



# Cryptographic Assurance: Security & Compliance

Cryptography as an Essential Tool for  
Compliance Programs

# Your Speaker

- Cryptographic Assurance Services LLC
  - Chief Cryptologist and President
  - [www.cryptographicassuranceservices.com](http://www.cryptographicassuranceservices.com)
  - [www.ralph-s-poore.com](http://www.ralph-s-poore.com)
  - (888) 380-1595 or (817) 446-5881
- Texas State Licensed Investigation Company
  - A15833



# Ralph Spencer Poore



- Certified Fraud Examiner (CFE)
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- Certified in Homeland Security (CHS-III)
- Certified TG-3 Assessor (CTGA)
- PCI Qualified Security Assessor (QSA)

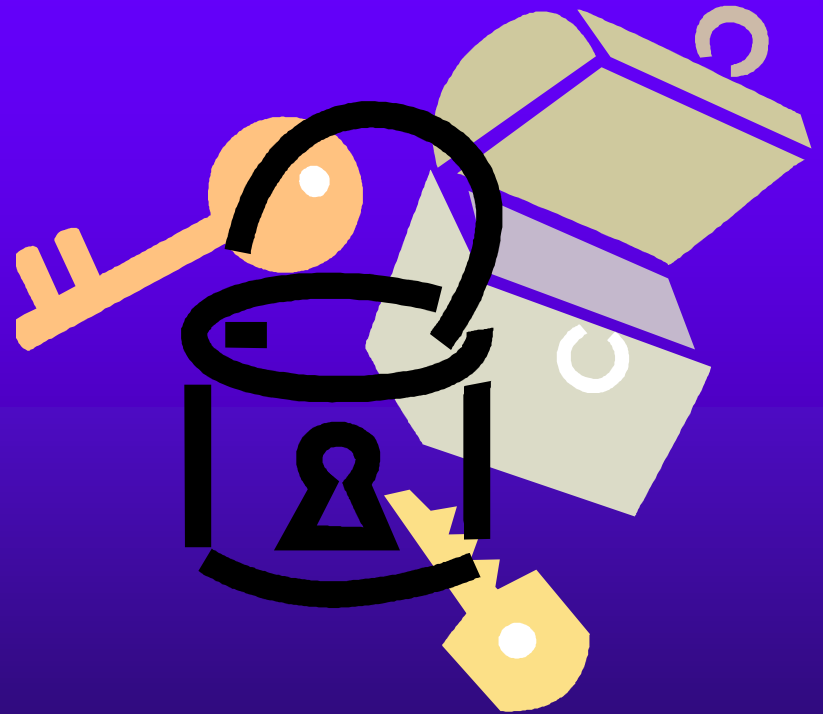


# Presentation Outline

- I. Introduction to Cryptography
- II. Key Management
- III. Standards & Regulations
- IV. Compliance
- V. Transitions

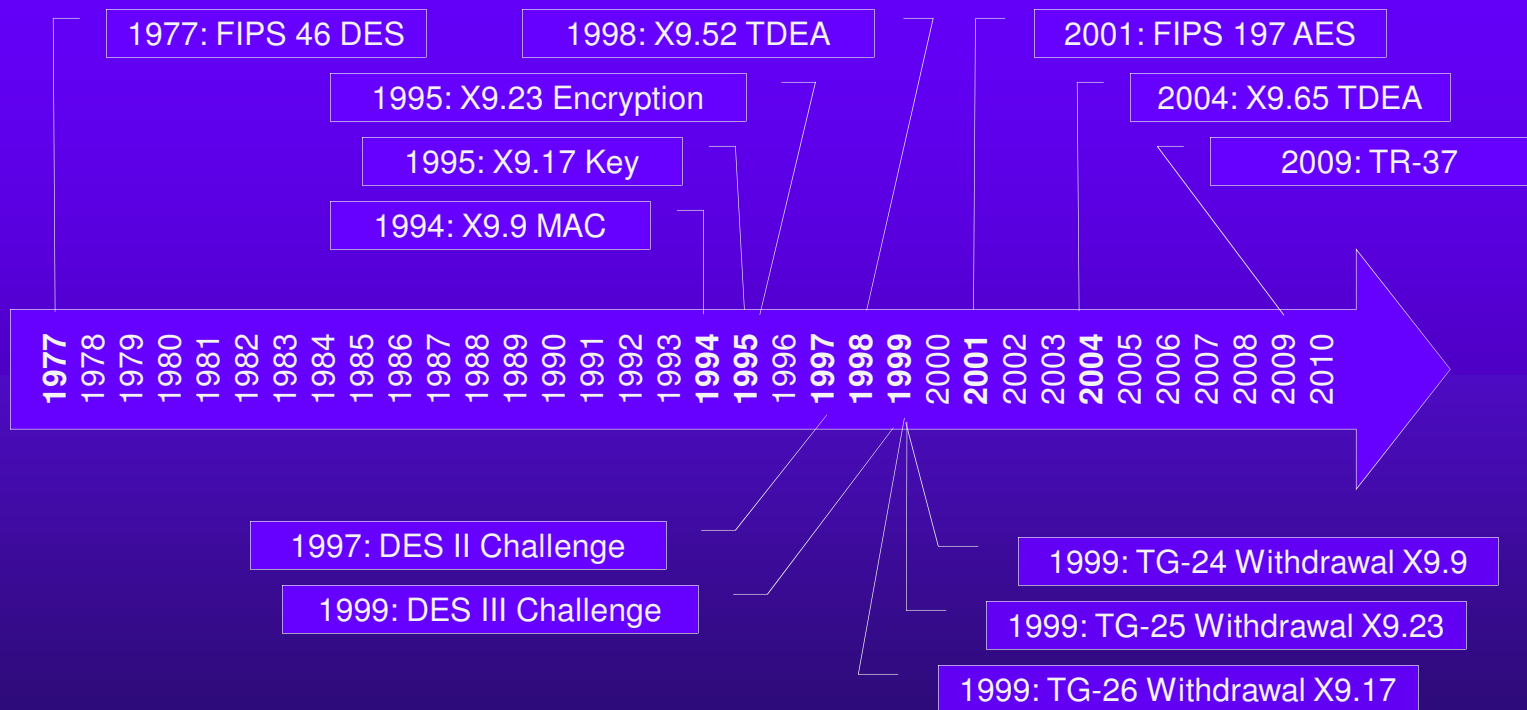
# Introduction to Cryptography

- Governmental province
- Commercial use
- Infrastructural use

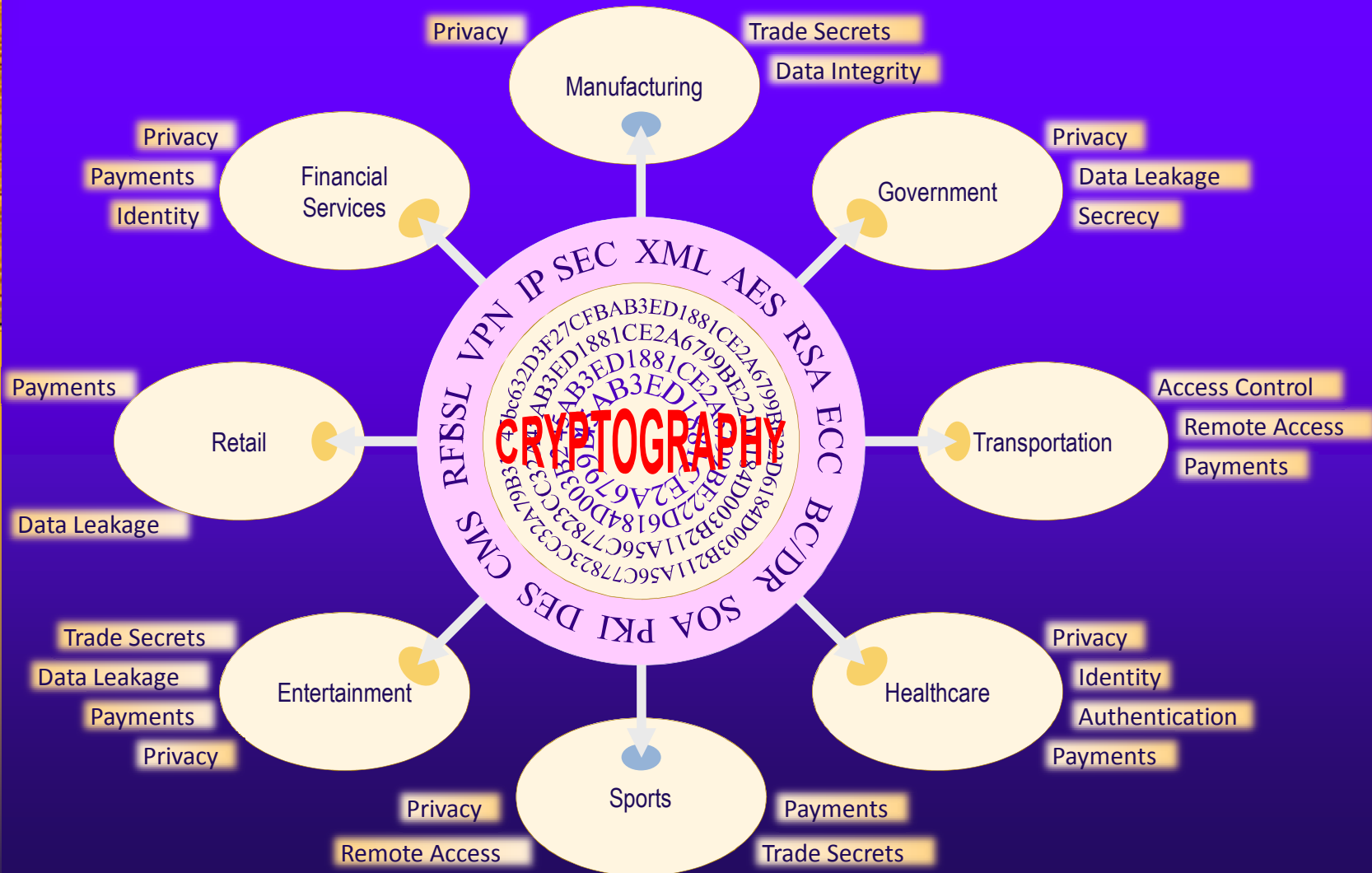




# Timeline



# Compliance/Business Needs

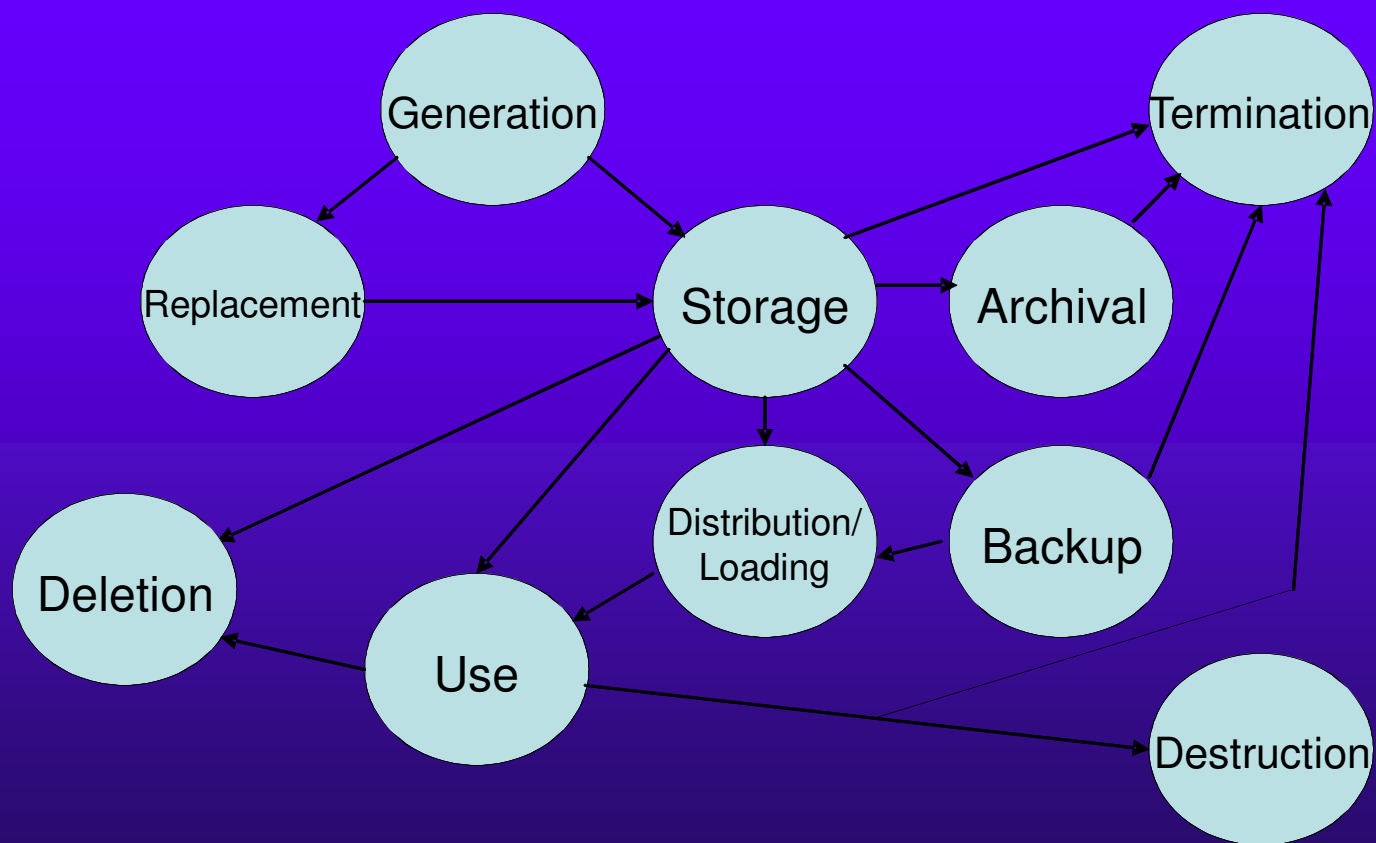


# Key Management

- Cryptographic keys
  - Symmetric
  - Asymmetric
- Management Issues
  - Policy
  - Standards
  - Processes



# Cryptographic Key Management Life Cycle



# Standards & Regulations



- Regulations
  - Based on statutes
  - Based on contract
- Standards
  - International
  - National
  - Industry

# Compliance

- Mandated
- Contractual
- Due Diligence





# Compliance—General

- Statutory (e.g., Federal, State & Local)
- Regulatory (e.g., Federal, State & Local)
- Contractual
- “Voluntary” Standards & Best Practices
  - Case law
  - Preemptive risk mitigation



# Authoritative Sources

- Laws
  - GLBA
  - FACTA
  - BSA
  - USA PATRIOT ACT



# Authoritative Sources

- Regulations
  - Executive Orders
  - Treasury Regulations
  - FFIEC Rules



# Authoritative Sources

- Standards
  - International Standards (e.g., ISO)
  - National Standards (e.g., ANSI, NIST)
  - Industry (e.g., PCI)



# Authoritative Sources

- Contracts
  - EFT Networks (e.g., PULSE)
  - Brands (e.g., American Express, Discover, MasterCard, Visa)



# Authoritative Sources

- Contracts
  - EFT Networks (e.g., PULSE)
  - Brands (e.g., American Express, Discover, MasterCard, Visa)
- Best Practice



# Compliance Programs

- SOX
  - Entities who are publicly traded [SEC]
- HIPAA
  - Entities who handle protected health information (PHI)
- State Data Privacy Laws (39 of 50)
  - Entities who handle personal information
- Gramm-Leach-Bliley Act of 1999 (GLBA)
  - Entities who are financial institutions
- PCI DSS
  - Entities who process payment card transactions [PCI SSC]
- TG-3
  - Entities who process PIN-based card transactions



# Compliance in Financial Services

- Cryptographic Security
  - TG-3
  - PCI DSS
  - FFIEC manuals



# Compliance in Financial Services

- Cryptographic Security
  - TG-3
  - PCI DSS
  - FFIEC manuals
- Identity Protection
  - Red Flag
  - PCI DSS
  - State disclosure reporting requirements



# Compliance in Financial Services

- Privacy Protection
  - GLBA
  - State laws
  - FFIEC manuals



# Compliance in Financial Services

- Privacy Protection
  - GLBA
  - State laws
  - FFIEC manuals
- Anti-Money Laundering (AML)

# Transitions

- Sources of change
  - Legal/regulatory
  - Technology
  - Risk profile
  - Cryptanalysis



# Summary



Questions?

