

# Virginia e-Identity

Mike Farnsworth



# The Phases of Evolution

- ▶ Initiation
- ▶ Concept
- ▶ Challenges
- ▶ Model Forward

# Initiation

- ▶ White Paper (Virginia Council on Technology Services)
  - ▶ Educational
  - ▶ Visionary, yet controversial
- ▶ Business Problem – Affordable Care Act/eHHR
- ▶ Strategic Alignment
  - ▶ COVA
  - ▶ AAMVA
  - ▶ CSDII
- ▶ NSTIC

# Concept

- ▶ Private sector authentication benefits not typically seen in government
  - ▶ Lower administrative costs, reduced theft and better/cheaper service to customers
  - ▶ Not using this technology results in losses

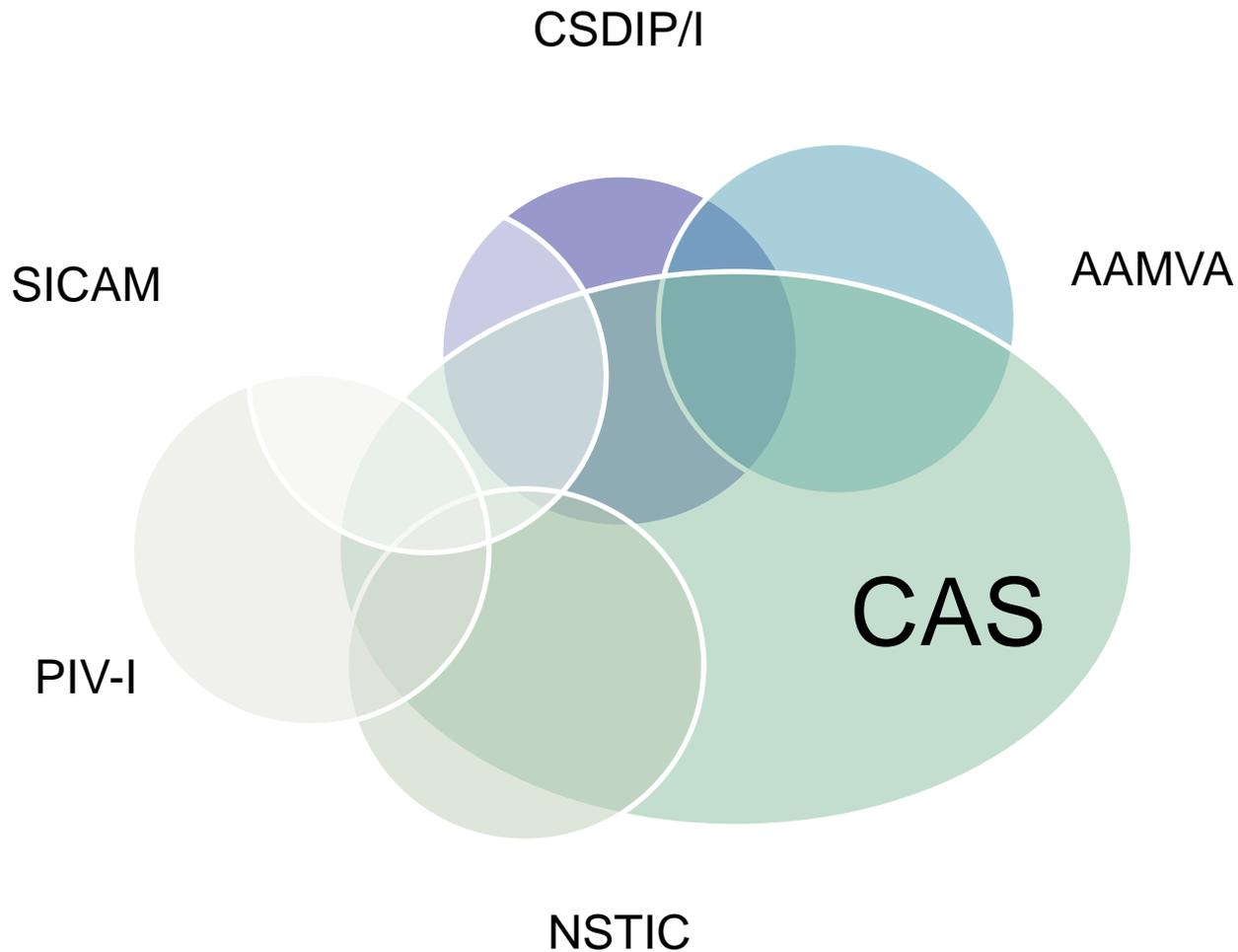
# Challenges

- ▶ Initial Funding
  - ▶ Healthcare (ACA)
  - ▶ NSTIC
- ▶ Self Sustainment – Long term value proposition
- ▶ Monetization – (However, not about making money!)
- ▶ Privacy – NSTIC framework guidelines

# Challenges

- ▶ Partnering States – Must demonstrate interoperability
- ▶ Interagency Relationships – Policy, regulations, territorial
- ▶ Legislative Impact
  - ▶ Liability
  - ▶ Public Perception

# Model Forward



# What is NSTIC?

Called for in President's Cyberspace Policy Review (May 2009): a "cybersecurity focused identity management vision and strategy"

NSTIC calls for an **Identity Ecosystem**, "...an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities."

## Guiding Principles

- Privacy-Enhancing and Voluntary
- Secure and Resilient
- Interoperable
- Cost-Effective and Easy To Use



# What does this mean to VA?

- On Sept. 20, 2012, NIST awarded more than \$9 million for pilot projects in support of NSTIC
- Five U.S. organizations will pilot identity solutions that increase confidence in online transactions, prevent identity theft, and provide individuals with more control over how they share their personal information
- AAMVA in partnership with VA Department of Motor Vehicles, Microsoft, CA Technologies, AT&T and Biometric Signature ID was one of the 5 organizations selected out of 187 applicants



# Cross-Sector Digital Identity Initiative (CSDII)

Paul E Blanchard

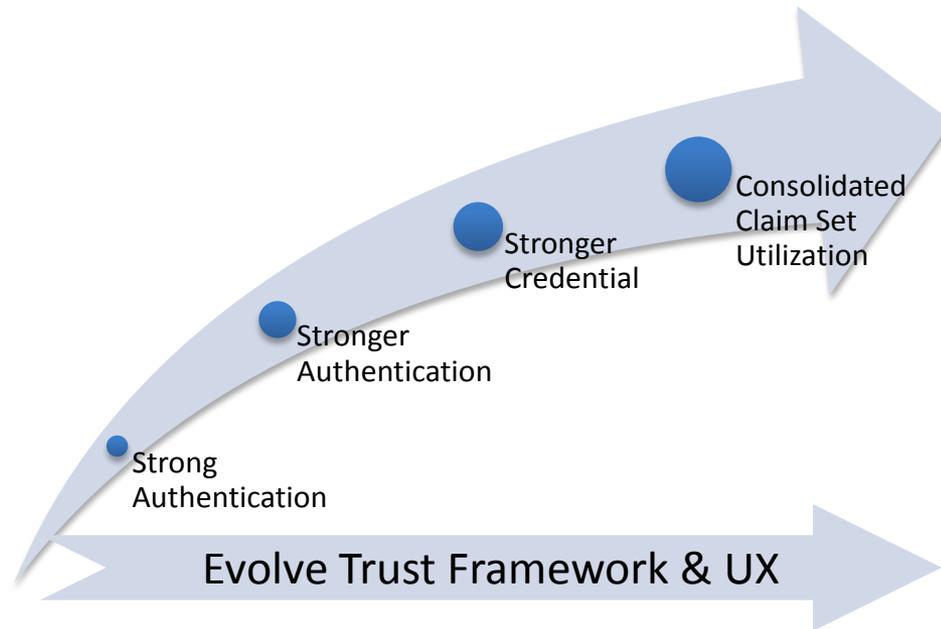


Work described in this presentation was supported by the National Strategy for Trusted Identities in Cyberspace (NSTIC) National Program Office and the National Institute of Standards and Technology (NIST).

The views in this presentation do not necessarily reflect the official policies of the NIST or NSTIC, nor does mention by trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

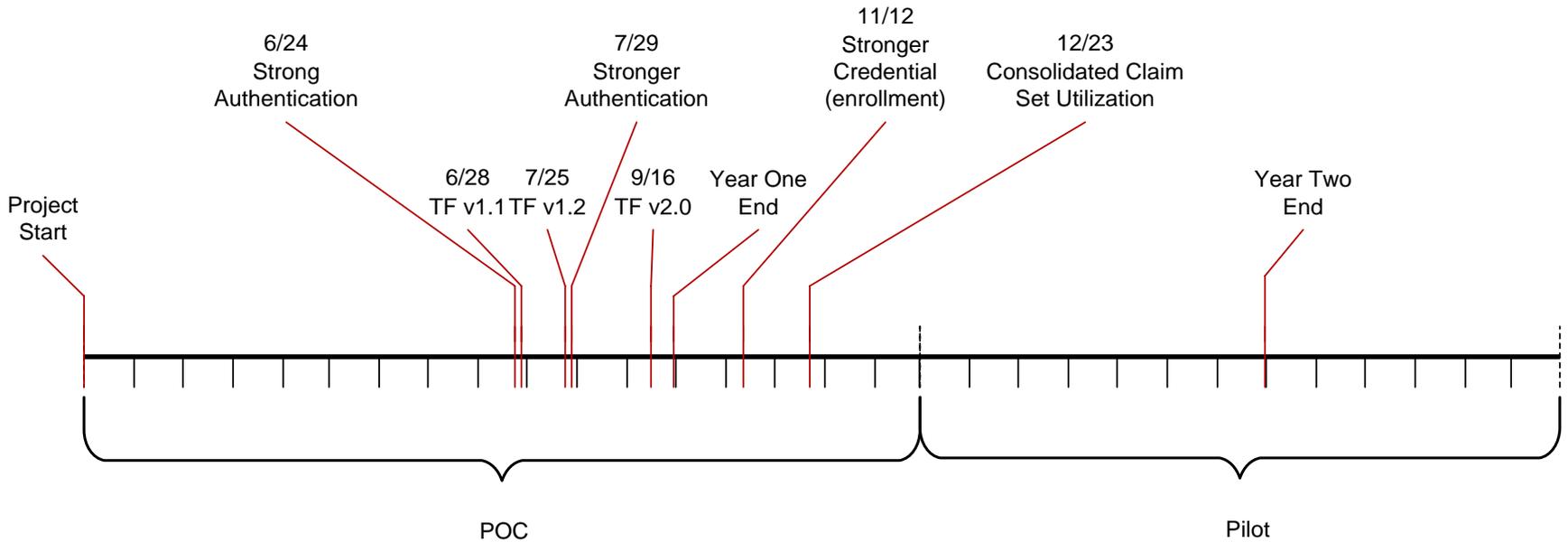
# Overview

- **Objective:** increase confidence in end-user identity by leveraging DMV in-person proofing to strengthen the authentication events while maintaining user privacy when accessing on-line services



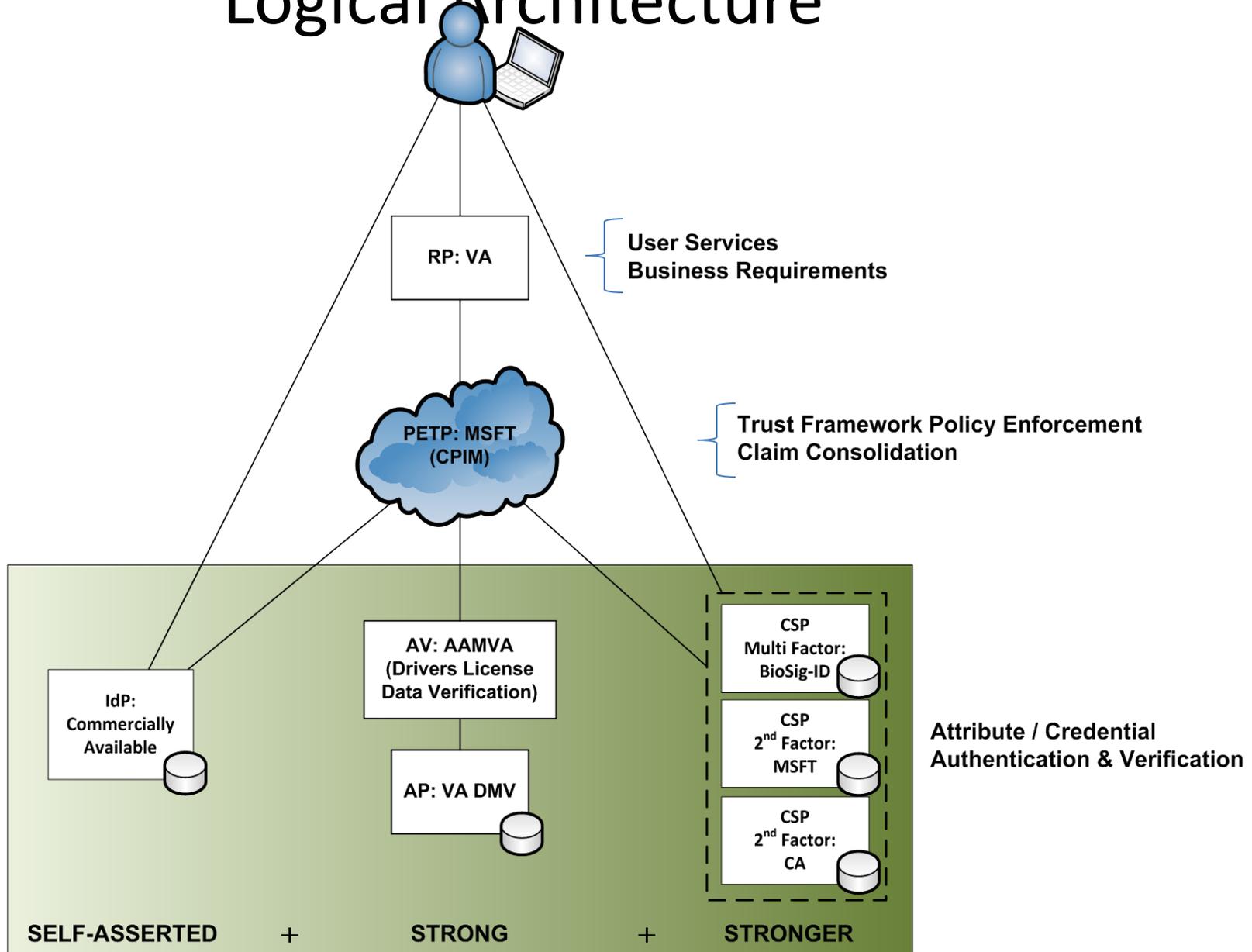
- **Challenges:**
  - Identify Trust Framework model to meet CSDII business needs
  - Bind self-assured credential to user without impacting IdP
  - Leverage DMV in-person proofing on remote authentication events
  - Create composite claim set with privacy enhanced attributes

# High Level Milestones and Timeline

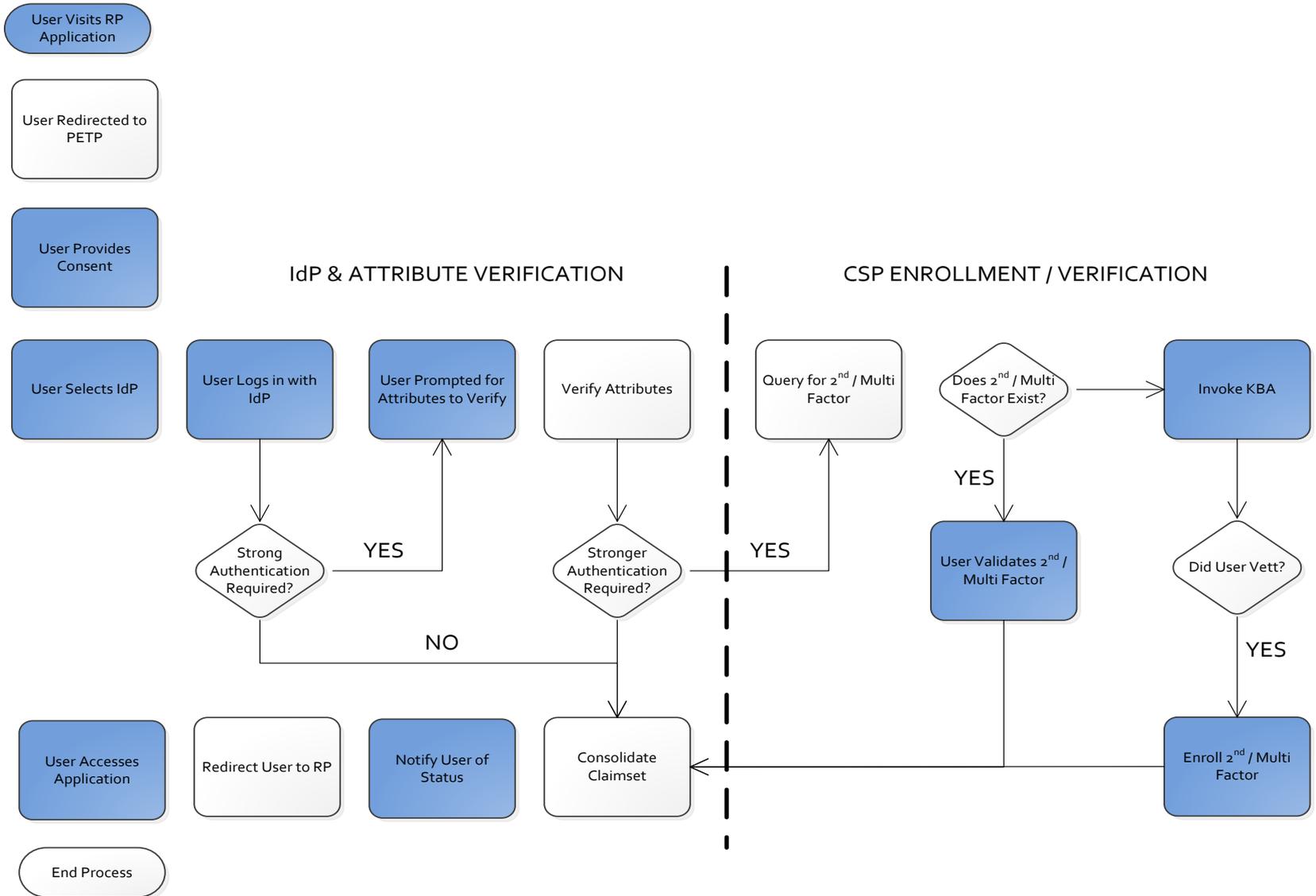


POC – Proof of Concept  
TF – Trust Framework

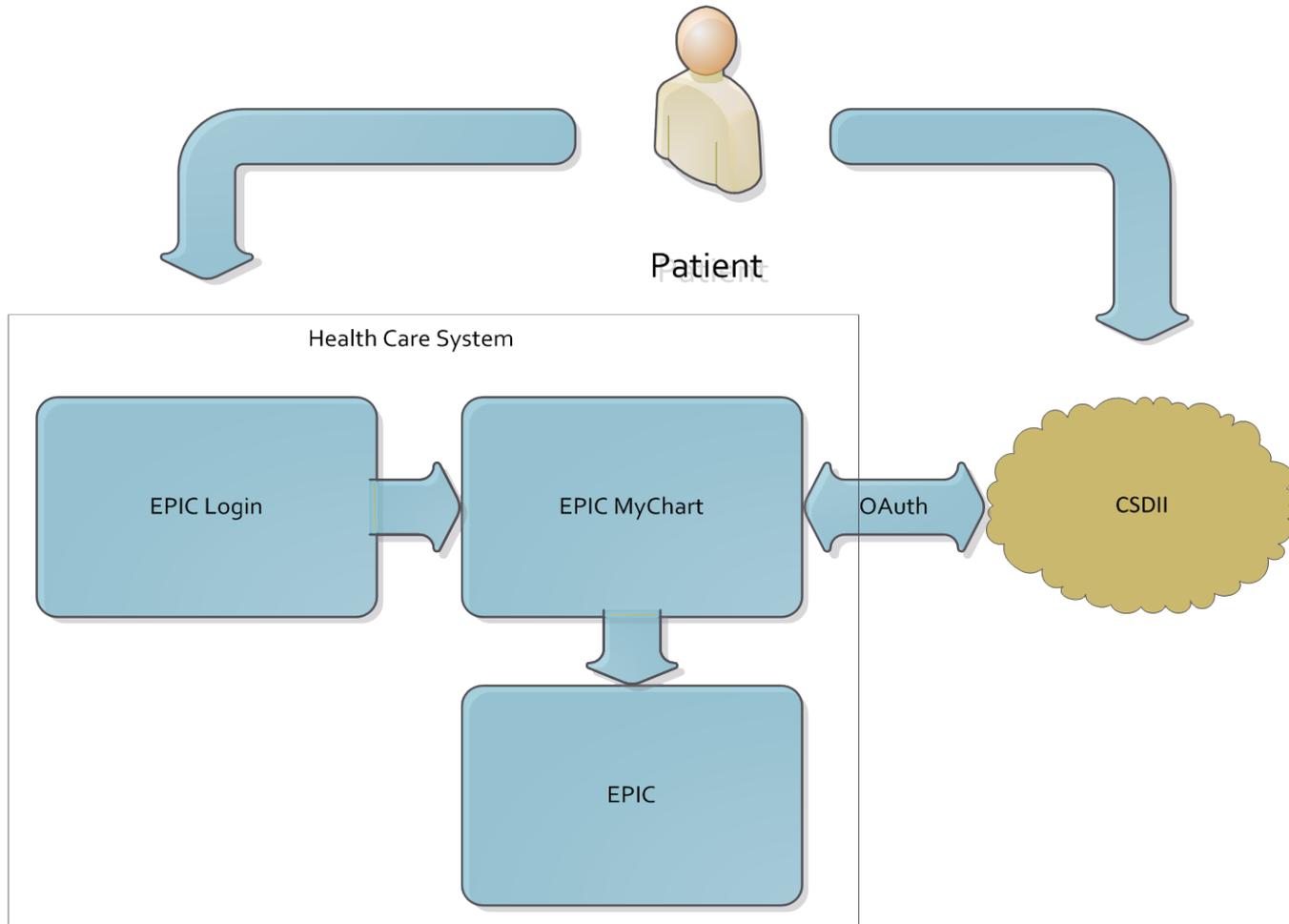
# Logical Architecture



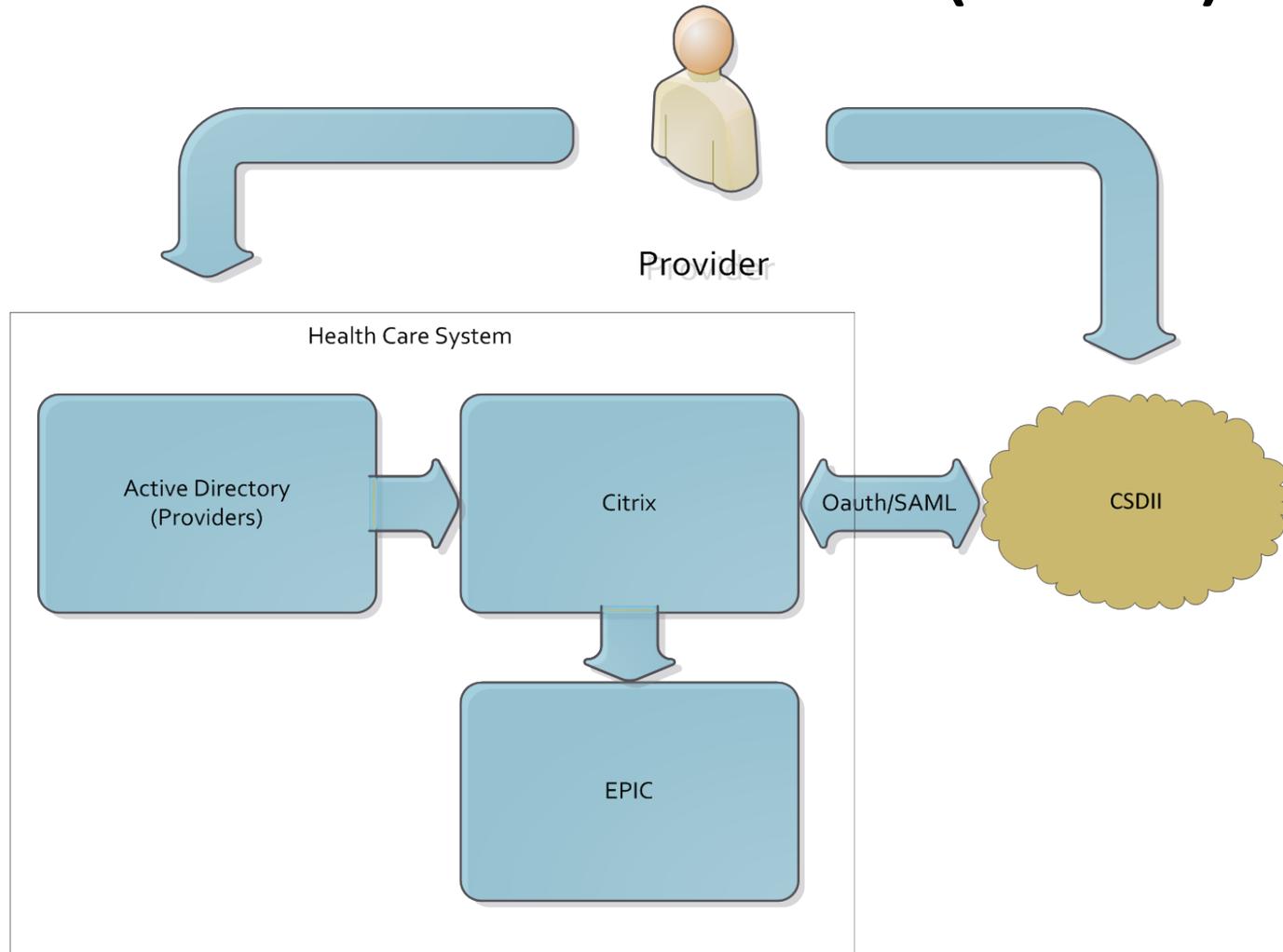
# User Journey



# Potential Use Cases



# Potential Use Cases (con't)



# Next Steps

- Business
  - Package Trust Framework (TF) v1.1
  - Appoint TF Governing Board & Assurance Committee members
  - Solicit interest from potential RPs & Define Use Cases
    - Health IT Provider
    - Higher Education
  - Identify RP Value Proposition
- Technical
  - Verify Strong Authentication Capability , i.e. Verified Attributes
  - Develop Stronger Authentication Capability , i.e. 2<sup>nd</sup> / Multi Factor
  - Enhance / Evolve User Experience

# Learn More

Paul E Blanchard  
Project Director, AAMVA PMO

+1.703.908.5780

[pblanchard@aamva.org](mailto:pblanchard@aamva.org)

# Backup Slides

# Use Cases / Workstreams



This use case specifies the sale of a vehicle from one private owner to another within the state of Virginia

The following assumptions are made for this pilot use case:

Vehicle must already be titled in the Commonwealth  
Both owners must be customers of the Virginia DMV  
There is only one owner on the current title  
There are no liens on the vehicle  
Vehicle will be titled with a single owner

**Basic policy for transaction:**

Both buyer and seller must be over the age of 18  
The application requires the following assertions to begin the transaction:

- Authenticated
- Name
- Email Address
- Driver License Number
- Indicator that individual is > 18

# Accomplishments and Near Term Milestones

- Business
  - Trust Framework - Gap Analysis
  - Trust Framework v1.0 – Operational
  - Trust Framework v1.1 – Operational with Component & Participant Type Extensions
  - Trust Framework v2.0 – VA OAG
  - Solicit interest from additional RPs (state / commercial)
    - Health IT Provider
    - Higher Education
- Technical
  - Brokered communications / end-to-end integration with key components
  - Strong Authentication, i.e. Verified Attributes (5/28)
  - Stronger Authentication, i.e. 2<sup>nd</sup> / Multi Factor (6/28)
  - Stronger Credential & Consolidated Claim Set Utilization (8/1)

# Lessons Learned

- The ecosystem must remain sensitive to public sector needs as it defines a system usable by private sector.
- Because of the legal and political complexities, there is no 'easy solution' to implementing public / private participation in the ecosystem.
- Difficult to operate using existing / dated standards with requirements from current communities... Harmonize existing standards with application needs and pending standards / documentation.
- Technical path is clearer / cleaner than definition of business approach.
- End User and Administrator UX is critical in wide-spread adoption of ecosystem.