

# **Michigan Criminal Justice Information Network (MiCJIN)**

**State of Michigan  
Department of Information Technology &  
Michigan State Police**



**NASCIO 2006 Recognition Awards  
Enterprise Architecture Category**

## Executive Summary

The State of Michigan's Criminal Justice Information Network (MiCJIN) was developed to meet federal mandates while at the same time providing the foundation for application migration, reduced administrative overhead, while being flexible and scalable to adopt open source technology. The initiative was started in April of 2002 no identified funding but a number of identified issues that required resolution in a very short period of time. The initiative was generated by parallel drivers of federal mandates and needs for a flexible next generation architecture able to support the emerging technologies and development languages. The parallel drivers established two sets of goals those items that were business solutions and those which were technical solutions. The MiCJIN environment established the infrastructure for criminal justice agencies in Michigan to share data in a secure, real-time environment.

With the State affected by a second early retirement and fewer personnel to support the aging technology, combined with limited funding to backfill necessary personnel, a serious situation was in need of a solution that could meet all of the related but diverse needs for the State. The solution would provide the foundation for the Michigan State Police to base the migration of numerous legacy applications and continue to evolve as off the shelf technology emerged. The decisions were made to architect a solution that would leverage proven Internet technologies and be flexible to plug-in JAVA and emerging .Net software development environments. The architecture would be required to be platform independent and not absorbing the common OS or vendor interdependencies. This independence provided baseline comparisons of vendor products and technologies stressing the capability to be flexible and standards based.

The need to leverage related technology that the State owned would provide benefits that reached far to the taxpayers as forklift replacement would not be a considered option. A review of the technology products and support environments occurred and identified key functional architectural components that could be reused by expanding the leverage of the initial agency investments. A key success in the project was a better understanding of the products that the State owned and how the State could more efficiently expand the use of the technology. Cost savings were identified that enabled the project to move forward focusing on the need to save money, while delivering the forward looking technology solution in a frugal economy.

The MiCJIN architecture has been in production since December 2003 having addressed a number of initially identified business and technology drivers for the State while providing the conformity of the federal mandates that initiated the project. The user base for the secure architecture represents State agencies, local agencies and federal agencies in Michigan. The architecture has the ability to scale for other State agency utilizations providing additional taxpayer benefits of reuse and repeatable processes.

The State of Michigan has shared lessons learned and overall design considerations of the architecture with criminal justice agencies in other States based on unsolicited calls by those other agencies. States in close proximity to the border of Michigan have showed interest in the same solution and federal grant dollars were awarded to the State for other criminal justice initiatives based on the success of the MiCJIN architecture.

Discussions have occurred with the Department of Homeland Security of addressing the possibility of cross boundary application integration with the MiCJIN architecture providing the security of sharing data utilizing the Identity Management and encryption controls that were established. The cross boundary sharing of criminal justice data may have been a mix of political and technology hurdles in the past, but the future of data integration and sharing may only be related to the proper discussions and planning as hurdles and roadblocks seem to be fading faster than advancements in technology. Technology solutions such as MiCJIN are the foundation for future enhances in criminal justice support and homeland protection in the State of Michigan. Accessibility to data will be more prevalent away from the brick and mortar building and move to portable solutions allowing the criminal justice community to have the right accurate data when and where it is needed.

## **A. Description of Project**

### **The Michigan Criminal Justice Information Network (MiCJIN)**

The Michigan State Police (MSP) serves as the interface for criminal justice and public safety related information retrieved from and provided to the National Crime and Information Center (NCIC) and the National Law Enforcement Telecommunication System (NLETS). The interface responsibilities provide access for State, Local and Federal agencies with criminal justice and other related public safety needs within the State of Michigan. It is widely understood that criminal justice agencies require very secure and highly reliable technology solutions to meet the demands of 24x7 operations. As new security and technology demands increase, legacy based technology solutions are not normally easily modified to accommodate the new demands, without rewriting the entire application(s) to take advantage of today's technology solutions.

These new demands, in the form of federal criminal justice policies establishing stringent controls for user access, authorization, and criminal justice data encryption, required the State of Michigan to develop a new enterprise solution that would bridge the gap for legacy applications, provide the foundation for new applications and technology, incorporate a centralized Identity Management solution, and establish encryption standards. The Michigan Criminal Justice Information Network incorporates the concept of a portal for centralized criminal justice application access and reduced sign-on, identity management for unique authentication and authorization, and enterprise application integration (EAI) efforts. This architecture provides the standards based technology solution utilizing leading edge technology with best of breed products to securely and efficiently deliver criminal justice applications. The project was initiated to bridge the gap between legacy applications and next generation applications while providing the users the seamless utilization of the applications from any PC capable of using a web-browser and an Intranet /Internet connection. This new delivery model for the users provided additional required encryption, and authenticated and authorized access to criminal justice applications that match the business needs of the end-user.

### ➤ **The Federal Criminal Justice Information Systems Security mandate that required the State of MI to meet the following items:**

- **Unique User Authentication and Authorization**
  - Migration away from the model where many users share a single session
- **Encryption**
  - 128-bit encryption for all criminal justice applications and data
- **Secondary Authentication from the Internet**
  - Traffic from outside the State's trusted network would require more than a user ID and password

### ➤ **The goals and objectives of the MiCJIN solution**

- **Implement standards-based scalable technology platform**
  - Build a security infrastructure that would scale for statewide use
  - Capability to be platform independent
  - Comply with new security regulations
  - Provide a gradual approach to migrate legacy applications
- **Support the integration of disparate applications**
  - Utilize standard technologies to facilitate integration
  - Extract presentation layer and security from application development solutions
- **Reduce the cost and time of managing identities, passwords and applications**
- **Securely identify and authenticate users**
  - Grant users access to applications based on their identity
  - Enable secure Web access to criminal justice applications
  - Ability to provision and de-provision a user's access to the entire architecture from a centralized security model.
- **Leverage existing technology and allow the major components to be "Plug and Play"**
- **Provides Architectural foundation for heterogeneous applications and databases to function within a homogeneous environment**

A proof-of-concept was developed in 30 days to validate the white board design ideas ensuring that the direction taken would meet the Federal and State Criminal Justice Information Systems (CJIS) policies. During the proof-of-concept and detailed design phase additional benefits were realized that would identify efficiencies around support and administration of the existing criminal justice applications. (Further detail will be described in the ROI section.) A secondary scope of the project would be to convert all of the agencies that interfaced with the State Police from multiple legacy connection types, to a standard IP based connection in order to realize long term application and data delivery benefits.

The existing legacy architecture was based on Mainframe applications developed in ALGOL, COBOL, LINC, and other development languages that will not easily migrate to a UNIX based solution nor provide “plug-in” capabilities for off-the-shelf technology that may have quickly addressed the CJIS mandates. In parallel, vendor efforts were underway to deliver new applications that were server based systems deployable via web servers and back end database servers. The MiCJIN solution would be required to be in place in order to meet the delivery dates of the vendors and the deadline to be compliant with the federal CJIS policies. Given these challenges, and very tight parallel deliverables it was necessary to architect a solution that was scalable and not dependent on proprietary technologies or solutions while providing the reliability that the users expected.

MiCJIN has provided the robust functionality to address state and federal standards surrounding technology utilization relating to identity management and encryption. MiCJIN provides the foundation for future advancements in technology allowing for integration seamlessly without major re-engineering of the initial technology investment. As business user needs evolve, devices accessing the essential business data may change as the requirements expand to more portable means without the need to redesign the backend business applications. The users are able to use applications more effectively and efficiently while administration of the security has been reduced by integrating user security and application security within a central LDAP directory. The secure central repository provides the capability to roll-down the administrative tasks of new user application associations to the administrators within the local agencies while providing the local agency administrators the appropriate rights to manage their local agency users.

Core technology components within the architecture include XML, XSLT, SOAP, LDAP, MQ JAVA, and .NET but are not limited to these technologies. These technologies married with the design based on open standards have allowed the ability to make architectural changes utilizing open source products to reduce the operating costs of the architecture. The same standards based direction will provide the State the ability to leverage additional open source solutions as they mature to meet the needs and demands of an evolving architecture. As new business applications are integrated within MiCJIN, the applications are provided enhanced levels of security and protection that were not available prior to the delivery of the architecture. Systems and associated data are protected by encryption from the user to the application, and only authorized users have access to the data. This added security can easily be migrated once newer mandates are established in the future, without the need to redesign any backend business applications or overhaul the architecture. A major portion of the success of the solution was to transition from terminals to PCs or commonly compared to terminal screens to web browsers. This transition provided the conditioning of the end user staff of the new delivery mechanism for the criminal justice applications. An associated efficiency realized is the ability to deliver updates to existing applications and new applications to the end users faster and in a uniform manner. The IT staff is able make all of the required changes on the backend servers no longer requiring staff to physically touch an end users PC when a new release of a criminal justice application is deployed. The legacy applications are front-ended with web interfaces that continue to interface with the mainframe, but an entire migration can occur in parallel and the end user of the application will continue to operate as if the application still resided in the previous location.

The benefit of having an architecture that can continue to evolve without the need to start over in a rebuilding exercise provides the investment benefits rather than those of simple product purchases. With the strategic investment in best of breed standards based technology, the State of Michigan’s environment is flexible and maneuverable to address future mandates and standards quickly and efficiently.

Timeframe for the MiCJIN architecture

- 30 Day Pilot concluded June 2002
- Detailed Design Phase concluded December 2002
- Development Phase concluded April 2003
- Pilot Production Implementation September 2003
- Full Production December 2003 - Providing the standard for access to criminal justice and emergency management business critical applications.

Timeframe for the ISERVICES Gateway architecture

- ITEP Grant Awarded September 2004
- Pilot Production Implementation December 2004
- Full Production March 2006 - Providing the standard for access to criminal justice intelligence via the “virtual pointer system.”

**B. Significance to the Improved Operation of Government**

Similar to what other government agencies were dealing with in regards to early retirements, the State of Michigan was burdened with two early retirements within a five year span that eroded the workforce and the experienced knowledgebase to support the existing legacy architecture and applications. In parallel, technology was rapidly evolving but government funding to leverage the new technology was not on the same pace. The MiCJIN architecture needed to fulfill multiple voids not just limited to the CJIS mandates. An assessment was made during the initial design discussions and the solution needed to also fulfill some of the support voids that the State was experiencing while at the same time gaining efficiencies that had not been envisioned or realized in the existing legacy architecture. Standardizing on a standards-based architecture it allowed the State to replace some of the lost staff with new personnel that had a knowledgebase of the new technology with little or no required training in order to mitigate any learning curves. The secondary benefit was the consolidation of the security administration for the criminal justice applications and delegating authority to the user agencies to manage their agency personnel accessing MiCJIN. MiCJIN, utilizing the identity management function, provided a simple capability to reduce the time it had traditionally taken to provision or de-provision a user in an agency anywhere in Michigan. This benefit of management at the local level for application access provides the ability for the State to re-task the remaining staff on other initiatives instead of the administrative tasks of application associations, password resets, and in some cases first-line support.

The MiCJIN architecture provides the solution that allows the cross boundary secure delivery of applications and data to authenticated and authorized users. The standards that were developed allowed the local agencies in the State to task grant dollars to upgrade to the State standards for encryption and interfaces. These published standards provided the much needed controls and direction that enabled the local agencies to have more control of their respective IT environments and associated operating costs. The MiCJIN architecture provides the mechanism to support new advanced lower cost technology solutions for bandwidth (broadband solutions) that traditionally had not been an available option. Utilization of lower cost bandwidth solutions provided additional potential IT savings for agencies to review as governments at all levels had fewer operating finances to work with in the tight budget times. A resultant operating and cost benefit for the state was the ability to reduce the number of interfaces that attached to MSP to access State and Federal criminal justice files. Java enabled phones and wireless PDAs will have the ability to access the architecture in the future enabling agencies to utilize existing portable devices in their arsenal as well as expand utilization of the technology into the community where the troopers/users need to be involved.

One of the significant benefits was the ability to leverage the MiCJIN environment to establish the criteria used in the 2004 Homeland Security Information Technology and Evaluation Program (ITEP) Grant (#2004-GR-T4-K001) to develop and integrate the Integrated System for the Electronic Retrieval of Vital Information for Crime Enforcement and Security (ISERVICES) Gateway. MiCJIN and the ISERVICES Gateway provide access to an unprecedented amount of information from local criminal justice databases, as this information was previously unavailable to entities external to the originating agency. With the development of MiCJIN and the ISERVICES Gateway, the State of Michigan has established a statewide network to share intelligence and criminal justice information throughout the law enforcement community in Michigan ensuring that the information in these disparate databases is immediately getting to the officers and agents on the streets that need it most.

### **C. Benefits Realized by Service Recipients, Taxpayers, Agency or State**

The State of Michigan has identified the MiCJIN solution as one of the state standards that would be leveraged by other state agencies for an Identity Management solution, reduced Sign-On and secure web application delivery. This type of solution allows the State of Michigan to reduce the number of similar technologies introduced into the state that would require additional State or Federal dollars to implement. Increased application delivery efficiency can be realized as the lessons learned have been established and repeatable processes are in place to shorten the time frame for other State agencies to leverage the MiCJIN architectural foundation. This added benefit of a developed standard allows the Department of Information Technology (DIT) to redeploy support staff into other areas that may have traditionally supported multiple parallel agency dependent solutions.

Cross agency benefits may be realized with lower operating costs as existing office PCs can be utilized to access the MiCJIN architecture and associated criminal justice applications. Productivity for troopers/users can be quantified as more PCs are available to access the job specific criminal justice applications, possibly reducing the time the trooper/user is spent waiting in the office. The additional cross agency benefits afford the IT staffs within the local agencies to be redeployed as media is no longer sent to the user agencies when application updates occur. Support savings can be attributed as patch management or version management is uniform for all users reducing the complexity of users requesting support with application issues. In the past, it was not uncommon to identify users who were still using early or no longer supported versions of the software; this issue was mitigated for all support personnel at the State and local levels.

Benefits as it relates to Homeland Security have already been realized as the Department of Homeland Security is a user of the system in the State of Michigan. Cases have been reported of the MiCJIN architecture enabling user access to applications that previously they did not have access to away from the office that identified individuals on watch lists or other related reports. The benefit may not have been related to financial or direct productivity but as the tools have been delivered in a secure way to be more available to the user away from the office, Homeland Security protection becomes even more of a realized safety benefit.

Existing IT staff that have been transitioning from supporting the legacy environment to newer technologies provide the added security of the taxpayer that dollars are well spent supporting the needs of protecting the State of Michigan's citizens. This transition enables the migration of mainframe based applications to web based applications and the business and IT knowledge of the legacy applications is not lost as the staff migrates the applications away from the mainframe.

Gartner developed a strategy paper on Identity Management based on the State's MiCJIN solution. The paper describes the success of Identity Management and reduced administration of applications based on best of breed products in the solution.

Within the first four weeks of operation of the ISERVICES Gateway, a federal user of the system identified an individual on the terrorist watch list that was attempting to enter the State of Michigan from the border. This was identified as a significant return on investment of the two integrated technologies of MiCJIN and ISERVICES for the citizens of Michigan, and enhanced level of homeland security. The same success model that was garnered with the MiCJIN environment for other entities to take notice was also utilized and identified with the ISERVICES Gateway. Both integrated initiatives sparked interest within the public safety and Homeland Security communities at all levels to leverage and adopt the same framework for reuse.

## **D. Return on Investment, Financial Benefits**

The short term ROI is the ability to use technology efficiently to reduce the staff overhead for administration, and security controls while enhancing the ability for the end user to gain access to the required criminal justice applications. By developing the MiCJIN architecture and establishing the role of Identity Management, reduced sign-on, and application integration in the migration efforts away from the legacy technologies, a substantial reduction in maintenance costs will be realized as the legacy environment is migrated. Reduction of 40% in the cost of administering identities by automating identity management and providing the decentralized approach for administration of local user identities by the associated local agencies.

### **Financial Savings**

Savings realized to date after migrating from terminal based applications to web based applications is **\$471,000** for a single legacy based application and associated vendor support. These savings were maintenance costs and support identified as one of the successful factors promoting the benefits of migrating away from the legacy solutions and towards more viable current technology. Another **\$500,000** has been identified in annual savings as an effort to migrate all of the agencies that were connected to the criminal justice systems with legacy based connections types.

The ability to deliver an application from idea to production will be much faster as the security and presentation layer can be removed and leveraged from the MiCJIN architecture. IT staff are focused on the migration of legacy applications utilizing the repeatable solutions sets architected in MiCJIN.

Application manuals and training is delivered from the MiCJIN portal reducing the need for staff to print and send materials to the end user. This mechanism provides the ability for the user to access user manuals and training online and updates passed on to the users so version control or outdated manual usage is mitigated. Estimated savings for printing and delivery costs of the manuals is **\$135,000**. The delivery of training via the web allows travel to be reduced to keep pace with travel restrictions associated with shrinking budgets and still providing the user community with training needs.

There are no distinct cost savings related to the ISERVICES Gateway and its implementation. One item that can be reviewed as a cost identifier is the ability to use the system to retrieve data from the locally administered databases by the participating agencies without the need for the State to build a data warehouse or other such repository that retained a copy of the data from the disparate database systems. This becomes a clear politics savings, as the “owners” of the data in the disparate repositories across the state are still maintaining and owning their data, but are providing controlled access into their systems for use by their peer criminal justice agencies around the state.