NSTIC IDENTITY EXCHANGE PILOT

NOMINATING CATEGORY:

CYBERSECURITY

NOMINATOR:

JOHN MACMILLAN,
CHIEF INFORMATION OFFICER

COMMONWEALTH OF PENNSYLVANIA
1 TECHNOLOGY PARK
HARRISBURG, PA 17110
717-772-8013
JMACMILLAN@PA.GOV

INITIATION: JANUARY 2014
COMPLETION: JUNE 2015

EXECUTIVE SUMMARY:

In order to further safeguard sensitive information entrusted to state government and provide safer, more convenient online services, the Commonwealth of Pennsylvania is pursuing an enterprise Identity Exchange to enable constituents to access multiple applications across state agencies using a single user name and password. The Pennsylvania Identity Exchange aligns with the National Strategy for Trusted Identity in Cyberspace (NSTIC) and was piloted through a grant from the National Institute of Standards and Technology (NIST) in 2013.

The Identity Exchange serves as a centralized communications hub to connect identity providers that create and store user credentials, applications that consume the credentials and identity verifiers which provide the identity proofing of the person behind the credential. The exchange provides registration and management services for online identities. The constituent's physical identity is voluntarily verified by either internal or external sources and passed along to the consuming application. The service and online identities it provides are shareable across multiple agencies.

The Pennsylvania Identity Exchange builds upon the existing "Keystone ID," which is a single user name and password that a constituent can use to access certain programs offered by DHS, Labor & Industry and other state agencies. Pennsylvania is seeking to increase the number of state agencies and programs that utilize the Keystone ID and, in the process, provide added convenience and improved customer service, while at the same time reducing fraud and false, stolen and outdated identities.

The Identity Exchange went live in October 2014, with the first agency application to use it rolling out in the spring of 2015. The Pennsylvania Human Relations Commission is using the Identity Exchange to verify the identity of constituents who file various types of discrimination complaints (sexual harassment, age discrimination, etc.) online. Later this year, DHS will integrate its COMPASS application used to apply for various social service programs with the Identity Exchange.

The benefits of the Identity Exchange to state agencies include cost savings and enhanced security. Constituents enjoy the ease and convenience of a single trusted identity that can be used across multiple applications or services, eliminating the need to remember multiple user names and passwords and to re-enter the same information into multiple applications or services.

In the future, Pennsylvania looks to expand the use of the Identity Exchange to other agencies and applications. Expansion of the identity verifiers and identity providers is being looked into and will further enhance our constituents' experience by giving them other options to transact with their state government.

BUSINESS PROBLEM:

The Commonwealth of Pennsylvania is entrusted with a wide variety of citizen, business and government data, some of which is highly sensitive and/or confidential; including Social Security numbers and records related to employment, health, taxes, criminal history and education. It offers services to its constituents ranging from providing routine public information to licensing and registration services, health and medical benefits, financial assistance and more.

For many of these programs and services, state agencies need to know, or to have some assurance of, the identity of the person involved in the transaction. Traditionally a constituent would come to a state office with identifying information such as birth certificate and photo ID or a state-issued ID such as a driver's license. As more and more transactions move to the Internet, there is a need to perform this identity verification electronically in real time.

Currently in Pennsylvania, as in many other state governments, constituents' online identities exist within information silos across agencies and even across applications within an agency. As a result, a constituent needs to register independently for each, provide the same basic information such as name and address for each, have their identity verified by whatever internal processes are followed, and then log in with a user ID and password unique to that application or service. This is a burden to the constituent, an inefficient use of taxpayer dollars in the replication of the same basic processes, and a security risk in not being able to consistently apply security standards and practices across all of these silos. While there are some instances of sharing of common constituent credentials across multiple agencies, this has been the exception and not the rule.

In 2011, the White House issued the National Strategy for Trusted Identity in Cyberspace (NSTIC), which calls for unified identity and access management systems that are robust and secure, shareable across the enterprise, cost effective, easy for the constituent to use and maintain privacy. NSTIC is being promoted by the private and state government sectors, and is supported by a series of federal grants through the Department of Commerce, National Institute for Standards and Technology (NIST) and the Office of Management and Budget (OMB).

In 2013, the Commonwealth of Pennsylvania applied for and was awarded a grant to build a cross-agency interoperable identity exchange. The effort was led by the Pennsylvania Office of Administration, Office for Information Technology (OA/OIT), in partnership with the state Department of Human Services (DHS), formerly the Department of Public Welfare.

SOLUTION APPROACH:

In developing the Pennsylvania Identity Exchange, the commonwealth chose to build upon an existing enterprise directory of the state's constituents known as Keystone ID. This directory is shared by DHS, the Department of Labor and Industry, the State Employees' Retirement System and others and contains approximately 2.2 million user

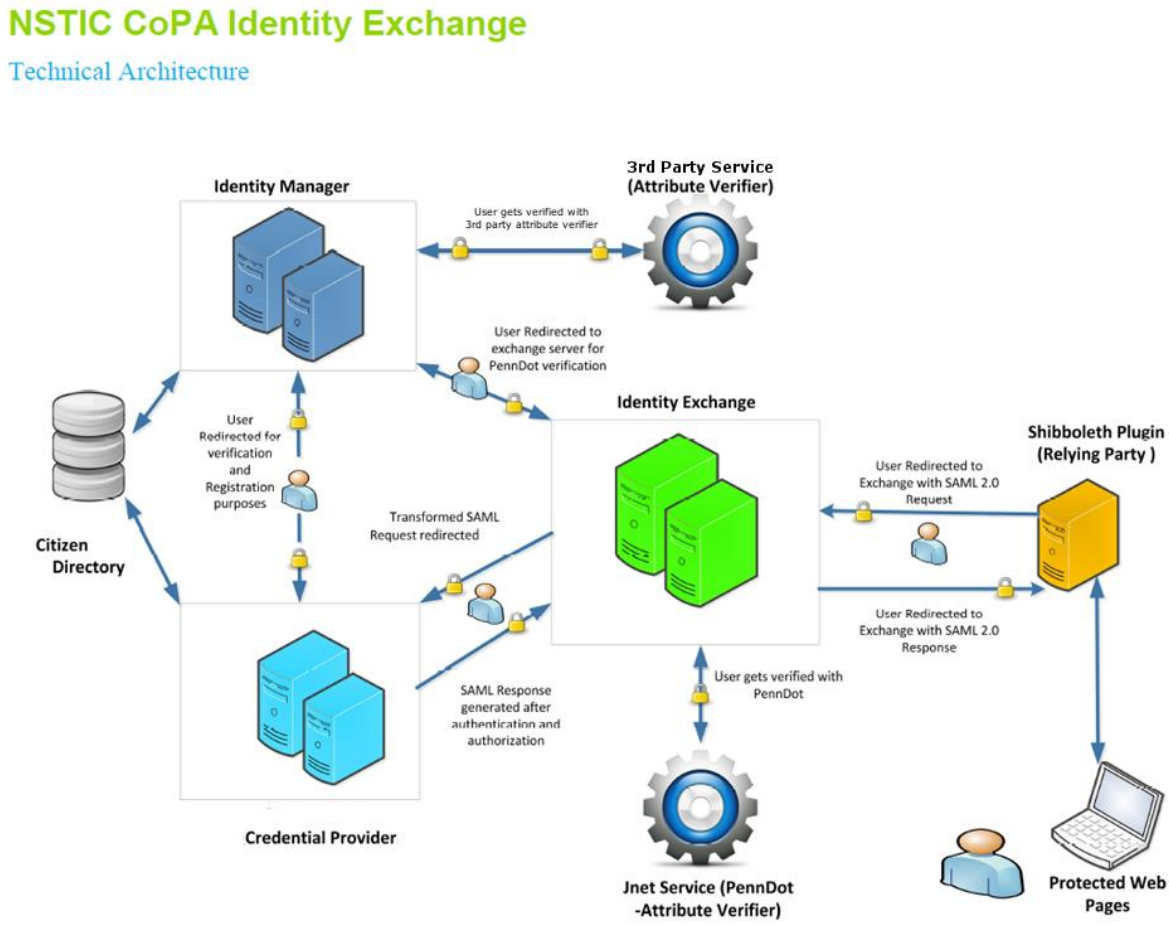
accounts. Some number of these accounts had already been identity proofed through the federal hub provided by the Centers for Medicare and Medicaid Services (CMS) as part of their eligibility for medical assistance programs.

The Pennsylvania Identity Exchange serves as a centralized communications hub to connect:

1. **Credential Service Providers (CSPs):** identity providers that create and store the user credentials
2. **Relying Parties (RPs):** applications that consume the credentials
3. **Identify Verification Providers (IVPs):** identity verifiers which provide the identity proofing of the person behind the credential.

Where possible we relied on existing support services for registration, password maintenance, etc.

The following figure depicts a high-level overview of the architecture for the Identity Exchange and some of the components and product sets in use by it. Central (in green) is the main Identity Exchange service. This service shunts requests between the other components in a double-blind manner. It was built in a componentized manner to facilitate the plugin of additional CSPs, RPs, and IVPs.



A constituent accessing an agency website or online application (the RP) is re-directed to the Identity Exchange to either login or, if the user is new, create a login account. Upon successfully logging in, a security assurance markup language (SAML) token with the user's credentials is sent back to the RP and consumed by the Shibboleth-based plugin provided by the Identity Exchange. If the RP has a business need for a verified or proofed identity, the Identity Exchange either retrieves the previous proofing that was done or offers the constituent the opportunity to undergo the proofing process. This process, in keeping with the NSTIC principles, is voluntary. The requirement for a proofed identity is a business decision by the RP and it is their prerogative to not allow access based on that business decision.

Constituents agreeing to be identity proofed are currently given two options. They can provide information from their driver's license or state ID card which is then verified by the PA Department of Transportation (PennDOT) based on an exact match of the information provided. The second option is to undertake a Knowledge Based Authentication (KBA) which is currently provided as a service for this pilot by a 3rd party provider. For the KBA, the constituent is asked for identifying information (name, address and optionally other pieces of information). The 3rd party provider matches the user against its data system and returns a series of multiple choice questions which the constituent should be able to correctly answer. A score is then returned based on the responses and other criteria such as the vendor's fraud alert system.

Regardless of the option chosen, the outcome is recorded in the citizen directory. It is important to note that while the outcome is recorded, information such as the driver's license number or KBA questions and responses are never maintained or otherwise recorded in the directory system. We expect the identity verification will be valid for a period of three years after which the constituent will need to have their identity re-proofed.

Currently, an application from the Pennsylvania Human Relations Commission (PHRC) is using the Identity Exchange as a relying party. This application allows constituents to file various types of discrimination complaints (sexual harassment, age discrimination, etc.) online, eliminating much of the previous paper-based processes and significantly speeding up the handling of complaints and improving accuracy. Since these transactions are of a sensitive nature, PHRC has chosen to require that all constituents filing a complaint be verified through the Pennsylvania Identity Exchange.

Late in 2016, DHS will be integrating its COMPASS application with the Identity Exchange. Through COMPASS, a constituent can apply and be qualified for multiple human services programs through a single online application. Currently COMPASS users applying for medical assistance benefits are identity proofed by a federal program. This integration will enable applicants for any benefit to be identity proofed. Initially this will be an optional and voluntary on the part of the constituent, but may become a requirement in the future.

SIGNIFICANCE:

Through its grant, Pennsylvania has demonstrated that a shared enterprise-wide service for online registration, proofing and authentication of our constituents is viable and will:

- Increase the overall security posture of our applications and systems
  - Provide a standard baseline of services to which enterprise security policies can be applied
  - Move to eliminate identity silos that exist across the agencies, many of which may not adhere to the enterprise security policies
  - Facilitate application of new or revised security policies as needed on a single enterprise service
- Facilitate the development life-cycle of new applications and existing ones.
  - Provide standard services which can be reused across agencies and their applications without the need to develop the same over and over again
  - Standardize processes for managing user identities
- Improve the customer experience for constituents in their online dealings with the commonwealth and its agencies
  - Single, trusted user ID and password allowing access to multiple agencies and applications – “one stop shopping”
  - Standard interface for registration and management of the user ID and password
  - Once and done identity proofing, eliminating the need to do so for each application or service that requires it
  - Protects the constituent’s data by helping to ensure that only they have access to it
- Fraud reduction
  - By verifying the constituent’s identity, where appropriate, agencies and their applications have assurance of the identity of the person they are interacting with
  - Allows agencies to make business decisions based on further knowledge of their constituents.

These outcomes map to the OA/OIT strategic objectives of providing better, safer services to state agencies and their constituents.

BENEFITS:

While at present, the Identity Exchange is running as a pilot with a limited number of users from PHRC, we expect that the commonwealth will see benefits, both tangible and intangible, in various areas:

- Cost savings
  - Fraud reduction
  - Faster development lifecycle with reusable components

    - Centralized service not needing to be duplicated across the agencies
- Enhance security
    - Protects constituents data from unauthorized or fraudulent access
    - Standardizes application and enforcement of enterprise security policy
    - Provides assurance of who the constituent behind the user ID is.
- Increased user experience
    - End-user can use a single trusted identity across multiple applications or services
    - Single interface to manage that identity
    - Reduced need to “data-entry” the same information to multiple applications or services.