Creating an Identity Ecosystem in the Cloud

Jennifer Nowell

Director, Government Solutions and Federal Healthcare
Symantec, Public Sector

Answering the Government' Call

- As part of VanRoekel's 2012 *Digital Government Strategy*
- Core challenge: "enabling secure access to digital government information and services anywhere, anytime, on any device"
- This will support the shift from securing devices to securing the data itself and ensure that data is only shared with authorized users
- Government must focus on new solutions in areas such as continuous monitoring, identity, authentication, and credential management, and cryptography

Building for the future

Strategy Principles

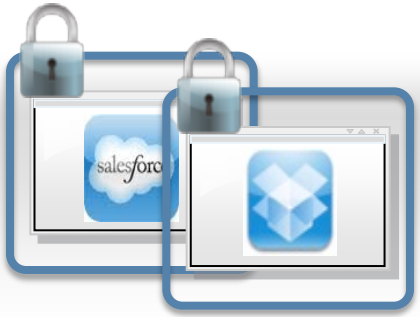
To drive this transformation, the strategy is built upon four overarching principles:

- An "***Information-Centric"*** *approach—Moves us from managing "documents" to managing discrete pieces of open data and content which can be tagged, shared, secured, mashed up and presented in the way that is most useful for the consumer of that information.*
- A ***"Shared Platform"*** *approach—Helps us work together, both within and across agencies, to reduce costs, streamline development, apply consistent standards, and ensure consistency in how we create and deliver information.*
- A ***"Customer-Centric"*** *approach—Influences how we create, manage, and present data through websites, mobile applications, raw data sets, and other modes of delivery, and allows customers to shape, share and consume information, whenever and however they want it.*
- A platform of ***"Security and Privacy"*** *—Ensures this innovation happens in a way that ensures the safe and secure delivery and* ***use of digital services to protect information and privacy.***

The Breakthrough: Information-Centric Security

Device Protection

Enable, Secure, Manage Devices



App/Data Protection

App Store, App Policy, Content Center

Access

Protect Identities, Access SaaS Apps

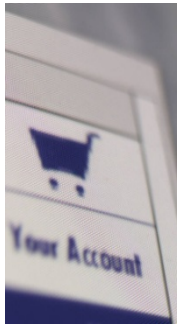
Building for the Future

Managing Online Identities is Hard

The User's Perspective

- Multiple identities with varying password rules
- Registration required for each site
- Password recovery is an everyday task
- Keeping account information current across sites is impossible

An Agency's Perspective



- Managing identities for large populations introduces cost and scale issues
- Customers are frequently lost at the registration page
- Identity assurance and strong authentication add complexity

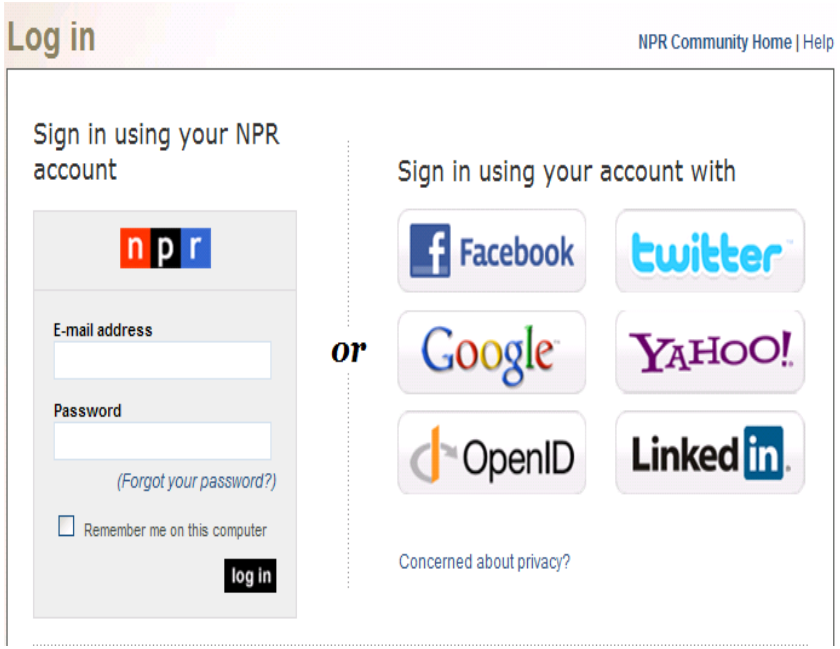
Identity Federation is the Solution: Two examples

PayPal is an identity provider in online shopping market

- Provides trusted identity, shipping and payment information attributes to relying parties
- Integrated into X.commerce online shopping platform

PayPal

Online consumer websites accept identities from external sources



However there are issues…

- Identity Assurance
  - It's hard to determine the quality of an identity produced by a third party.
- Privacy concerns
- Trust
  - Consumer trust on the ID provider
  - Relying Party trust on the ID provider

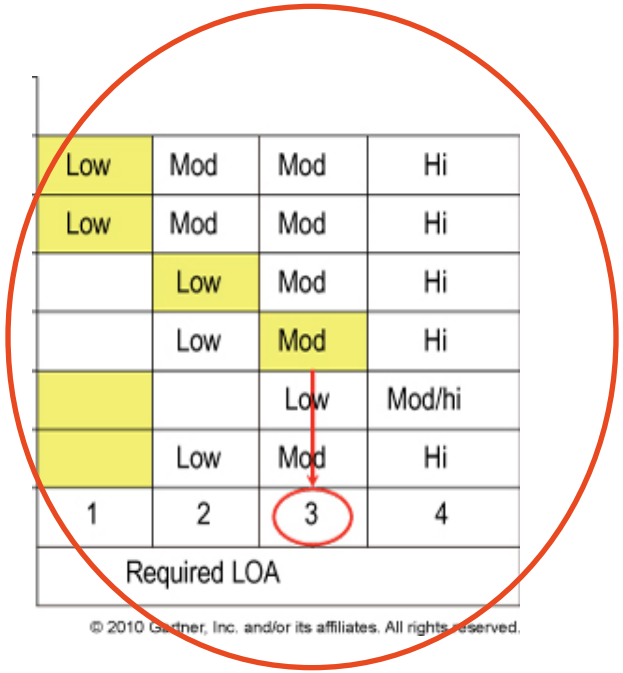
Work needs to be done before identity federation goes mainstream for higher value transactions

…But Progress is Being Made

Standards for assessing identity quality are emerging

- Office of Management and Budget **(OMB) M-04-04** requires identity risk assessment and defines four Levels of Assurance (LOAs) for identity

Risk				
Inconvenience, reputation	Low	Mod	Mod	Hi
Financial	Low	Mod	Mod	Hi
Mission		Low	Mod	Hi
Information disclosure		Low	Mod	Hi
Safety			Low	Mod/hi
Legal		Low	Mod	Hi
	1	2	3	4
	Required LOA			



OMB-M-04-04

- Electronic authentication (E-Authentication) is the process of establishing confidence in identities presented remotely over an open network to an information system.

- OMB M-04-04 defines four levels of identity assurance for electronic transactions requiring authentication, where the required level of assurance is defined in terms of the consequences of authentication errors and the misuse of credentials.

- Level 1 – Little or no confidence in the asserted identity
- Level 2 - Some confidence in the asserted identity
- Level 3 - High confidence in the asserted identity
- Level 4 - Very high confidence in the asserted identity

New Standards are Emerging

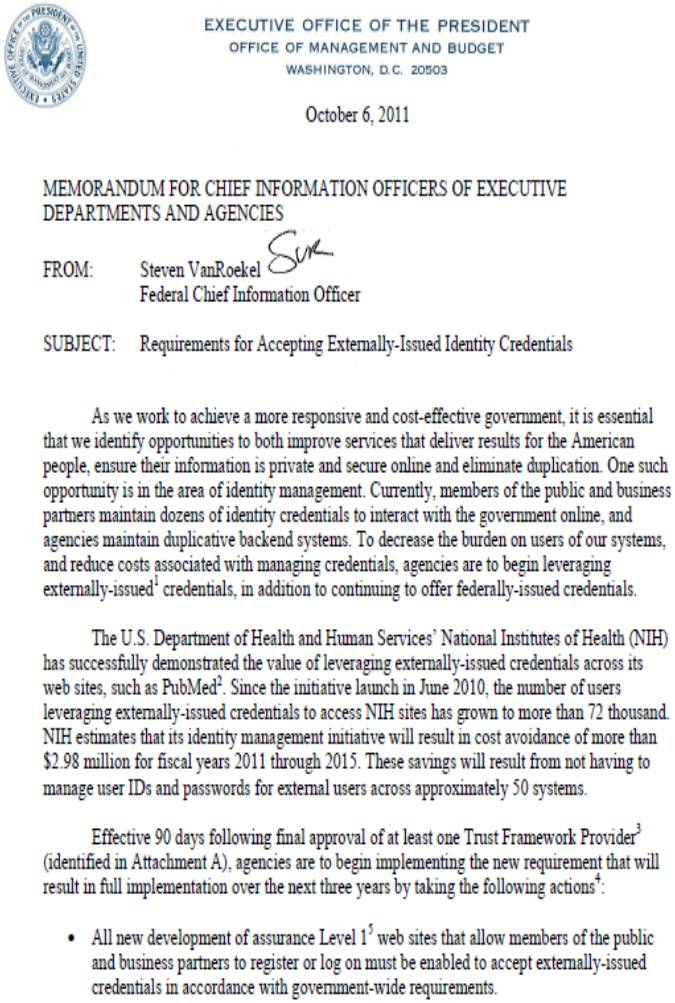
Standards for assessing identity quality are emerging

- NIST Special Publication (SP) 800-63 maps each LOA to specific proofing procedures and credential types

LOA	Proofing	Credential
1		Password
2	Doc presentation	Single-factor nonshared pw or token
3	Doc verification	Multi-factor hard, soft, or OTP token
4	In-person check of two gov/financial docs + capture biometric reference	Multi-factor FIPS 140-2 hard token + encryption

Federal Government is Leading

- Identity, Credential and Access Management (ICAM):
  - Federal CIO Council initiative
  - ICAM has adopted NSTIC
  - Establishes a framework for auditing identity providers (IDPs):
    - To determine whether they meet the OMB M-04-04 and NIST SP 800-63 requirements
  - Three organizations implement this framework (so far):
    - Kantara Initiative
    - Open Identity Exchange (OIX)
    - InCommon Federation



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

October 6, 2011

MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Steven VanRoekel
Federal Chief Information Officer

SUBJECT: Requirements for Accepting Externally-Issued Identity Credentials

As we work to achieve a more responsive and cost-effective government, it is essential that we identify opportunities to both improve services that deliver results for the American people, ensure their information is private and secure online and eliminate duplication. One such opportunity is in the area of identity management. Currently, members of the public and business partners maintain dozens of identity credentials to interact with the government online, and agencies maintain duplicative backend systems. To decrease the burden on users of our systems, and reduce costs associated with managing credentials, agencies are to begin leveraging externally-issued[1] credentials, in addition to continuing to offer federally-issued credentials.

The U.S. Department of Health and Human Services' National Institutes of Health (NIH) has successfully demonstrated the value of leveraging externally-issued credentials across its web sites, such as PubMed[2]. Since the initiative launch in June 2010, the number of users leveraging externally-issued credentials to access NIH sites has grown to more than 72 thousand. NIH estimates that its identity management initiative will result in cost avoidance of more than $2.98 million for fiscal years 2011 through 2015. These savings will result from not having to manage user IDs and passwords for external users across approximately 50 systems.

Effective 90 days following final approval of at least one Trust Framework Provider[3] (identified in Attachment A), agencies are to begin implementing the new requirement that will result in full implementation over the next three years by taking the following actions[4]:

- All new development of assurance Level 1[5] web sites that allow members of the public and business partners to register or log on must be enabled to accept externally-issued credentials in accordance with government-wide requirements.

What is NSTIC?

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

Guiding Principles

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

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."

NSTIC Vision: January 1, 2016

The Identity Ecosystem: Individuals can choose among multiple identity providers and digital credentials for convenient, secure, and privacy-enhancing transactions anywhere, anytime.

Sign mortgage with digital signature

Alternative payment mechanisms; convenient transactions

Trustworthy critical service delivery

Single Sign-On to her corporate portal

Security ‘built-into’ the system to reduce user error

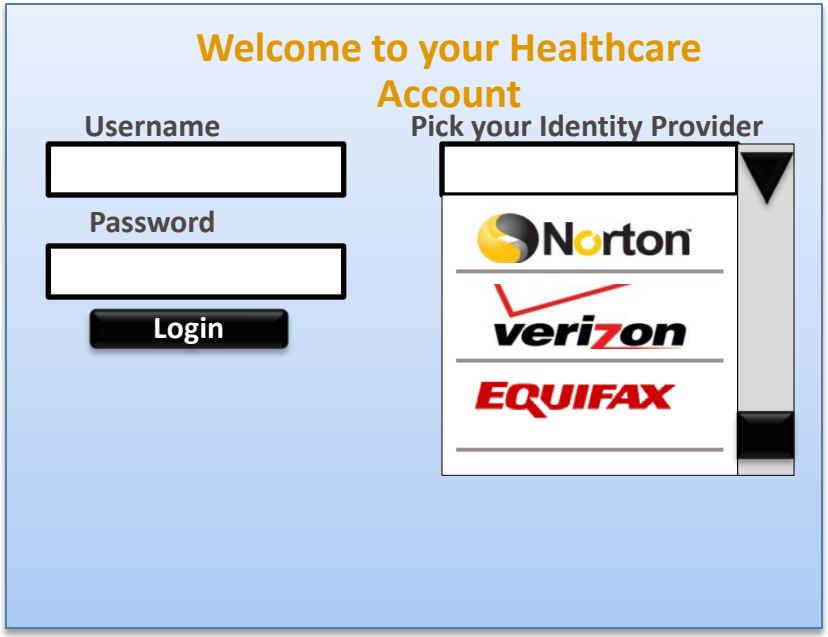
Privately post location to her friends

Symantec.

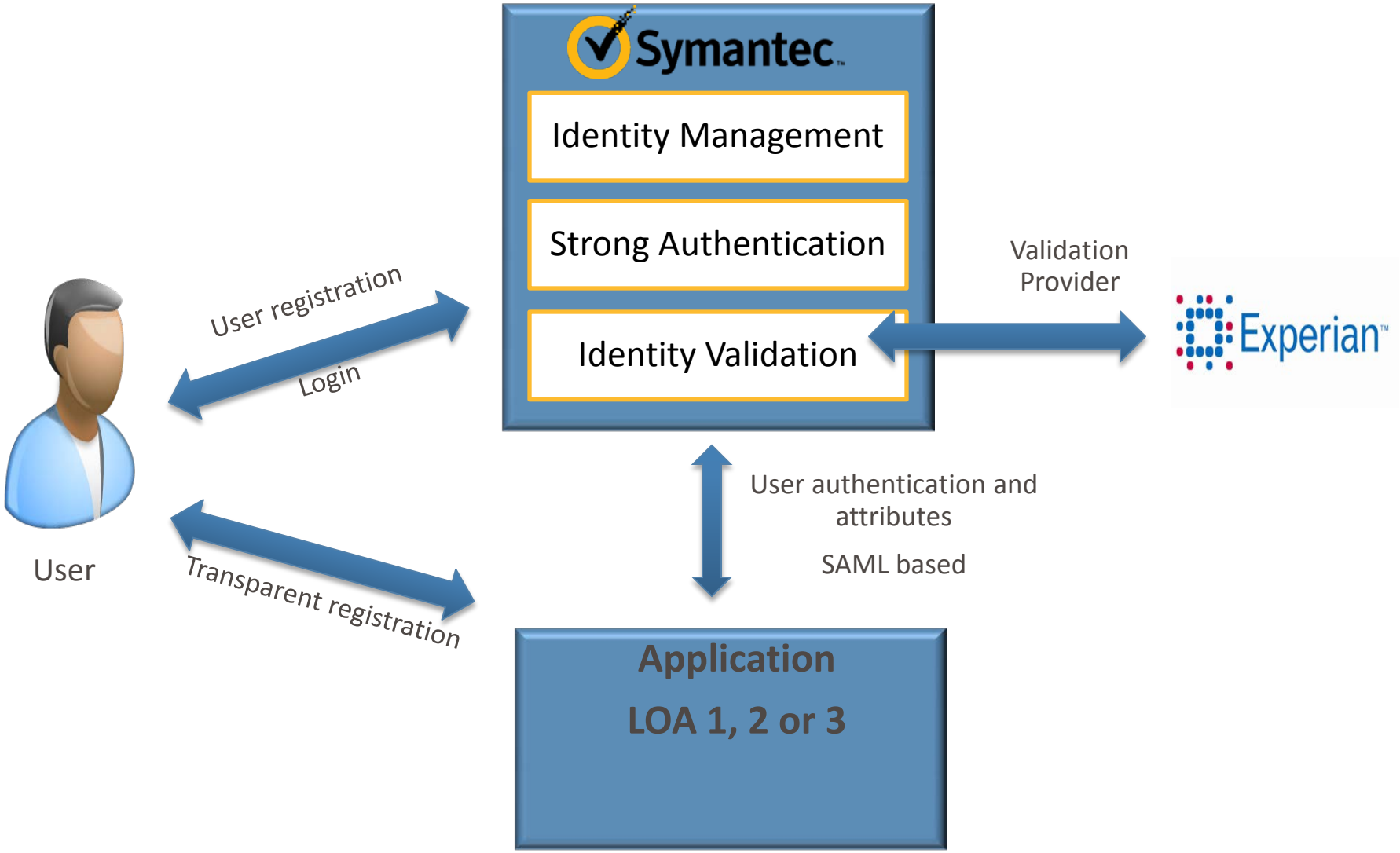
Building an Identity Ecosystem in the Cloud

Symantec IdP as a Service

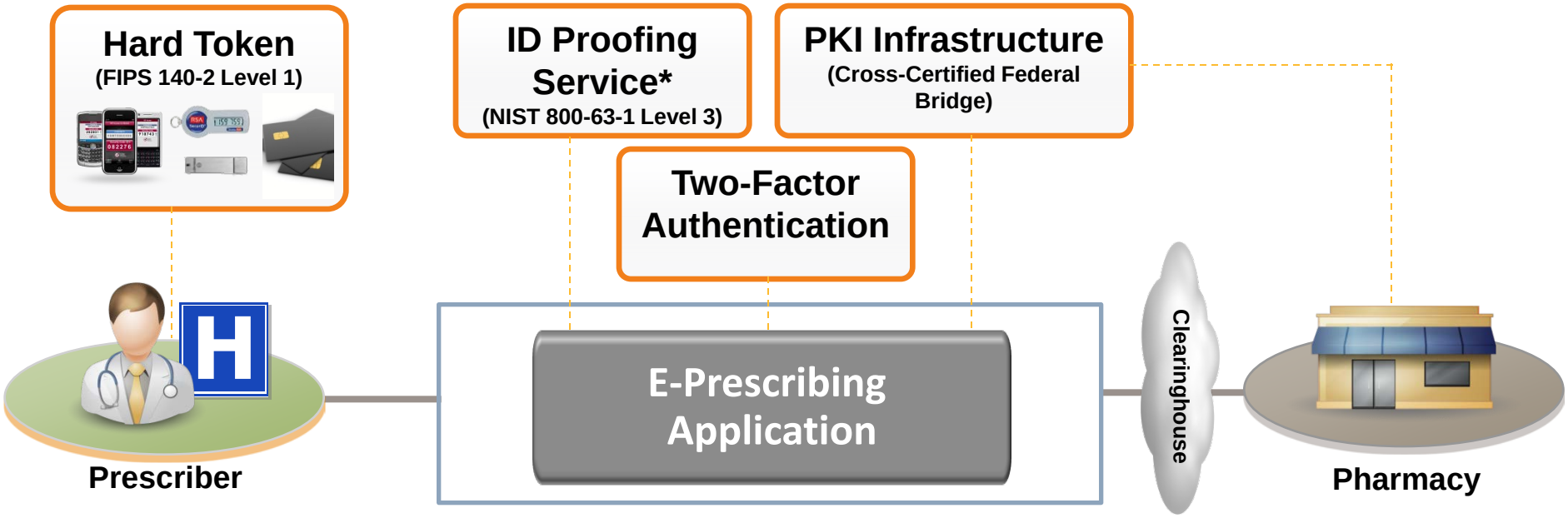
- Consumer authentication service
- Provides Level of Assurance 1, 2 and 3 identity as per NIST 800-63-1 guidance
  - Online identity proofing
  - Strong authentication
  - Kantara Certified



IdP System Overview



Symantec E-Prescribing Authentication Solution



1. Remote Identity Proofing (Level 3) enabling positive identification of prescribers on user setup
2. Multiple form-factors for hard tokens enabling support across multiple platforms (PC, Workstation, Mobile) and access locations
3. Two-Factor Authentication validation service supporting authentication of prescribers at time of prescription approval using hard token
4. Public Key Infrastructure (PKI) enabling the application of digital signatures to support non-repudiation of e-prescribing transactions as well as certificate validation

*Partner

Thank you!