U.S. Federal e-Authentication Initiative

TERENA 2003

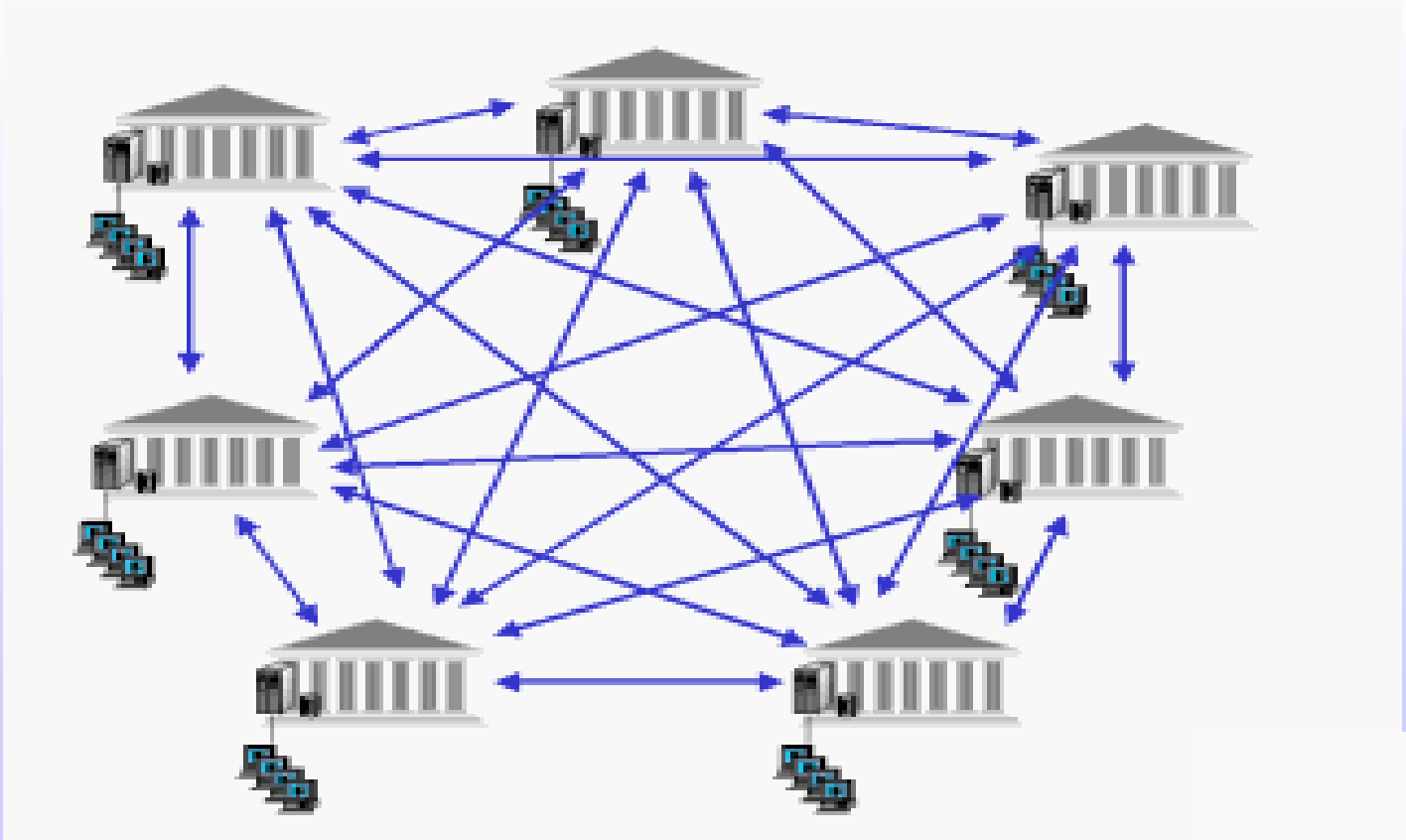
Peter Alterman, Ph.D.
Senior Advisor to the Chair, US Federal PKI Steering Committee

U.S. e-Authentication Initiative Goals:

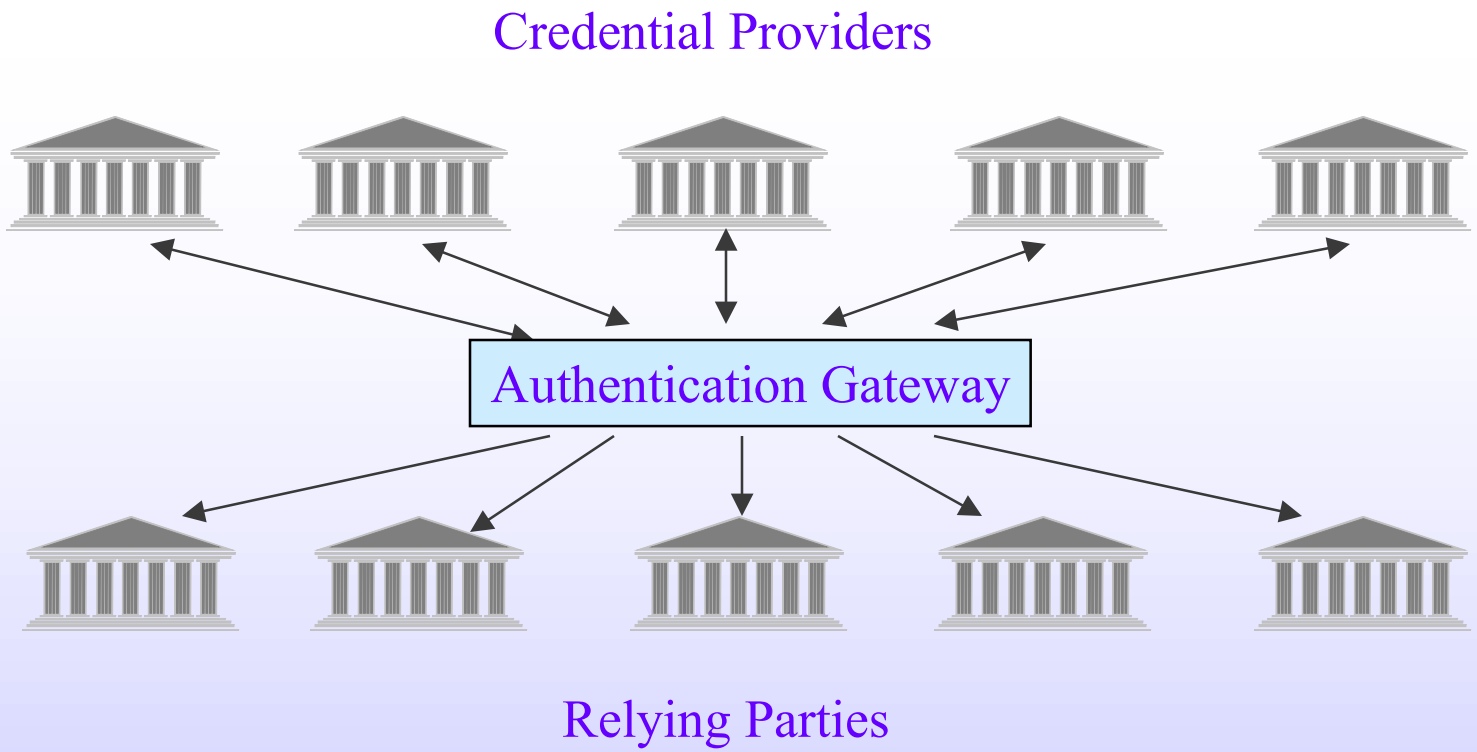
- To build and enable mutual trust needed to support wide spread use of electronic interactions between the public and Government, and across Governments
- To minimize the burden on the public when obtaining trusted electronic services from Government agencies
- To deliver common interoperable authentication solutions, ensuring they are appropriate matches for the levels of risk and business needs of each e-Government initiative

The Challenge to Interoperability

Authentication interoperability becomes much more complex as the number of credential providers and relying parties increases.

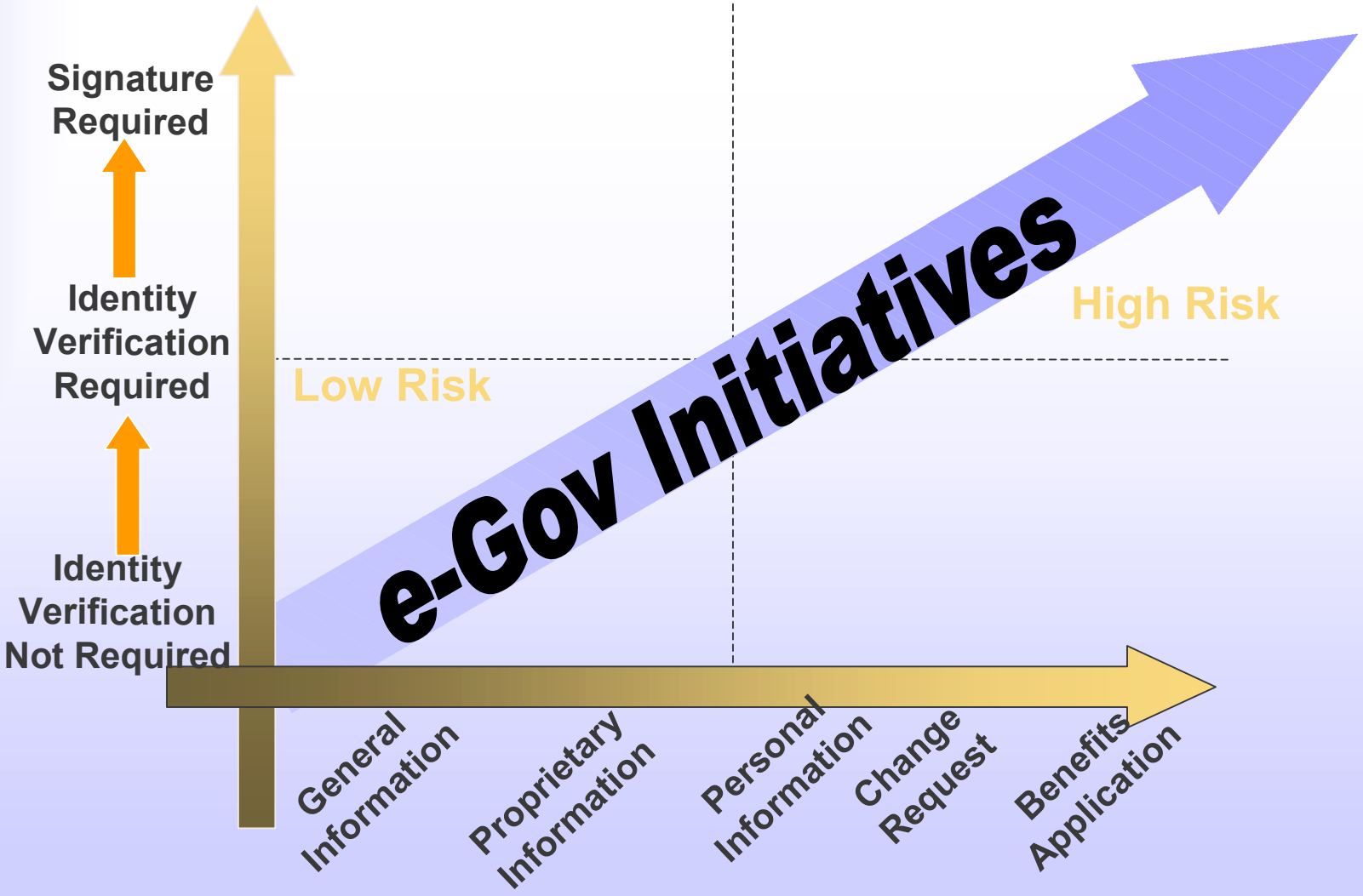


The Need for the Authentication Gateway



- The Authentication Gateway simplifies interoperability:
  - Common way to determine and validate "Trusted" credentials
  - "Common Rules" for Agreements among Gateway, Agencies and Credential Providers.

Defining the Need



Privilege Management

A Vision for the Future

Citizen

Agent

Business

Direct Access Capability Preserved

Identity Verification Not Required

FIRSTGOV
Your First Click to the U.S. Government

Identity Verification Required

Credential Providers

State or Federal Government

Credential Validation Process

Health Care

Federal Agency Relying Parties

USDA

eAuthentication Gateway

Academia

The U.S. e-Authentication Gateway

- **Is not:**
  - An issuer of ID credentials
  - A collector of personal information
  - A repository of information
  - The Federal Bridge Certification Authority
  - e-Security
- **Is:**
  - A provider of validation services for multiple forms of ID credentials
  - A source of risk/assurance levels for multiple forms of ID credentials
  - Available for all e-Gov initiatives

Status of U.S. e-Authentication Program

- R&D has shown that the E-Auth industry is currently:
  - Enterprise-based rather than inter-enterprise
  - Centrally managed rather than distributed
  - Proprietary solutions rather than open
  - Priced for the enterprise rather than multi-enterprise
- The RFI responses and other research has shown that the E-Auth industry is:
  - Adopting federated solutions
  - Evolving to distributed management
  - Utilizing open standards
  - Adapting pricing to multi-enterprise solutions
- Agency E-Gov systems are becoming ready to utilize a common open, standards-based e-Auth infrastructure

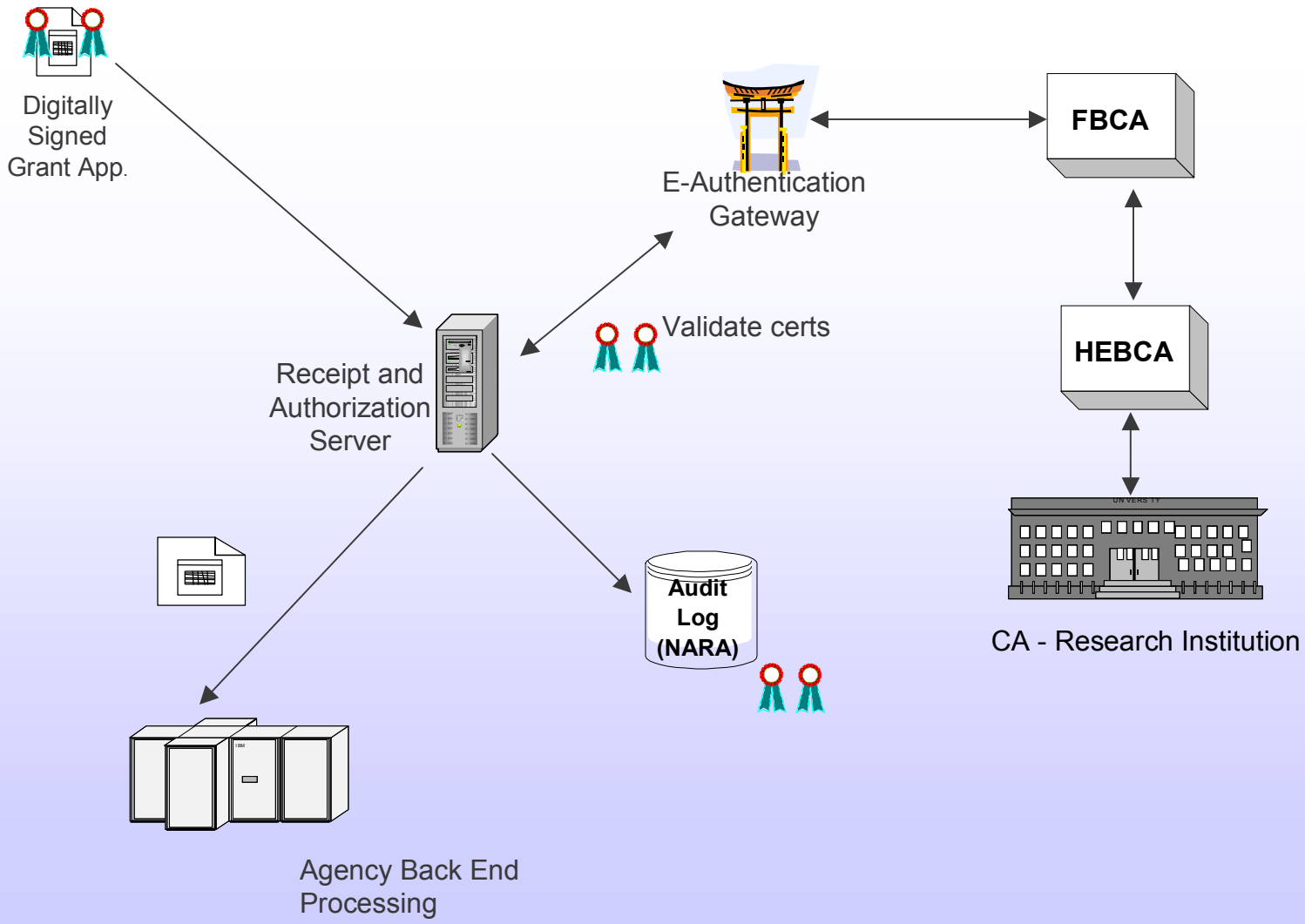
U.S. e-Authentication Message to Government:

- Prototype Gateway is operational in a test environment as of 9/30/02
- It will undergo a delta certification and accreditation (C&A) for live transactions by 01/06/03
- Gateway will provide authentication and verification services to the 24 e-Gov initiatives
- Gateway will provide authentication services across Government lines of business

U.S. e-Authentication and Higher Education:

- E-Grants project will create standard XML objects to assemble various grant application "forms"
- Universities will fill out forms locally and upload them to the e-Grants site
- Extended NIH-EDUCAUSE PKI Interoperability Pilot Project will:
  - Use e-Grants XML forms
  - Incorporate the e-Authentication Gateway into the certificate validation path
  - Demonstrate alternate signing and authZ approaches

Simplified Concept of Operations



Contact Information

- Dr. Peter Alterman, Assistant Chief Information Officer for Electronic Authentication, NIH
  - Peter.alterman@nih.gov
- Deborah Blanchard, Project Manager, Digital Signature Trust / Identrus
  - dblanchard@trustdst.com