



F E D E R A L
S T U D E N T A I D
We Help Put America Through School

System Security Officer Briefing: FSA Security and Privacy Architecture Framework

August 26, 2003

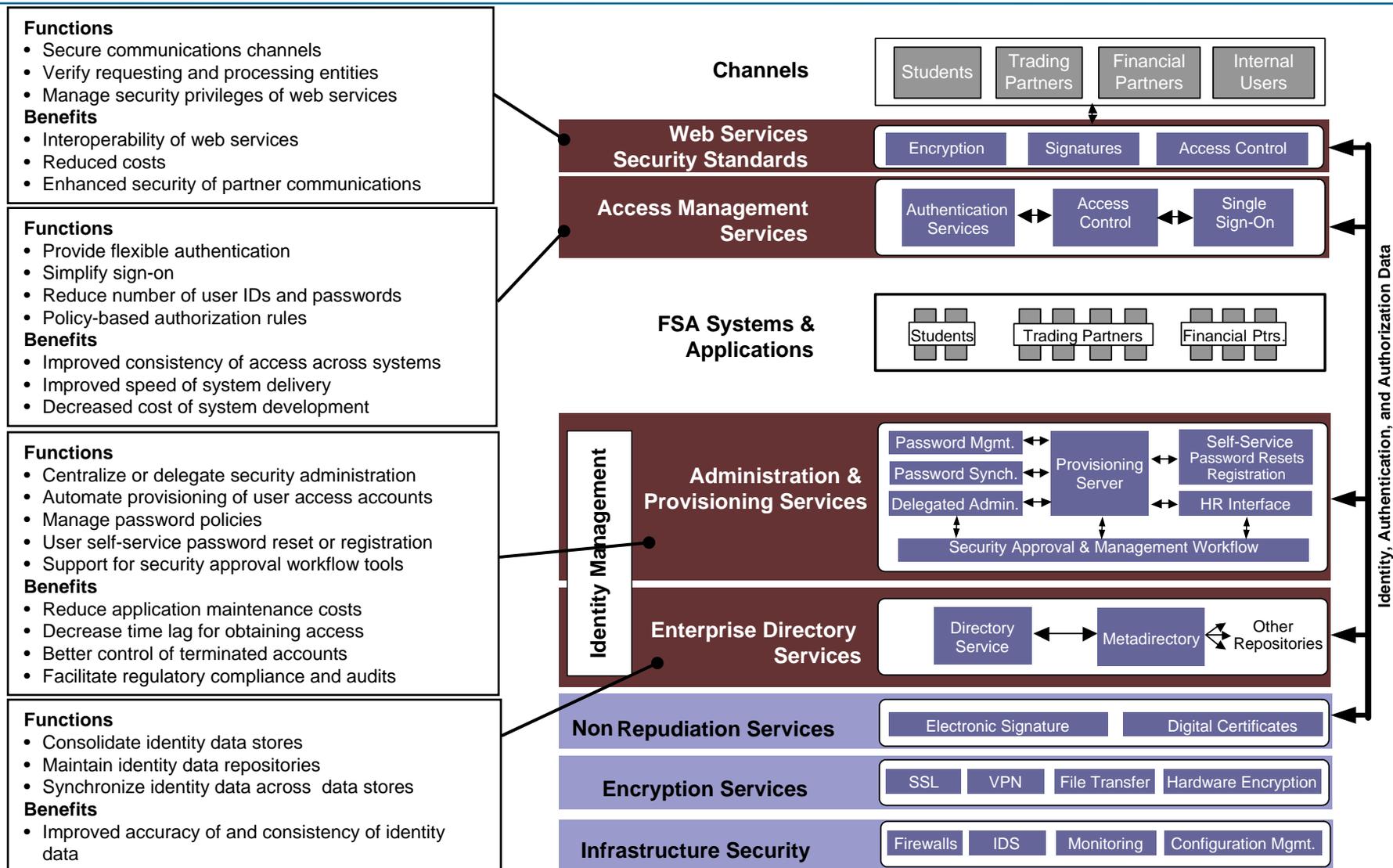


Objectives for the Security & Privacy Architecture

- Improve FSA security and privacy controls to protect FSA systems and information:
 - Confidentiality
 - Integrity
 - Availability
 - Accountability
- Simplify security design and deployment
 - Speed development of systems
 - Capture successful and proven security solutions
 - Promote structured, systematic, and repeatable security controls
 - Increase consistency of security across FSA systems
- Identify security functions that can be deployed as security services
 - Decrease cost, effort, and risk associated with development of security functions
 - Define technical services, components, and standards that will simplify compliance with regulatory requirements



Proposed Security & Privacy Architecture Vision



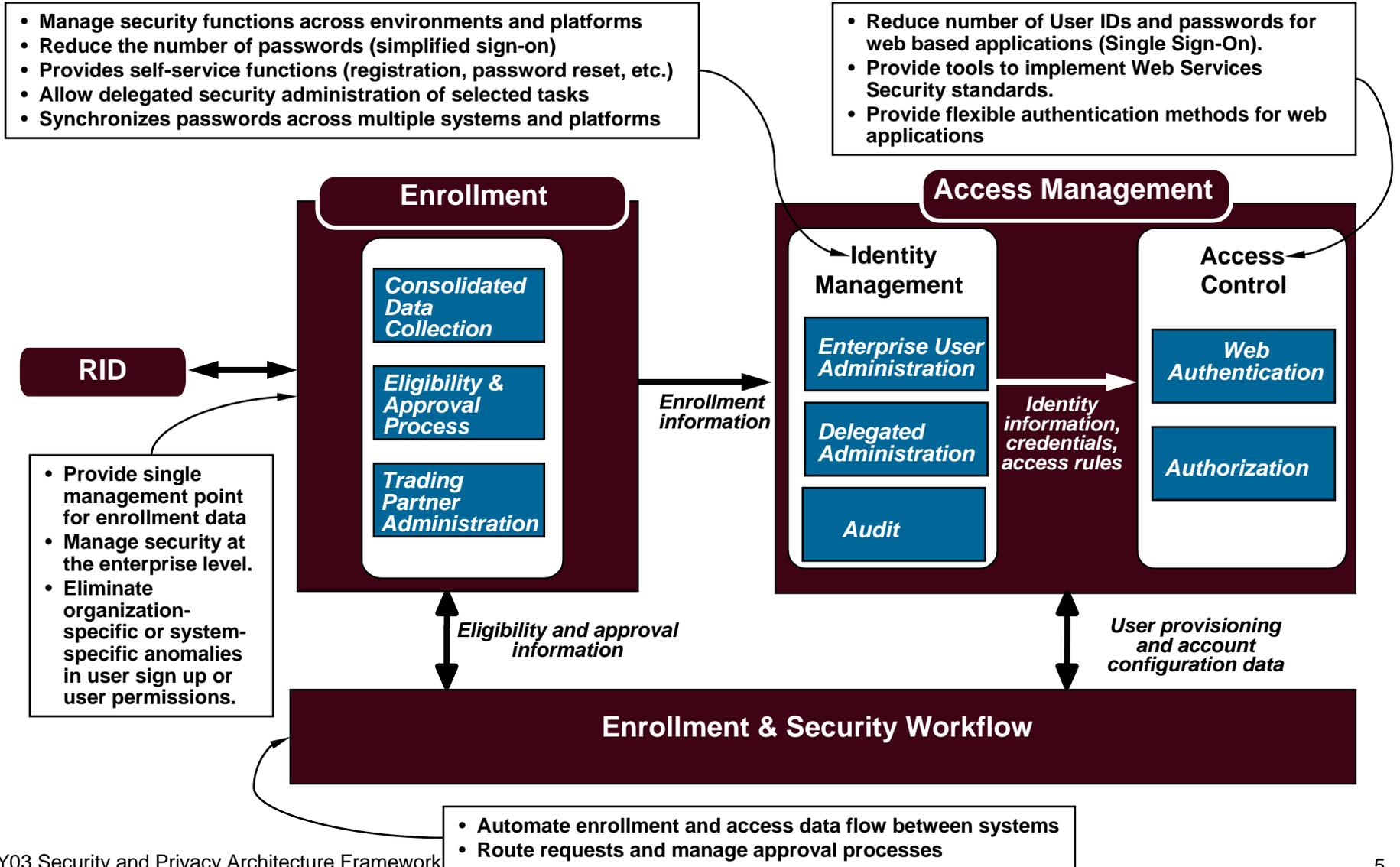


Key Points and Next Steps

- The FSA Security and Privacy Architecture will need to be updated periodically
- Communicate Security & Privacy Architecture Vision
- Select and define FSA security functions that can be deployed as services
- Coordinate with business initiatives to define common requirements for security architecture services
 - Data Strategy (Enrollment and Access Management, Technical Strategies)
 - PIN Reengineering Analysis
- Develop standards to support the Security & Privacy Architecture, e.g.,
 - Web security standards
 - Data classification
 - Enterprise authorization standards and access roles
 - Standards for web services security
- Create security architecture standards for outsourced services
 - Network security
 - Security monitoring



Example: Enrollment & Access Management Vision

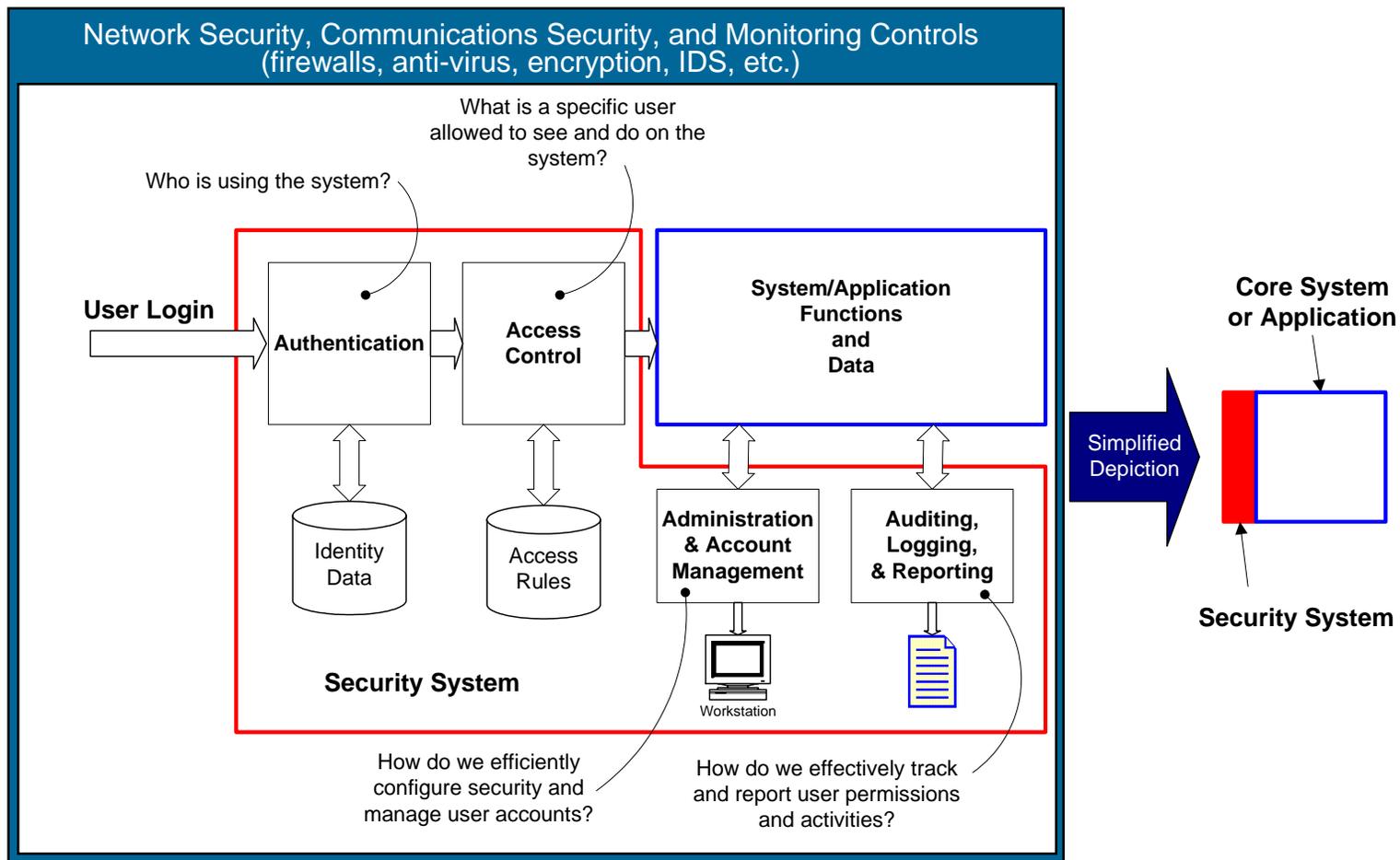




Appendix A: Generic Application Security Functions

This diagram shows a simplified view of security functions commonly built into individual systems or applications.

- The callouts show high-level business questions and functions addressed by each type of security component.
- The outermost box in the diagram represents the perimeter and infrastructure security functions required for a complete security capability.

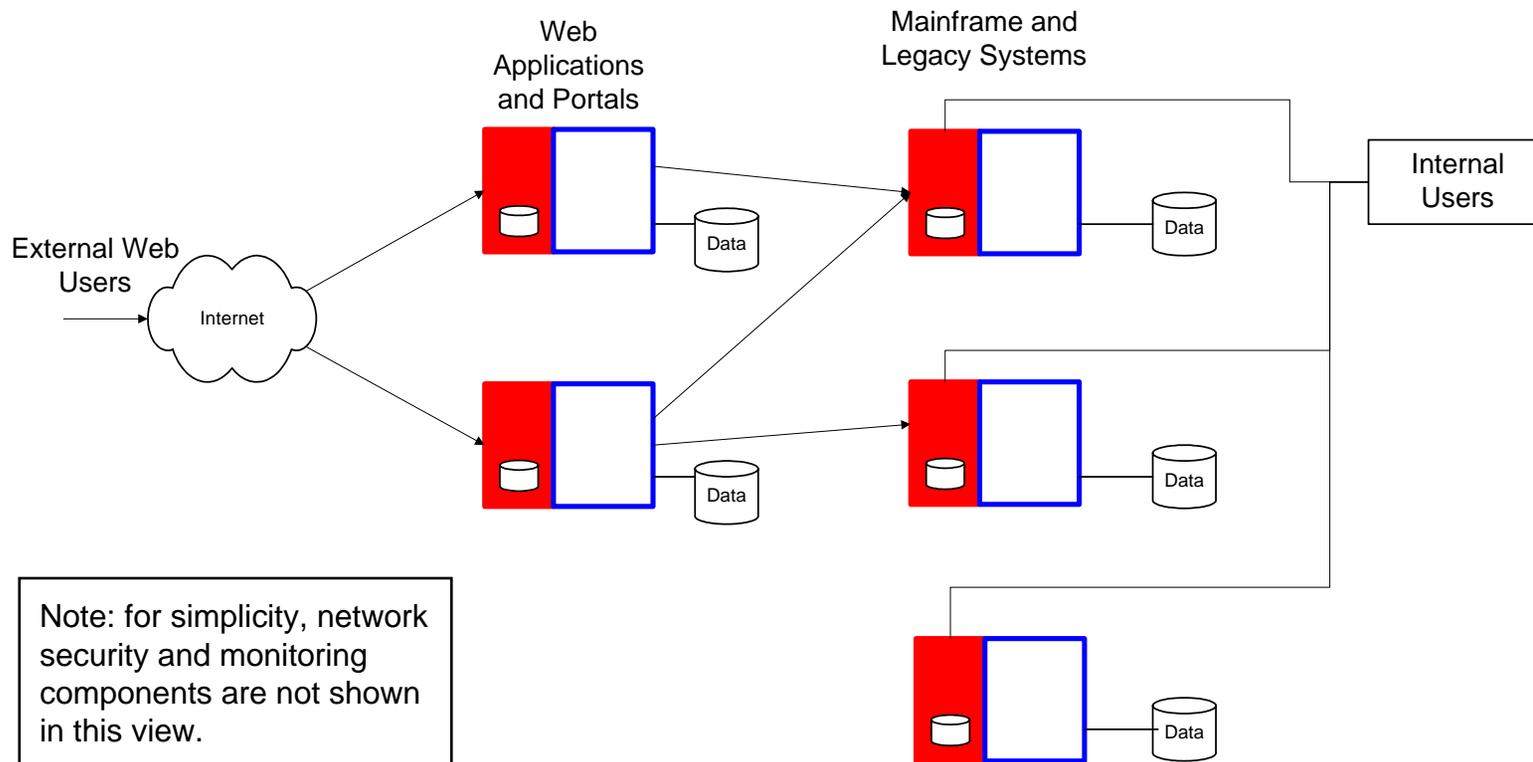




Appendix B: Typical Application Architectures

The diagram below shows a more typical situation, with multiple web applications and mainframe or legacy systems interacting to perform a business function.

- Each system or application has its own security functions and security database.
- As a result, identity and profile information for users with access to multiple systems must be configured and managed in separate operations using different administrative interfaces.





Appendix C: Proposed Security Services

Security Services proposed for the FSA Security Architecture include Identity Management and Web Access Management.

- Access Management provides login and authentication functions for multiple web applications.
- Identity Management provides enterprise administrative and management functions by communicating with the security components of systems across the organization.

