

## Michigan Finds Value in Identity and Access Management

**To comply with federal mandates, the Michigan State Police created a leverageable, secure identity and access management and application integration infrastructure. In doing so, it reduced security administration costs.**

---

### Core Topics

Government: Government Infrastructure & Applications

Security and Privacy: Security Administration

### Key Issues

What applications will affect the operations of government?

How will identity and access management evolve as an enterprise infrastructure?

By following the lessons learned in this case study, government IT managers can use identity and access management (IAM) capabilities to reduce security administration costs, ensure regulatory compliance, increase operational efficiency and effectiveness, facilitate new business and improve their overall IT risk management posture (see "Identity and Access Management Defined" and "Five Business Drivers of Identity and Access Management"). Although whole-of-government IAM projects often fail or have to be reduced in scope (see "Government ID and Authentication: The Right Project Scope"), subvertical domains — or communities of interest with common or similar security requirements — are emerging as proving areas for shared IAM services that can be leveraged in other jurisdictional domains. Justice communities that include justice, law enforcement and correctional agencies are creating information networks to join multitier government agencies in a common information network. For example, Pennsylvania's Justice Network (JNET) initiative includes federal, state and local agencies that access the standards-based online criminal justice record information via a Web interface. Thirty-two state agencies use JNET's secure e-mail for sensitive information.

**Problem:** The Michigan State Police (MSP), in conjunction with the Michigan Department of Information Technology (DIT), needed to develop a criminal justice domain portal and secure single-sign-on infrastructure for multiple law enforcement applications, based on the need to comply with federal security rules for securing criminal justice information. Fiscal conservatism and a firmly established Novell operating environment helped to establish the initiative's architectural direction. The MSP also had to meet federal National Crime Information Center (NCIC) security standards, including:

### Gartner

- *Unique user sessions and IDs:* Michigan needed to move from a model where users shared an ID and logon session at a given location, to a model where users had unique authenticated IDs with appropriate authorization controls.
- *Strong secondary authentication for Internet access:* Traffic from outside the MSP's trusted network would require more than a user ID and password for authentication.
- *Encryption:* 128-bit encryption is required for criminal justice applications and data traversing the network.

The state was heading toward a fiscal downturn when the project was conceived, and the budget for IT and program enhancements was severely constrained.

**Objective:** The MSP and DIT saw an opportunity not only to meet the federal mandate, but also to build an architecture that could become the standard for the justice community and be leveraged by other state agencies. After a requirements assessment was conducted, technical, security and IAM-specific objectives were defined:

- Comply with new NCIC security regulations.
- Build an identity-based portal that could: 1) integrate disparate applications from the criminal justice community and other state agencies; 2) enable secure Web access to criminal justice applications and data; and 3) enable users to access applications from their offices or remote locations.
- Implement a standardized, secure IAM architecture that: 1) centralized management, but allowed local administration of users to reduce the cost of managing user identities and applications; 2) centralized user identity information; 3) synchronized user identity information across multiple applications; and 4) provided application-level authentication and authorization based on the unique identity of the user, as opposed to a shared logon ID.
- Use standards-based technology to ease application integration, provide for reuse of components and remain adaptable in the face of changing technology products.
- Offer support and incentives to replace legacy systems within the agency by leveraging the new IAM architecture, and provide opportunities for other agencies to leverage their application development technologies.
- Ensure the solution could scale for statewide use — 3 million to 4 million users, including commercial vehicle system users, as well as 55,000 executive-branch state employees — and operate with high availability and reliability to support 20,000 concurrent users.

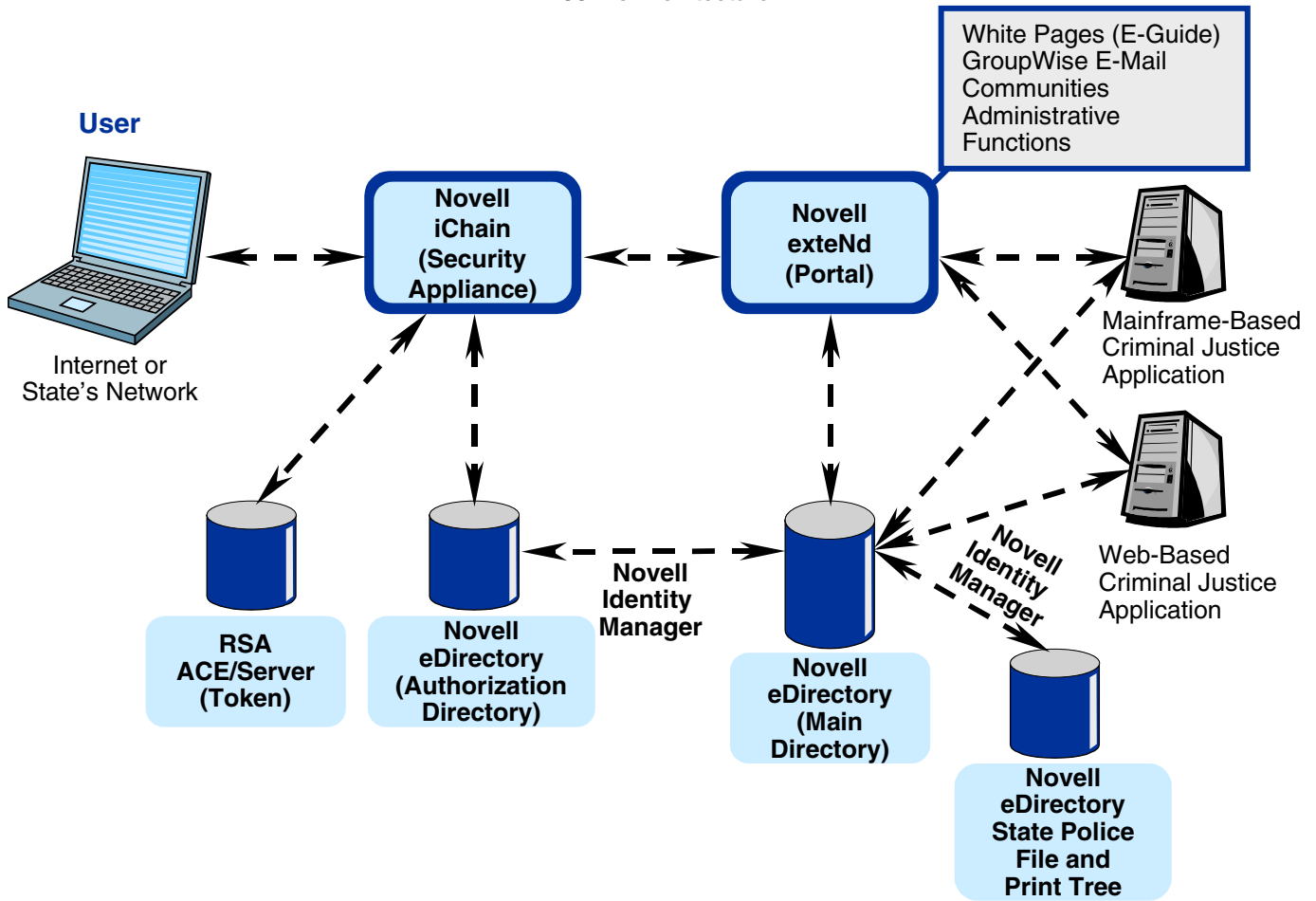
- Use IT assets wherever possible, given budget limitations.

**Approach:** Because Michigan was a large Novell customer (the 14th largest worldwide), the MSP and DIT turned to Novell for assistance. Novell helped MSP develop a strategy using many Novell products that the state owned, which amounted to approximately 80 percent of the needed capabilities. IAM functional products used were:

- Novell Nsure iChain for single sign-on
- Novell Nsure Identity Manager for identity management
- Novell eDirectory for the directory
- Novell exteNd for the portal XML interface and legacy application wrapper
- RSA Security's Secure ID for authentication via remote-access tokens, rather than passwords only, for access to a subset of applications with higher assurance requirements

MSP began the project in May 2002 with a 30-day pilot to demonstrate the technology vision with a workable architecture (see Figure 1). Two full-time equivalents from Novell Worldwide Services supported the state's team. The detailed design phase and development phases were completed by December 2002 and April 2003, respectively. The initial production implementation was finished by September 2003 and went live with the first set of users in December 2003. The infrastructure and application set are collectively called the Michigan Criminal Justice Information Network (MiCJIN).

Figure 1  
MiCJIN's Architecture



Source: Novell and the Michigan State Police

**Results:** The MiCJIN portal allows managed access to business-critical criminal justice applications, such as the Law Enforcement Information Network, and applications that provide criminal and suspect photographs, access to pistol registrants, officer daily reporting, news alerts, and disaster preparedness and response collaboration functionality. During the next 12 to 18 months, the state plans to add 20 integrated applications, and to retire or redeploy the remaining core mainframe-based applications in the new Web-based framework.

The MSP and DIT implemented a directory, hardware and software platform architecture that will scale to meet their needs — 3 million to 4 million users within a directory, and 55,000 state employees. They implemented two iChain boxes to accommodate the potential volume of 20,000 concurrent users.

The IAM infrastructure now delivers a unique user ID for every user, which is a NCIC requirement. If the state had implemented the new security rules without the IAM infrastructure, local law enforcement agencies would have moved from practically no ID administration — because they shared IDs — to having an

administrator at each location, thus creating and supporting multiple unique IDs for every application. The state estimated labor savings of 40 percent from using a single ID for multiple applications. For example, it estimated that each location has 30 users and eight applications per user, for a total of 240 IDs per location.

Because the responsibility was moved from the MSP to the DIT — the central IT organization for Michigan — during the project, the IAM infrastructure can be used by other state agencies.

The total project cost was approximately \$1.4 million, including data center hosting, security support, telecommunications support, hardware and internal services. The largest cost was for Novell consulting services. The state already owned the software, so there were no software costs. Only two consultants from Novell were needed. The project was completed in 10 "man-months" spread over one-and-a-half years.

**Critical Success Factors/Lessons Learned:** Michigan and Novell took an equal ownership stake in the project's success. Novell's reputation was on the line, and the state had a large project that needed to succeed. Each took portions of the project and delivered. Michigan maintained a program management role, while Novell provided the project consultants. Michigan's financial constraints put a strain on the relationship, but Novell stayed with the project, and the state came through with funding.

Integration with the mainframe was a challenge. Novell recommended its exteNd product, Java 2 Platform, Enterprise Edition technology, that it had acquired through its acquisition of SilverStream Software. The state's mainframe/COBOL-style developers had to become skilled in the new development technology. There was no training budget as part of the project, so Novell provided two trainers to train six people for four days at no cost. DIT also ensured that knowledge was transferred from Novell on the technical aspects. Michigan's business units were also involved to transfer IAM administrative skills.

iChain was selected due to its appliance characteristics and flexibility with low-cost servers.

**Acronym Key**

<b>DIT</b>	Department of Information Technology
<b>IAM</b>	identity and access management
<b>JNET</b>	Justice Network
<b>MICJIN</b>	Michigan Criminal Justice Information Network
<b>MSP</b>	Michigan State Police
<b>NCIC</b>	National Crime Information Center

It was important to include knowledge transfer in an IAM project. DIT has taken the knowledge transfer from Novell on the project's technical aspects, and state business units have been involved from an administrative capability perspective.

**Bottom Line:** Government efficiency opportunities often are driven by legal or political requirements. Although a security mandate was a key driver for Michigan's implementation of a

new identity and access management architecture, the benefits of reduced identity administration, simplified sign-on and a flexible architecture were real. Government IT project managers who are integrating legacy environments to Web-based IAM architectures should evaluate product suite vendors that can provide multiple components of the IAM architecture, as well as portal and application integration capabilities. They should also allocate resources for training legacy developers during the transition.