The Western Identification Network: Identification as a Service in a Federated Architecture

Roger KONECNY

Abstract

The Western Identification Network (WIN) is a not for profit corporation in the United States, providing a multi-state, multi-modal, biometrics identification system. Formed in 1988, WIN created a revolutionary concept: gaining the backing of governors, attorneys general, legislators, and chief law enforcement officials to combine technical and financial resources enabling the first multistate biometric network sharing fingerprint data across state lines. The outcome was the formation of WIN, providing identification services for criminal and civil identification purposes.

Keywords

multi-modal biometrics identification system, automated fingerprint identification system, active, active disaster recovery system, criminal and civil, IDaaS model, configurable, policy-driven workflow

1. History of WIN

Beginning strictly with fingerprint matching, WIN brought together a consortium of western states utilizing NEC's Automated Fingerprint Identification Systems (AFIS), some sharing a common infrastructure while others interfaced to share data. In addition to providing identification services, WIN continues to provide network services and expert consultation to its members. In the 1980's, AFIS provided state of the art technology

Fig.1 Contiguous states can identify suspects committing crimes across borders.

at the time but which would appear rudimentary by today's standards. Memory, storage, and bandwidth were at a premium – tradeoffs were necessary to reduce demands upon these resources. Oftentimes, fingerprint images themselves were not stored and AFIS was used to perform automated comparisons followed by human examination.

The founders of WIN recognized the value of sharing data and resources, leading to the vision of a biometric matching system with the ability of identifying criminals who moved across jurisdictions. This bold strategy preceded by ten years the implementation of the United States first national biometrics platform provided by the Federal Bureau of Investigation (FBI) in 1999 (**Fig.1**).

In the three decades since its inception, WIN has undergone a series of upgrades, which added capabilities and new services to its members. In 2014, WIN underwent its most recent upgrade. Significant within this upgrade was the implementation of an Active/Active Disaster Recovery System. Moving from a single, redundant, centralized system to dual redundant systems located in disparate locations, WIN was able to decrease their risk profile due to natural or fabricated disaster.

2. Challenges of a Federated System

The use of biometrics in a federated environment has inherent challenges. Different states have different laws and policy governing the search and storage of fingerprints, facial images, and other biometrics. A configurable, policy-driven workflow is necessary to accommodate variances between agencies. Considerations within workflows are given to maintain a standardized base flow, with decision points to handle the nuances between state jurisdictions entities such as applicant processing.

Common within the United States is the use of fingerprint-based background checks for positions of public trust. Jurisdictional differences include mandates to either include/exclude the searching of applicant fingerprints against unknown, criminal suspect fingerprints. Similarly, the ability to store applicant fingerprints varies among the states based upon local statute.

These elements require a robust business policy and validation layer within the system. Eight member states currently belong to the WIN consortium, and the implementation of 8 distinct components would reduce the cost effectiveness and benefits of the system. Overcoming this challenge is not simply a technology exercise – operational policy is required to promote and maintain standards.

WIN overcame this challenge by standardizing workflows, data input and output specifications, and adhering to open standards to the maximum extent possible. For example, most biometric systems today utilize the National Institute of Standards and Technology (NIST) record formats for the exchange of biometric information (searches and results). The base NIST standards are enhanced by the FBI's Electronic Biometric Transmission Specifications (EBTS). By electing to utilize the NIST EBTS protocols, WIN provided a common framework across multiple agencies to share information. Additionally, a standard validation layer is utilized across the platform. Using a widely recognized standard allows for the addition of new biometric modalities as they become commonly used.

It is worth noting that data capture needs do vary across entities, which requires additional data input checks for some agencies. These validations are layered above the standard validation component to gain the most efficient use of common components for all members.

3. Tangible Benefits are Realized

The uniqueness of the WIN organization and system provides benefits to its membership in financial, operational, and social values.

3.1 Financial Benefits

Using the Identification as a Service model provides member agencies improved cash flows as they can use Operating funding models. The operating model mitigates the need for costly-periodic-and risky-capital-funding approval for hardware and infrastructure that will age and require replacement throughout the serviceable life of the system.

Leveraging the financial backing of multiple agencies provides WIN with greater purchasing power. The inclusion of a fully redundant, Active-Active Disaster Recovery capability would be subjected to budgetary constraints for most single-state systems. Shared costs amongst the organization, in conjunction with a common platform makes this capability an achievable reality.

3.2 Operational Benefits

A number of operational benefits can be achieved with the pooling of resources to support a common platform. Help Desk and support staff can be combined to provide greater coverage and quicker response times. Specialization for multiple systems isn't required, Support center resources can be focused on the same standardized platform, thus mitigating support center training over-

head reducing the cost of 24/7 support.

The service model, in conjunction with its architecture, provides users with a scalable platform. Priority setting and resource sharing allows users to utilize greater than 100% of their required resources – consuming biometric matching resources that may be idle for other members. This in turn allows for faster response times and more efficient use of human resources.

Long term sustainability becomes accessible under the IDaaS model. As new biometric modalities, matching algorithms, and national/local requirements evolve, they can be applied to a larger consumption base. This evolution of a broad base facilitates national advances in inter-agency cooperation and policy advancement.

3.3 Social Value

The immeasurable benefit of a federated system is the ability to solve crimes which occur in contiguous states. Criminals are known to commit crimes across borders, particularly when they reside near state lines. A federated system allows for cross-searching of the dataset, making these identifications from fingerprints left at crime scenes possible.

National criminal identification systems are also subject to budget and resource constraints; it is not always feasible to store and make available for matching, fingerprints of known subjects for minor offenses. These offenders can be (subject to local statute) stored within the federated IDaaS system, providing the capability of these identifications.

The forum for identification professionals to collaborate and improve data sharing is inherent within a structure such as WIN. Agencies are free to create policy dictating the level and manner of information to be shared. In addition to data sharing, strategies for the adoption of new technologies and requirements can be formulated by a like-minded group of professionals.

4. Service Architecture Components

The system itself can be thought of as a three-tiered design, each with multiple sub-components (**Fig. 2**).

At the point of user interaction are the applications specialized to the user needs. These include tools for the comparison and examination of unknown subject latent fingerprints, comparison of known subject fingerprints against the stored gallery, and administrative tools for reporting and archival purposes. The federated nature of the system is transparent to the users, excepting cases where an identification is made from a record sourced from another agency (in which case the fingerprint expert can view the source details of the record or contact the originating agency for further information).

A chief component at the agency level, is a localized workflow manager. In the case of WIN, one such component is located within each of the eight member states. This component provides a number of benefits, but primarily serves as a caching mechanism in the event the network connectivity between the agency and central database & infrastructure is lost.

Above the state workflow and workstation level re-

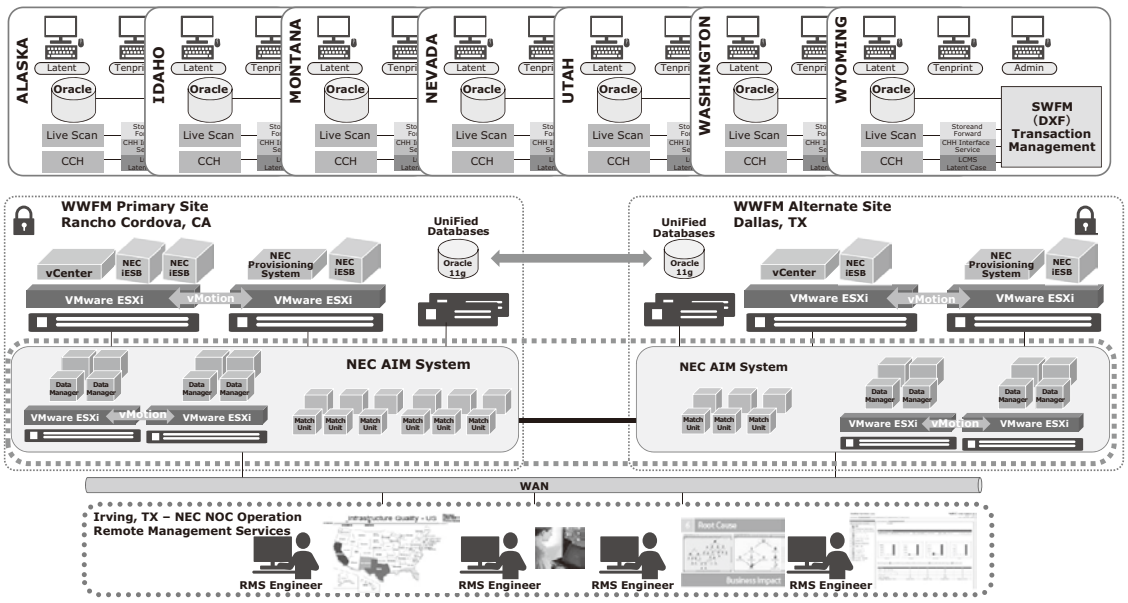

Fig. 2 Architecture of the three-tiered WIN system.

sides the centralized tier. This application layer can be further subdivided into three major sub-systems: transaction management, biometric matching, and database storage.

The transaction management system provides the workflow and routing of biometric submissions. It is here that transactions are evaluated for submission for searching, storage in the database, or forwarding to other, external agencies. Where and how the transactions are routed is dependent upon the type of transaction as defined within the EBTS. Transactions are further evaluated on a priority basis, where the WIN organization sets the precedence of traffic for the greatest need. For example, a mobile identification of a subject encountered by law enforcement in the field is prioritized for officer safety.

The biometric matching subsystem provides the actual matching and potential candidates returned to a human operator for verification, or upon achieving pre-defined thresholds, declaring an automated identification.

As routed by the transaction controller, and in conjunction with the results of the identification & matching process, the biometric data is stored within the database.

Scalability and elasticity are necessary components of the IDaaS model – federated or otherwise. These requirements are met through the use of virtualization within the middle, centralized tier. Technologies such as VMWare allow the system to expand and contract by adding matching resources and routing components.

A unique characteristic of the WIN system is the provisioning and active use of dual central sites. Each site features full copies of an actively synchronized database and biometric matching data. Further, redundant network connectivity and external interfaces to the FBI allow for seamless failover in the event one of the hosting datacenters should be struck by disaster.

The final layer in the IDaaS model is the support and monitoring system. Remote Managed Services capitalize on the pooling of resources to proactively monitor and maintain the system. Trends in submissions and processing are monitored, allowing for real-time adjustment of thresholds and priorities. Support staff can effectively maintain and remotely monitor the health of the infrastructure, without requiring an onsite presence.

5. Evolution of the System

From the inception of the WIN system to its current state, the capabilities, design, and communication mechanisms have improved tremendously.

The original design of the system is analogous to the early days of Unix-based systems; with multiple clients competing over resources centrally located in the backend. Advances in computing power, and equally important, network capabilities allowed for the advancement of the system to its current state. These advances allowed WIN to migrate those members sharing data only via interface to eight states fully populating a shared database.

Reduction in the costs of network bandwidth, coupled with the speed of transmission, alleviates the need to restrict data sharing based upon cost.

WIN pioneered the Service Level Agreement (SLA) method of obtaining IDaaS. Under the SLA model, metrics for accuracy, throughput, and response time are key performance indicators of the system and tied to the payment of services.

At the time of this writing, WIN is embarking upon the next generation of its federated system. It has taken this opportunity to further refine its methods of operation. Chief amongst these are requirements and design to create a framework for anticipated changes in future technology. Interoperability features and the addition of new, as-yet undefined biometrics are included the mechanisms provided by the service bus layer.

Operational and deployment methods are also under evaluation. Expanding the disaster readiness capabilities for individual members is made possible through virtual desktop technologies – allowing entire state identification bureaus to relocate in the event of a disaster at one of the member state locations.

6. Conclusion

WIN has combined the use of two unique approaches to maximize their return on investment. Either of these methods provides ample ROI on their own, and when combined act as a force multiplier. The federated model provides social, financial, and operational benefits. Identification as a Service amplifies these gains and creates technology benefits.

The IDaaS model pioneered by WIN has influenced agencies within the United States and abroad to take advantage of these benefits, and is increasingly requested by law enforcement agencies. The incorporation of a federated system is not so easily applied. Federation is best suited to large, state-level entities and at times may be subject to territorialism, legal hurdles, and interoperability challenges that may prohibit the forming of such an organization.

When these methods can be combined, the benefits are enormous and provide greater safety for citizens and our society.

* VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions.
* UNIX is a registered trademark of The Open Group in the United States and other countries.
* All other company and product names that appear in this paper are trademarks or registered trademarks of their respective companies.

Authors' Profiles

Roger KONECNY
Senior Director,
Systems Integration & Delivery,
Advanced Recognition Systems Division,
NEC Corporation of America

The details about this paper can be seen at the following.

Related URL:

Western Identification Network
http://www.winid.org/winid/

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese English

Vol.13 No.2 Social Value Creation Using Biometrics

Vol.13 No.2
April 2019

Special Issue TOP

Papers for Special Issue

NEC Information