

## Federated Identity Management: Lower Risk, Improve Security, Streamline Airport Operations

For years, airports have managed identity access and control for secured areas by conducting intensive identity proofing and issuing credentials of their own – an expensive and time consuming process. This silo-based approach may appear to be an effective way to achieve identity assurance, but in reality, much of this effort is redundant as it doesn't leverage the work done by others toward the same goal – a strong ID to enable access that has high assurance of integrity.

There is a better way. Interoperable credentials that take advantage of federal standards may benefit airport operators both in terms of cost of operations and the security of facilities. Born from the 9-11 attacks and the clear need for cooperative efforts across jurisdictions, standards have been defined and are in production for reliable identity credentials that can be used locally as appropriate.

The Federal Information Processing Standard 201 Federal Information Processing Standards **(FIPS) 201** Personal Identity Verification **(PIV)** for Federal Employees and Contractors is recognized as the gold standard for issuing identity credentials. These credentials serve as the authentication mechanism in federated identity management models within the Federal Government. FIPS 201 provides a secure chain of trust between the identity proofing and issuance of a strong identity credential that is secure, interoperable and operationally useful.

With these credentials, airport officials have a substantially easier time of verifying the identity of anyone purporting to be from a community of interest – local police, fire and rescue; flight crews; concession staff or construction teams. From there, access decisions can be made more quickly – and with greater assurance – as the information behind them is truly the best available, it is directly from the source.

By adopting CertiPath compliant credentials and standards, you can recognize any FIPS 201 or PIV Interoperable (PIV-I) credential. After completing local suitability and trustworthiness checks, and making the access decision (either in a role based mode or explicit authorization mode), these credentials provide integrity and interoperability -- significantly reducing the time and overhead required for making access control decisions, while deploying state of the art capabilities for physical and logical access control.

The result is an opportunity to significantly reduce the risks and improve security through consistent identity proofing and credentialing.

### Leveraging CertiPath's solution for federated ID management, airport officials can

- Reduce the time and resources needed for comprehensive identity proofing
- Shift the liability for identity proofing and credentialing to partners using an accredited process guided by FIPS 201
- Not issue a local badge, depending on access control policies
- Locally revoke access in a timely manner

## CertiPath Solves the Federated Identity Management Challenge for Airports

### Meet Tomorrow's Access Control Challenge, Today

CertiPath meets or exceeds medium-hardware assurance – the highest a commercial organization can be recognized by the U.S. Federal Government, the United Kingdom, Netherlands and French governments, and in particular, the respective aviation and defense agencies. The CertiPath Bridge itself operates at the “high” assurance level.

While many airport workers might not have a requirement for credential interoperability, there are benefits for adoption at every airport.

Today, the largest drivers of evolving requirements are the aircrafts themselves; meeting those requirements ultimately delivers broader and more robust identity management solutions for both today and tomorrow.

- Airport airframe maintenance workers must sign for every action they take on a particular aircraft in the maintenance log of that aircraft. This manual process is being updated to an automated process by Boeing and Airbus. Both of these manufacturers require use of CertiPath-certified PKI for this new automated process. An airport issued credential that is CertiPath compliant can then be used by that worker for:
  - Physical access to the security identification display areas (SIDAs) housing the aircraft
  - Logical access to the updates of software downloads for maintenance of the aircraft
  - Signature on certified logs on actions taken for a particular aircraft
- The newest planes in the Boeing and Airbus fleets will leverage CertiPath-certified PKI for interaction with gate landing systems, called GateLink. This is a growing trend for identification and access control. It extends beyond traditional PACS for controlled areas while maintaining interoperability with local PACS solutions for SIDA and secured access. An airport issued credential that is CertiPath compliant can then be used by gate agents and ramp workers for:
  - Coordination of maintenance requirements
  - Baggage handling procedures
  - Gate management procedures

CertiPath credentials are interoperable with those being deployed for GateLink applications by the ATA and ultimately, airports will need to credential gates leveraging CertiPath-compliant credentials.

### Identity Management that Gets the Job Done

CertiPath PKI (public key infrastructure)-based credentials combine software, encryption technologies and services to establish trusted “identities.” It offers a flexible model, allowing for the procurement of trustworthy credentials from certified service providers. Larger organizations with an in-house identity management capability can become CertiPath-certified, meeting the interoperability objectives.

It's a simple, efficient and extremely reliable approach to identity management that eliminates redundancy, reduces the risks associated with lost or stolen passwords and ensures that employees have been vetted by the most rigorous processes and – based on the “trust” established by that process – are authorized to do the work they've been employed to do.

***For more information on how you can use CertiPath credentials to reduce costs, streamline operations and improve security, please contact Alison Kidd at [alison.kidd@certipath.com](mailto:alison.kidd@certipath.com) or (703) 793-7871.***