | <i>Break and Vendor Exhibit</i>                     |
| <i>3:00 – 4:30 p.m.</i>   | <i>Consumer Concerns<br/>Questions and Answers</i>  |



**ID**CERTIFY

## **Who We Are**

- **Established in 1997**
- **Licensed Certification Authority headquartered in Seattle, WA**
- **Enable secure electronic business communication in a mode that assures the identity, authority, integrity and non-repudiation of the transaction**
- **Applications are tailored to specific business needs to replace, enhance or integrate effectively with existing paper-based processes**

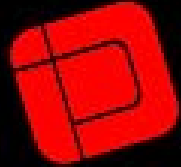


IDCERTIFY

## Part I

# Electronic Commerce – Where Are We Going?



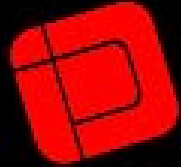


**IDCERTIFY**

## **Market Dynamic**

**“For any business, large or small, not to have an E-commerce Strategy is a big mistake.”**

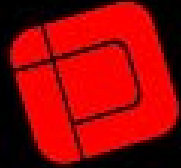
**William Daley  
Secretary of Commerce  
February 8, 1999**



**ID**CERTIFY

## **E-commerce Barriers to Entry/Challenges**

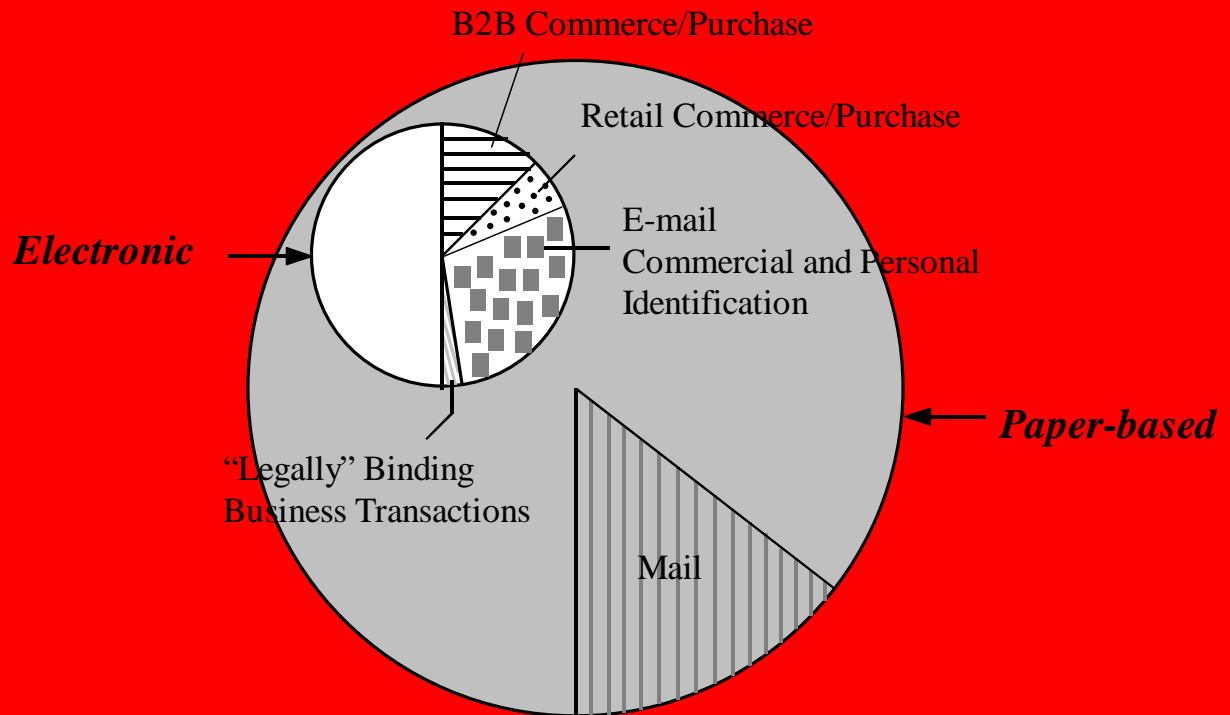
- **Multiple platforms for interoperability**
- **Lack of effective and trusted payment mechanism**
- **Convergence to paperless medium**
- **Inability to identify sender or recipient of message**
- **Lack of standards**
- **Lack of binding legal signatures**
- **Relatively unknown advertising medium**

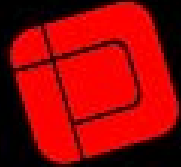


IDCERTIFY

# Market Dynamic Paper-Based vs. Electronic

**TODAY**



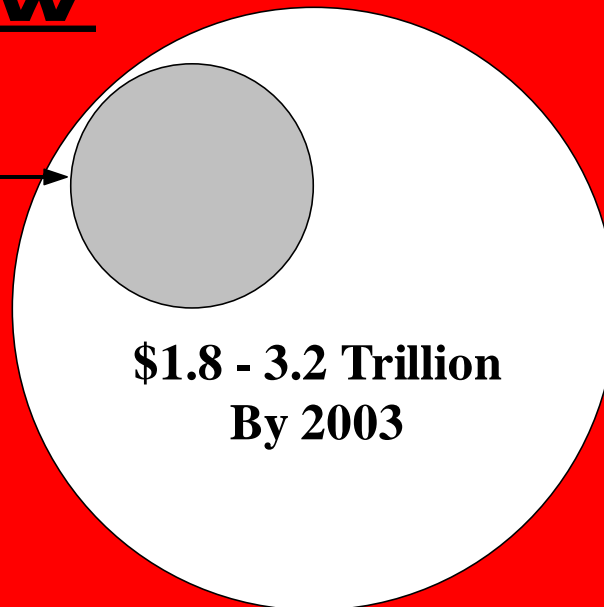


IDCERTIFY

# Market Dynamic Paper-Based vs. Electronic

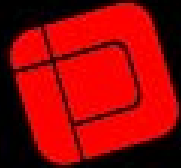
## TOMORROW

*Paper-based Processes*



**\$1.8 - 3.2 Trillion  
By 2003**

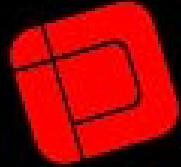
*Electronic Marketplace*



ID CERTIFY

## Market Pressure

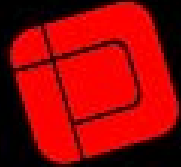
The Internet is not only the new market place, it is also the new market medium for **information exchange**.



**ID**CERTIFY

## **Market Dynamic**

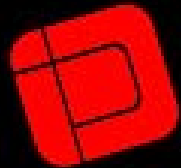
- **E-Commerce Growth (Forrester Research 12/98)**
  - \$ 43 Billion in 1998
  - Between \$ 1.8 - \$3.2 Trillion by 2003
- **Numerous Drivers**
  - Government Mandate & Legal Exposure
  - Business Initiatives
  - International Phenomenon



**ID**CERTIFY

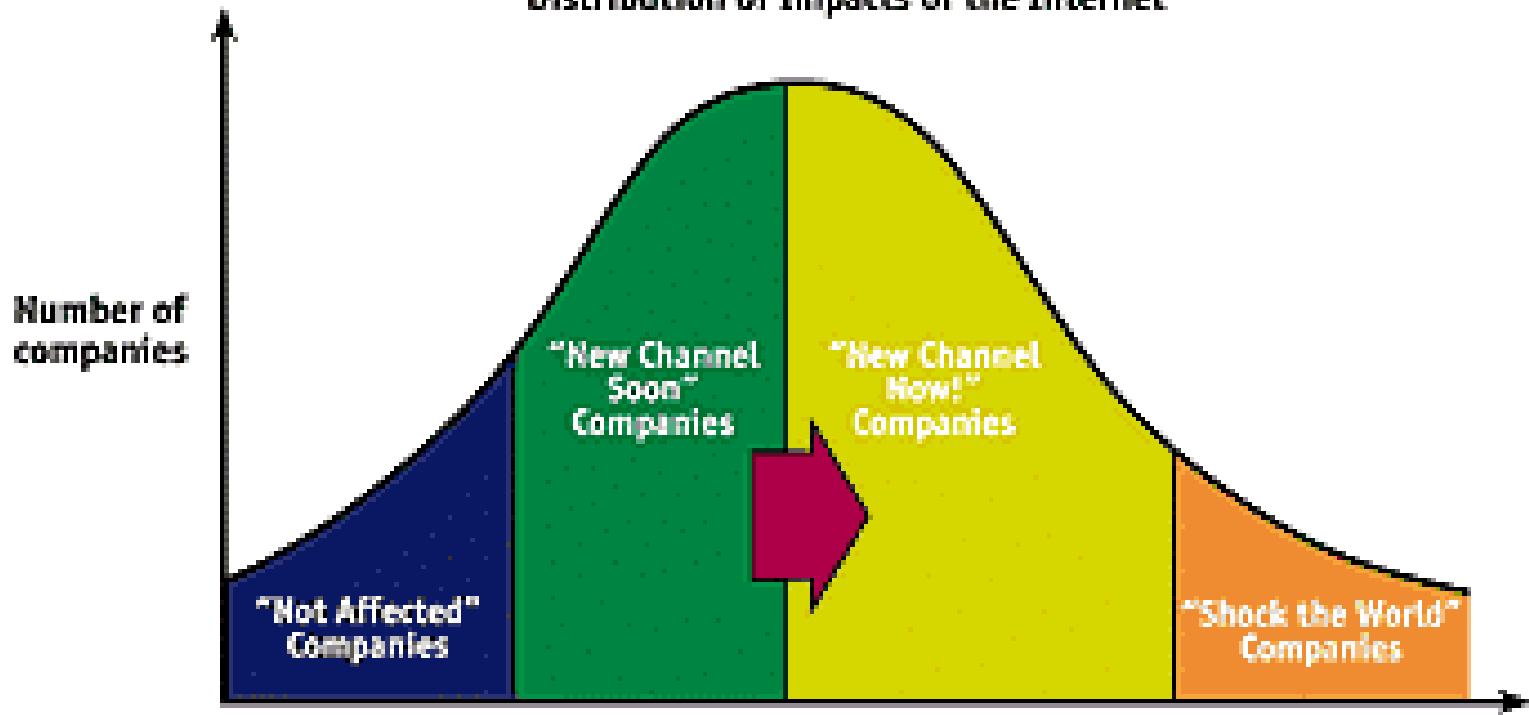
## **Market Dynamic**

- **40% of U.S. Companies are currently engaged in E-Commerce**
- **On-line purchasing (B2B) has increased from 19% in 1995 to 27% in 1999**
- **80% of companies using Intranet applications have seen a 38% annual return on investment**



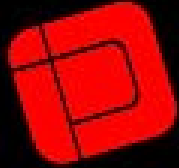
IDCERTIFY

### Distribution of Impacts of the Internet



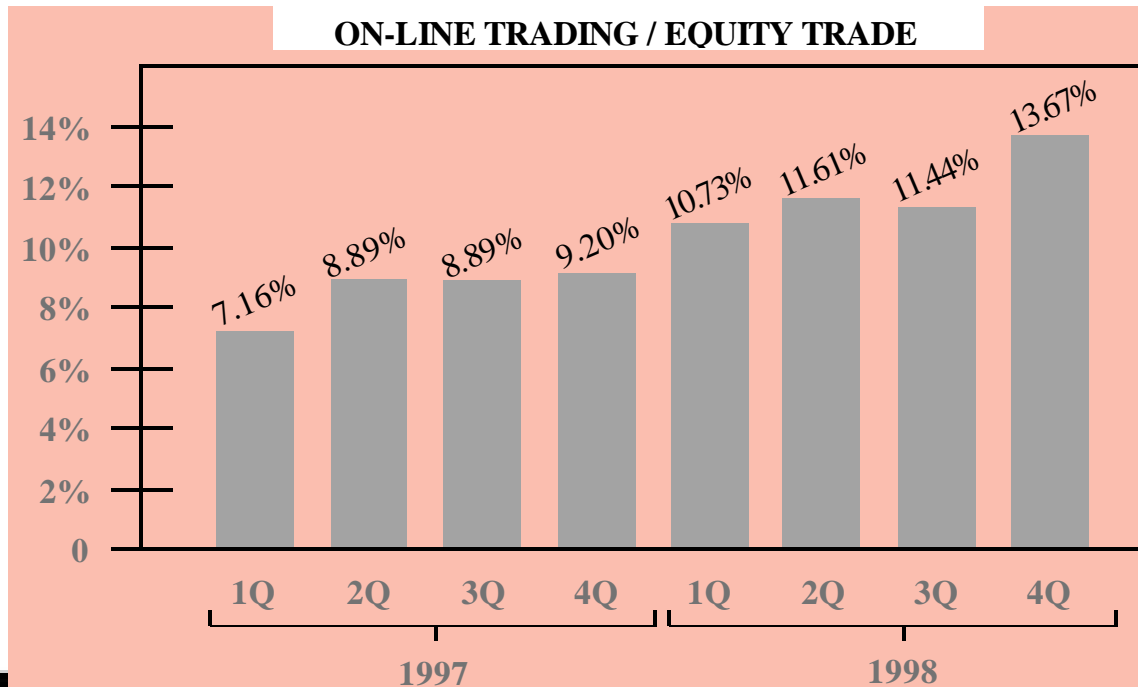
ITGOGO (1) DL002 - 2/98/NY.R

Source: Booz\* Allen Hamilton

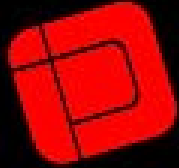


## Market Dynamic

- E-Commerce is re-engineering how business is conducted:  
On-line trading now accounts for 14% of all equity trades

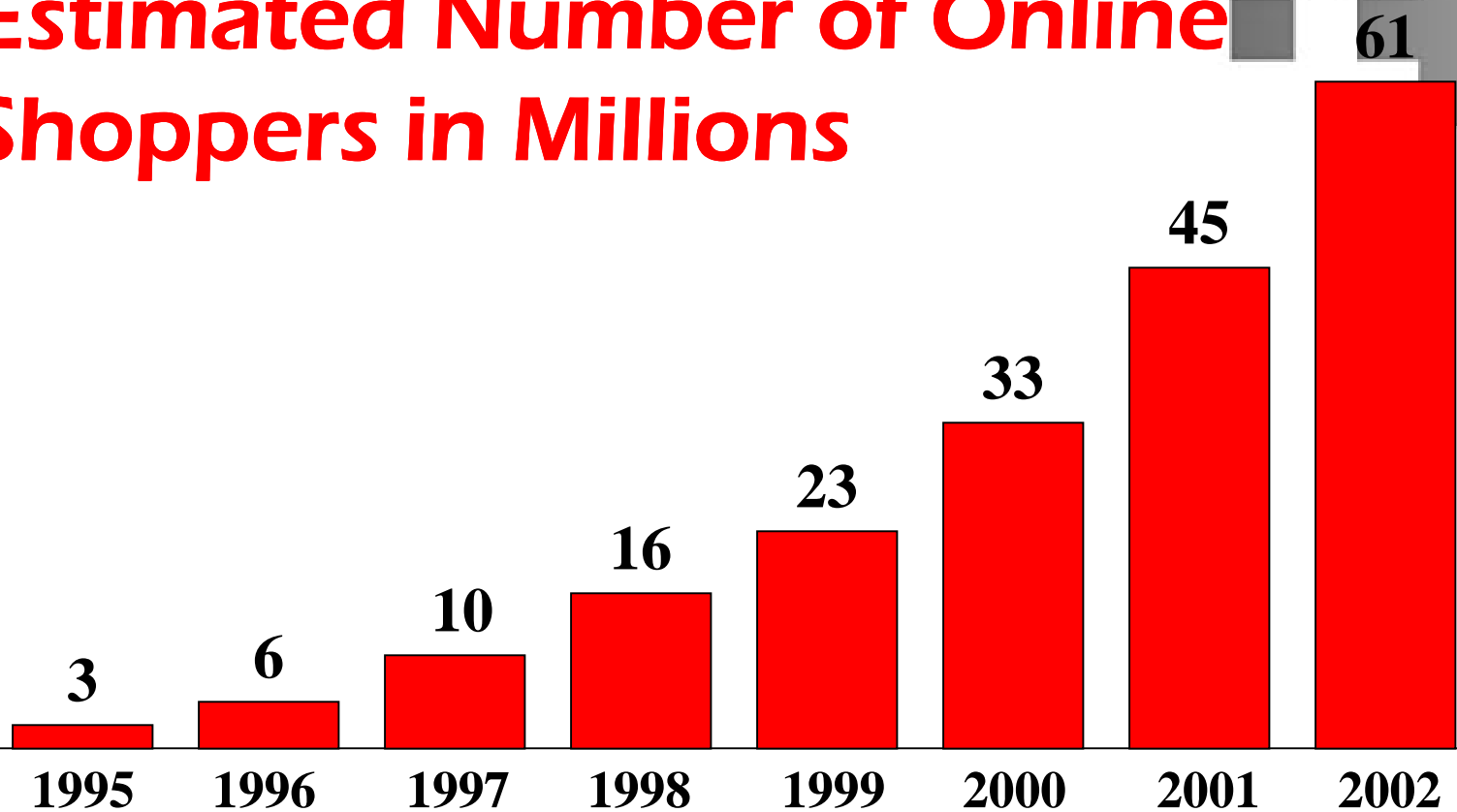


Source: Credit Suisse  
First Boston



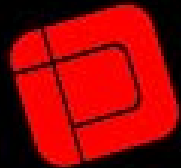
IDCERTIFY

## Estimated Number of Online Shoppers in Millions



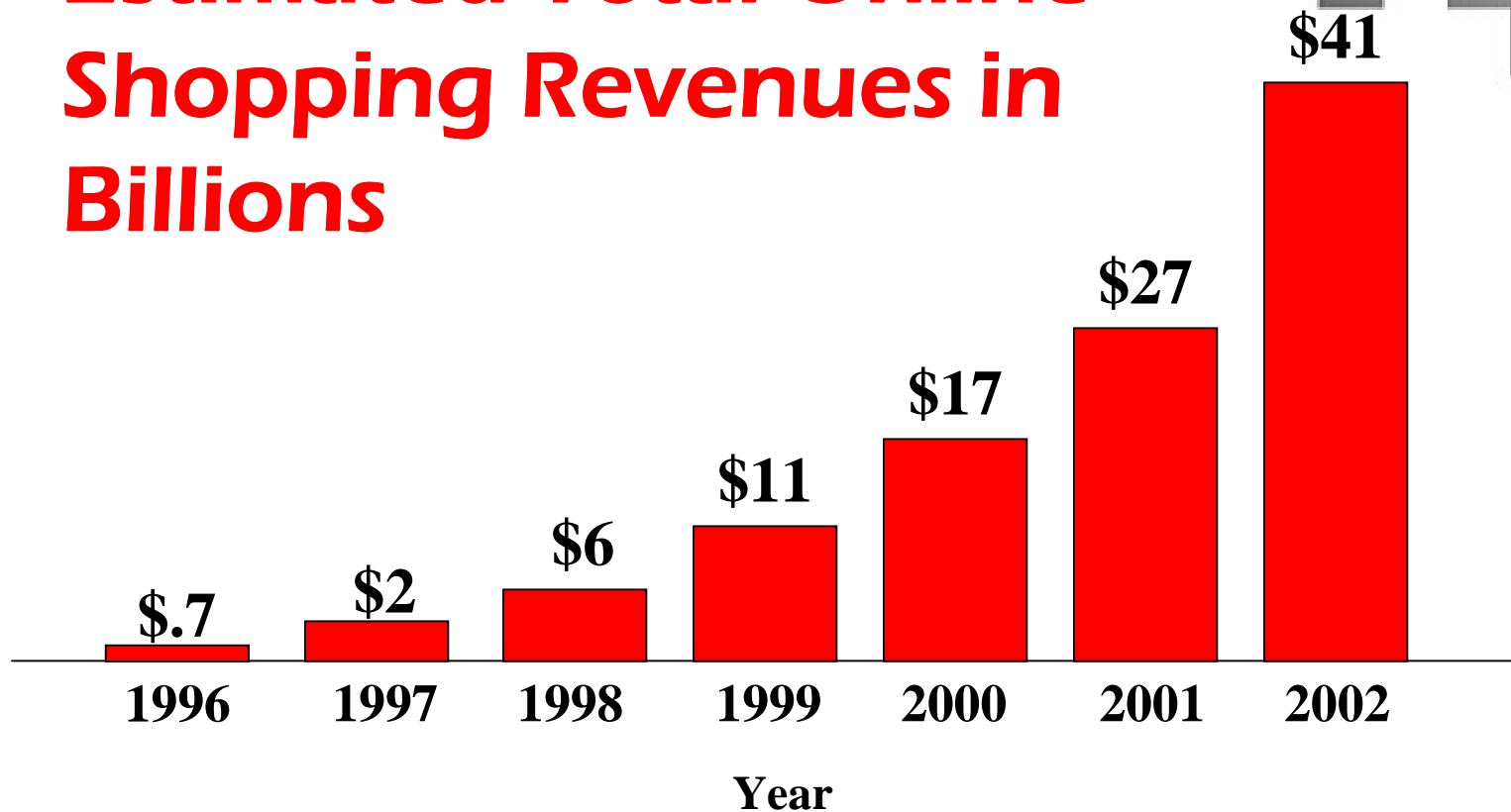
Year

Source: Jupiter Communications

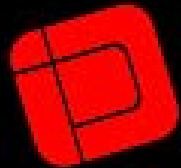


IDCERTIFY

## Estimated Total Online Shopping Revenues in Billions



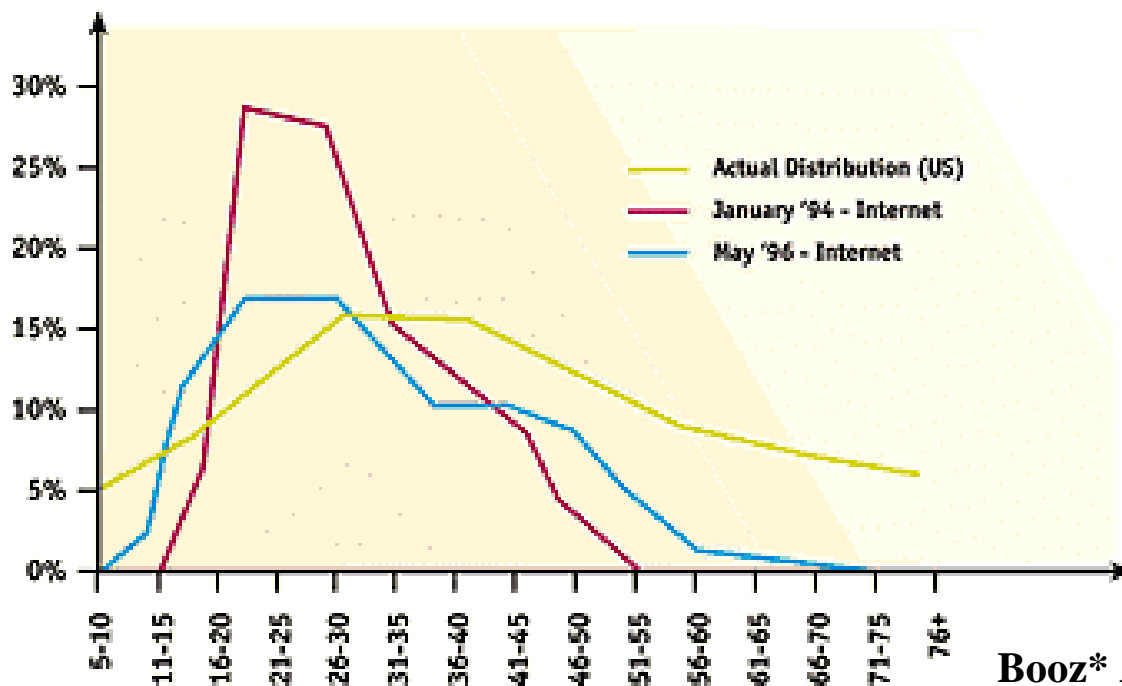
Source: Jupiter Communications



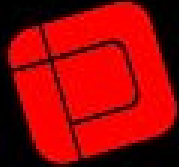
IDCERTIFY

## The Internet is Migrating Into the Mainstream

Age Distribution



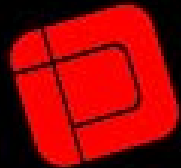
Source:  
Booz\* Allen Hamilton



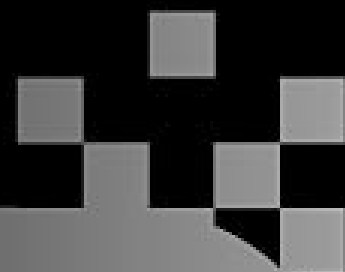
**ID**CERTIFY

## **Impact of Internet Growth**

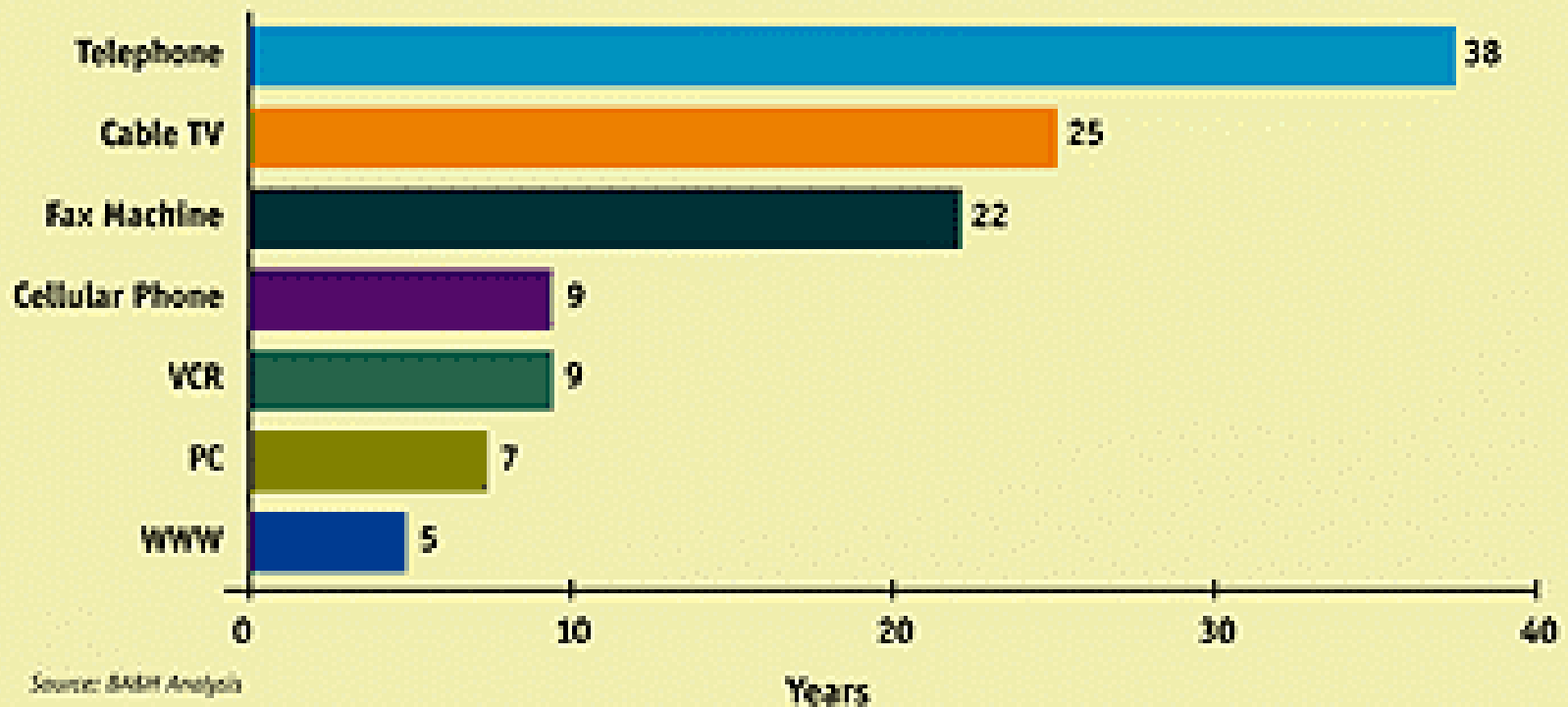
- **Supply chain of communication services is shifting**
- **In 1995, personal computers out sold televisions for the first time in history**
- **Explosion of retail and B2B E-commerce applications has dramatically escalated adoption of internet as transactional medium**
- **E-mail utilization has more than doubled since 1996 to over 130 million users**



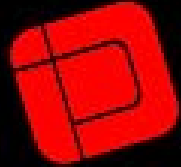
**IDCERTIFY**



### Number of Years to Reach 10 Million Customers (Mass Market)



Source: Booz\* Allen Hamilton

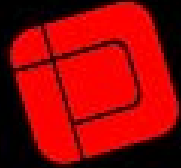


**ID**CERTIFY

## **The E-commerce Revolution Is Here**

- **Unforgiving to slow adopters**
- **Where market share is king**
- **Where experience will beat image in attracting the virtual audience (Source: M. Modahl - Forrester Research)**
- **Where members must be given the tools necessary to wield their own power (Source: Net Gain)**





**ID**CERTIFY

## Part II

# **The World of PKI**

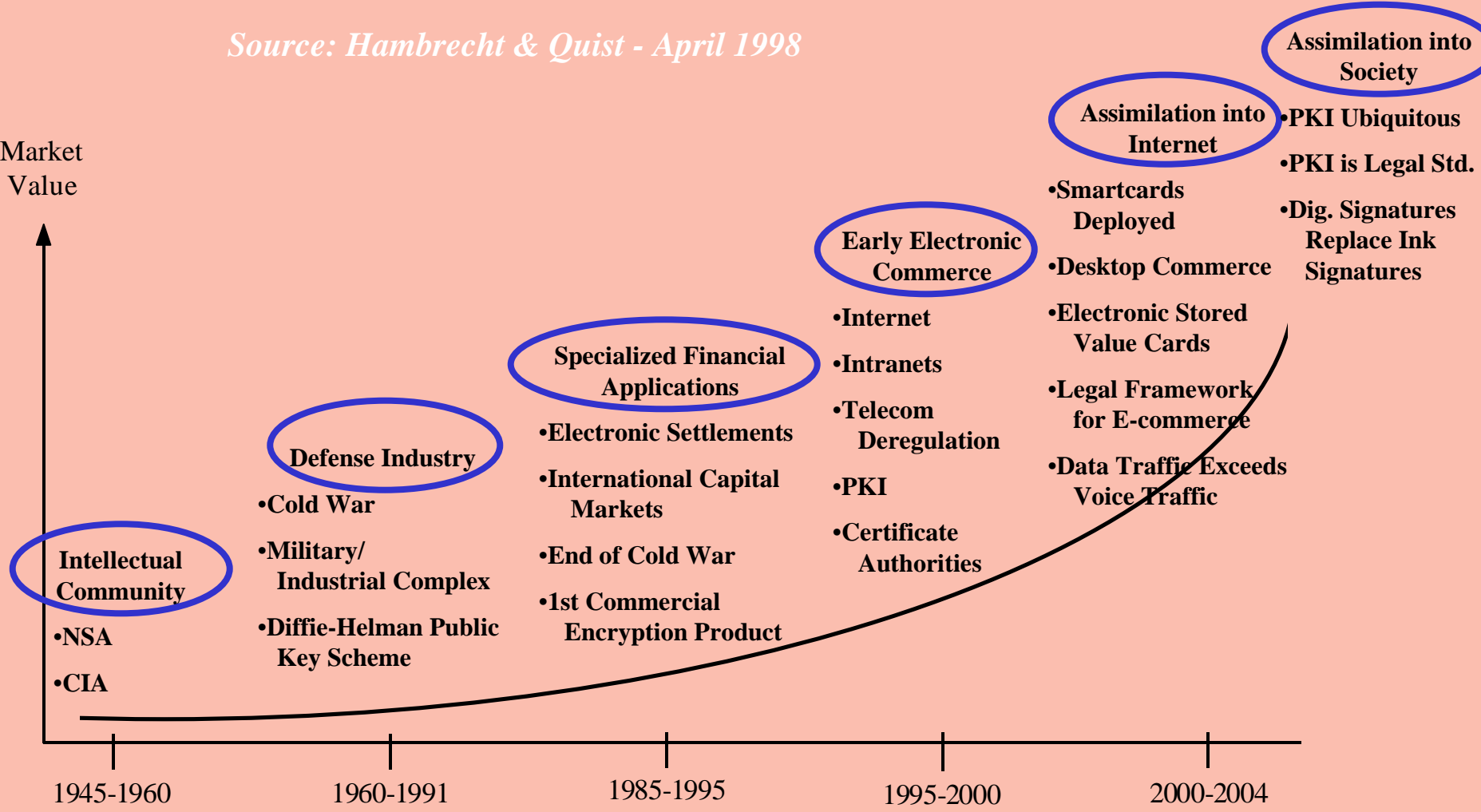
**(Public Key Infrastructure)**

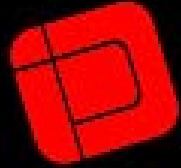


# The Origin of Digital Signature Technology Resides in PKI

Source: Hambrecht & Quist - April 1998

Market Value





**ID CERTIFY**

## **Through PKI - Fundamental Security Requirements are Assured**

**Access Control**

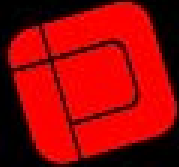
**Determines who may have access to information within a system**

**Authentication**

**Verifies the identity of communicating parties**

**Privacy**

**Protects sensitive info from being viewed indiscriminately**



**ID**CERTIFY

# Through PKI - Fundamental Security Requirements are Assured

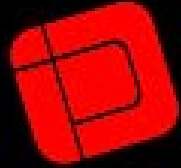
**Integrity**

**Guarantees that info is not  
tampered with or altered**

**Non-Repudiation**

**Inability to disavow a  
transaction**

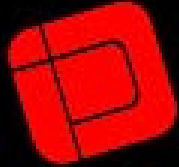
*Source: Hambrecht & Quist*



**ID**CERTIFY

## **A Digital Signature Is . . .**

**A digital code that can be attached to an electronically transmitted message that uniquely identifies the sender.**



IDCERTIFY

# Digital Signature

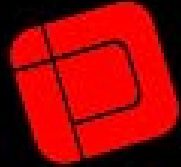
Certificate Fingerprint (MD5) :

3740f5f8d7d3c3332c3133df89dee844

-----BEGIN CERTIFICATE-----

```
MIICATCCAcACBDUcVHowCQYFKw4DAhsFADCBpTELMakGA1UEBhMCMVVMxCzAJBgNV
BAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMRUwEwYDVQQKEwxJLkQuIENlcnRpZnkn
ITAfBgNVBAAsTGFNpZ25hdHVyZSBQYXNzcG9ydCBEZXB0LjEibkGA1UEAxMSU2ln
bmF0dXJlIFBhc3Nwb3J0MSAwHgYJKoZIhvcNAQkBFhFJRUFdQUBoYmFpbmZvLmNv
bTAeFw05ODAzMjgwMTM4MDJaFw05OTAzMjYwMTM4MDJaMIGGMQswCQYDVQQGEwJl
czELMAkGA1UECBM0ExEDAOBgNVBACTB1JlZG9uZG8xFTATBgNVBAoTDEkuRC4g
Q2VydGlmTEZMBcGA1UEAxMQTGluZGEgTWJfja2ludG9zaDEmMCQGCSqGSIb3DQEJ
ARYXbG1hY2tpbnRvc2hAaGJhaW5mby5jb20wXDANBgkqhkiG9w0BAQEFAANLADBI
AkEAtvojXKaNj1kmOgeS1APcacXqo77kjUa6h70gd8E35isP7Uy0pP/mYujq4Lj3
mrVFO+6ZXbXhASM6JML4hANgeQIDAQABMAkGBSsOAwIbBQADMAAwLQIVAMjBkJ+L
JzJl+UWyXTVQLmvNUjHrAhR/wyNonHt9m5hHvD3oQJcdAxljUA==
```

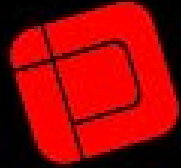
-----END CERTIFICATE-----



**IDCERTIFY**

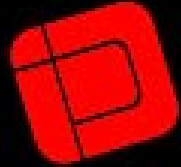
## **Common Misconceptions. . .**

- **Digital signature=Digitized signature**
- **Popular business applications use digital signatures**
- **All digital signatures are the same**
- **A digital signature is legally binding**
- **Smart cards are not needed for secure storage of private keys.**



**ID**CERTIFY

# **What is a Certification Authority?**

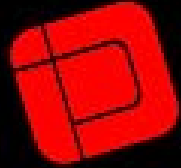


**ID**CERTIFY

## **A Certification Authority Is . . .**

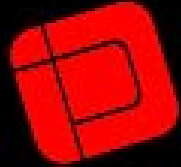
**A trusted third-party organization or company that issues digital certificates used to validate the signer of a document signed with the private key creating a digital signatures.**

**The CA guarantees that the individual is who they claim to be.**



ID CERTIFY

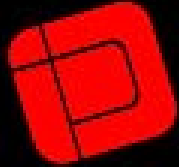
# What is a Repository?



**ID**CERTIFY

## **A Repository Is . . .**

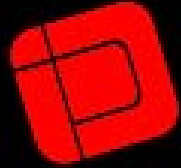
**A repository is a data center that stores the electronic certificate. The relying party checks the certificate in the repository to ensure that it is valid.**



**ID**CERTIFY

## **How is Risk Assigned?**

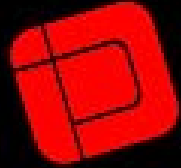
- **Through the Certification Practice Statement (CPS) – document on file by all Certification Authorities that assigns portions of risk to the Subscriber, the Certification Authority, and the Relying Party.**
- **Through Insurance – The CA can purchase insurance on the certificates it issues. For example, ID Certify digital certificates carry insurance by Lloyds of London.**



**ID**CERTIFY

## **Adoption of Digital Signature Legislation**

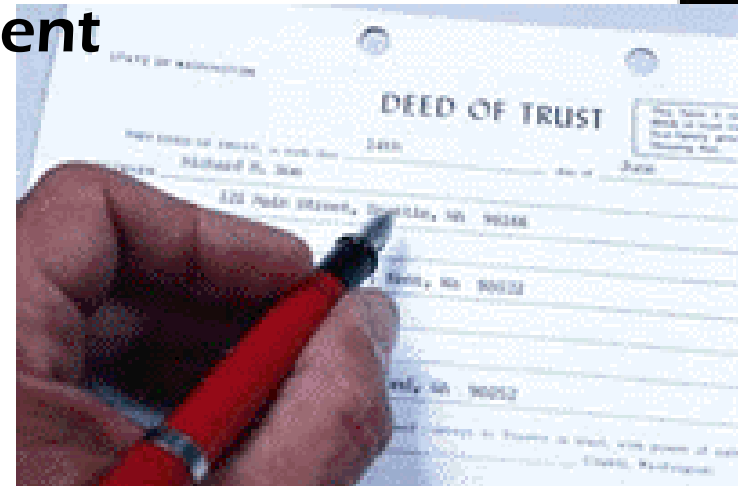
- **Nine States have adopted legislation similar to Washington State**
- **37 States have legislation that recognizes digital signatures**
- **European Community has adopted Uniform regulations for licensing of Certification Authorities**
- **Federal legislation that incorporates UETA**

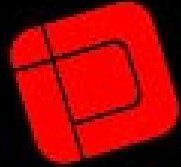


**IDCERTIFY**

## **Legal Significance of Using a Licensed Certification Authority**

- **Certificates issued are proof of I.D.**
- **Constitutes a notarized signature**
- **Certification Practice Statement (CPS) is a 3-party contract**
- **Certificates can be proof of authority**
- **Indemnity bond guarantee**

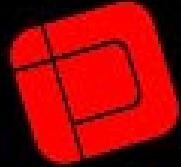




**ID**CERTIFY

## **Trends Are Emerging**

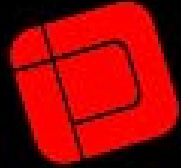
- **Licensed/Unlicensed**
- **Private/Public**
- **Proprietary/Open**
- **Industry Specific/Generic**
- **Outsourced/In house**



**IDCERTIFY**

## **Law and E-Commerce**

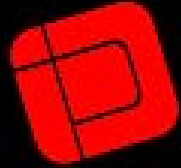
- **The Laws of the paper-based world apply to the virtual electronic world.**
- **The challenge resides in combining technology and legal infrastructures that permit enforcement of existing laws - both national and international.**



**ID**CERTIFY

## Part III

# Creating a Digital Signature and Certificate

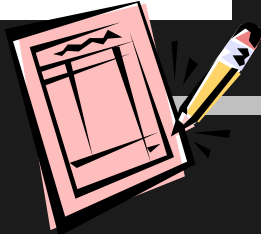


ID CERTIFY

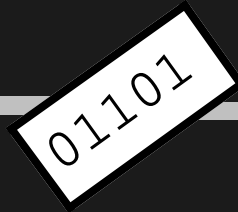
**SIGNING ON THE**  
**DIGITAL LINE**

# CREATION OF A DIGITAL SIGNATURE

**Sign**



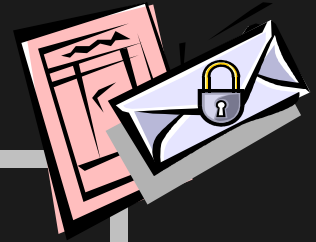
**Create document**



**Hash code creates a unique digital fingerprint of original document**

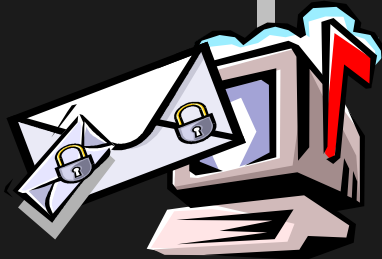


**Sign hash code using sender's PRIVATE key**



**Append the signed hash code to document**

**Deliver**



**Mail electronic envelope to recipient**

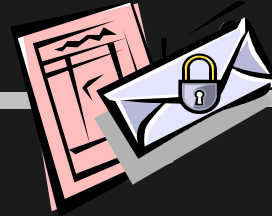
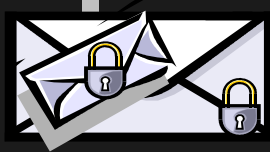
# CREATION OF A DIGITAL SIGNATURE

**Receive**

Digital envelope arrives at destination



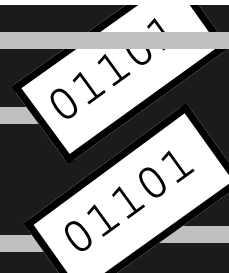
**Verify**



Check Repository

**Accept**

Verify digital fingerprint using sender's PUBLIC key

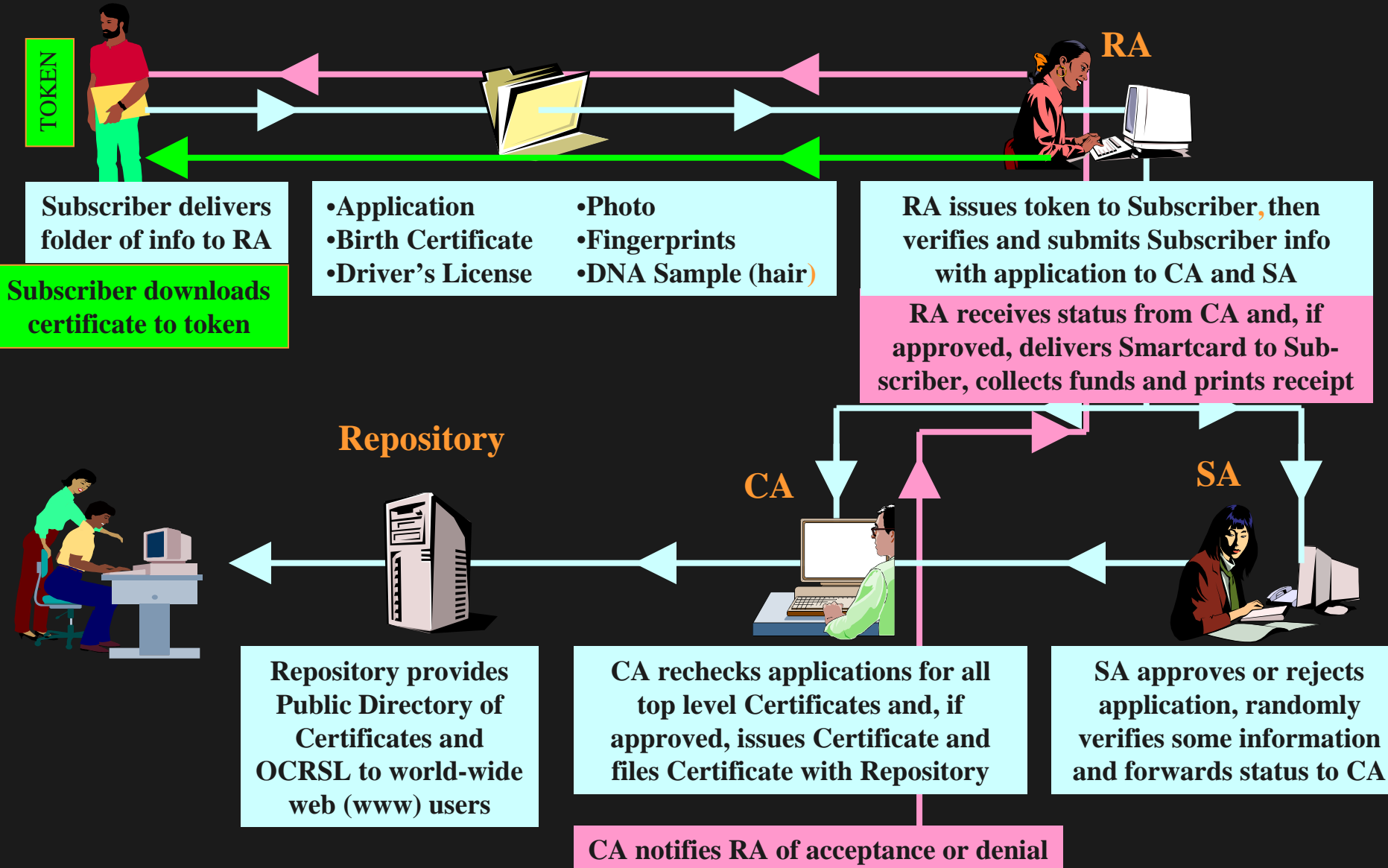


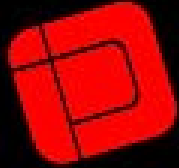
Repository check establishes valid certificate

Rehash creates a new digital fingerprint from decrypted document for comparison with the original

Becomes legal signature

# CREATING A KEY PAIR AND ISSUING A CERTIFICATE

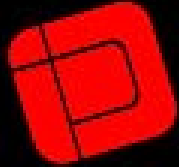




**ID**CERTIFY

## **Verification Methods**

- **Certification Revocation List (CRL)**
- **Online Certificate Status Protocol (OCSP)**



**ID**CERTIFY

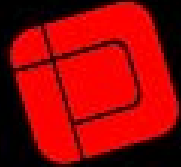
## The Enabling Tools are Simple

### ALREADY HAVE

- PC
- Modem
- Browser

### NEED

- Smartcard
- Smartcard Reader
- Certificate/  
Digital Signature

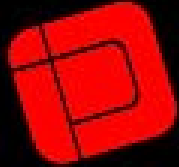


**ID**CERTIFY

# Signing Documents and Forms

- MS Word Document
- Prescription
- Time Sheet

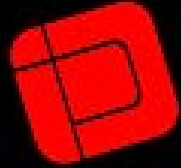




IDCERTIFY

## How Do Digital Signatures Provide Proof of ID?

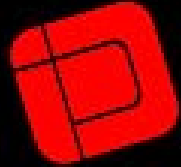
- I have the public key of a person. If they sign with their private key and the keys match, I know who signed the document. This assumes I trust the ownership of the public key.
- If I don't know for sure who owns the public key, I must trust the agent who certifies the identification of the person who owns the public key.
- The agent that certifies the identity of the person who holds a public key is a Certification Authority (CA).
- If I trust the CA, then I can trust the identity of the person who signed the document.
- The purpose of a government entity licensing a CA is to provide trust in the digital signature.



**ID**CERTIFY

## Part IV

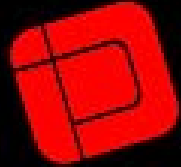
# Consumer Concerns Questions and Answers



**ID**CERTIFY

**“E-Commerce offers great potential growth to companies, but there is a lot companies need to be aware of before they attempt to ‘cash in’ on the net.”**

**Source:  
Booz\*Allen Hamilton  
White Paper**

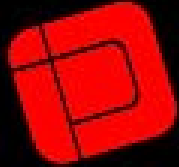


**IDCERTIFY**

## **Mandates and Regulation**

- **HIPAA(Health Information Portability & Accountability Act)**
- **UETA**
- **UCITA**
- **Paperwork Reduction Act**

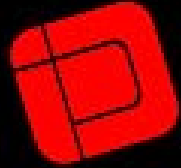




**ID**CERTIFY

## **Electronic Commerce – New Security Issues**

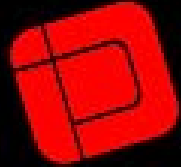
- **Are the communication links secure for the web environment?**
- **Is communication traffic via the web auditable by sender and receiver?**
- **Can the sender and recipient be identified?**
- **Are the database links to the Internet secure?**
- **Can data transmitted be altered?**
- **Can receipt of data be verified?**



**ID**CERTIFY

## **Security Considerations in Design**

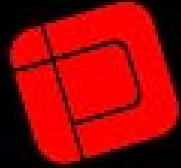
- **Computer facilities**
- **Dual mirrored redundant/disparate sites**
- **Software certificates vs. smart cards**
- **Server based vs. client based**
- **Distribution of certificate considerations**
  - **Single source**
  - **Distributive RA network**



**ID**CERTIFY

## **Design/Audit Considerations**

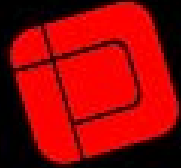
- **Define target of evaluation**
- **Licensed vs. unlicensed**
- **Auditor as design architects**
- **Static membership vs. open membership**
- **Define the standards**
  - **CS2**
  - **SAS 70**



**IDCERTIFY**

## **Policy Design Considerations**

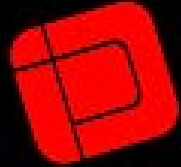
- **CPS or Rule Book**
- **Distributed liability**
- **Distributed risk**
- **Distributed responsibility**
- **Scaleable security vs static model**
- **Conflict resolution**
- **Choice of law/jurisdiction**
- **Defined Standard of Conduct**



**IDCERTIFY**

## **Policy Design Considerations**

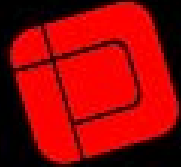
- **Cross certification**
- **CRL vs. OCSP**
- **Vetting**
  - **Face to face with credential**
  - **On-line with URL verification**
  - **HR directories**
  - **3rd party validation**
  - **2nd level authentication**



**IDCERTIFY**

## **Policy Design Considerations**

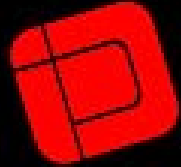
- **Repository Functions**
  - **Archiving**
  - **Time-stamping**
  - **Secure e-mail service**



**ID**CERTIFY

## **Scott McNealy, Sun Microsystems**

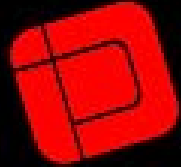
**“In the Internet age, privacy is gone...  
get over it.”**



**IDCERTIFY**

## **Electronic Commerce – Privacy**

- **Privacy in stored and transmitted data**
  - Can someone take data as it moves across the Internet
  - Can someone take data as it sits on your server
- **Privacy of your personal information**
  - Mining of information or profiling
  - Distribution of “cookies”

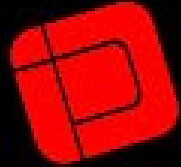


**ID**CERTIFY

## **Survey by Electronic Privacy Information Center**

**Survey of top 100 shopping sites**

- **18 did not display privacy policy**
- **35 have profile based advertisers on their page**
- **86 used cookies**
- **none addressed all the elements of the Fair Information Practices Act.**

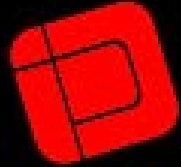


**IDCERTIFY**

## **How Can Digital Signatures Provide Proof of Authority?**

Special attributes can be embedded in a digital certificate, which limit or allow its usage. For example, Employee A could digitally sign and authorize a Purchase Order up to \$5,000, while Employee B could sign and authorize a Purchase Order up to \$50,000. Authority Levels could be set up to control:

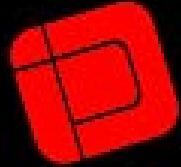
- Spending
- Hiring
- RFPs
- Access to private information



IDCERTIFY

## How Do Digital Signatures Improve Efficiency?

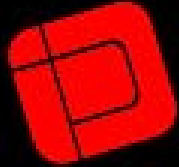
- **Signing and Routing of Common Forms**  
Using PKI, forms can be filled out, signed and sent to the appropriate reviewers, electronically. This saves time, paper, storage and handling costs.
- **Document Filing by the Public**  
Citizens can file documents with government agencies, electronically, eliminating waiting time and delivery costs, while facilitating handling, processing and storage.
- **Electronic Bids Made Easier to Compare**  
Bid documents submitted electronically provide purchasing departments with the ability to capture data directly to spreadsheets or a database, making bid comparison more efficient



IDCERTIFY

**WHERE ARE YOU  
IN THE TRANSITION  
TO AN E-ECONOMY?**

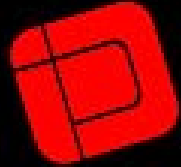




**ID**CERTIFY

## **Where is Wyoming in the Race?**

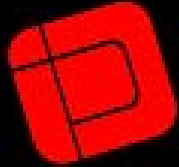
- **Last year, Wyoming established the Online Government Commission to build the entire electronic enterprise portal for all state agencies.**
- **They issued a broad-based RFP for this electronic portal, due February 14, 2000, which did not establish platforms or indicate how digital signatures would be handled (unknown if Sec. State will manage, or be privatized).**
- **It is anticipated that a complete system will be fully implemented later this year (2000).**



**IDCERTIFY**

## **What Do YOU Need to Be Doing Today?**

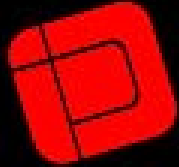
- **Know the electronic commerce industry and how it will effect your organization's mission**
- **Set company policy on privacy and encryption**
- **Specify your needs in terms of legal signatures, storage and ease of storage migration**



**IDCERTIFY**

## **What Do YOU Need to Be Doing Today**

- **Set policy on digital signatures that you will accept for legal signatures and for the verification process that you require**
- **DoD has 5 levels of certificate security**
- **Make sure that your company researches the industry and picks products that fit your business needs**



**ID**CERTIFY

## **Further References**

ID Certify's website:

[www.idcertify.com](http://www.idcertify.com)

State of Washington's website:

<http://access.wa.gov/>

PKI Page:

<http://www.pca.dfn.de/eng/team/kelm/pem-dok.html>

Legislation:

<http://www.mbc.com/ecommerce.html>

Booz-Allen E-Commerce White Paper:

<http://boozallen.se-com.com/>

National Electronic Commerce Coordinating Council info on UETA

<http://ec3.org>



**ID**CERTIFY

# *Law & E-Commerce*

## *All State Laws Are NOT Equal*

### Real Law

- Electronic documents are admissible as evidence
- Electronic filing for bid submissions, tax filings, electronic recording of deeds, mortgages, etc., are legally binding

### E-Comm Law “Lite”

- Some states provide no mechanism for allocation of risk and liability (ex: CA)
- E-documents cannot be proven to be authentic in court (SD, ID, DE, PA)

# *Law & E-Commerce*

## *Laws in Enforcement today*

### The Significance of the State Licensing Laws:

- Provides a framework for parties to allocate risk and liability
- Recognizes electronic notarization of documents world wide
- Mandates that digital signatures are legally binding
- Requires trustworthy verification of identity

# *Law and E-Commerce: Bottom Line*

- Adequate existing law
- Available models for risk allocation
- Ability to enforce electronic contracts
- Current law is designed to be technology neutral and standards based
- E-Commerce standards will become ubiquitous