

# HIPAA and CPR Architecture

## Baptist Health Systems of SF

# Overview

- Main risks in CPR related to security
- HIPAA and its role in CPR risks
  - Brief overview
  - Related [proposed] regulations
- Projects related to CPR security
- What CORBA security covers in HIPAA-related security requirements and what it does not

# All Requirements from One Goal

- to earn as much money as possible and
- to **lose as little money as possible**
- “security” has never brought any money to a healthcare organization
- a security infrastructure can either cause or prevent loss of money

# Main Risks: Loss of Money

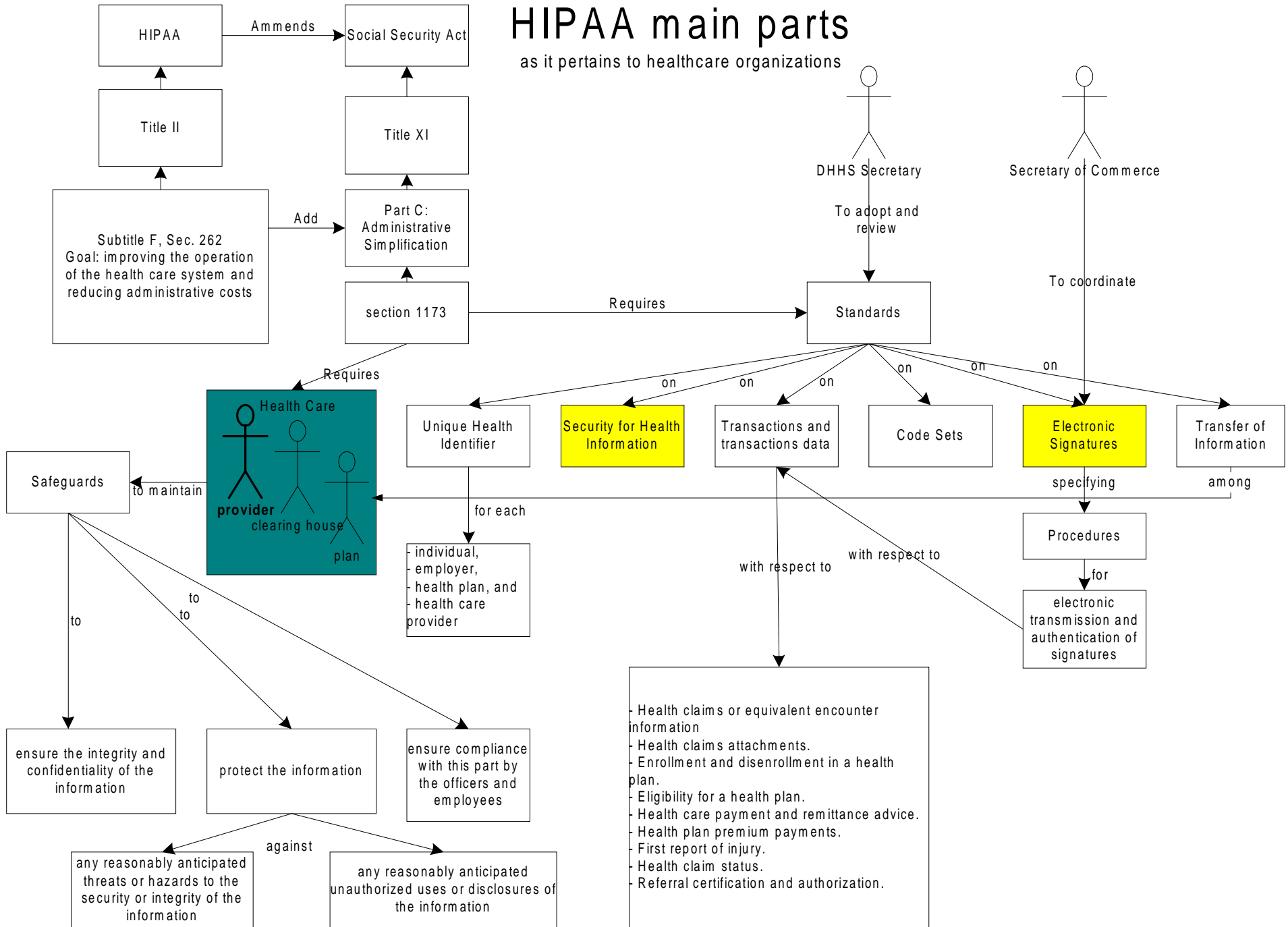
- Lawsuits because of mal-treatment
  - Occasionally, < \$10M
- Loss of customers
  - Loss of accreditation
    - Up to 50% of revenues
  - Customers prefer more “secure” providers
    - Maybe in the future, < 10-20% of revenues

# Main Risks: Loss of Money (2)

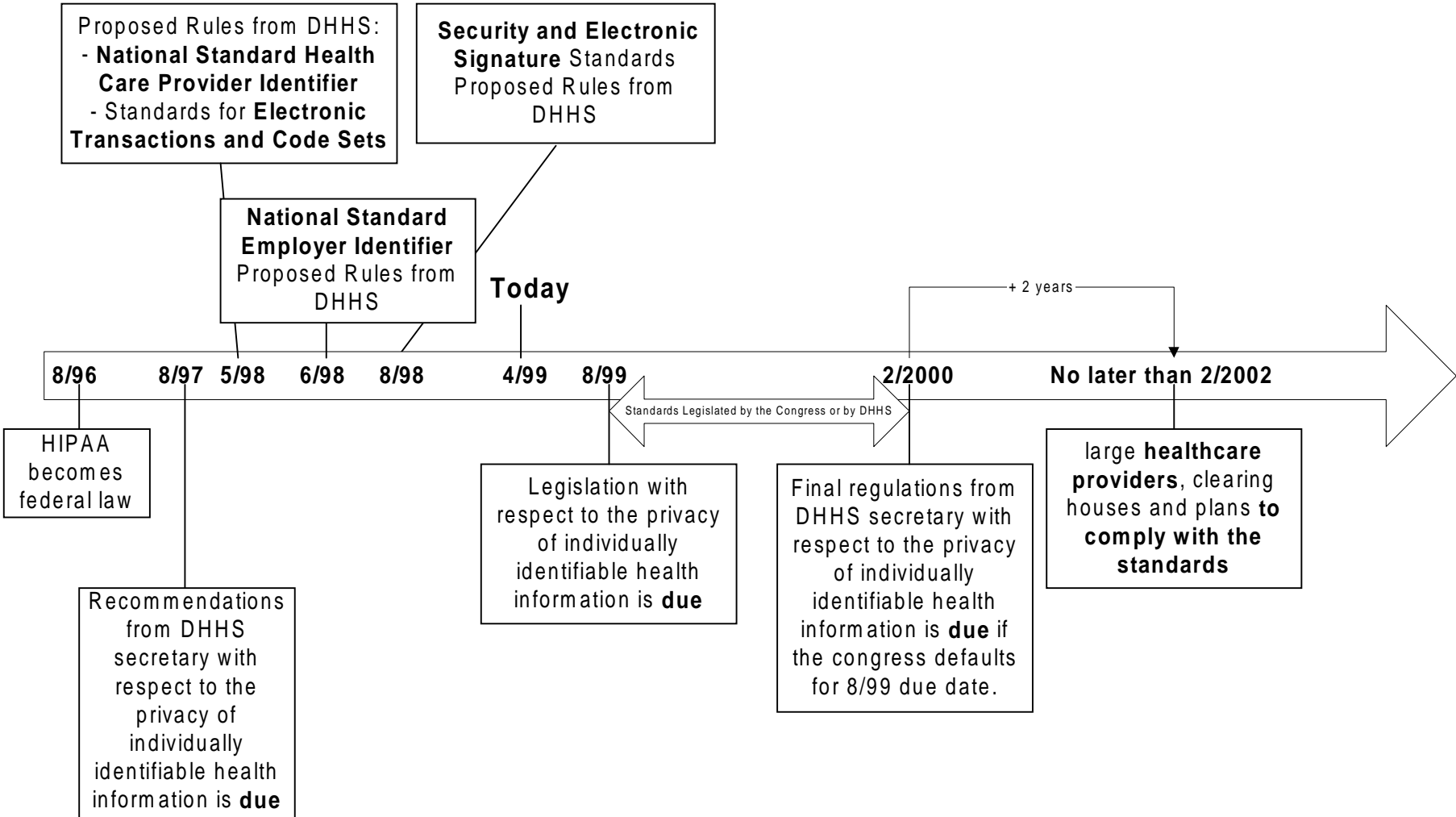
- Financial penalties
  - $< \$100\text{K}/\text{year}$
- Classaction lawsuits because of federal or state legislation breaches
  - Rarely,  $\cong \$100\text{M}$

# HIPAA main parts

as it pertains to healthcare organizations

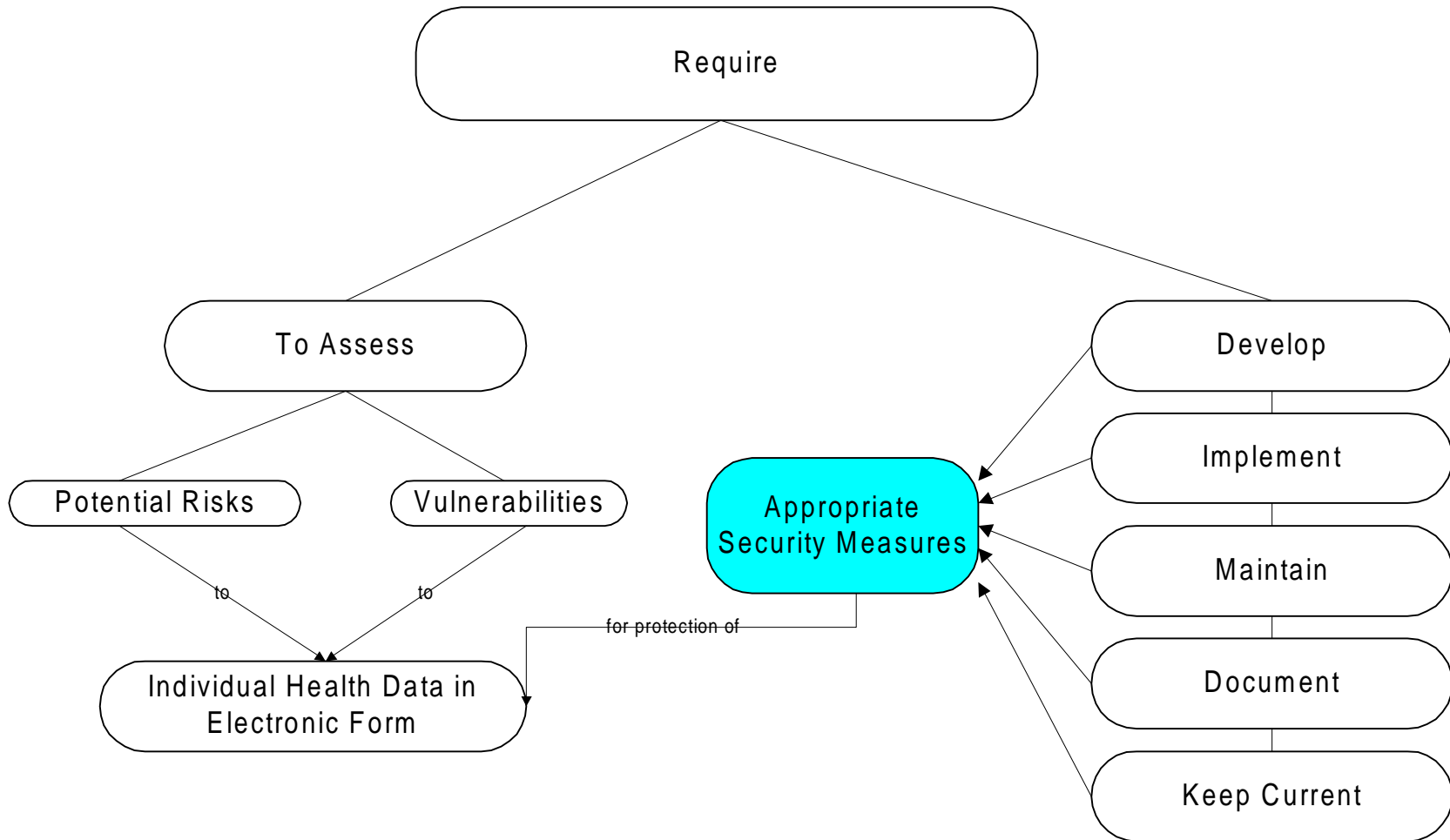


# HIPAA Milestones



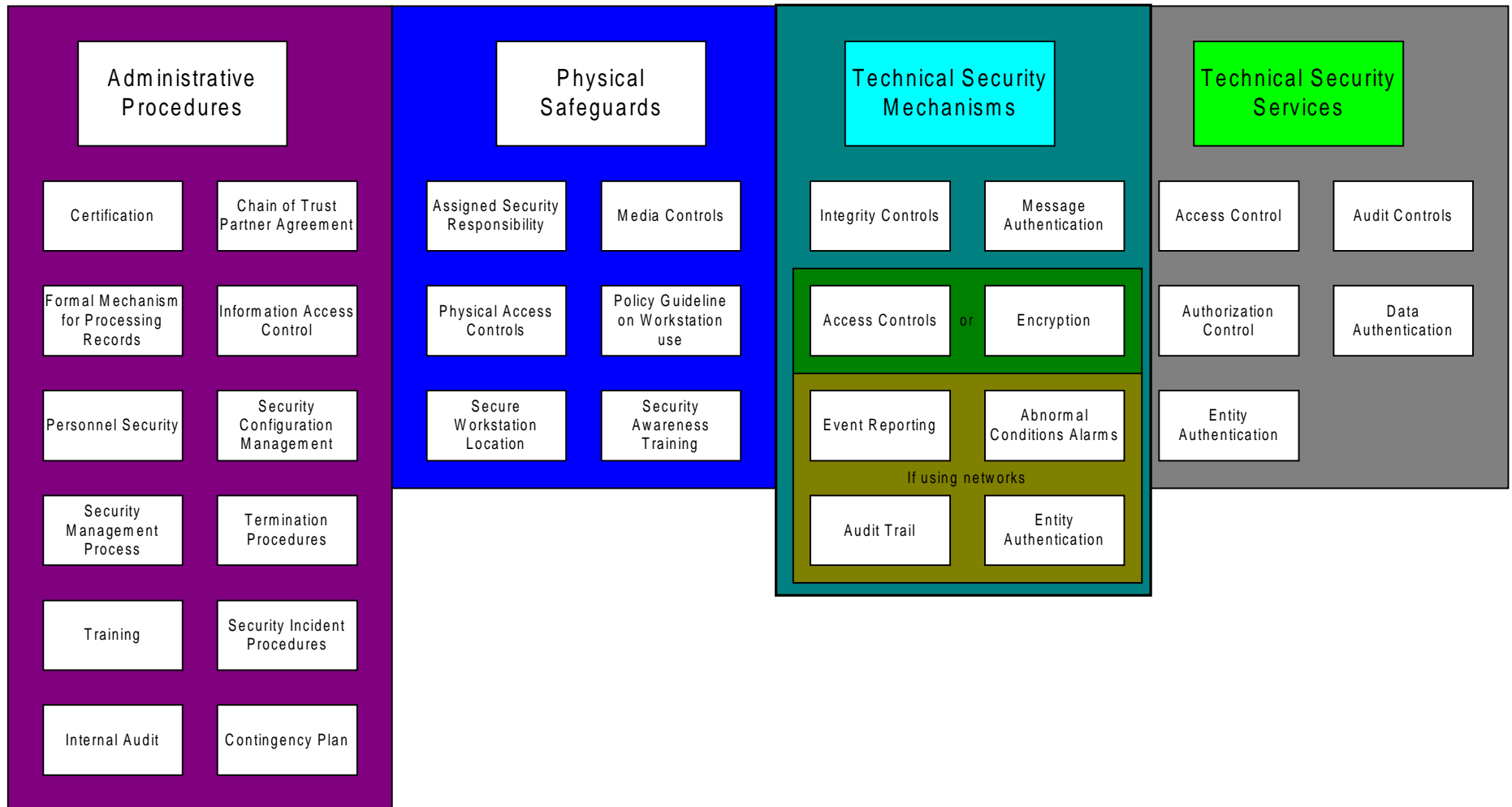
April 19, 1999

# HIPAA: Security Requirements

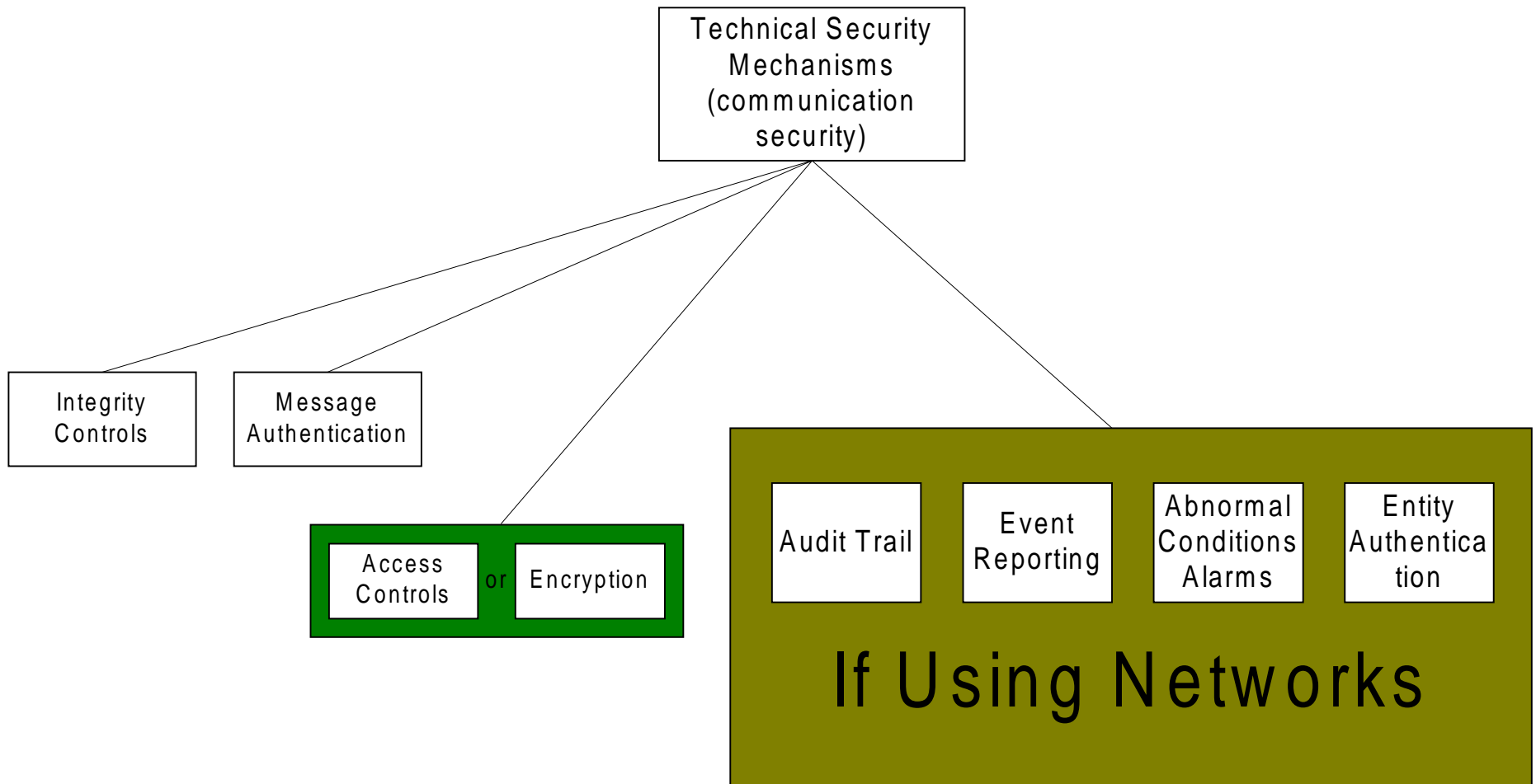




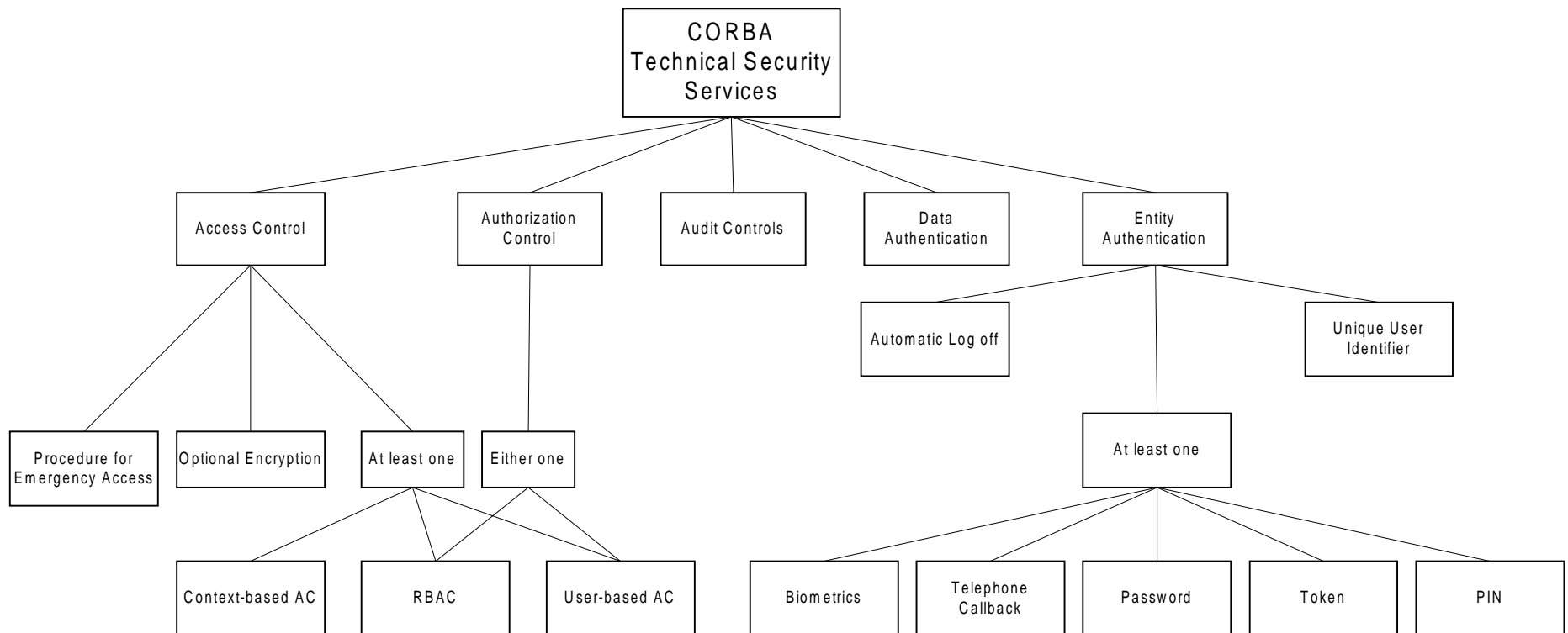
# HIPAA: Security Requirements



# HIPAA: Communication Security Requirements



# HIPAA: Technical Security Services Requirements



# CPR Architecture Goals

- Based on CORBA technology
  - Use CORBA Security, HRAC/RAD
- Integrated with exiting systems
  - Integration via CA's Unicenter/TNG
  - Integration with firewall infrastructure
  - Integration with directory infrastructure
- Integration with upcoming technologies
  - PKI
  - Smart card and biometric authentication

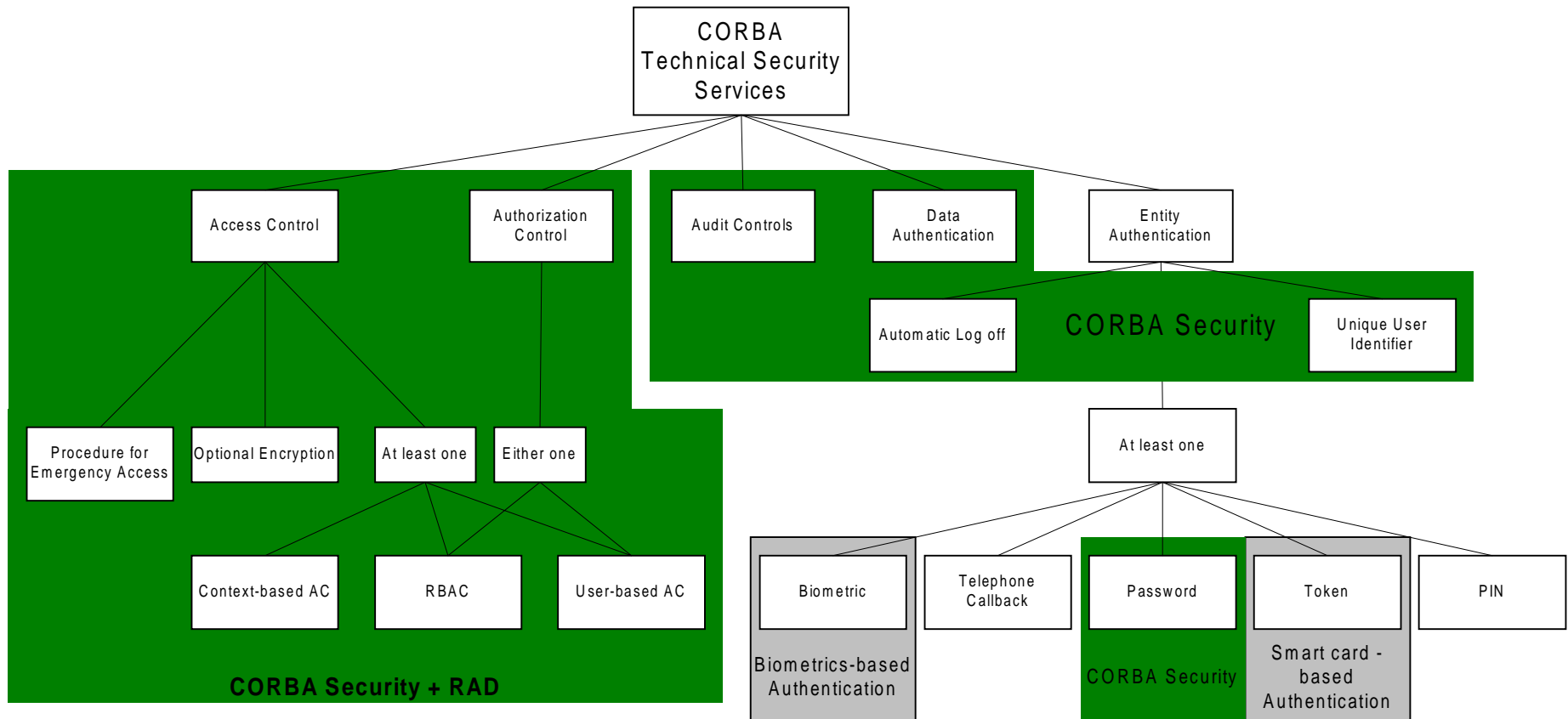
# Current Projects towards CPR security

- SSO with Unicenter/TNG for existing systems
- New firewall
- Computerized Patient Record (CPR) security policies WG
- NDS redesign
- Standard authorization service for application-level access control
- CORBA-security services

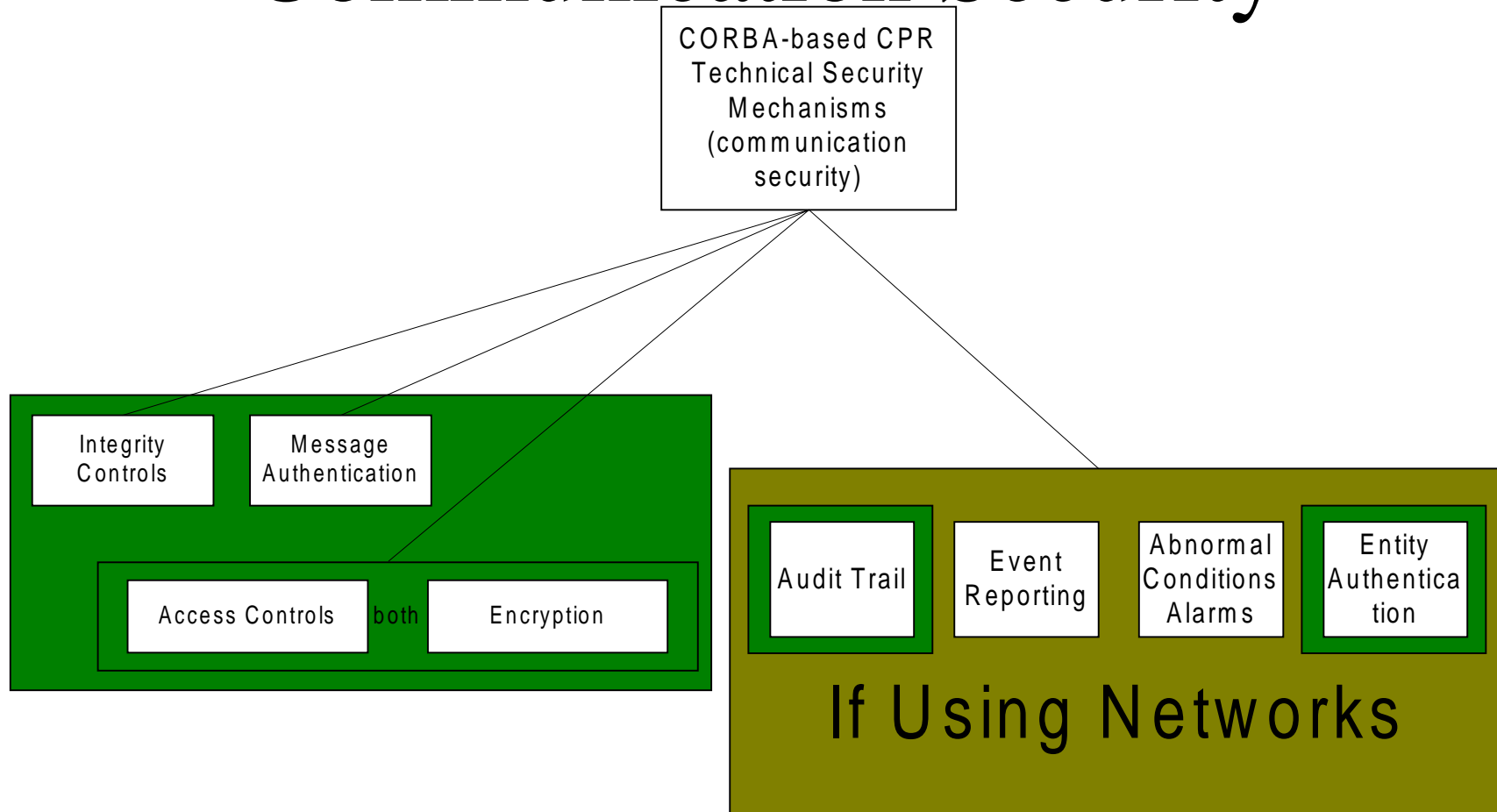
# Future Projects towards CPR security

- PKI
- Smart cards
- Biometric authentication
- VPN

# Security of CORBA Technical Services



# CORBA-based CPR: Communication Security





# FYI: CORBA and RAD

