JavaOne℠

Sun's Worldwide Java Developer Conference

JavaOne℠

Sun's Worldwide Java Developer Conference

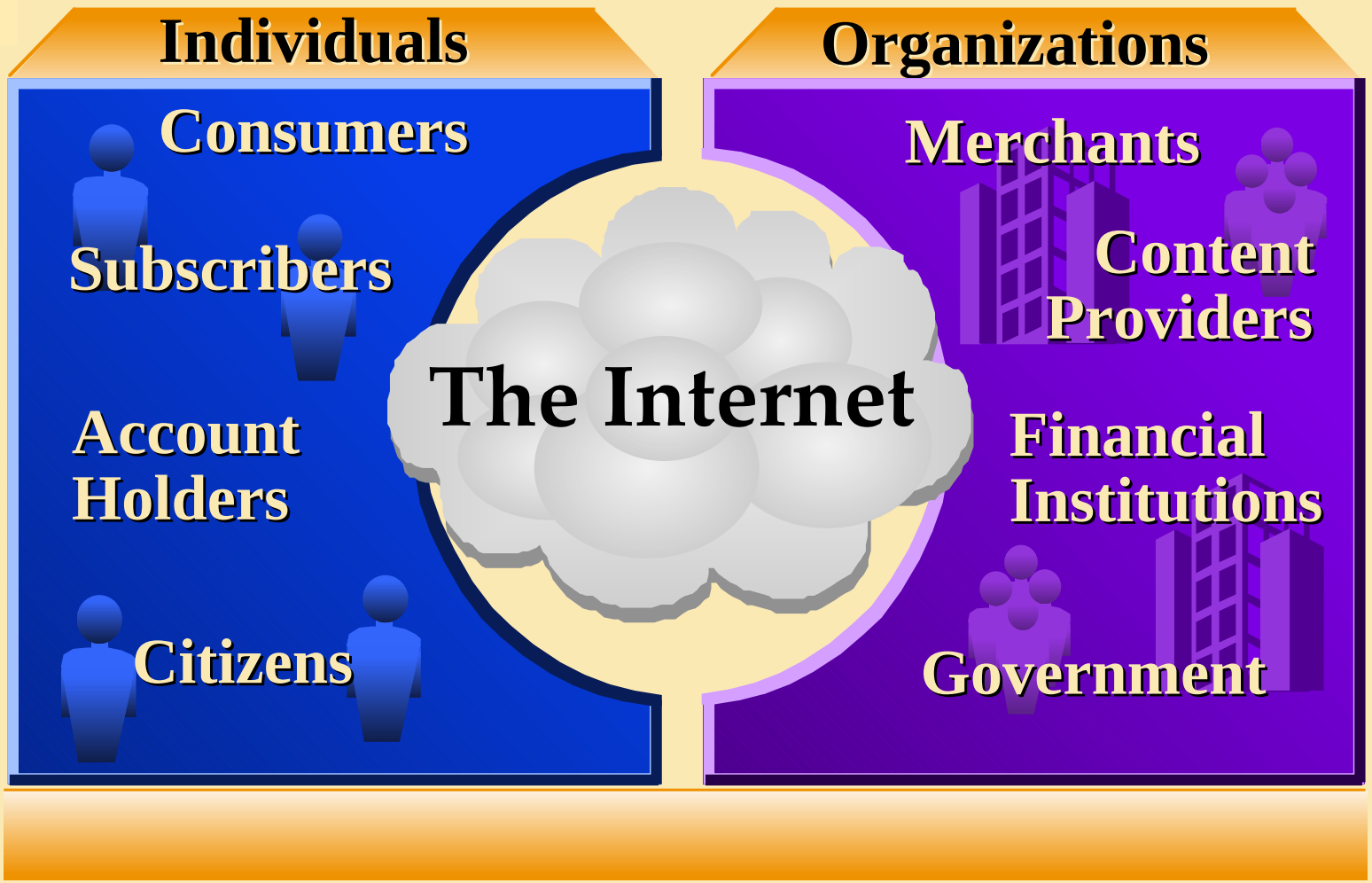
Digital Authentication on the Internet: It's all about relationships

Stratton Sclavos
President and CEO
VeriSign Inc.

The Internet - 1996

- 30 Million browsers downloaded
- 115 Million active e-mail accounts
- Financial and information services in demand
- Fortune 1000 piloting Internet EDI
- Intranets explode
- Secure payment protocols go live

Enabling Trusted Commerce

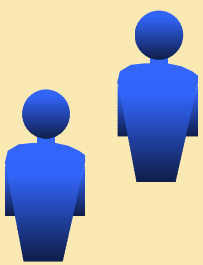


Internet Security

Policies	Gov’t, Credit Asso.
Authentication	VeriSign
Application Protocols	Netscape, VISA
H/W and S/W Platforms	Microsoft, SUN
Network Protocols	Netscape, Terisa
Encryption	RSA

Digital Authentication

INDIVIDUALS

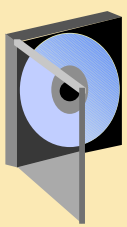


- Identity
- Authority

ENTITIES

- Identity
- Viability

CONTENT



- Origin
- Integrity

PKI Technology Review

PRIVATE KEY

- Used by owner to sign messages
- Used by owner to decrypt messages
- Matched with a unique public key

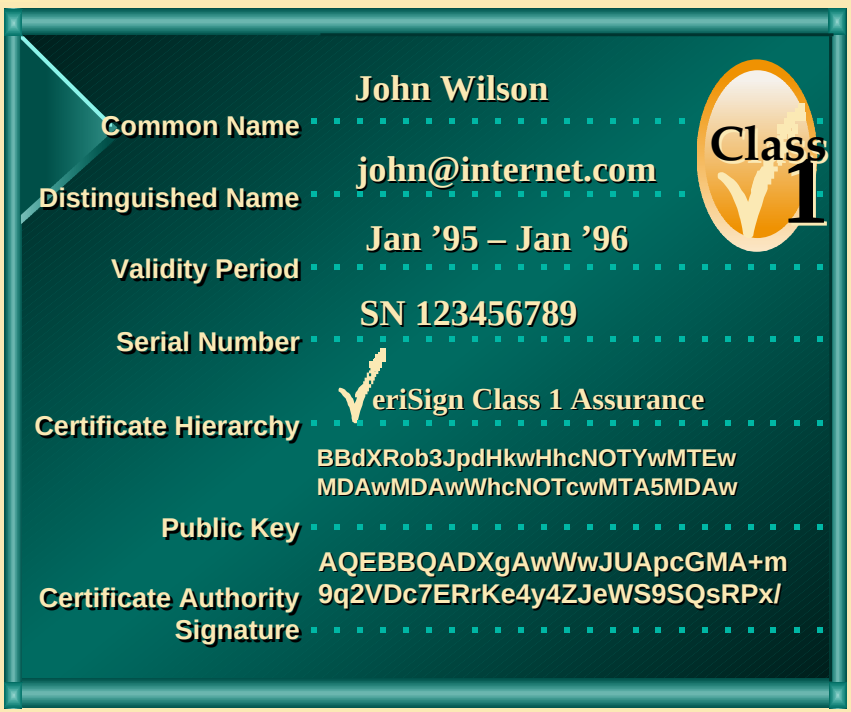
PUBLIC KEY

- Used by message sender to encrypt message for owner
- Used by message receiver to verify signature of owner
- Matched with a unique private key

DIGITAL CERTIFICATE

- Verifies public key of an individual or organization
- Sent along to authenticate digital signature
- Used by message sender to access owner's public key
- Digitally signed by a trusted party

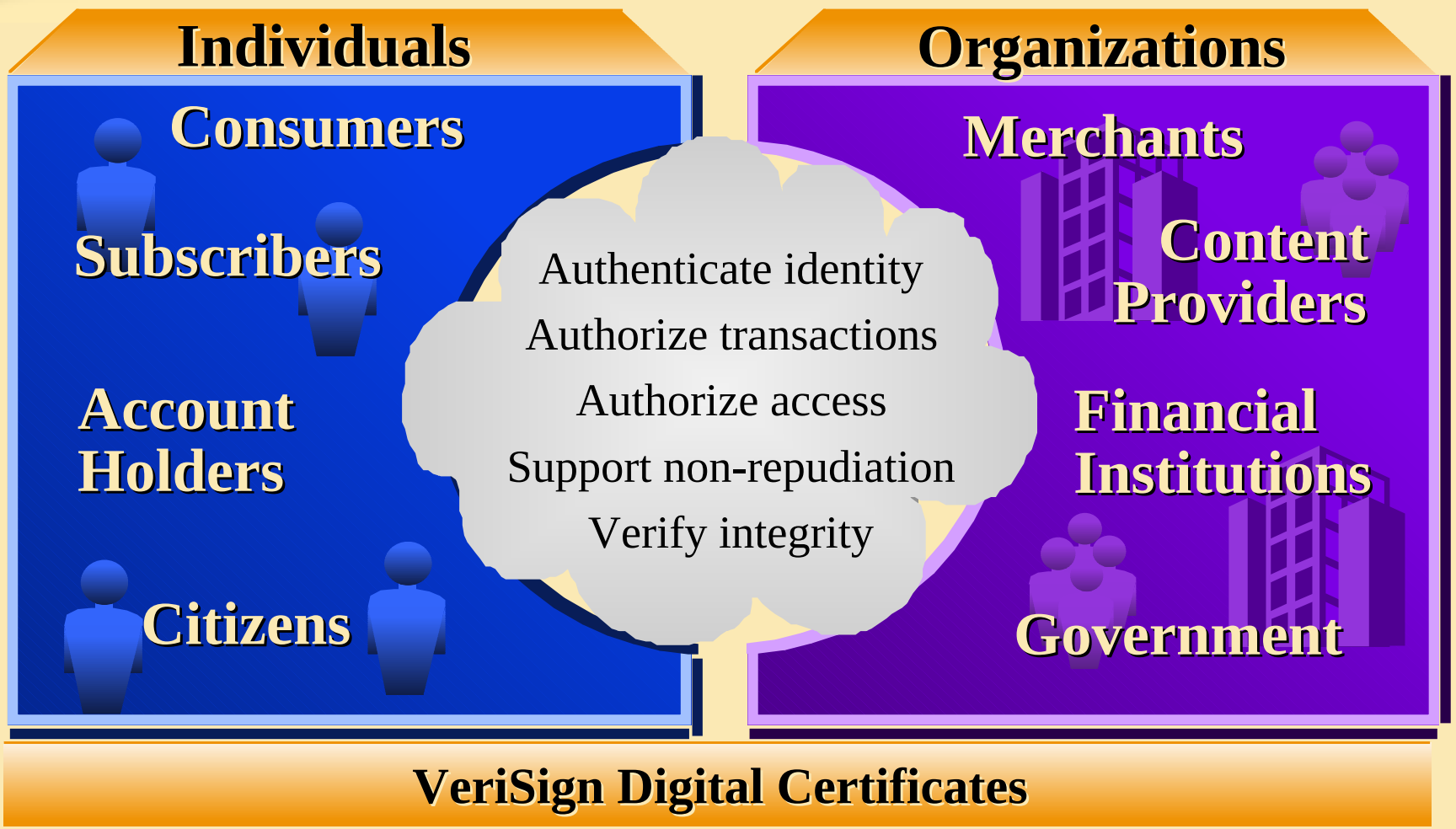
What is a Certificate?



“Digital ID”

- Cryptographically encoded binary file
- Binds public key to individual
- Notarized by trusted third party
- Used to verify digital signature of owner
- Used to safely encrypt messages for owner

Role of Digital Certificates

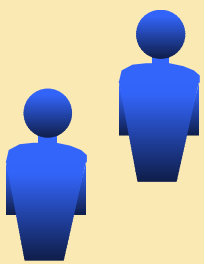


Advantages of Digital Signatures

- Encryption scrambles the bits
  - Very effective for privacy
  - RSA a de-facto standard
  - Export controlled
- Digital Signatures authenticate the source
  - Proof of origin and integrity
- Digital Certificates provide the trust
  - Validate the relationship

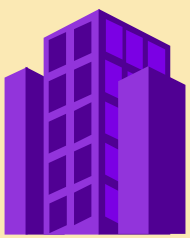
Certificate Usage on the ‘Net

INDIVIDUALS



- Personal ID
- Credit Card
- Bank Book
- Brokerage
- Membership
- Badge

ORGANIZATIONS



- Business ID
- Merchant ID
- Trading Partner

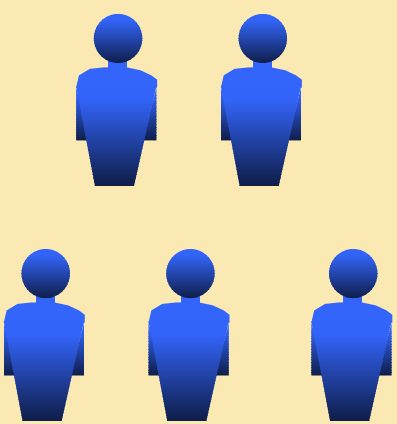
CONTENT

- S/W Publisher
- News Publisher
- IP Owner

What is a Certificate Authority?

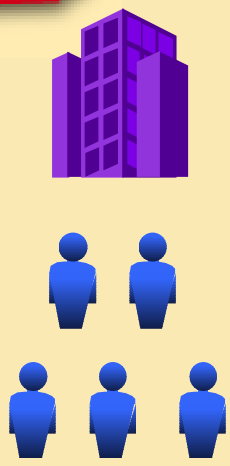
- Trusted third party
- Issues and manages certificates
- Specific trust domains
- Subscribers agree/depend on practices
- Acts as arbiter of trust in a digital relationship

Trust Domains



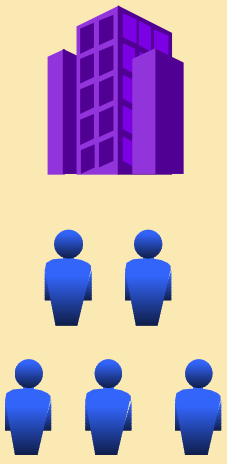
- Describes relationships between parties
- Pre-defined policies and expectations
- Certificates validate membership in domain
- Digital relationships

Who Will be a CA?



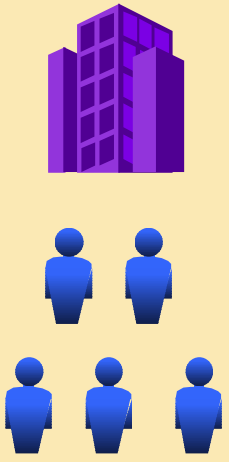
VeriSign

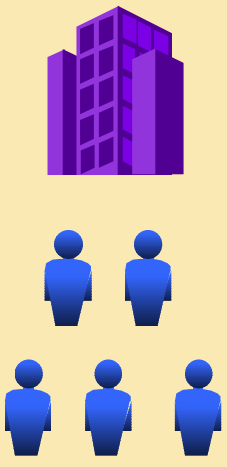
Gov't



Credit Asso.

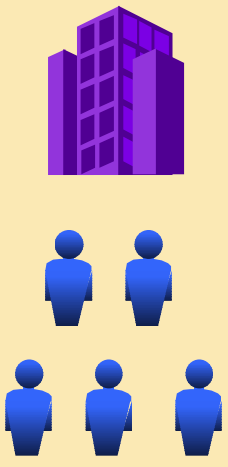
Banks





Publishers

Companies



CA Requirements Checklist

TECHNOLOGY

- Crypto
- Cert encoding
- 1024 signing
- Key directories
- Secure messaging
- Internet expertise

INFRASTRUCTURE

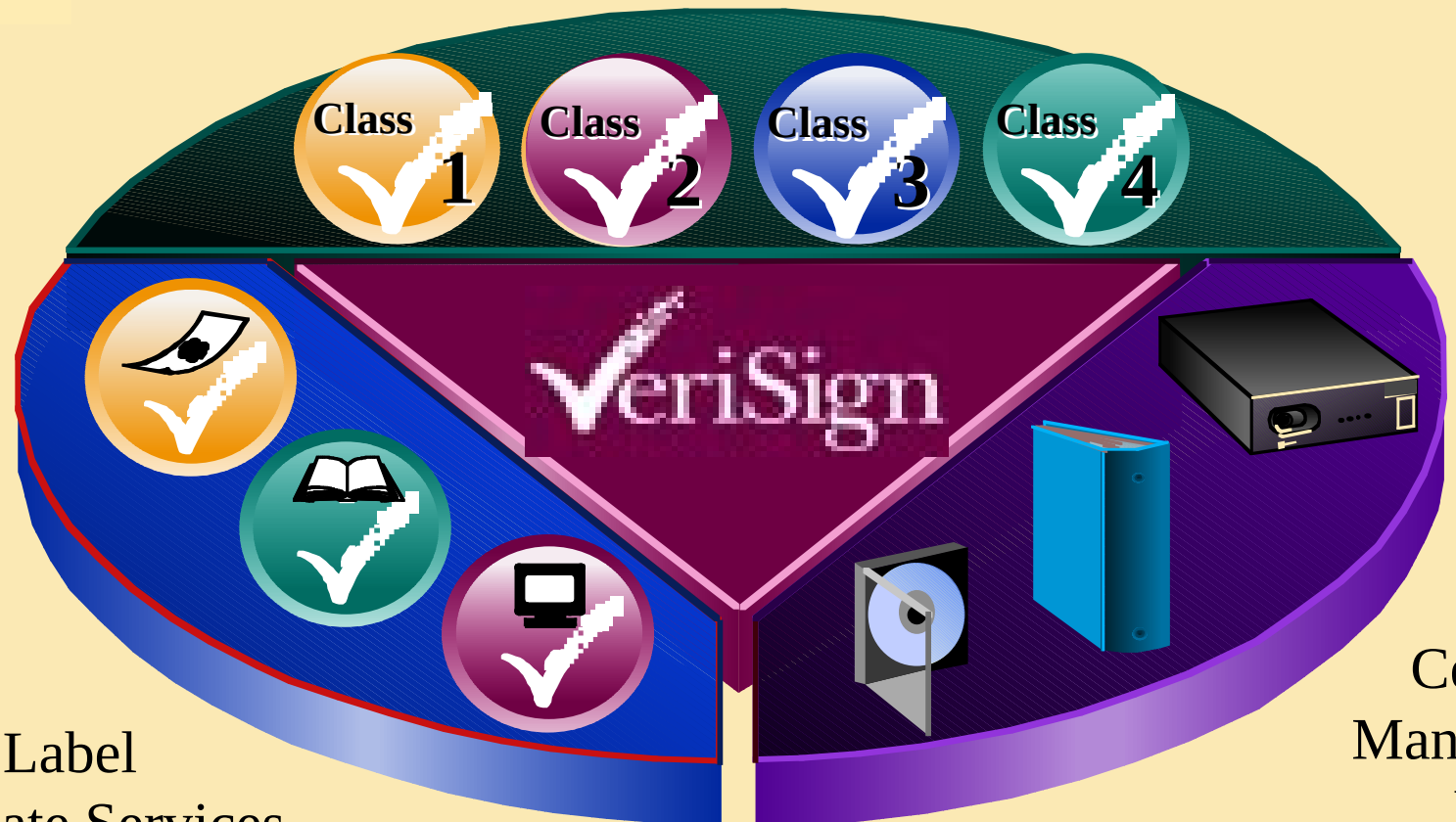
- Secure facilities
- High availability
- Scalability
- Telecom
- Customer service

PRACTICES

- Practices
- Standards
- Localization
- Compliance
- Insurance

VeriSign's Business

Public Certificate Services



Private Label Certificate Services

Certificate Management Products

Company Overview

- Formed April, 1995
- Spin-out from RSA Data Security Inc.
- Strong Investor Backing
  - Bessemer Ventures, Kleiner-Perkins
  - VISA International , Ameritech, Mitsubishi, Security Dynamics, Fischer Int'l
- 100% Focus on *Digital Authentication* Technologies and Services

Mission

Providing trust for the Internet and Electronic Commerce through our Digital Authentication services and products

Company Milestones

4/95	Company formed
6/95	Netscape Server IDs ship
10/95	Add’l Server partners
1/96	Secure e-mail partners
2/96	VeriSign Japan formed w/NTT
	Second Round Financing
3/96	Code Signing with Microsoft
4/96	Digital ID Center Opens
	VeriSign IDs in Navigator 3.0

VeriSign Today

TECHNOLOGY

- RSA, others soon
- X.509 v3
- 1024 bit signing
- On-line DBMS
- SSL, S/MIME
- Web-based services

INFRASTRUCTURE

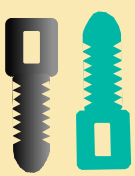
- US, Japan, Europe
- Redundant systems
- Designed for Millions
- Multiple telcom lines
- Staffed service teams

PRACTICES

- Practice statement
- PKCS, NIST, IETF
- Japan/Europe localization
- Bonded operators
- Liability coverage

Digital ID Center

http://digitalid.verisign.com



- On-line issuing system
- Web and e-mail access
- Enabled directly in key apps
- Simple instructions, fast response
- Scaleable to millions
- Links to 3rd party proofing sources
- On-line certificate directories

VeriSign Digital ID Partners

- Secure Servers

Netscape	Microsoft	Oracle	IBM
OpenMarket	StarNine	FTP	Internet Factory
Connect	SPRY	Glaci	Luckman
Navisoft	Apache -SSL	O’Reilly	Spyglass

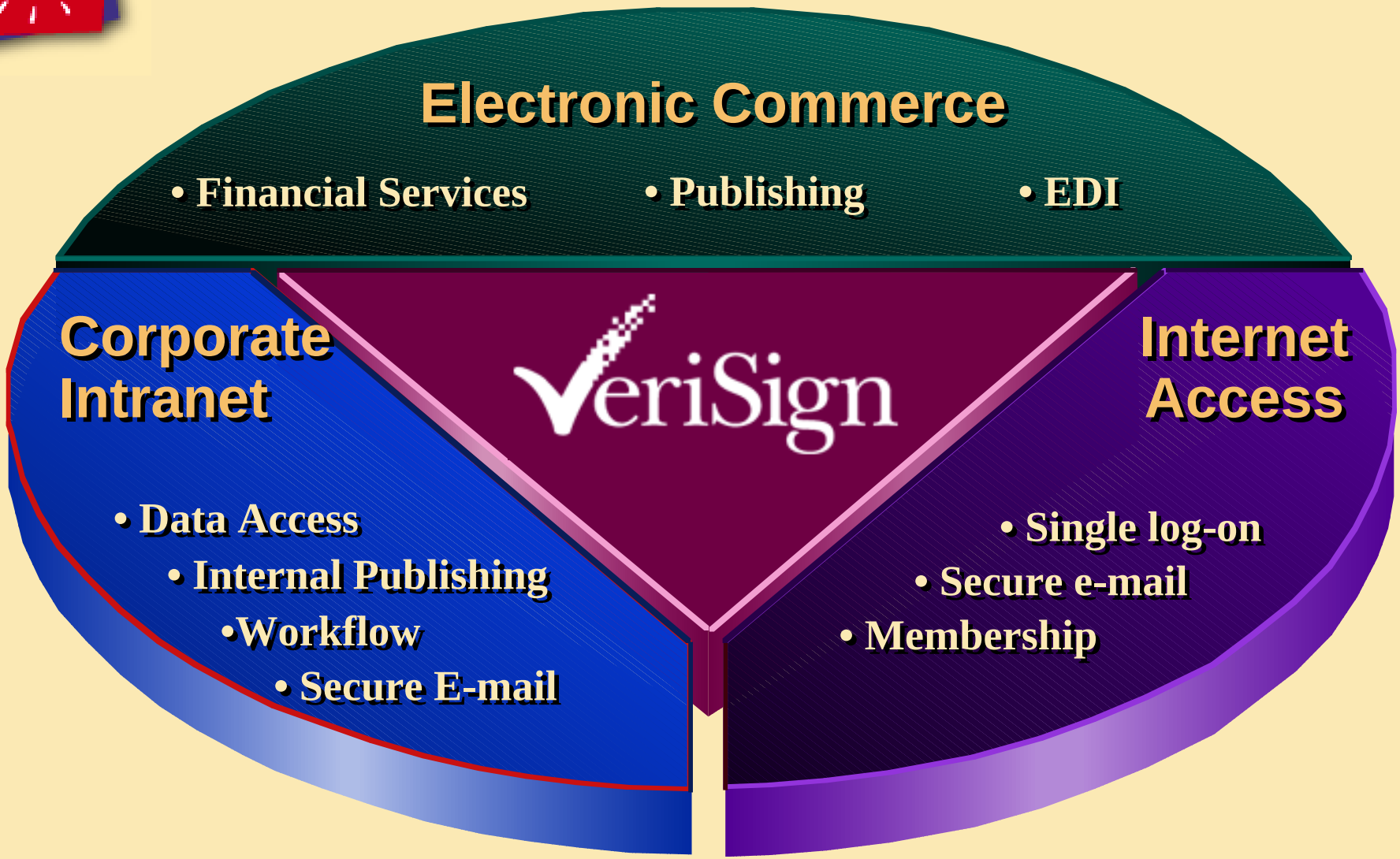
- Secure Clients

Netscape	Microsoft	Oracle
IBM	FTP	CyberCash
Deming	Banyan	Worldtalk
Frontier	ConnectSoft	OpenSoft

Secure Operations

- New facility in Mountain View, CA
- State-of-the-art provisions
  - Electronic access control on perimeter
  - Biometric access control in data center
- Isolated systems
  - Latest firewall technology
  - Tamper-proof key storage units
- International sites by Q4’96

Target Markets



Conclusion

- Security is the key issue for ‘96
- Pieces are now in place
- Digital Signatures/Certificates play a vital role in establishing trust
- Certificate Authorities (CAs) will be the arbiters of trust domains
- VeriSign is ready to deliver Internet trust today