Identity Credential, and Access Management: Lessons Learned and Best Practices

*Case Studies from Domestic and Foreign Government Organizations*

The ACT-IAC Associates Program Class Report to the IT Management & Modernization Community of Interest

**Released:** January 3, 2022

**Synopsis**

This report provides best practices and lessons learned on Identity, Credential, and Access Management (ICAM) technologies through examination of case studies from US federal and foreign government organizations.

The case studies in this report provide a set of lessons learned that government stakeholders can use as they plan ICAM strategies. These are real-world examples that provide insight into successful implementations of ICAM instances. Readers will find information in these case studies that can assist them with ICAM efforts.

The represented Government agencies and organizations made choices of vendors and solutions are based on program-specific selection criteria. The IT Management & Modernization Community of Interest respects the independence of these choices and does not advocate any one vendor or solution over another.
American Council for Technology-Industry Advisory Council (ACT-IAC)

The American Council for Technology-Industry Advisory Council (ACT-IAC) is a non-profit educational organization established to accelerate government mission outcomes through collaboration, leadership and education. ACT-IAC provides a unique, objective, and trusted forum where government and industry executives are working together to improve public services and agency operations through the use of technology. ACT-IAC contributes to better communication between government and industry, collaborative and innovative problem solving, and a more professional and qualified workforce.

The information, conclusions, and recommendations contained in this publication were produced by volunteers from government and industry who share the ACT-IAC vision of a more effective and innovative government. ACT-IAC volunteers represent a wide diversity of organizations (public and private) and functions. These volunteers use the ACT-IAC collaborative process, refined over forty years of experience, to produce outcomes that are consensus-based.

To maintain the objectivity and integrity of its collaborative process, ACT-IAC welcomes the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of technology. For additional information, visit the ACT-IAC website at www.actiac.org.

IT Management & Modernization Community of Interest

The IT Management & Modernization (ITMM) Community of Interest (COI) advises and equips government with best practices and lessons learned, focused on strengthening IT management and implementation and accelerating IT modernization. The COI covers all aspects of IT management and modernization to include strategy and policy making, governance, Capital Planning Investment Control (CPIC), Federal Information Technology Acquisition Reform Act (FITARA) implementation, and operations management.

Disclaimer

This document has been prepared to contribute to a more effective, efficient, and innovative government. The information contained in this report is the result of a collaborative process in which several individuals participated. This document does not – nor is it intended to – endorse or recommend any specific technology, product, or vendor. Moreover, the views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development. Every effort has been made to present accurate and reliable information in this report. However, neither ACT-IAC nor its contributors assume any responsibility for consequences resulting from the use of the information herein.

Copyright

©American Council for Technology, 2022. This document may not be quoted, reproduced, and/or distributed unless credit is given to the American Council for Technology-Industry Advisory Council.
Table of Contents

Introduction and Executive Summary ................................................................................................... 5

Case Studies .......................................................................................................................................... 7
  South Korean Digital Driver’s License .............................................................................................. 7
  Mexican National Digital Strategy (NDS) Digital Birth Certificate Initiative ............................... 10
  Login.Gov .................................................................................................................................. 13
  USAccess Point Pilot .................................................................................................................. 15
  TSA Biometrics Roadmap – For Aviation Security & the Passenger Experience ....................... 17

Lessons Learned .................................................................................................................................. 19

Authors & Affiliations .......................................................................................................................... 23

References .......................................................................................................................................... 24
Introduction and Executive Summary

In an increasingly digitized world, Identity, Credential, and Access Management (ICAM) continues to be at the forefront of technical evolution. Accuracy, security, and convenience are essential pillars to the evolving nature of identity management, which is both challenging and opportunistic.

ICAM maturity varies among government organizations, and understanding the experiences of other organizations benefits those making progress towards similar transformations. The IT Management & Modernization Community of Interest (ITMM COI), in partnership with the 2021 ACT-IAC Associates Program, developed this project focused on:

- Distillation of best practices and lessons learned on the topic of ICAM transformation;
- Analysis of challenges, opportunities for improvement, and value-based solutions as executed by foreign and domestic government entities; and
- Mapping similarities and differences between unique solutions used to achieve digital transformation in ICAM technologies.

The ITMM COI and the 2021 Associates Program Team set forth to analyze different strategies and tactics that enabled both government and industry entities to modernize and mature their current ICAM systems, with a focus on how they impacted end-users and customers. The team sought to gain insights through industry research and analysis, focusing on applicability to the United States government and deciphering what went well and opportunities for improvement.

This effort entailed research of two foreign organizations:

- South Korean Digital Driver’s License under the “Digital New Deal”

This effort also included three US federal organizations:

- Login.gov’s Citizens Service
- USAccess Point Pilot between GSA and USPS
- TSA’s Biometrics Roadmap

The team looked specifically at how these organizations were able to accomplish an ICAM transformation and laid out how it was implemented. These case studies were documented with a particular focus on the challenges, their approach used, and their valued-based results. Among the findings, the common lessons learned throughout each ICAM implementation strategy were as follows:
Lesson 1: Safeguarding User Data

Privacy of user data builds trust and adoption of new services

- A focal point to ICAM is safeguarding user information, particularly Personally Identifiable Information. As agencies take steps to advance their digital footprint, it is imperative that they advance IT security in tandem. Confidence and assurance in any system are important to its overall acceptance and longevity. In each of the case studies, safeguarding of user data was deservedly emphasized.

Lesson 2: Pilot Programs for Incremental Implementation

Incremental implementation through Pilot Programs allows for flexibility during development

- Incremental implementation of ICAM technology with pilot programs helps determine the best course of action for improvement and refinements before a full, public solution is implemented.

Lesson 3: Continual Improvement

Modernization is a continual effort, requiring ongoing improvement

- To maintain data privacy and system security, governments need to continually improve to defend their systems and contents from threats as the technology available to malicious actors evolves rapidly. Similarly, the needs of the citizens and other users are constantly changing, and governments need to continually enhance these solutions to support those changes.

Lesson 4: Increased Infrastructure Capability

Enhancing the user experience through infrastructure capability

- As IT modernization frequently results in the transition from decades-old legacy systems to the cloud, the primary focus of ICAM transformation is enhancing the user experience.

Commonly throughout the stories documented here, these best practices proved beneficial to the organizations executing them, and can be used as a guide for organizations looking to pursue similar efforts.
Case Studies

South Korean Digital Driver’s License

With Blockchain, Self-Sovereign Identity (SSI), and Decentralized Identity (DID) Technology

Title of Project: Digital Driver’s Licenses under South Korea’s “Digital New Deal”

Organization: (South Korean Government) Ministry of the Interior and Safety (MOIS) and Korea Minting, Security Printing and ID Card Operating Corporation (KOMSCO)

Vision: The Korean “Digital New Deal” aims to accelerate a transition towards a digital economy, with investments focusing on the integration of data, network, and AI (DNA), digital education infrastructure, contactless industries, and digitalizing social overhead capital.

Goals/Objectives: To implement a safe, secure, and private digital driver’s license that can be used for identification and authentication at all locations where physical driver’s licenses are accepted.

Solution: As part of the Korean Government’s “Korean New Deal” introduced in 2020, the “Digital New Deal” component aims to lead digital transformation by improving the ecosystem of Data, Network, and AI (DNA), digitalize education infrastructure, nurture contactless industries, and digitalize social overhead capital [1]. A piece of the “Digital New Deal” is the development of a digital driver’s license to enable the use of digital ID cards via smartphones, implementing “the dual identity verification system with offline physical identification and online certificate-based identification” [2]. As a trial run during the first half of 2021, civil servants at central government organizations could download mobile ID cards to their smartphones for identity verification and log into an online system for administrative purposes, instead of using their physical ID card [3].

In a partnership between the three largest South Korean mobile carriers (SK Telecom, TK Corporation, and LG U+) and the Korean National Police Agency and Road Traffic Authority System, a publicly available digital driver’s license was rolled out on the identity authentication mobile application “PASS” as a pilot program for testing of digital driver’s licenses. Launched in July 2018, the PASS app is an identity verification service offered to users of the three mobile carriers and is mainly used for authentication purposes in financial transactions on mobile devices [4]. As of July 2020, when the digital driver’s license service was introduced, the PASS app boasted over 30 million individual users.

Within the first month (August 2020), over 1 million users had registered their driver’s licenses to the app [5]. The digital driver’s license on PASS still required users to have a physical driver’s license to register, thus not being truly digital, and was only accepted for identity verification in limited settings such as convenience stores. Banks and certain government institutions did not accept the digital driver’s license on PASS for identity verification [6].

In mid-2021, the Ministry of the Interior and Safety (MOIS) and Korea Minting, Security Printing and ID Card Operating Corporation (KOMSCO) selected LG CNS and RAON Secure to develop a digital driver’s license that will be fully digital, not requiring an existing physical card. It will be issued by the Korean Police Agency.

American Council for Technology-Industry Advisory Council (ACT-IAC)
3040 Williams Drive, Suite 500, Fairfax, VA 22031
www.actiac.org ● (p) (703) 208.4800 ● (f) (703) 208.4805

Accelerating Government Mission Outcomes Through Collaboration, Leadership and Education
The digital driver’s license will incorporate lessons learned from the PASS app digital driver’s licenses and the digital identification service for government workers.

The licensing service will be blockchain-based with Self-Sovereign Identity (SSI) and decentralized identity (DID) system technology. These technologies should increase cybersecurity while giving users control over their identity and personal information, as their data is stored on their own device and not a centralized server. Similar to the mobile ID cards used by civil servants at central government organizations during trial runs, the digital driver’s license will use OmniOne, a blockchain-based platform developed by RAON [8]. SSI is the concept that users’ identity and information are stored on their own devices, instead of central servers. This gives users more control about exactly what personal information is shared and with whom. In theory, this will increase resilience to losing sensitive personal information in the event of a cyber-attack. DIDs are an integral component of SSI, as they allow for “unique, secure, and private peer-to-peer connections” between a user and a service [9]. DID cuts out intermediaries such as mobile network operators, email providers, companies such as Google or Facebook, etc., to connect users to services. Again, this increases resilience against cyber-attacks and prevents companies from collecting user metadata. The digital driver’s licenses will use “public DID,” meaning that only certain publicly identifiable information is shared between a user and a service/partty, at the user’s consent. SSI and DID together allow a user to only share certain information during a transaction or authentication process, instead of all personal information contained in an identity card. For example, at an airport, only authentication information may be shared to verify identity before boarding a flight. Or, when purchasing alcohol, only that a user is of legal drinking age is shared, instead of information about the exact date of birth or home address [9].

The Korean Government plans to begin demonstrations of the digital driver’s license service by the end of 2021, with a full rollout targeted for 2022. The mobile ID card service for public servants is set to expand beyond central government workers, including additional officials at other organizations and public-school teachers [10].

In the United States, Apple is working with states including Arizona, Georgia, Connecticut, Iowa, Kentucky, Maryland, Oklahoma, and Utah to enable a citizen to add their driver’s license to Apple Wallet. The Transportation Security Administration (TSA) will enable select airport security checkpoints at participating airports to accept the ID in Apple Wallet [11]. Apple claims that the service will be convenient and secure, “offering superior security and privacy over a physical wallet” [12]. Identity data will be encrypted and protected, biometric authentication will be implemented, and information will be presented directly between the device and the identity reader. The mobile ID implementation uses the ISO 18013-5 mDL (mobile Driver’s License) standard, which sets “clear guidelines for industry around protecting consumers’ privacy when presenting an ID or driver’s license through a mobile device [13].

Outcomes/Results: Pilot programs have shown that government users and the public are receptive to adopting digital driver’s licenses. These programs require public-private partnerships to collaborate and communicate to effectively apply technology that best benefits the public. Cybersecurity is paramount, as SSI and DID system technology protect users from information theft and gives users more control about exactly what personal information is shared and with whom. Once the full rollout is complete in 2022,
outcomes and results can be better assessed.

**Lessons Learned:**

- Public-private partnerships are needed to implement the best technologies and provide the best cybersecurity for users;
- Digital driver’s licenses must be accepted everywhere that physical licenses are accepted;
- A similar digital solution may be difficult to implement in the United States due to each state operating on a different digital infrastructure for licensing; and
- Users desire control over their identity and personal information, and what information is shared with whom.
Mexican National Digital Strategy (NDS) Digital Birth Certificate Initiative

**Title of Project:** Digital Birth Certificate Initiative under Mexico’s National Digital Strategy

**Primary Organization:** National Digital Strategy Coordination at the Office of the President of Mexico

**Partner Organizations:** President of Mexico, Digital Government Unit of the Ministry of Public Administration, Government agencies of the Federal Public Administration, States and Municipalities, Mexican Congress, civil society & the general public (consultation process), and industry organizations.

**Lead:** The National Digital Strategy Coordination reports directly to the Office of the President and is led by Alejandra Lagunes Soto Ruiz.

**Vision:** Democratize access through digital tools, progress National Digital Strategy to bring digital service delivery processes country-wide.

**Mission:** To digitize birth certificate issuance, making essential identifying documentation available anytime and anywhere. This would provide a service that encompasses a whole of government approach for the user, covering numerous institutions with one interface.

**Challenges:** Physical documents were deeply ingrained with public and private services, providing no other means of establishing identity and without an overarching entity or jurisdiction to coordinate. Additionally, multiple actors with jurisdiction over birth documents created issues. The need to coordinate policies and procedures from all levels of government and a multitude of actors across the technical and policy-making parts of government also contributed to the challenges.

**Goals/Objectives:**

- Democratize access to the identity documents;
- Design a digital service to provide a birth certificate focused on the needs of the citizens;
- Offer excellent service 24 hours a day, 365 days a year;
- Provide the ability to access the service from anywhere in the world with internet access;
- Reduce costs to the citizens and government; and
- Promote interoperability of digital services.

**Solution:** The National Digital Strategy (NDS) is an action plan that the Mexican government is implementing to encourage the adoption and development of information and communication technologies and lift Mexico into the information and knowledge society. The main purpose of the strategy is to achieve a Digital Mexico with the adoption and use of information and communication technology (ICT) to maximize its economic, social, and political impact for the benefit of the quality of life of citizens. The NDS is the result of collaborative efforts, discussions with experts, industry and academics, legislators, civil organizations, and citizens. As a part of the NDS, the Digital Birth Certificate initiative was one of the first major ICAM projects in Latin America [14].
Similar to the US, Mexico is a federal republic, and each of the 32 states have significant power within the federal system. This project required the authority over and ownership of various processes to shift from the state level to a federally centralized solution – the National Birth Certificate Database of the Ministry of Interior [15]. To broker this shift of power, the change leaders proactively engaged the 32 state governors in the process, making them active collaborators rather than potential opponents. Through a cost-benefit analysis, the federal leaders demonstrated the proposal to replace the current state systems with a federal one would save the states money. To assuage governors concerned about their revenue, the federal project owners and state representatives changed the proposed project from a system that would replace the state systems to one that integrated them. This compromise resulted in an interoperable set of systems and services, allowing states to determine the cost of services.

Historically, birth certificates would vary from state to state because of the disparate systems and processes. Creating a single-format birth certificate design was vital to the success of the initiative. This design would need to satisfy state and federal requirements for security while linking the document to numerous additional sources for verification and documentation. Additionally, a significant percentage of the population is without computer or internet access, so the solution needed to accommodate both digital and physical birth certificates. The resulting digital solution eliminated the need for a physical signature, security paper, watermarks, and seals, all of which were used across various legacy state forms. Online validation was widely accessible through various means, including:

- A bar code linked to the National Birth Certificate Database
- An electronic identifier number unique to each discreet copy of the birth certificate
- A QR code that includes the information un-encrypted through the GOB.MX birth certificate portal
- The electronic signature of the Civil Registry

The actual system design also required significant cross-organizational collaboration to meet the needs of the 32 states, each of which had the power to stall the initiative [16]. The goal was to consolidate the numerous processes, resources, and related information to support the birth certificate services into a single online portal. This unified interface would be the one-stop-shop for users to request, pay for, update, correct, and verify their birth certificates. To facilitate these functions, the system had to be integrated with the National Birth Certificate Database, each legacy state database for document management, each state treasury system, and numerous third-party financial services for payment processing. Since only 37 percent of adults in Mexico had an account with a formal financial institution (as of 2017), this also required negotiating agreements with convenience store chains to facilitate local payments to serve those without formal financial services [17]. The project also established and implemented new data standards, security measures, firewall requirements, traceability protocols, and data governance procedures to support interoperability.
The new services were strategically rolled out in phases due to the scale of the initiative. Adoption was facilitated and encouraged through collaboration with local authorities in all 32 states. Extensive testing was required to ensure the various stakeholders were satisfied. Activities included end-to-end user experience (UX) and functionality testing, user testing to refine the intuitive interface, and functional testing of payment services connected to multiple state financial systems, banks, and alternative financial service providers. Legacy paper birth certificates remained valid and because the states still determined the pricing, these services remained available in-person as they were before, in addition to newly being available online. Following the initial implementation, additional functionality was developed to provide a help desk and enable users to record invalid data on non-digitized records.

**Outcomes/Results:** The rollout was fully completed in January 2018 and the national government issued three million birth certificates by the end of the Peña Nieto administration in December 2018.

**Lessons Learned**

- Integration of existing systems and services (state-level payment processes, various payment methods) in combination with new functionality facilitates stakeholder buy-in and supports strong change management;
- Change is not just technical, but also has social/societal components and successful public-facing programs require considering the social context (distrust of unfamiliar financial systems and services); and
- Solutions must continually improve, since most of the practical restrictions for the Digital Birth Certificate program came lack of connectivity with older generations. There will be significant opportunities for development as more of the population is “plugged in”.

**Login.Gov**

**Title of Project:** Login.gov implementation and roll-out

**Organization:** General Services Administration (GSA) in partnership with US Digital Service (USDS)

**Vision:** “Login.Gov is the public’s one account for government. Use one account and password for secure, private access to participating government agencies.”

**Goals/Objectives:** To modernize, simplify, and secure a user’s personally identifiable information, while providing digital access to a myriad of public services.

**Challenge:** Since September 2000, USA.gov has been a hub of information for US citizens and residents to access public services digitally [18]. On USA.gov, users can search through many different agencies, search by service to access resources hosted directly on the site itself, or access redirect links to agency-specific websites. Although USA.gov is a roadmap of resources, most services are accessed via links to agency-specific websites, many of which require unique accounts and credentials.

In a December 2016 Report to Congress, the US Digital Service identified a problem faced by many Americans when accessing public services in an increasingly digital world—citizens are “often met with confusing navigation systems, conflicting visual brands, and inconsistent interaction patterns—all factors that can erode trust in our government’s services.” [19]. With the rise of the digital environment, many agencies had created a siloed online presence resulting in a variety of experiences and platforms, and little to no communication between systems [19]. Users needed individual credentials for each agency system and had to share personally identifiable information repeatedly to access different services, exposing themselves to greater identity risk [20].

**Solution:** Login.gov was proposed as the solution to the disjointed ICAM architecture for the federal services’ customer experience. Revitalizing earlier projects, connect.gov and gov.uk, and drawing upon lessons learned, GSA established the Login.gov initial requirements:

- An elegant user interface, modern infrastructure
- Availability for quick agency integration
- An iterative improvement process
- Adherence to federal privacy guidelines
- The use of multi-factor authentication [19]

Login.gov acts as an identity credential provider enabling partner agencies to continue using their own websites that users are familiar with but leverage Login.gov for access management. A user’s personally identifiable information (PII) is verified at different Identity Assurance Levels (IALs) dependent upon the requirements of the partner agency being accessed and is encrypted by Universally Unique Identifiers (UUIDs). Users with privileged access to user data are regularly audited and permission levels are verified. In
accordance with GSA privacy policies to leverage industry best practices and encourage transparency, GSA constructed Login.gov on an open-source platform. Public forums on the code repository are maintained to promote discussion of the project [21].

GSA partnered with the Department of Homeland Security’s Customs and Border Protection (CBP) main public recruiting page for the Login.gov pilot; with memorandums of understanding (MOU) to incorporate the Social Security Administration, Department of Education, and Railroad Retirement Board by 2018 [20]. In 2018 USAJobs, the federal government’s career recruiting site, integrated with Login.gov as well. USAJobs, like Login.gov, is not a federally-mandated system. Agencies can continue using websites that do not subscribe to the modern experience offered by Login.gov (examples include the Federal Bureau of Investigation (FBI) and Central Intelligence Agency (CIA) recruiting websites, the Department of Education’s Office of Federal Student Aid, and the Department of Veteran Affairs).

GSA continues to improve Login.gov, and in February 2021, GSA announced that it would be partnering with federally funded agencies at state and local levels to expand Login.gov’s usage to a broader audience [22]. In August 2021, GSA released a request for information (RFI) regarding identification document authentication. In this RFI, GSA announced that the agency was looking for a vendor to integrate with Login.gov to address the identity gap made more prominent by the increasingly remote workforce. The intent is to enable comparing user-uploaded images of state and federal identification forms against a database of acceptable sample documents and analyze for fraud. Requirements for the RFI included being able to compare against US Government ID types for American citizens and ID types for non-citizen residents [23]. In October 2021, GSA announced plans to seek additional partnerships with federal agencies to utilize Login.gov, including the Internal Revenue Service (IRS) [24].

Outcomes/Results: Login.gov successfully implemented a uniform ICAM architecture for participating federal agencies. In keeping with the initial requirements of Login.gov, the site continues to undergo iterative development and modifications to ensure it remains relevant and useful to the public.

Lessons Learned:

- Implement a continuous improvement mindset and methodology to keep up with technologies’ evolving ICAM architecture in order to ensure data remains secure;
- Promote transparency within project development to strengthen the agency’s accountability and public trust in the system; and
- Until all federal agencies integrate with Login.gov, the benefit is limited and does not solve the key issue of “confusing navigation systems, conflicting visual brands, and inconsistent interaction patterns”.

American Council for Technology-Industry Advisory Council (ACT-IAC)
3040 Williams Drive, Suite 500, Fairfax, VA 22031
www.actiac.org ● (p) (703) 208.4800 ● (f) (703) 208.4805

Accelerating Government Mission Outcomes Through Collaboration, Leadership and Education 14
USAccess Point Pilot

**Title of Project:** USAccess Point Pilot

**Organization:** General Services Administration (GSA) in partnership with United States Postal Service (USPS)

**Vision:** Utilize existing infrastructure among government agencies to streamline credentialing for federal employees and contracting staff.

**Goals/Objectives:** USAccess Point is a shared service that aims to provide Personal Identity Verification (PIV) credentialing services for federal employees and contractors at established locations throughout the country.

**Challenge:** For personnel onboarding, the federal government largely uses a Personal Identity Verification (PIV) credentialing shared service called USAccess, which serves more than 110 federal agencies [25]. This existing system for federal credentialing requires in-person visits at a USAccess location to collect biometric data to confirm identity before a PIV card could be issued. Amid the COVID-19 pandemic and with new safety regulations, agencies with USAccess offices limited who could use the service, while other sites had to close entirely. Roughly 500 of these locations closed their door, creating an influx of traffic to the sites that remained open [26].

Even before the closing of these 500 locations, employees in certain geographical locations did not have access to a site that was convenient, causing a disruption to their workday when required to obtain or update their credential certifications. The impact of the pandemic exacerbated this issue, with fewer credentialing locations yet with the same amount of personnel onboarding needs.

**Solution:** In response to the need for additional local credentialing centers, GSA and USPS partnered to conduct the USAccess Point pilot in select postal offices. This pilot provides greater access to convenient credentialing services by leveraging seven Washington, DC metro area post offices as USAccess credentialing sites [26].

The pilot was conceived in November 2020 during a USPS-led presentation at a GSA Identity Summit [28]. Following the impressive display of biometric infrastructure already in place at the USPS, GSA and the Office of Management and Budget (OMB) leadership began to consider a potential partnership with USPS.

Most post offices serve as a storefront to obtain a passport from the Department State, in addition to biometric fingerprinting services for the FBI Identity History Summary Checks [27]. In addition, the USPS also uses these technologies to vet their own employees, which amounts to approximately 120,000 screenings annually [28]. USAccess Point was able to leverage this pre-existing biometric infrastructure to enable continued credentialing services for federal employees and contractors during the pandemic. The number of federal employees and contractors credentialed through this pilot program since inception is approximately 5,000 [29].
The pilot not only maintained credentialing services during unprecedented times, but also increased customer satisfaction during the process. The ACT-IAC Associates team had the opportunity to speak with Darlene Gore, Director of ICAM at the Office of the IT Category in the Federal Acquisition Service in GSA, who spoke to the satisfaction employees experienced using the USAccess Point pilot. Gore said that based on surveys released, customer satisfaction came in at 90% favorable of the pilot and services rendered. Gore noted that this is largely in part to the ease of online scheduling of credentialing appointments, as well as the close proximity of postal offices to DC-metro area residents.

Given the success of the USAccess Point pilot to date, GSA and the USPS may continue to work together in credentialing federal employees. Gore believes that this partnership is the future of federal credentialing due to its incredible flexibility, scalability, and sharing of biometric technology among government entities.

Outcomes/Results: New and existing federal employees and contractors were able to experience uninterrupted customer service throughout this ICAM transformation during a global pandemic, with approximately 5,000 federal employees having obtained new or updated credentials from post offices during the initial stages of the USAccess Point pilot.

Lessons Learned:

- Crisis response and management can be catalysts for major digital innovation;
- Federal shared services provide a myriad of benefits to government agencies and the personnel that support their missions; and
- Talent acquisition does not have to be curtailed by geography constraints.
TSA Biometrics Roadmap – For Aviation Security & the Passenger Experience

Title of Project: TSA Biometrics Roadmap

Organization: Transportation Security Administration (TSA)

Mission: “To protect the nation’s transportation systems to ensure freedom of movement for people and commerce.”

Vision: “To improve security, safeguard the Nation’s transportation system, and accelerate the speed of action through smart investments and collaborative partnerships.” [30].

Lead: Mr. David P. Pekoske is the Administrator for the Transportation Security Administration. The TSA progressed through partnerships, innovation, and the development of a dedicated workforce under his lead.

Challenge: The increasing volume of air travelers has challenged airlines and airports, both domestic and international. Security regulators, like TSA, must also keep up with facilitating screening procedures. In addition, personnel staffing for security screening is stagnating or declining. If unaddressed, rising travel volume combined with operational constraints will result in longer wait times and more missed flights.

Goals/Objectives: Identity verification is crucial in the commercial aviation sector. Satisfying the demands of rising air traveler volume, resource constraints, and operational capacity will require TSA and international aviation regulators to automate manual and paper-based identity verification processes through modernization investments.

Solution: To reach its objectives, TSA will leverage biometric technologies through modernization investments for identity verification [31]. Improved security, operational efficiency, and positive passenger experience are the expected outcomes after the investments are made and fully implemented.

TSA must efficiently screen individuals seeking to board aircraft to fulfill its mission. Air travelers are often identified through analyzing biographic data and examining physical identifications and travel documents. Physical facial recognition has long been TSA’s method when conducting these screenings [32]. Currently, Transportation Security Officers and airline employees perform a visual comparison between a passenger and their respective identification card or passport. To enhance the process, facial recognition technology will be used. Facial recognition capabilities can be automated to improve the performance and security of TSA procedures by increasing the assurance of a traveler’s identity beyond what travel documents alone can provide. For example, the use of fraudulent or doctored credentials can be reduced by being less reliant on physical IDs at security checkpoints [33].

Biometric devices provide several benefits: systems can be efficacious, self-serving, and include anti-tampering features [34]. This enables TSA and aviation security partners to lessen dependence on the manual inspection processes. The availability of high-performance and commercially available camera systems further highlights the benefits of facial recognition.
Imagery contained in Federal and State identity documentation may already be suitable for recognition ability [33]. The standards for physical facial image authentication continue to develop, as different formats are widely adopted and used for verification per International Civil Aviation Organization Doc 9303. The TSA abides by the requirements of the FAA Reauthorization Act of 2018 when implementing the biometrics strategy. This also includes consultation with the Commissioner of Customs and Border Protection (CBP) and requires creating and presenting a report to the relevant Congressional committees.

Privacy is and will be of utmost importance to the TSA. The biometric solution’s design will be centered on confidentiality through the planning, configuration, and implementation stages of the project. Protecting privacy will involve restrictions that ensure user data will only be used for purposes pertaining to transportation security or for purposes set forth by law, with the consent of individual travelers. All modernization solutions will adhere to robust cybersecurity protocols. Capabilities must also follow current and changing security guidelines set by the Department of Homeland Security (DHS) and TSA, as well as cybersecurity industry best practices. It is crucial that all solutions secure data, both resting and moving, to protect both travelers and the integrity of the infrastructure.

**Outcomes/Results:** Biometric facial recognition implementations are currently ongoing. With input from the Office of Biometrics and Identity Management (OBIM), TSA, and CBP efforts implementing pilot projects at checkpoints that automate the Travel Document Checker (TDC) process provide insights into best practices and lessons learned. Emphasis is placed on developing pilot programs at airports where appropriate stakeholders have committed to making their own investment in modernization to streamline the passenger experience. Travelers are notified of pilot project activities and can opt-in to various biometric procedures. TSA and CBP continue to analyze biometric technology pilot results and refine approaches for future efforts.

More pilot programs by TSA are scheduled to begin in early 2022 [35]. Specifically, travel credential images such as what is found on passports, will be verified with live image captures. Travelers will be able to scan their credentials and the device will verify the authentication with biometric identity matching. The process decreases interaction with TSA officers, allowing the officers to focus efforts on higher priority tasks. Travelers who opt-in will ultimately experience a faster check-in and TSA/airport security operations will become more efficient [36].

**Lessons Learned:**

- Modernization will always be an ongoing effort for the TSA and streamlining the passenger experience is the first of what is to come;
- Pilot programs will continue to help decision-makers determine the best course of action for future implementations to meet evolving challenges and business needs; and
- Upgraded infrastructure can be used to secure data to protect both travelers and airline staff.
Lessons Learned

Through the analysis of the ICAM case studies presented in this paper, the project team derived four overarching lessons learned:

Lesson 1: Safeguarding User Data

Privacy of user data builds trust and adoption of new services

A focal point to ICAM is safeguarding user information, particularly personally identifiable information. As agencies take steps to advance their digital footprint, it is imperative that they advance IT security in tandem. Confidence and assurance in any system are important to its overall acceptance and longevity. In each of the case studies, safeguarding of user data was deservedly emphasized.

The South Korean Digital Driver’s License project deployed a blockchain-based service with Self-Sovereign Identity (SSI) and Decentralized Identity (DID) system technology, which increased resilience to losing sensitive personal information in the event of a cyber-attack. The use of DIDs, an integral component of SSI, allowed for cutting out intermediaries such as mobile network operators, email providers, and third-party companies, to connect users to services. South Korea gave digital driver’s license users control over exactly what personal information is shared and with whom.

When implementing the Mexican Digital Birth Certificate program, it was found that transferring the regulation of a system from disparate states to a single, federally regulated system presented the need to establish and implement new data standards, security measures, firewall requirements, traceability protocols, and data governance procedures.

Login.gov provides a singular database of PII for users accessing multiple federal agencies, which created a significant risk to user data. The system utilizes different Identity Assurance Levels (IALs) dependent upon the requirements of the partner agencies being accessed and encrypts user data by Universally Unique Identifiers (UUIDs). Permission levels for users with privileged access are also regularly audited.

The USAccess Point pilot was able to leverage pre-existing biometric infrastructure already in use by the FBI (for conducting background investigations) and the Department of State (for passport issuance) to expand access to credentialing services to federal employees and contractors during the pandemic.

TSA Biometric Advances are being implemented that ensure user data will only be used for purposes pertaining to transportation security or as set forth by law with the consent of individual travelers. DHS and TSA also prescribe robust cybersecurity protocols and security guidelines that biometrics advances will adhere to.

Lesson 2: Pilot Programs for Incremental Implementation

Incremental implementation through Pilot Programs allows for flexibility during development

Incremental implementation of ICAM technology with pilot programs helps determine the best course of
action for improvement and refinements before a full, public solution is implemented.

With the **South Korean Digital Driver’s license’s** project, two pilot programs were implemented as part of the Korean “Digital New Deal.” The first, a mobile ID card for civil servants at central government organizations, allowed a small, focused user group to use their smartphones for identification and authentication for government administrative operations. This allowed for a trial run of OmniOne, the blockchain-based security platform. As a proof-of-concept, the successes of the trials for civil servants will enable the government to expand cooperation with smartphone carriers and makers, and with cybersecurity institutions to further improve the quality and safety of mobile ID cards. The second program was making the digital driver’s license publicly available on the PASS mobile application. The application’s license saw moderate success, with millions of adopters within the first few months. However, there were limitations on where the license was accepted that hampered further adoption. These two programs illustrated how the government must work cooperatively with mobile carriers and other institutions to ensure cybersecurity for all users, and that digital driver’s licenses are accepted everywhere physical licenses are currently accepted.

In their biometrics program for civilian air travelers, the **TSA Biometric Advances** initiative also relied on pilot programs to iron out problems and ensure a refined, complete solution would be presented to the public. TSA and Customs and Border Protection (CBP) are implementing pilot programs at select checkpoints to test out the automation of the biometrics program to glean insights into best practices. Travelers at these checkpoints are notified of the pilot program activity and can opt-in or -out of the various biometric procedures. Lessons learned from these programs will refine approaches for future programs before a complete program is rolled out at all checkpoints. More pilot programs are already planned for identity verification and authentication based on biometric identity matching.

**Login.gov** partnered with CBP to launch a Login.gov pilot on their main public recruiting page. Based on successes and lessons learned from this pilot, the solution was then expanded to the Social Security Administration, Department of Education, and Railroad Retirement Board. Further, USAJobs, the largest US government job site, was integrated with Login.gov due to its successes in 2018. GSA continues to refine and improve the site based on lessons learned from their rollout of the platform. In late 2021, GSA released an RFI for further adoption, and has announced plans to seek additional partnerships with more federal agencies to utilize the Login.gov site.

Lastly, the **Mexican Digital Birth Certificate** program recognized the need for gradual implementation and continual improvement for their digital birth certificate initiative. Testing was required to appease diverse stakeholders, and gradual adoption was facilitated through collaboration with local authorities in Mexico’s 32 states. Based on lessons learned from the initial rollout, additional functionality was developed, including providing a help desk.
Lesson 3: Continual Improvement

Modernization is a continual effort, requiring ongoing improvement

This theme was evident throughout the included case studies and applies to IT management and modernization practices beyond those related to ICAM. To maintain data privacy and system security, governments need to continually improve to defend their systems and contents from threats as the technology available to malicious actors evolves rapidly. Similarly, the needs of the citizens and other users are constantly changing and governments need to continually enhance these solutions to support those changes.

As seen with the South Korean Digital Driver’s License project, the South Korean solution depends on smartphones, third-party applications, and the security of blockchain technology. As the mobile ID card service developed from a narrow identity authentication service in 2018 to a fully digital agency-specific ID in 2021, the South Korean government continues to expand the digital service to a fully-digital driver’s license service to be rolled out in 2022. This continual improvement is vital to providing and maintaining an essential service for the South Korean people.

In a similar instance, the Mexican Digital Birth Certificate program demonstrates continual improvement from the very start of the initiative. The initial proposal underwent many iterations of changes to be useful to the intended audience in a way that would not compromise their personal data. As access to and trust in digital platforms and financial institutions grows in Mexico, the Digital Birth Certificate service will need to evolve to accommodate those changes as it did at the start.

The TSA Biometric Advances illustrates external changes in air traveler volumes and the availability of biometric technology driving opportunities to improve the security and passenger experience in support of the TSA mission. Just as these external changes provided opportunities, others will continue to drive development out of necessity, such as cybersecurity protocols, agency guidelines, federal regulations, and malicious threats.

Login.gov continues to expand and improve its services through partnerships with federally funded agencies, and at state and local levels to expand Login.gov’s usage to a broader audience. These improvements support the GSA and USDS in their missions to support the US Government in providing efficient and effective government for the American people.

Finally, GSA and USPS leverage physical locations as well as various digital platforms from across the government in supporting USAccess Point. GSA will need to continually improve the solution to maintain and expand the personal identity verification credentialing services in support of its agency mission.

Lesson 4: Increased Infrastructure Capability

Enhancing the user experience through infrastructure capability

As IT modernization frequently results in the transition from decades-old legacy systems to the cloud, the
primary focus of ICAM transformation is enhancing the user experience.

Other benefits from ICAM transformations, however, are evident. For example, increased infrastructure capabilities associated with ICAM modernization efforts should be acknowledged. Agencies, stakeholders, and all relevant parties must assess future upgrades made to existing infrastructure during all phases of IT implementations, from planning to execution. Doing so enables operations, data, and regulatory requirements to be satisfied.

Insights from the foreign and domestic case studies include:

The **South Korean Digital Driver’s License** project leveraged blockchain technology to mitigate security concerns. The application’s use of blockchain also gave users more control of their identity and personal information. Physical IDs carry different risks compared to digital IDs, as they can be lost, stolen, or used fraudulently. The use of blockchain on improved IT infrastructure allows for users’ identities and information to be stored on their personal devices instead of a central server, further minimizing potential cyber threats.

The **Mexican Digital Birth Certificate** program established and implemented new data standards, security measures, firewall requirements, traceability protocols, and data governance procedures to support interoperability. This allowed them to effectively assess the capability of the new IT infrastructure that would be needed to support their main objective of democratizing access to identity documentation for user convenience.

The **TSA Biometric Advances** initiative used biometric facial recognition technology to reach its ICAM objective of enhanced customer experience. The machines themselves, however, present several benefits: systems can be efficacious, self-serving, and include anti-tampering features. Also, the improved IT infrastructure supporting those machines has capabilities that follow current and changing security guidelines set by DHS and TSA. Upgraded infrastructure can be used to secure data to protect both travelers and airlines.

**Login.gov and USAccess Point** recognized the value of integration. Multi-factor authentication was a key strategy used to promote an integrated architecture. This allowed for support permissions, verifications, audits, and other features of a central ICAM architecture for Login.gov. GSA also expanded credentialing capabilities with the help of existing biometric infrastructure through teaming with the USPS for the USAccess Point Pilot program.
Authors & Affiliations

This report was written by participants of the 2021 ACT-IAC Associates Program with oversight from the IT Management and Modernization Community of Interest. The organizational affiliations of these contributors are included for information purposes only. The views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development.

Authors and Contributors:
Virginia Mattingly, ECS Technologies
Jordan Psaltakis, Booz Allen Hamilton, LLC
Mary O’Connor, Agile Defense, LLC
Kyle Carrick, U.S. General Services Administration
Omid Mahban, CGI Federal

Government Sponsor: Daniel W. York, General Services Administration
ACT-IAC Associates Coach: Sheena Burrell, National Archives and Records Administration
References

1. https://english.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&n
   ttSeqNo=443&searchOpt=&searchTxt=
2. https://medium.com/raonsecure/raonsecure-to-develop-the-korean-digital-drivers-license-
   9269aacc74e0
3. https://www.korea.net/NewsFocus/policies/view?articleId=201851
    safety-usingomnione-did-f0a53e9e27e8
11. https://www.cnet.com/tech/mobile/you-can-add-your-drivers-license-or-state-id-to-apple-wallet-in-ios-
    15-heres-how/
    and-state-ids-in-wallet/
    Retrieved from: https://www.eluniversal.com.mx/nacion/sociedad/se-desata-boom-de-actas-de-
    nacimiento-en-linea.
15. Rodríguez Álvarez, Alberto (2020). Digital Innovation in Latin America: Mexico’s Online Birth Certificate,
    Beeck Center for Social Impact + Innovation, Georgetown University, Washington, D.C. Retrieved from:
    https://www.state.gov/countries-areas/mexico/.
    https://documents1.worldbank.org/curated/en/893791553110483160/pdf/Concept-Program-
    American Council for Technology-Industry Advisory Council (ACT-IAC)
    3040 Williams Drive, Suite 500, Fairfax, VA 22031
    www.actiac.org ● (p) (703) 208.4800 ● (f) (703) 208.4805

Accelerating Government Mission Outcomes Through Collaboration, Leadership and Education 24

18. https://www.usa.gov/history-of-website
23. https://sam.gov/opp/5cf3aba333904749a13a056b47d1c5c4/view
27. https://about.usps.com/what/government-services/
29. Darlene Gore, Director of ICAM at the Office of the IT Category in the Federal Acquisition Service at GSA: Interview
34. https://www.gensler.com/blog/biometrics-in-aviation