Establishing A Multi-Factor Authentication Solution

Report to the Joint Legislative Oversight Committee on Information Technology

Keith Werner

State Chief Information Officer

Department of Information Technology

December 2015

This page left blank intentionally

Contents

This page left blank intentionally

Legislative Request

SECTION 7.19. (a) *The State CIO shall develop and implement a plan to provide a standardized, statewide two-factor authentication system. Development of the plan shall be accomplished in coordination with the Criminal Justice Information Network Board of Directors. On or before January 15, 2016, the State CIO shall provide the completed two-factor authentication plan to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division.*

SECTION 7.19.(b) *Funding appropriated to the Information Technology Reserve for two-factor authentication, along with any remaining funding from prior appropriations for authentication, shall be used to support implementation of the plan."*

See http://www.ncleg.net/Sessions/2015/Bills/House/PDF/H97v9.pdf for reference.

Introduction

In enterprise IT, identity and access management (IAM) is about establishing and managing the roles and access privileges of individual network users. At the most basic level, IAM involves defining what users can do on the network with specific on-line resources and under what circumstances.

Identity Management (IdM) deals with identifying individuals in a system (authentication), such as a network or an enterprise, and controlling their access to resources (authorization) within that system by associating user rights and restrictions with the established identity.

In an enterprise setting, IdM refers to the policies, processes and technologies that establish user identities and enforces rules to securely control access to digital resources. Enterprise information systems require users to authenticate themselves, typically with a username and password. An authorization process then determines which systems an authenticated user is permitted to access. With an enterprise identity management system, rather than having separate credentials for each system, a user can employ a single digital identity to access all resources to which the user is entitled. An IdM system increases security and productivity, while decreasing cost and redundant effort.

Types of authentication include:

- Single-factor: employs username and password techniques
  - Something you know: such as a user ID & password or personal identification number (PIN)
- Two-factor authentication: adds a second level of authentication to a users' digital identity
  - Something you have: such as an ATM card, phone or fob
  - Something you are: such as a biometric like a fingerprint or voice print

A Federated Identity Management (FIM) program will permit extending this approach above the enterprise level, creating a trusted authority for digital identities across multiple organizations. In a federated identity management system, participating organizations share identity attributes, based on agreed upon standards, to obtain access to networks and online resources of the federation. This approach streamlines access and securely protects resources as required. It is an authentication-sharing mechanism designed to allow users to employ the same user name, password or other ID to gain access to more than one network. It is what is known as a "single sign-on."

A single sign-on standard lets users who verify their identity on one network carry over that authenticated status when moving to another. The federated model works only among cooperating organizations, but it can simplify administration and enable the State to extend ID and access management to third-party users and third-party services.

The goal of an enterprise IAM strategy is to initiate, capture, record and manage user identities and their related access permissions to proprietary information and other government resources. User identities can extend beyond government employees and include vendors, citizens, generic administrator accounts, and electronic access badges.

As a result, improving access to network resources and managing an identity's life cycle can provide significant dividends for the State, such as:

- A lower total cost of ownership through the increased efficiency and consolidation of identification and authorization procedures.
- Security improvements that reduce the risk of internal and external attacks.
- Greater access to information by employees, partners and citizens, thus leading to increased productivity, satisfaction and revenue.
- Higher levels of regulatory compliance through the implementation of comprehensive security, audit and access policies.

Background

The State of North Carolina (the State) currently maintains numerous user credentials in disparate systems for citizens, businesses, state employees, and other consumers of IT systems such as local city and county governments, educational entities and law enforcement organizations.

Approaches and processes for provisioning, maintaining, supporting and retiring these credentials vary greatly across various state government communities despite the fact that the consumers are indeed the exact same population. Additionally, many of the current identity and access management solutions lack capabilities such as single sign-on, multi-factor authentication or the ability to federate with external identity providers.

The 2014-15 state budget appropriated $2.2M in the IT Reserve Fund to begin addressing IAM gaps and develop an enterprise IAM strategy that, when fully executed, will provide:

- A lower total cost of ownership through the increased efficiency and consolidation of identification and authorization procedures.
- Higher levels of regulatory compliance through the implementation of comprehensive security, audit, and access policies.

It is recognized that this level of funding is not enough to fully displace any of the major solutions already in place, but it is expected that appreciable progress can be made in reaching consensus amongst the key enterprise stakeholders for developing and implementing enterprise standards and shared solutions. Implementation of a standardized, statewide two-factor authentication system is an integral part of the overall IAM strategy.

Benefits

The Department of Information Technology conducted a thorough requirements identification effort with the agencies. An immediate need identified from the workgroup assessments is the requirement for two-factor authentication services. The recent increase in quantity and sophistication of password- based authentication attacks have significantly reduced the confidence of single username and password authentication methods. State and Federal government agencies handle sensitive citizen data requiring an increasing need for the State to develop a Multi-Factor Authentication (MFA) solution to meet regulatory and compliance requirements.

There are many potential benefits for government use of two-factor authentication services. Two primary benefits are:

- A higher level of assurance against financial loss, agency liability and unauthorized release of sensitive information
- Compliance with state and federal regulatory compliance requirements.

Data collected from agencies through the workgroup assessments revealed that many of the organizations require two-factor authentication to complement the existing first factor username and password methods with NC Identity Management (NCID) and Enterprise Active Directory Service (EADS).

The compliance regulations that the statewide MFA solution should abide by are:

- Criminal Justice Information System (CJIS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- IRS Publication 1075
- Payment Card Industry Data Security Standard (PCI DSS)

Potential Participants

The MFA Working Group identified potential government uses that would benefit most from implementation of a standardized MFA solution:

1. VPN (Administrator Access)
    - Department of Information Technology
    - Department of Public Safety
    - Department of Revenue
    - Department of Human and Health Services
    - Department of Natural and Cultural Resources
    - Department of Administration
    - Department of Transportation
2. Payment Card Industry Servers
    - Department of Information Technology
    - Department of Human and Health Services
    - Department of Transportation
    - Department of Natural and Cultural Resources
3. Criminal Justice Law Enforcement Automated Data Services
    - Department of Information Technology
    - Department of Public Safety
    - Government Data Analytics Center
    - Law Enforcement Agencies
4. North Carolina Financial Accountability and Compliance Technology System
    - Department of Public Safety
    - Government Data Analytics Center
5. NC SAS Enterprise Authentication Tool (NCSEATS)
    - Department of Public Safety
    - Government Data Analytics Center
6. NC TRACKS
    - Department of Human and Health Services
7. Network Policy Server (NPS)
    - Department of Administration
8. Beacon
    - Office of the State Controller

The MFA Project

Development and implementation of the plan to provide a standardized, statewide two-factor authentication system.

Goals

The goals of the MFA project are to:

1. Establish an enterprise-level, statewide, standards-based MFA solution.

2. Provide executive branch agencies and other eligible government entities with a MFA service that will provide two-factor authentication capabilities for their services and applications.
3. Aid the agencies in complying with all the MFA related federally mandated regulations.

Key Deliverables

The MFA project will provide the State multi-factor capabilities for those services and or applications integrated with EADS as first factor authentication.

The project will deliver:

- MFA services meeting the requirements of the agency stakeholders
- Integration options meeting the requirements of agency applications and services
- Self-enrollment functionality for end users of the MFA service
- Delegated administration functionality for agency administrators to enable and support their MFA users
- Infrastructure, software and support for the MFA service
- Migration of users from the existing Department of Information Technology (DIT) MFA product to the new MFA service and retirement of the existing system
- Integration of the DIT Virtual Private Network (VPN) service with the new MFA service

Requirements Prioritization Process

Key drivers for the MFA solution include:

- Alignment with future IAM and Security Strategies
- Reduced security risk and exposure for critical applications
- Regulatory compliance – CJIS, PCI, HIPAA, IRS 1075, etc.
- User Self-Service
- Delegated Administration

In order to develop a complete and accurate MFA Service that meets the compliance and security needs necessary, a series of workshops were held to compile an inclusive list of applications and requirements for all stakeholders. The executive branch agencies and other government entities that were involved in the process were:

- Department of Health and Human Services (DHHS)
- Department of Public Safety (DPS)
- Department of Revenue (DOR)
- Department of Transportation (DOT)

- Government Data Analytics Center (GDAC)
- Department of Information Technology (DIT)
- Office of State Controller - (OSC)
- Statewide Chief Information Risk Officer (CIRO)
- Criminal Justice Information Network Board of Directors (CJIN)

The results of the requirements gathering analysis identified 134 requirements that were grouped into 15 categories which were used to assess, design, and procure the infrastructure and services required to implement a standardized, statewide MFA solution.

Methodology

As described above, DIT conducted a thorough requirements identification effort with the stakeholders.

In order to identify the best vendor for the MFA program, the following approach was used:

1. Gathering, verifying, and finalizing requirements with state agencies using the Requirements Analyst Services from the Office of the State Chief Information Officer (SCIO)
2. Determining, documenting, and vetting project and service scope with stakeholders
3. Developing strategy that aligns with IAM and Security roadmaps
4. Leveraging the ICenter to conduct Proof of Concept (POC) testing of proposed solutions' functionality met defined requirements
5. Procuring MFA components and or services
6. Executing implementation of the MFA Service per requirements and specifications defined in the planning process (including defining guidelines, processes, reference architectures, policy, etc.)

Plan

The plan is to have the MFA solution operational in June 2016 and ready for agencies to transition services and applications to the MFA service with the objective of onboarding users during the 2016-2017 fiscal year.

The MFA Project status is outlined below:

1.	Requirements Analysis Phase	Complete	
2.	Stakeholder Consensus Phase	Complete	
3.	Development of Strategy	Complete	
4.	Proof of Concept	Complete	
5.	Procurement Phase	Pending	Jan 2016

6. Implementation	Pending	Apr 2016
7. Pilot Testing	Pending	May 2016
8. Service Operational	Pending	June 2016
9. Customer Onboarding	TBD	July 2016 – June 2017

Budget

MFA Project Budget FY 2015-2017

Expenses - FY 2015 - 2016	Amount	
Staff Augmentation		
Technical Writer	$56,860	
Vendor Professional Services		
Service Installation Engineering Support	$235,441	
Infrastructure		
Hardware	$52,428	
Software Services		
Licenses	$125,400	
Operations Technical Support		
2X FTEs	$109,996	
Project Management Services	$43,090	
Total budget – FY 2015 – 2016		$623,215

Expenses - FY 2016 - 2017	Amount	
Staff Augmentation		
Technical Writer	$56,860	
Infrastructure		
Hardware	$52,428	
Software Services		
Licenses	$250,800	
Operations Technical Support		
2X FTEs	$219,991	
Project Management Services	$5,090	
Total budget – FY 2016 – 2017		$585,169
Total budget for FY 2015 - 2017		**$1,208,384**