State of North Carolina
Office of Information Technology Services

Pat McCrory
Governor

Chris Estes
State Chief Information Officer

January 16, 2013

Mr. George White
FBI CJIS Information Security Officer
FBI CJIS Division ISO
1000 Custer Hollow Road
Clarksburg, West Virginia 26306-0102

Dear Mr. White:

The Office of Information Technology Services (ITS) is a state agency providing IT services to state and local entities. One of the services provided by ITS is known as NCID, which is the state's standard Identity Management system for authentication and authorization for various programs and it is used by state, county, and local employees, businesses, and citizens. NCID is compliant with a number of Federal standards including HIPPA and IRS 1075.

As our customer needs evolve, so is the need to enhance our services. Recently, we had several requests to provide a form of second factor authentication as an optional offering to our NCID service. Since the announcement of the CJIS Security Policy Version 5.1 issued in July 2012, many local law enforcement agencies have been assessing various methods for compliance. As an alternative to each locality developing their own unique solution, ITS has partnered with the NC Criminal Justice Information Network (CJIN) Governing Board to build a proposal for a single statewide alternative to extend the NCID service to meet these new requirements. This alternative would provide consistency across local law enforcement agencies to access data covered by the CJIS policy.

The purpose of this document is to present North Carolina's proposal for your consideration. Should you concur that this proposal will meet the requirements, ITS will expeditiously develop and implement the solution, so that the September 2013 target dates can be met.

Thank you for your consideration.

Sincerely,

Chris Estes

c: Roy Cooper, North Carolina Attorney General
Bob Brinson, CJIN Chair

Proposed Enterprise Integration

Advanced Authentication

CJIS Solution

State of North Carolina
Office of Information Technology Services
December 2012

Executive Summary

Law enforcement agencies within North Carolina have been addressing advanced authentication based on the expansion of the Criminal Justice Information Services (CJIS) security management structure; consistent with CJIS Security Policy, Version 5.1, July 13, 2012, published by the US Department of Justice, Federal Bureau of Investigation. North Carolina has in excess of five hundred law enforcement agencies, in addition to the state-wide agencies, that need to comply with CJIS's enhanced policy.

In an effort to evaluate the feasibility of providing the law enforcement community with a proposed state-wide solution, the Office of Information Technology Services (ITS) has partnered with the NC Criminal Justice Information Network (CJIN) Governing Board. This partnership was expanded to other state agencies along with numerous county and municipal law enforcement agencies; NC Department of Justice/State Bureau of Investigation, NC Department of Public Safety, Office of State Controller, etc. In addition to discussing solutions with other states, the Naval Criminal Investigative Service (NCIS) was contacted because their Law Enforcement Information Exchange (LInX) initiative has a large presence in North Carolina. North Carolina is also fortunate to have three Computer Aided Dispatch/Record Management System vendors that serve over ninety-five percent of the law enforcement agencies; these vendors are also located within our state.

The CJIN Board was fortunate to have Mr. George A. White, FBI CJIS Security Officer, in October 2011, provide a detailed presentation regarding advanced authentication and participate in a lengthy discussion with members and guests. At the November 15, 2012 CJIN Board meeting, various law enforcement agencies were invited to share their solutions along with NCIS and ITS. The Board, based on the presentation from ITS, requested that they develop a proposal and submit the details to the CJIS Office for consideration.

The Board expressed the desire to explore the possibility of having a state-wide solution, especially since the solution would be an extension to an existing enterprise system; the North Carolina Identity Management (NCID) Service. This system has proven successful and is currently being utilized by the Department of Revenue, Department of Health and Human Services, Department of Transportation, and Office of State Controller. NCID also possesses various federal certifications including the ability to provide advanced authentication.

This report provides a background, details of NCID, architectural diagrams, a process flow, and an example of how advanced authentication would be incorporated into NCID. Implementing an enterprise solution would not only be cost effective, it would also have the support of the law enforcement community, other state agencies, and the vendors. This is critical since every agency will be impacted and the vendors are receptive to working with ITS on the required development effort.

Background

Overview

In the November 15, 2012 CJIN board meeting Information Technology Services (ITS) presented an example showing how CJIS Advanced Authentication could be integrated with the North Carolina Identity Management System (NCID). As a result of this meeting the CJIN board requested that ITS produce the following proposal on Advanced Authentication for approval.

Objective

Ensure law enforcement agencies comply with CJIS/FBI standards. Create one enterprise Advanced Authentication service for all statewide agencies and organizations using NCID as the integration point.

What is NCID?

The NCID Service is the standard identity management and access service provided to state, local, business and citizen users by the NC Office of Information Technology Services (ITS). NCID is an enterprise service that was implemented in 2005 and has been utilized statewide by agencies such as DOR, DHHS, DOT, and OSP. NCID enables its customers to achieve an elevated degree of security and access control to real-time resources such as customer based applications and information retrieval. Simply stated NCID provides one User ID and Password for many statewide applications such as North Carolina's Criminal Justice Law Enforcement Automated Data Services (CJLEADS) application and North Carolina's SAP ERP HR/Payroll application (BEACON).

Enterprise features of the NCID Service provide an efficient and effective means for securing access to online services. Customers can leverage the service to:

- Authorize Individual accounts using passwords
- Manage user accounts
- Assign appropriate access to online resources
- Delegate authority or distribute administrative tasks
- Automate certain key functions

NCID accommodates many types of user communities for the State of North Carolina:

- Business Users requesting access to the State of North Carolina on the behalf of a business.
- Individuals requesting access to conduct online transactions with the State of North Carolina. These users may or may not be citizens of the State.

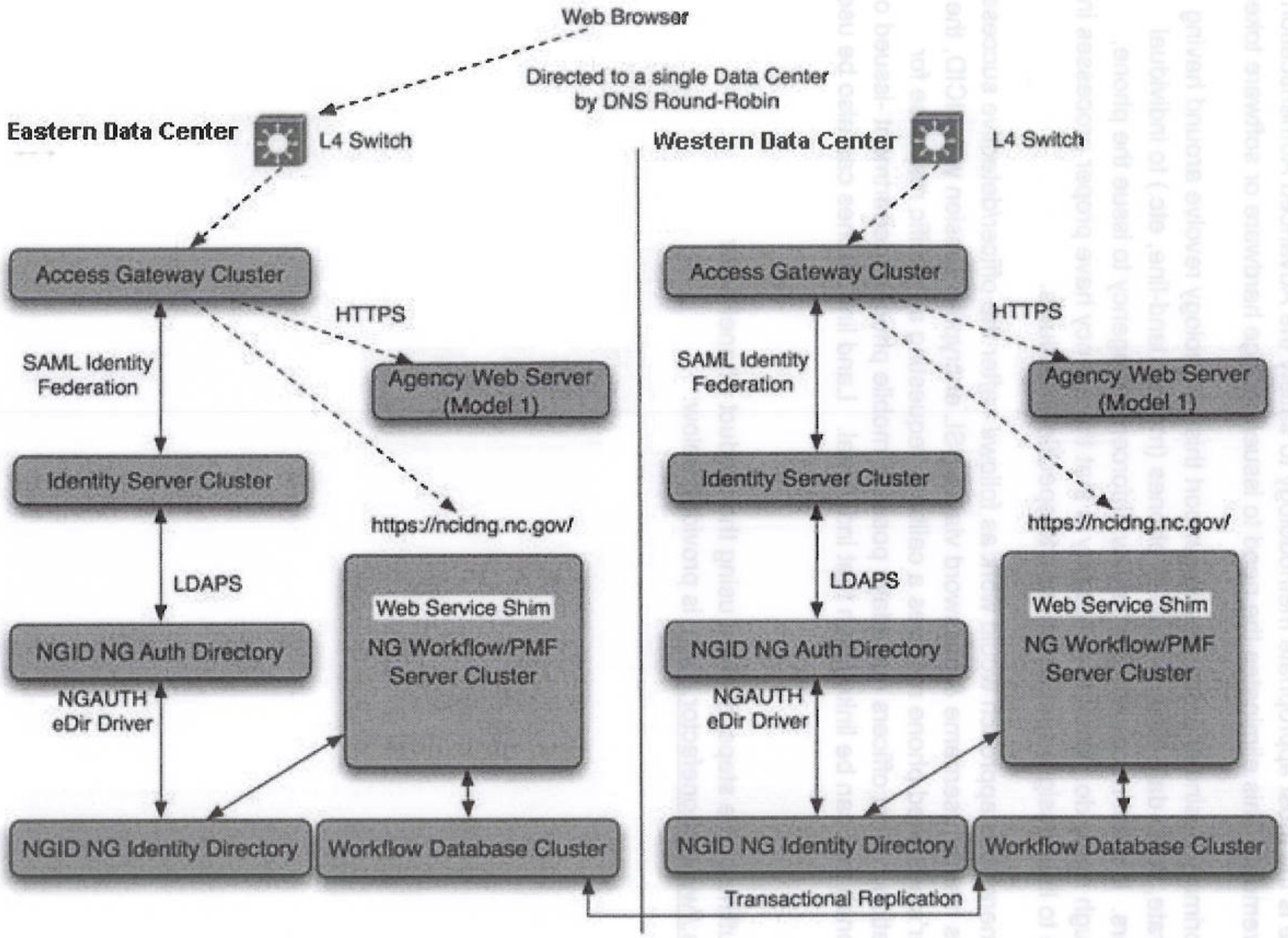
- State Government Employees employed or contracted to work for an agency within the State of North Carolina government.
- Local Government Employees employed or contracted to work for a North Carolina county or municipality.
- Administrators State and Local government employees who can administer user accounts within the same organization.

Technical Details

NCID Current Infrastructure:

- The infrastructure utilizes the NetIQ/Novell Identity & Access Management solution
- This infrastructure provides the ability to have one solution for statewide as opposed to many solutions
- Production infrastructure environment consists of Novell Access Manager which includes 10 proxy servers, 6 Identity Management servers, and 2 admin consoles spread across two state data centers, one being in Raleigh NC and other in Forest City NC. The entire environment is clustered. This provides fault tolerance for disaster recovery. An additional NetIQ product utilized for Identity Management functions is User App running under JBoss and connected to a SQL Server database cluster. All attributes are stored in an eDirectory backend.
- NCID meets HIPAA, PCI, IRS1075, etc. standards
- In addition to clustered production environments ITS provides lab, dev, and pre production staging environments. Customer applications are required to go through pre production testing before moving to production.
- The existing customer base is approx 275,000. With the expansion of NC-DHHS and NC-DOR applications coming on board in 2013 the customer base is estimated to grow to 1.2 million.
- Today NCID offers three types of authentication shown below. NCID is also federation enabled for future use
    - Reverse Proxy using NetIQ Novell Access Manager
    - Directory Sync using Novell IDM product
    - Webservices based on soap xml
- In development phase
    - Externalizing federation based on SAML Ver. 2
- Below are architecture diagrams for the current ITS NCID service

NCID Architecture Diagram (12/3/12)



Advanced Authentication Approach

Pursuant to section 5.6.2.2 (Advanced Authentication) of the CJIS Security Policy 5.1 we believe an approach leveraging challenge/response questions sent to the officer's phone is the most appropriate methodology to satisfy the Advanced Authentication requirement. This eliminates the need to issue/manage hardware or software tokens.

The primary business processes to support this technology revolve around having accurate, up-to-date assignments of phones (mobile, land-line, etc.) to individual officers. It is not necessary for the law enforcement agency to issue the phone, although many do. What is necessary is that the agency have proper processes in place to link (assign) specific phones to specific individuals.

In general, this approach would work as follows - after the officer/detective successfully enters his/her username & password via an SSL encrypted session with NCID, the officer's assigned phone receives a callback requesting a specific response for validation. Most officers nowadays possess mobile phones (department -issued or personal) that can be linked with that individual. Land line phones can also be used.

An outline of the steps involved using the product PhoneFactor (https://www.phonefactor.com) is provided below:

Vendor specific flow example scenario

Step 1 – Officer requests access with a user name and password to an application protected by NCID and requiring Advanced Authentication for verification

Step 2 - Officer Username and password are passed to the NCID proxy servers

Step 3 – Officer Credentials are authenticated by NCID which utilizes Novell eDirectory

Step 4 – NCID will pass encrypted username and password to an ITS maintained RADIUS server.

Step 5 – NCID will pass encrypted username and password to the proposed Advanced Authentication servers for validation

Step 6 – Validation of the encrypted username and password is then sent to the vendor cloud service, e.g. PhoneFactor

Step 7 – Call from the vendor cloud service is placed to the officer's assigned phone asking for input such as some sort of text, static pin, pound sign.

Step 8 – Officer enters the required information for Advanced Authentication

Step 9 – Officer cell/land phone response returned to vendor cloud service

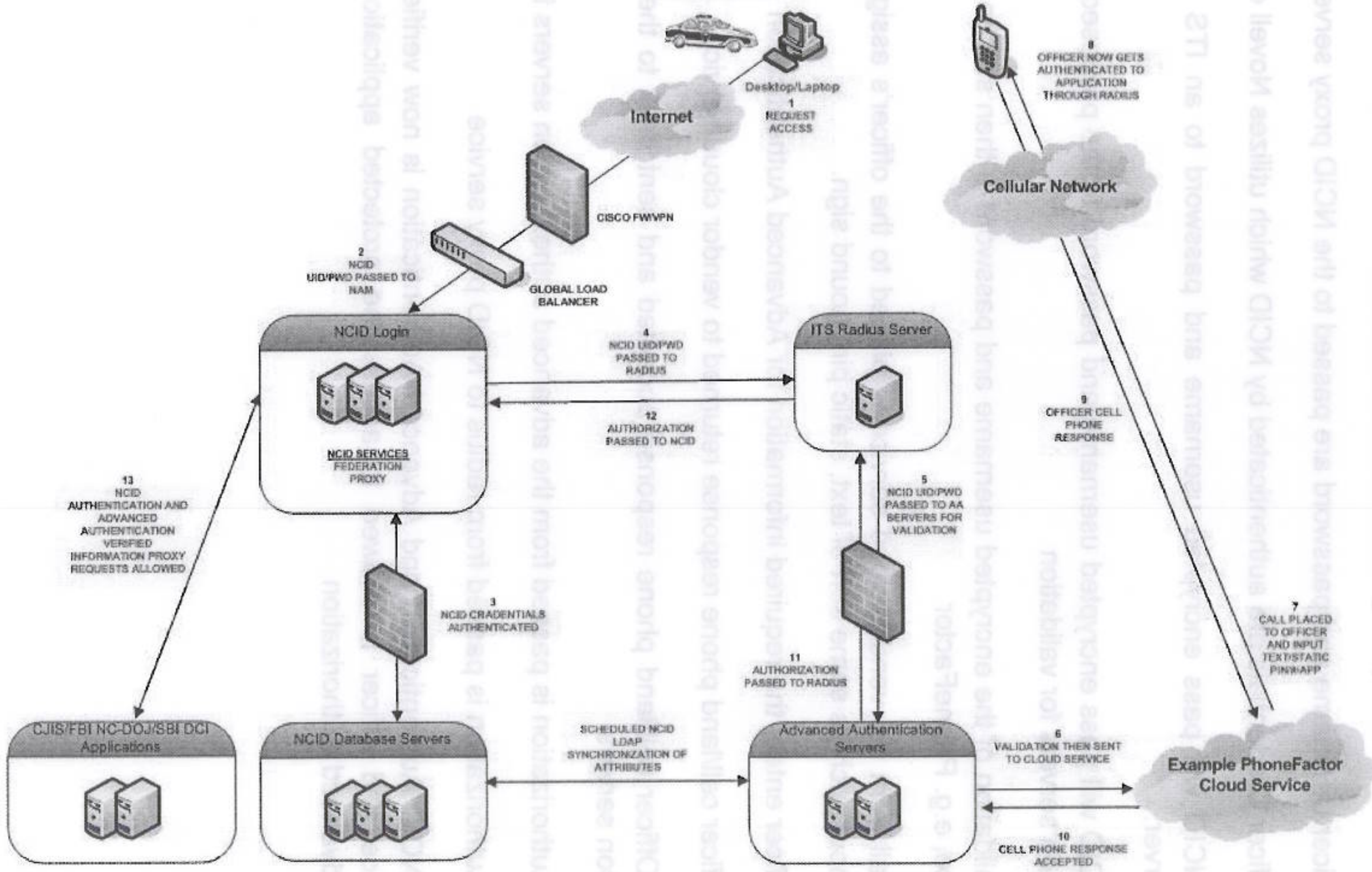
Step 10 – Officer cell/land phone response accepted and sent back to the Advanced Authentication servers

Step 11 – Authorization is passed from the advanced authentication servers to RADIUS

Step 12 – Authorization is passed from radius to NCID proxy service

Step 13 – NCID Authentication and Advanced Authentication is now verified from the proxy service and officer is allowed to access the protected application with the validated Advanced Authorization

EXAMPLE OF NCID ADVANCED AUTHENTICATION
11/29/2012


Internet
Desktop/Laptop
1
REQUEST ACCESS
CISCO FW/VPN
GLOBAL LOAD BALANCER
2
NCID UID/PWD PASSED TO NAM
NCID Login
NCID SERVICES FEDERATION PROXY
4
NCID UID/PWD PASSED TO RADIUS
12
AUTHORIZATION PASSED TO NCID
ITS Radius Server
5
NCID UID/PWD PASSED TO AA SERVERS FOR VALIDATION
11
AUTHORIZATION PASSED TO RADIUS
3
NCID CRADENTIALS AUTHENTICATED
13
NCID AUTHENTICATION AND ADVANCED AUTHENTICATION VERIFIED INFORMATION PROXY REQUESTS ALLOWED
CJIS/FBI NC-DOJ/SBI DCI Applications
NCID Database Servers
SCHEDULED NCID LDAP SYNCHRONZATION OF ATTRIBUTES
Advanced Authentication Servers
6
VALIDATION THEN SENT TO CLOUD SERVICE
10
CELL PHONE RESPONSE ACCEPTED
Example PhoneFactor Cloud Service
7
CALL PLACED TO OFFICER AND INPUT TEXT/STATIC PIN/APP
9
OFFICER CELL PHONE RESPONSE
Cellular Network
8
OFFICER NOW GETS AUTHENTICATED TO APPLICATION THROUGH RADIUS

Next Steps

In summary, the attached ITS proposal is being submitted to CJIS/FBI for approval. Upon receipt of approval, ITS intends to begin integration with CAD/RMS state providers. Upon conclusion our intent is to deploy statewide.