Client story

Securing justice with automated digital identity solutions

How a state law enforcement agency strengthened cybersecurity and built tamper-resistant audit trails

Client overview

- A large state law enforcement agency provides high-quality statewide public safety for citizens and visitors
- The agency's Information Technology division supports local, state and federal law enforcement by maintaining eight mission-critical criminal justice systems and public registries
- Responsible for securing sensitive personal data, designing non-repudiable court-mandated document signing and improving public trust in the judicial system

Objectives

- Protect sensitive personal information and secure systems from external and internal cybersecurity threats
- Develop a system to securely manage user identities and access to multiple critical systems used by local, state and federal law enforcement
- Ensure that all actions and signatures, including those mandated by court orders, are non-repudiable, bound to user identities and protected by strict access controls
- Automate identity life cycle management and develop an access provisioning system without incurring additional infrastructure costs
- Provide detailed and trustworthy audit trails designed to support regulatory compliance and allow every action to be traced to a digitally signed attestation

Why Unisys?

- Unisys partners with highly regulated public sector organizations to power secure, customized identity-based solutions for access control
- We provide regulated clients with an identity-focused approach that reduces risk exposure, minimizes cyber vulnerabilities and improves operational efficiency
- Our teams are capable of integrating AI-powered intelligence and advanced cybersecurity protections that support operations without compromising data privacy
- Unisys delivers scalable and cost-effective solutions that use existing cloud-based services without the need for additional infrastructure investments
- Unisys experts collaborated with the agency to align every step with federal and state compliance requirements, cybersecurity best practices, and workflow automation for public agencies

Solution

- Implemented Digital Identity and Access Management (IAM) solution to create a centralized user directory
- Deployed Okta-powered Single Sign-On (SSO) capabilities for user provisioning, identity verification and role-based access control (RBAC)
- Used the DocuSign digital signature tool to allow for non-repudiable, legally-binding signings for court documents and attestations
- Created a comprehensive audit logging and compliance reporting system that makes every action traceable
- Automated cloud-based identity life cycle management to help streamline access reviews and align with Zero Trust security practices

Results and benefits

- Helped reduce cybersecurity vulnerabilities, protected sensitive personally identifiable information and achieved compliance with regulations
- Improved operational efficiency and reduced the number of manual errors by automating onboarding, user provisioning and access management
- Reduced costs associated with additional technology infrastructure and developed a scalable system using cloud-native solutions
- Enhanced audit readiness and regulatory compliance by creating a tamper-proof record of system actions
- Established a benchmark for best practices for identity governance and cybersecurity for highly regulated public safety agencies
- Non-repudiable identity attestation and document signing help maintain compliance with data privacy regulations and court-mandated actions
- Automated user provisioning and reduced the number of manual errors with RBAC
- Created an audit trail that helps ensure end-to-end traceability for actions and attestations
- Helped lower cybersecurity vulnerabilities and sustain an industry-leading cybersecurity risk score
- Enhanced data privacy, improved cybersecurity and increased compliance with regulatory standards without additional infrastructure costs

A state law enforcement agency launches a digital identity transformation

A large state law enforcement agency envisioned a modern, secure digital identity ecosystem built for the next era of public trust. Its current approach involved manual user onboarding and access provisioning, resulting in human errors and labor-intensive workflows that constrained administrative efficiency. Together, the agency and Unisys developed automated digital identity processes, increased cybersecurity protections and created audit trails to comply with court orders.

By replacing manual steps with automation, the agency strengthened efficiency and resilience

The agency's Information Technology division supports a wide range of public safety goals, managing the state's eight mission-critical criminal justice systems and public registries. These systems handle employment background checks, vehicle safety inspections, traditional law enforcement investigations and executive protection. The agency took proactive steps to stay ahead of rising internal and external threats that posed a risk to the applications' information security and hampered administrators' ability to track actions within the system.

The agency recognized an opportunity to enhance security and accountability: ensuring that court-mandated actions could be securely bound to user identities with proof of integrity and origin. They needed automated user creation and provisioning based on attributes from court-mandated workflows while maintaining a single auditable trail for every executed action.

The agency sought a trusted technology partner to automate a digital identity, develop audit trails with non-repudiable document signing and meet court-mandated requirements for actions tied to verified user identities. Even more challenging, it needed a partner who could accomplish all of this without additional infrastructure investments.

Highly regulated public agencies choose Unisys for customized IAM

After evaluating several potential partners, the agency chose to work with Unisys to develop a custom digital identity solution. It chose Unisys because of our experience working with highly regulated public sector clients and expertise in developing data security protections for complex technology environments. Unisys created a customized identity-focused approach to user onboarding and provisioning, combined with advanced cybersecurity protections and AI-powered intelligence to identify and prevent both internal and external threats.

Streamlined digital identity management improves operational workflows and cybersecurity protections

Working side by side, Unisys and the agency achieved their digital identity transformation goals with our comprehensive IAM solution, using a combination of Okta-powered SSO, seamless user provisioning and automated RBAC. Unisys also integrated DocuSign to create legally binding, non-repudiable court documents and attestations, meet court mandates, and establish a clear audit trail for traceable law-enforcement actions.

The solution includes an automated workflow engine that orchestrates identity provisioning and access approvals based on court-mandated attributes. This helps ensure compliance with legal requirements while reducing manual intervention and delays.

Using cloud-based identity life cycle automation, the agency streamlined workflows, reduced administrative workloads, and aligned with Zero Trust security policies that exceed industry standards without adding infrastructure costs.

IAM boosts efficiency and helps this agency comply with stringent data privacy regulations

The state law enforcement agency achieved numerous tangible results from this partnership. It strengthened cybersecurity and data privacy protections, meeting federal, state and local regulations governing personally identifiable information and maintaining a cybersecurity risk score well below the industry average. This set a new benchmark for identity governance, cybersecurity and efficiency for public-sector law enforcement agencies.

In addition, administrative efficiency increased significantly due to automated user onboarding, provisioning and access management. Errors from manual entry were also considerably reduced. Finally, the agency was able to save substantial costs by using cloud-native solutions and existing systems to transform its identity management processes without additional infrastructure investments.

Unisys builds a scalable environment that strengthens public trust and accountability

Unisys and the agency co-created a scalable identity management foundation designed to evolve with the state's future needs. The IAM platform can be scaled for more users, additional access controls, and to promote more public access to critical information regarding criminal offenders. The cybersecurity protections put in place will help guard against insider misuse of personally identifiable information, defend against external cyberattacks and maintain public trust in law enforcement's actions.

With this strong technology foundation, the agency can address future cybersecurity challenges; scale its IAM solution to meet the needs of the state's growing population; and fulfill court-mandated, non-repudiable audit requirements.

Learn how Unisys is helping public sector organizations respond to the growing number of cybersecurity threats and build trust in public institutions. Visit us online or contact us today.

unisys

unisys.com

10/25 5720-10832