



**Federal PKI**  
**Management Authority**  
**Enabling Trust**

**GSA**

# FPKIMA Industry Day

## Shared Service Provider (SSP) Discussion Panel

Federal PKI Management Authority  
March 23, 2015

*Enabling Trust in the Federal Government*



# Agenda

- Background
- Program Overview
- Panel Participants



# SSP Program Background

- 2003, OMB E-Authentication memo directed federal agencies to use internal or commercial PKI services
- 2005, OMB M-05-05 directed GSA to create the SSP Program to provide strong oversight of PKI service providers and require Agencies to purchase PKI services
- 2015, six approved providers:
  - Entrust
  - Symantec
  - Operational Research Consultant (ORC)
  - Verizon Business
  - Treasury
  - GSA (USAccess – MSO)



# SSP Program Overview

- Intent of the program is to facilitate outsourcing of PKI services by Federal agencies
- Vendors must comply with the following provisions to be an approved provider:
  1. Operate under the federally owned Federal Common Policy Certificate Policy
  2. Comply with assessment and authorization (A&A)
  3. Receive approval from a Designated Authorizing Official (ATO)
  4. Demonstrate compliance with an annual third-party audit



## SSP Program Value

- High level of trust in government credentials from commercial service providers
- High level of trust in the commercial service provider PKI operation
- Government-only focus



# SSP Provider Certificate Policies

- Software certificates (digital signature, encryption, device and derived PIV)
- Hardware and authentication certificates (i.e. PIV and other hardware-based tokens, derived PIV, and device)
- High assurance credentials (LOA4)



## Panel Participants

- Entrust – Mike Wisner
- ORC – Richard Webb
- Symantec – Steve Kruse
- Verizon – Russ Weiser