Security Requirements in Healthcare

Konstantin Beznosov

beznosov@baptisthealth.net

Baptist Health Systems of SF

OMG doc # corbamed/99-03-16

Introduction

- OMG -- forum for software vendors
- What about users?
  - to let them know about distributed technology we need
  - wanted technologies are standardized
- This presentation objective
  - What US healthcare wants from security vendors

Overview

- Risks
- Requirements
  - Security requirements to the healthcare organizations
  - functional and non-functional requirements for security architectures
- BHSSF example to illustrate

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

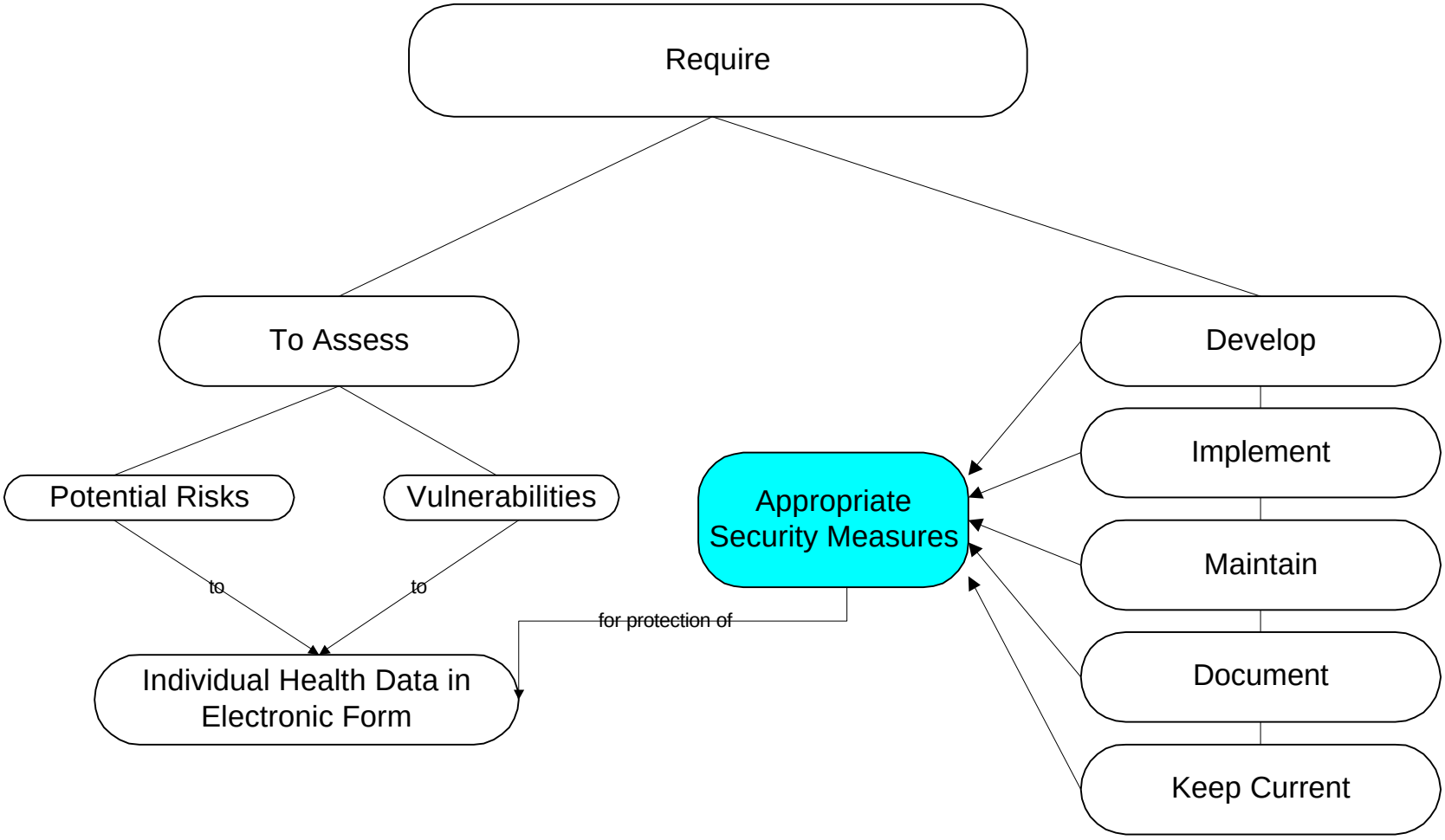
Main Risks: Loss of Money

- 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

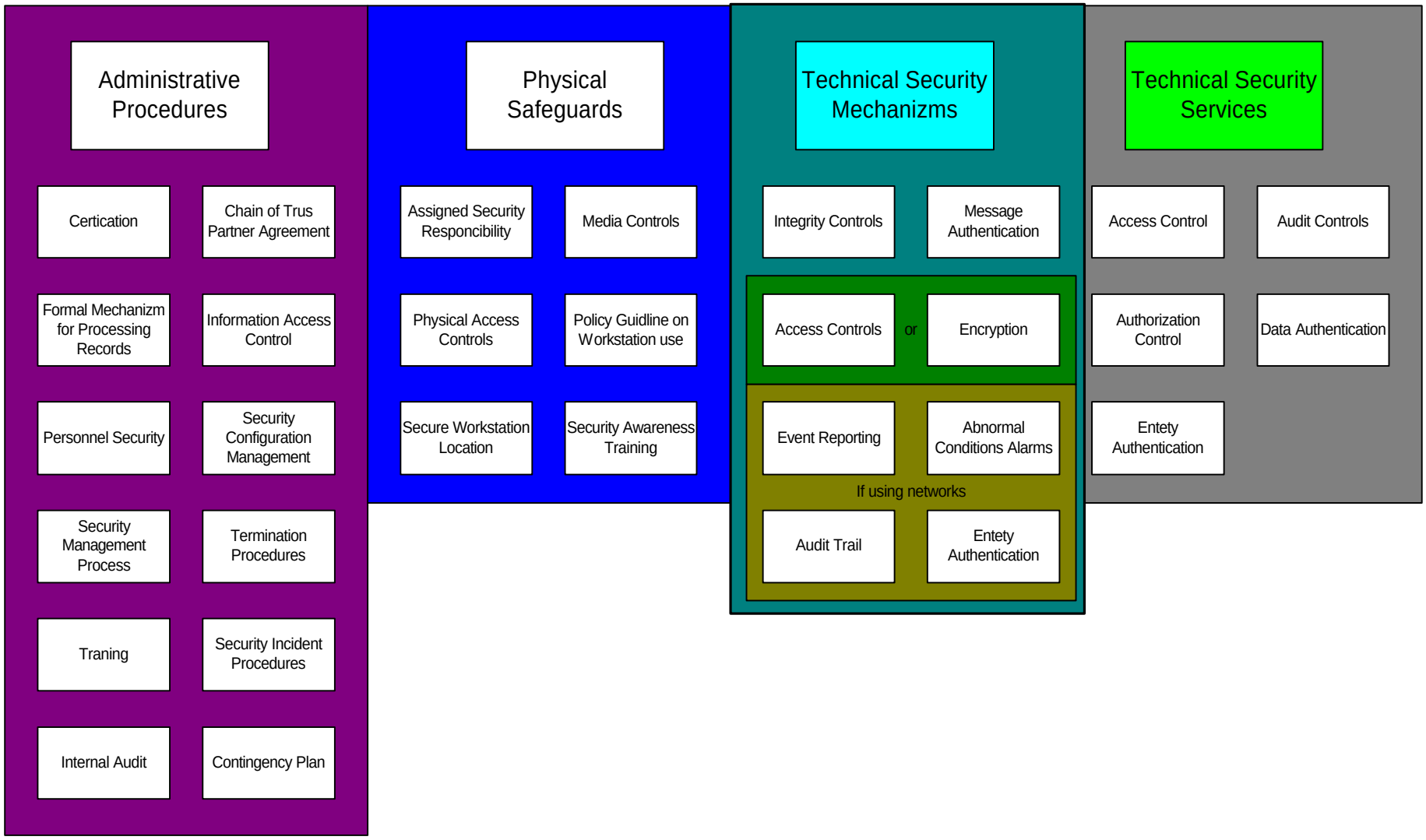
Main Risks: Loss of Money (2)

- Financial penalties
  - < $100K/year
- Class lawsuits because of federal or state legislation breaches
  - Rarely, ≅ $100M

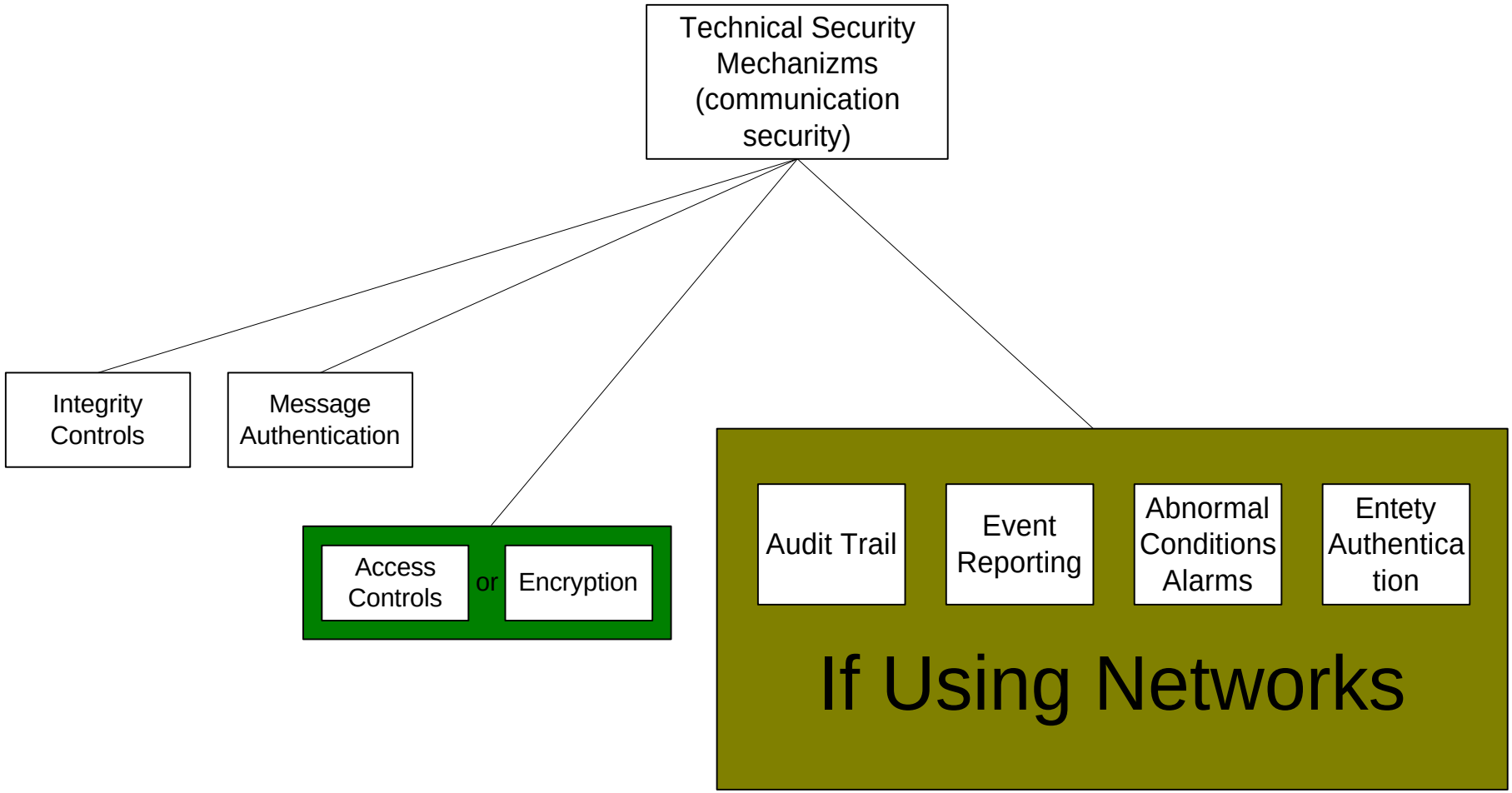
HIPAA: Security Requirements



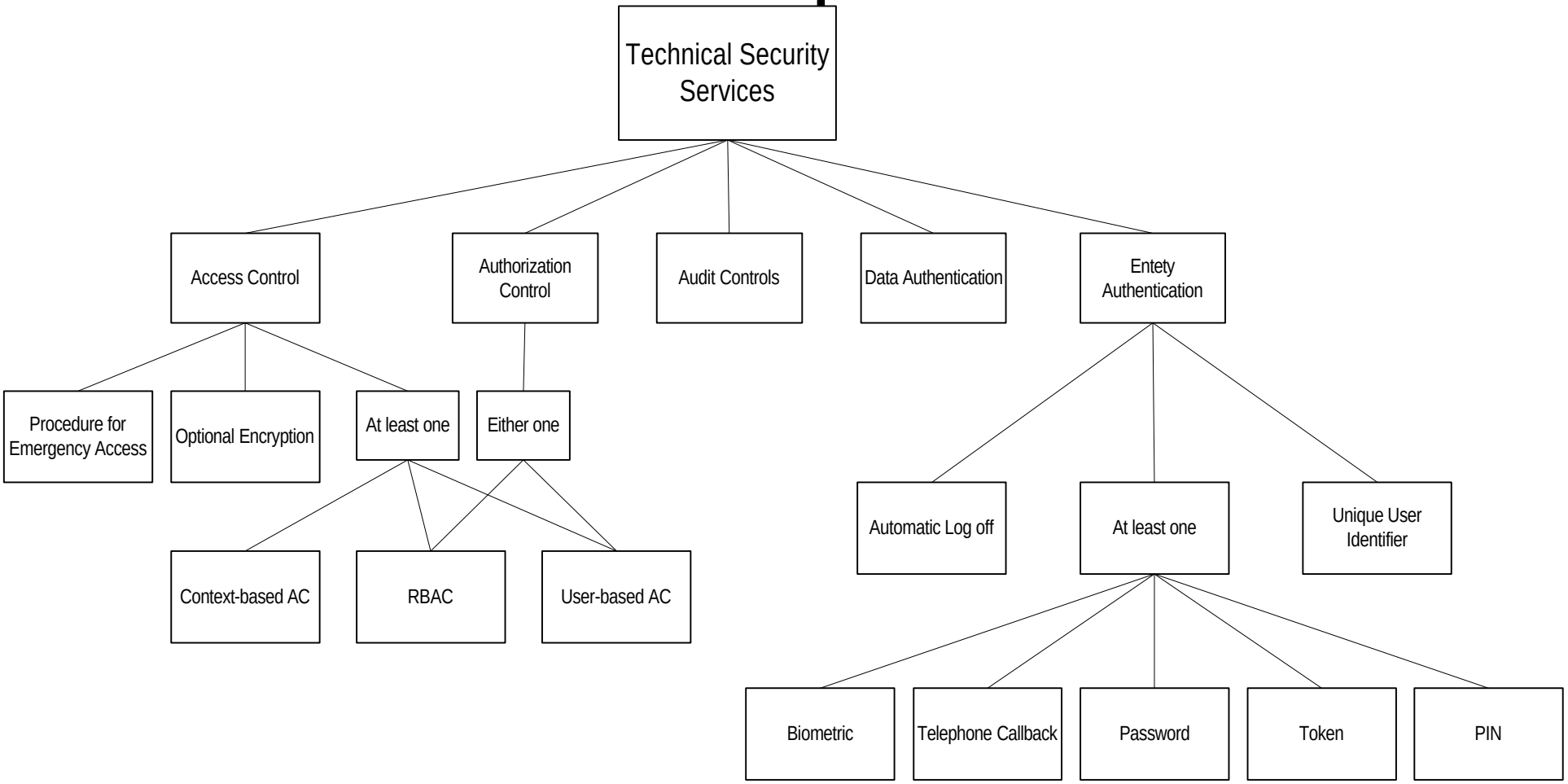
HIPAA: Security Requirements



HIPAA: Communication Security Requirements



HIPAA: Technical Security Services Requirements



BHS Example: Background

- 5 different hospitals and clinics covering most of South Florida residents
- y2k inventory listed about 150 applications
  - probably 50 are pure clinical
- Centralized IT department
- Average IT professional
  - does not have formal CS degree
  - around 5 years of experience in healthcare IT

BHS Example: existing systems

- Clinical systems are from all major vendors
- Separate user name and password for each system
- Developed NDS infrastructure used for file, printer, groupware services
- Firewall, NT-based dial-up
- Deploying CA's Unicenter/TNG for legacy integration; will work with NDS

BHS Example: New Systems

- All CORBA-based
- Use HRAC/RAD for authorization
- Integrated with exiting systems

BHS Example: Security-related Projects

- Computerized Patient Record (CPR) security policies WG -- to produce consistent set of security pollicies
- Consolidation of user security attributes in NDS, and deployment of LDAP gateways
- PKI & smart card plans
- Deployment of CORBA-security services

BHS Example: Functional Requirements for Security

- Enable compliance with HIPAA-related requirements on security and digital signatures
- Enable compliance with state legislation
- Help to pass inspections from state and federal accreditation commissions
- Provide unified (access control, QoP) policy languages.

BHS Example: Nonfunctional Requirements for Security

- Integrate with CORBA technology
- Use LDAP-compliant directory service for storing user security attributes and public keys (at least)
- Integrate with access control mechanisms of legacy systems via CA's Unicenter/TNG
- Provide maintenance and administration tools useful for average IT professionals
- Be known, reliable and dependable vendor