Veterans Health Administration

Presentation to the Federal Health Care Public Key Infrastructure (PKI) Work Group

28 March, 2001

Mike Davis (SAIC)
VHA Security Architect

GCPR Overview

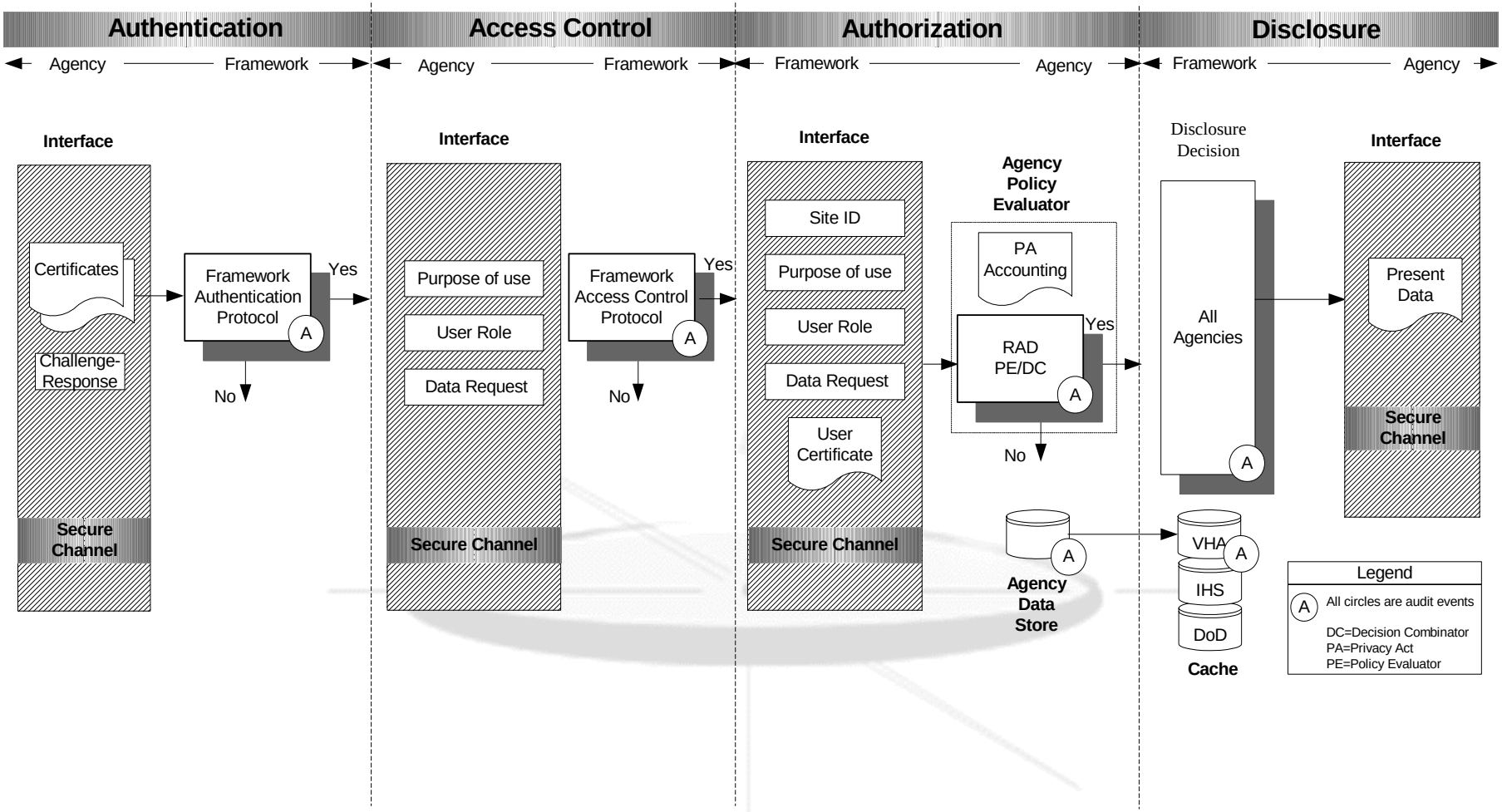
- The GCPR Framework is a middleware framework to connect healthcare systems within and between organizations.
- It is a component-based infrastructure for information interchange between disparate systems.

A single standards-based authentication service using PKI

Role, entity or context based access policy

RAD-based authorization
Agency-side PA accounting
Patient control through consent

RAD-based disclosure
Verifiable Trust
No blind Trust



Pervasive Audit Service

Strong user authentication.

Access to framework with a purpose of use and user role compatible with the sensitivity of information requested.

Full accountability-Each access auditable
No anonymous access to agency data.
Agency managed policy evaluator
Agencies accounting for all disclosures of data

Framework executes agency authorization policies

GCPR Security Issues

//////////////////ISSUES //////////////////

- How to establish assured user identity (authentication)?
- How to achieve trust between organizations?
- How to establish role information (authorization)?
- How to achieve interoperability?
  - Among Federal Agencies
  - Among Private Sector participants

GCPR Authentication

Provide assured, strong user authentication to the framework as the basis for any further service.

- Use agency PKI to set the authentication bar
- Use X.509 V3 identity information
- No GCPR user accounts

In GCPR there are three identification and authentication methods:

1. **System Entity Authentication**. In system entity (application or server) authentication, an agency server authenticates itself to the framework.
2. **User Entity Authentication**. In user entity (person) authentication, an agency user (person) authenticates directly to a authentication server (either agency heritage system=Local user authentication or Framework).
3. **Distributed Authentication**. In distributed authentication, agency system entity authentication and user entity authentication (Local user authentication) is combined to forward user authentication (X.509 V3 certificate) information to the framework. The Framework uses this information just as though the user had authenticated directly to the Framework.

GCPR Authorization

Provide a purpose of use and verified access rights compatible with data sensitivity.

- Use OMG RAD
- Implement Patient Consent (Privacy)
- May be Facilitated through HC CP Extensions for:
  - Roles
  - Licenses
  - Credentialing

The authorization interface provides information to an agency Resource Access Decision (RAD) that allows the agency to decide whether or not to release healthcare information to the Framework. Information provided on the authorization interface includes:

•Site ID of the requesting agency system

•Purpose of use (4)

•User role

•Specific data requested

•User information from X. 509 V3 Certificate

The authorization interface provides information sufficient for an agency to maintain a record of accounting of certain disclosures in accordance with the requirements of the Privacy Act. The information is also sufficient to allow an agency to maintain a continuous security audit trail recording all disclosures made to all individuals through the GCPR Framework.

GCPR Trust

Ensure verified Trust-No blind trust.

- Use Federal Bridge CA CP
- GCPR Security Policy
- Other authentication methods must provide same level of trust as PKI

In order for GCPR's distributed authentication method to be trusted, both the agency-strong authentication method and shared security policy must be known.

GCPR agencies will use a PKI-based identification method and published security policies that guarantee a consistent and verifiable level of trust between agencies.

GCPR Interoperability

Develop architecture that is requirements and standards based.

- Establish Interoperability (both Federal and Private Sector) through Standards:
  - Applicable Federal Standards
  - OMG RAD (ANSI Std?)
  - PKI
- Monitor development of ASTM Standards
  - ASTM PMI
  - ASTM HC CP

Summary

- Agency PKI provide a means to implement distributed security services required by GCPR and VHA Security Architectures.
- Federal PKI CP, Federal HC CP and ASTM CP facilitate inter-agency trust.
- HC PKI CP may support intra and inter-agency authorizations (role /context/entity-based) and patient privacy through certificate extensions.

ASTM Standard
Healthcare Certificate Policy

March 28, 2001

Status Report

Background

- ASTM E31 Healthcare informatics consensus standard
  - Healthcare Certificate Policy is nearing completion after 3 year development effort
  - Balloting targeted for May 2001
- Contributions from 60 different healthcare organizations
  - Scope and applicability defined for the healthcare industry
  - Includes subscriber classes and applications that address the creation, access or disclosure of patient information and supporting processes

Adoption

- Industry support
  - Draft form: Kaiser, SSA, California Medical Association with California pilot projects underway
  - Adoption by VA pending resolution of Federal PKI policy issues
- Commercial CA support
  - Draft form: Arcanus, CHIMETrust, MEDePass
  - Pending final form: Entrust, Baltimore
  - Evaluating: Certicom

Mapping to Federal Policy

- Comparison of ASTM Policy to FBCA Policy
  - 30 items identified to meet FBCA medium assurance level
  - ASTM has removed conflicts for all but 2
  - Remaining items reflect unique healthcare requirements
    - Suspension
    - CRL refresh rate
  - Solicit assistance of Federal HC PKI Workgroup to support reconciliation with FBCA
  - Would like input for May ASTM committee meeting

End