Airside DRAIC - Digital Restricted Area Identity Certificate

Smarter, faster, safer access control.

Introduction

The **Digital Restricted Area Identity Certificate (DRAIC)** represents the next generation of secure access management in Canadian airports, advancing beyond the traditional **Restricted Area Identity Card (RAIC)**.

While the RAIC has been a cornerstone of airport security, providing physical badges for authorized personnel, the DRAIC leverages cutting-edge digital technology to transform how access to restricted areas is managed and enforced.

By moving away from the limitations of a physical card, the DRAIC introduces a secure, digital-first approach, seamlessly integrated with mobile devices and existing airport security systems.

The term "Certificate" in DRAIC reflects its modern identity as a verified, digital credential rather than a tangible card. Like traditional RAICs, the DRAIC ensures that only authorized personnel can access restricted airport zones. However, it enhances functionality by combining biometric authentication, encrypted storage, and real-time geofencing to deliver unparalleled security and convenience.

This evolution aligns with the growing demand for flexible, efficient, and secure access solutions, paving the way for a fully digitized airport ecosystem while maintaining compliance with Transport Canada's stringent aviation security standards.

By embracing the DRAIC, airports and stakeholders can benefit from streamlined badge issuance, dynamic access control, and improved situational awareness, all without the logistical challenges associated with physical cards. It is not just an update to the RAIC—it is a significant leap forward in aviation security, meeting the demands of a digital future while safeguarding the integrity of Canada's air transport system.

Table of Contents

Introduction **1**
Enhanced Workflows **4**
1. Digital Badge Request and Application **4**
2. Badge Processing **4**
3. Digital Badge Issuance **5**
4. Operational Integration **5**
5. Compliance and Security **5**
6. Training and Support **5**
The Stakeholders **7**
1. Airside Operations Manager 7
2. Subcontractor Supervisor 7
3. Ground Air Traffic Controllers 8
4. Snow Removal Operators 8
5. Airport IT and Security Teams 9
6. Airport General Manager 10
7. Airline Operations Manager (External) 10
8. Ground Handling Subcontractor Operations Manager (External) 11
11. Transport Canada (External) 12
Steps to Develop a TC Compliant DRAIC **13**
1. Understand Regulatory Requirements 13
2. Security Framework 13
3. Access Control Integration 14
4. Data Privacy and Storage 14
5. User Experience 14
6. Testing and Validation 15
7. Operational Considerations 15
8. Potential Challenges 16
Conclusion **16**

Enhanced Workflows

The **Digital Restricted Area Identity Certificate (DRAIC)** is designed to modernize and enhance airport access management by leveraging advanced digital technologies.

The system transitions from traditional physical cards to a secure, efficient, and user-friendly digital platform.

Each stage ensures that the DRAIC delivers unparalleled security, functionality, and user convenience while adhering to regulatory standards.

This section outlines the core operational elements of the DRAIC implementation, from request and processing to operational integration, compliance, training, and continuous improvement.

1. Digital Badge Request and Application

Streamlining the application process is critical to improving efficiency and user satisfaction. This stage enables authorized personnel to request their digital badges through a seamless and secure platform.

- **Integration with Identity Management** Implement robust authentication mechanisms, such as SSO frameworks, for personnel verification and seamless user experience.
- **User Interface** Add a dedicated feature in the app where employees or contractors can request digital badges.
- **Document Upload** Enable users to upload necessary documentation, such as security clearance and photo identification, directly through the app.
- **Approval Workflow** Automate the badge approval process by integrating with HR and regulatory systems to ensure compliance.

2. Badge Processing

Processing digital badge applications efficiently requires secure and role-based systems to verify identity and define access permissions.

- **Real-Time Verification** Utilize secure document verification tools to speed up the processing of applications.
- **Role-Based Access Control (RBAC)** Implementing access level assignments based on specific roles to restrict access and ensure alignment with security protocols.

3. Digital Badge Issuance

Issuing digital badges involves delivering secure, functional credentials that integrate seamlessly with airport operations.

- **Integration with the Existing Platform** Leverage geofencing and real-time tracking capabilities to enable secure and location-aware digital badge issuance.
- **Mobile Integration** Deliver the digital badge to the Airside app, accessible as a scannable QR code or NFC-enabled credential for physical and digital access.
- **Offline Access** Ensure the badge can function offline through encrypted, locally stored credentials for seamless operations in restricted network environments.

4. Operational Integration

Seamless integration with existing systems enhances operational efficiency and security.

- **Vehicle and Zone Monitoring** Integrate badge data with existing vehicle tracking systems to control access to restricted areas.
- **Alerts for Unauthorized Access** Implement real-time notifications for security and operations teams to address unauthorized badge use.

5. Compliance and Security

Compliance and security are central to ensuring the DRAIC meets legal, operational, and user trust requirements.

- **Encryption** Secure data with advanced encryption methods, such as AES-256 for data at rest and TLS 1.3 for data in transit.
- **Data Retention** Store badge-related data in accordance with relevant legal and operational retention policies.

6. Training and Support

Effective training and robust support systems are essential for smooth deployment and user adoption.

- **User Training** Offer comprehensive training sessions for users and administrators to familiarize them with the digital badge system during rollout.
- **Help Desk Integration** Extend existing support and ticketing systems to handle badge-related issues, ensuring 24/7 availability.

7. Iterative Feedback and Updates

Continuous improvement ensures the system evolves to meet user needs and operational demands.

- **Pilot Deployment** Start with a limited deployment to test the functionality and identify potential improvements.
- **Feedback Loops** Establish mechanisms for collecting user feedback to refine and optimize the system iteratively.

8. Integrated Digital KYC (Know Your Customer)

A fully integrated Digital KYC ensures timely, efficient, error free and fully secure identity verification, meeting regulatory standards while enhancing user experience.

- **Identity Verification**: Leverages advanced AI-driven KYC systems to authenticate user identities by cross-referencing uploaded documentation with official databases, ensuring fast and accurate validation.

- **Biometric Matching**: Incorporates 3D facial recognition matching to confirm the applicant's identity against submitted credentials, adding an additional layer of security.

- **Fraud Detection**: Leverages real-time fraud detection algorithms to identify and flag discrepancies or suspicious activity during the verification process.

- **Regulatory Compliance**: Ensures the KYC process complies with all Transport Canada security standards and privacy laws, streamlining the onboarding process while maintaining legal adherence.

9. Instant Revocation Capability

The digital nature of DRAIC enables real-time revocation of access rights without the logistical challenges of retrieving physical cards.

- **Real-Time Deactivation**: Instantly revoke access to restricted areas through centralized system controls, ensuring immediate compliance with security protocols.

- **Elimination of Retrieval Hassles**: Removes the need to physically recover badges, reducing administrative burdens and risks associated with lost or misplaced cards.

- **Automated Notifications**: Notify security teams and the affected user immediately upon revocation, providing clarity and preventing unauthorized access attempts.

- **Enhanced Security Response**: Integrate revocation with alert systems to flag deactivated credentials if any unauthorized use is attempted post-revocation.

The Stakeholders

This expanded approach addresses the needs of both internal and external stakeholders, ensuring a holistic solution that improves safety, efficiency, and compliance across all levels of airport operations.

1. Airside Operations Manager

Description

Oversees all ground operations at the airport, ensuring compliance with safety, operational, and regulatory standards.

Pains

- Limited visibility into personnel access and movements in restricted areas.
- Manual processes for badge issuance and monitoring create inefficiencies.
- Risk of unauthorized access or non-compliance with regulatory requirements.

Gains

- Real-time tracking of personnel movements within secure zones.
- Streamlined badge management process reducing administrative overhead.
- Increased compliance with safety and regulatory standards.

Pain Relievers

- Automated badge issuance and role-based access control.
- Real-time alerts for unauthorized access attempts.
- Integration with monitoring systems to provide situational awareness.

2. Subcontractor Supervisor

Description

Manages subcontracted snow removal and maintenance crews working within airport grounds.

Pains

- Lack of visibility into subcontractor activities and hours worked.
- Difficulty validating subcontractor invoices due to limited operational data.
- High stress during snow events with insufficient tools for real-time coordination.

Gains

- Real-time visibility into the location and activities of subcontractor personnel.
- Tools to validate invoices against actual hours worked and tasks completed.
- Better coordination of crews, improving operational efficiency.

Pain Relievers

- Integration with subcontractor management systems for real-time tracking.
- Automated reporting and invoice validation tools.
- Navigation assistance and real-time updates for efficient deployment.

3. Ground Air Traffic Controllers

Description

Ensures safe and efficient ground movements, including vehicles and personnel, within restricted airport zones.

Pains

- High risk of runway incursions due to unauthorized personnel or vehicle movements.
- Limited tools to monitor non-airport personnel in real time.
- Difficulty responding quickly to dynamic conditions, such as snowstorms.

Gains

- Enhanced situational awareness with real-time visibility of all personnel and vehicles.
- Alerts for unauthorized access or potential safety hazards.
- Tools for proactive incident management and resolution.

Pain Relievers

- Integration of digital badges with geofencing and tracking systems.
- Real-time push notifications for unauthorized movements.
- Centralized dashboard for comprehensive situational awareness.

4. Snow Removal Operators

Description

Operates snow-clearing vehicles and equipment in restricted zones during adverse weather events.

Pains

- Stress and confusion navigating high-risk areas, especially during low visibility.
- Lack of tools for real-time coordination with other vehicles and supervisors.
- Risk of accidental incursions into restricted zones.

Gains

- Clear navigation guidance within secure zones, reducing stress and errors.
- Real-time visibility of other vehicles and equipment to avoid collisions.
- Alerts and notifications to ensure safety and compliance.

Pain Relievers

- Mobile app with real-time navigation and geofencing alerts.
- Visibility into nearby vehicles and equipment.
- Simple, intuitive tools for tracking tasks and updating status.

5. Airport IT and Security Teams

Description

Responsible for the implementation, monitoring, and security of all airport IT systems, including access control.

Pains

- Complexity in managing access rights for diverse groups, including subcontractors.
- Risk of data breaches or non-compliance with security regulations.
- Challenges in integrating new systems with existing IT infrastructure.

Gains

- Simplified management of access rights through role-based controls.
- Enhanced security with real-time tracking and auditing capabilities.
- Seamless integration of digital ID features into existing systems.

Pain Relievers

- Centralized access management integrated with SSO and IT security protocols.
- Encryption and compliance with data protection regulations.
- APIs for smooth integration with existing systems and tools.

6. Airport General Manager

Description

Oversees the entire airport's operations, including financial performance, safety, and regulatory compliance.

Pains

- Financial inefficiencies due to overbilling or underutilization of resources.
- Reputation risks associated with security or safety incidents.
- Difficulty ensuring compliance with complex regulations.

Gains

- Cost savings through improved oversight and accountability.
- Enhanced reputation due to improved safety and operational efficiency.
- Clear reporting and data-driven insights for decision-making.

Pain Relievers

- Tools for monitoring subcontractor efficiency and validating expenses.
- Comprehensive safety and compliance tracking.
- Dashboards and analytics for real-time and long-term decision-making.

7. Airline Operations Manager (External)

Description

Responsible for coordinating aircraft turnaround and ensuring operational efficiency at the gate.

Pains

- Delays caused by inefficient snow clearing or restricted area access.
- Limited visibility into ground crew activities during adverse weather conditions.
- Coordination challenges with subcontracted crews and airport personnel.

Gains

- Improved collaboration with airport ground operations.
- Visibility into snow clearing and gate readiness in real-time.
- Enhanced on-time performance through better situational awareness.

Pain Relievers

- Integration of the digital badge system with airline scheduling and resource management tools.
- Notifications for completed snow clearing tasks at gates.

8. Ground Handling Subcontractor Operations Manager (External)

Description

Manages operations such as baggage handling, fueling, and equipment maintenance.

Pains

- Coordination challenges due to restricted access zones.
- Difficulty tracking subcontractor personnel and vehicles in real-time.
- High risk of non-compliance with airport safety protocols.

Gains

- Real-time tracking of subcontractor vehicles and personnel.
- Streamlined access to restricted zones through digital badges.
- Improved compliance with airport safety guidelines.

Pain Relievers

- Digital ID integration with subcontractor tracking systems.
- Geofencing alerts to prevent unauthorized access or non-compliance.

9. Security Operations Manager

Description

Responsible for ensuring the safety and security of all airport operations and personnel.

Pains

- Unauthorized access to secure areas due to ineffective badge management.
- Delays in responding to security incidents or incursions.
- Limited ability to monitor all personnel in real-time.

Gains

- Improved control over access to restricted zones.
- Real-time alerts for unauthorized access attempts.
- Tools to track all personnel and vehicles on secure airport grounds.

Pain Relievers

- Automated alerts for security breaches or suspicious activity.
- Integration with airport-wide monitoring and response systems.

10. CATSA - Canadian Air Transportation Security Authority (External)

Description Oversees security screening and ensures compliance with federal aviation security regulations.

Pains

- Gaps in monitoring personnel movements between secure and non-secure areas.
- Inconsistent enforcement of security protocols at access points.
- Difficulty auditing compliance with airport security standards.

Gains

- Comprehensive audit trails for personnel movements.
- Real-time monitoring of badge usage at access points.
- Enhanced compliance with federal security regulations.

Pain Relievers

- Detailed reporting and analytics for personnel access.
- Integration with existing security screening systems.

11. Transport Canada (External)

Description Regulates and oversees airport security and safety standards.

Pains

- Ensuring consistent compliance across multiple airports with varying systems.
- Limited visibility into individual airport security performance.
- Challenges in auditing and validating adherence to national security protocols.

Gains

- Standardized access control and reporting mechanisms across airports.
- Enhanced ability to audit compliance in real-time.
- Tools to monitor trends and address systemic security gaps.

Pain Relievers

- Uniform implementation of digital badge systems across airports.
- Comprehensive data for national security audits and regulatory oversight.

Steps to Develop a TC Compliant DRAIC

Creating a **DRAIC (Digital Restricted Area Identity Certificate)** as part of a smartphone app is a feasible concept but would require strict adherence to **Transport Canada guidelines** and aviation security regulations.

It would involve leveraging Baseline's advanced security technologies to ensure the same level of protection, identity verification, and functionality as the physical RAIC.

1. Understand Regulatory Requirements

Compliance with the Canadian Aviation Security Regulations (2012)

RAIC must meet or exceed the security standards for physical cards, including tamper-proof and forgery-resistant measures.

Ensure secure storage and handling of personal and biometric data (e.g., fingerprints, iris scans).

Integration with Current Security Systems

The digital RAIC must integrate seamlessly with airport access control systems, which currently support biometric and RFID authentication.

2. Security Framework

Encryption

Use advanced encryption (AES-256) for data stored on the smartphone and during transmission to prevent unauthorized access or tampering.

Biometric Authentication

Require the use of device-native biometrics (e.g., Face ID, fingerprint) to authenticate users before accessing the digital RAIC.

Multi-Factor Authentication (MFA)

Combine app login, device biometrics, and a secondary authentication factor (e.g., a one-time password or push notification).

Device Security

Implement features like device attestation to ensure the app operates only on secure, unmodified devices.

3. Access Control Integration

Role-Based Access Control (RBAC)

Align the digital RAIC's functionality with the user's role, ensuring access is granted only to necessary areas.

Geofencing and Proximity Checks

Integrate geofencing technology to ensure the digital RAIC can only be used within airport premises.

Bluetooth / NFC / QR Code Scan Integration

Replace the physical RFID functionality of current RAICs with Bluetooth or NFC for secure and contactless access.

4. Data Privacy and Storage

Local Secure Storage

Store the digital RAIC credentials securely in the smartphone's secure enclave or a similar hardware-based storage solution.

Minimal Data Retention

Retain only necessary operational data and follow Transport Canada's requirements for data protection and retention policies.

PIPEDA Compliance

Ensure compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) for handling personal and biometric data.

5. User Experience

Offline Access

Allow offline functionality by securely caching access credentials for restricted zones, reducing reliance on internet connectivity.

Lost Device Protocols

Include features to deactivate a digital RAIC remotely if the smartphone is lost or stolen.

Onboarding and Training

Provide user-friendly onboarding with clear instructions on how to use the digital RAIC and comply with security protocols.

6. Testing and Validation

Transport Canada Certification

Submit the digital RAIC system for certification to ensure compliance with national aviation security standards.

Penetration Testing

Conduct thorough penetration testing to identify and address vulnerabilities.

Operational Field Trials

Test the digital RAIC in live airport environments to ensure functionality, reliability, and ease of use.

7. Operational Considerations

Fallback Systems

Maintain physical RAICs as a backup in case of technical failures or user access issues.

Real-Time Monitoring

Implement real-time monitoring for unusual or unauthorized access attempts, integrated with airport security operations.

Scalability

Ensure the digital RAIC solution can scale to support all airport personnel, subcontractors, and relevant stakeholders.

8. Potential Challenges

Resistance to Change

Personnel and regulatory bodies may be hesitant to replace physical RAICs without extensive testing and proven reliability.

Technology Adoption

Airports would need to update their access control infrastructure to support smartphone-based RAICs.

Data Breaches and Security Risks

Stringent measures must be in place to prevent hacking or unauthorized data access.

Conclusion

The **Digital Restricted Area Identity Certificate (DRAIC)** represents a transformative evolution in secure access management for airports, addressing long-standing challenges with modern, digital-first solutions.

By replacing traditional physical cards with advanced digital credentials, DRAIC enhances security, operational efficiency, and regulatory compliance while delivering unmatched convenience for airport personnel, subcontractors, and external stakeholders. Its seamless integration with existing systems, real-time monitoring capabilities, and instant revocation features set a new standard for access control in the aviation sector.

Collaborating with Baseline and Equans in the implementation of DRAIC offers the **Winnipeg Airport Authority (WAA)** a unique opportunity to pioneer a cutting-edge solution that aligns with the highest global security and operational standards.

Baseline's proven track record in delivering innovative airport management systems, coupled with Equans' expertise in large-scale system integration, ensures a robust and scalable deployment tailored to meet the demands of any airport environment. WACC's participation would underscore its commitment to advancing aviation security and efficiency, positioning it as a leader in modern access control solutions.

By participating in this initiative, WACC can contribute to shaping a globally replicable model for secure airport operations. DRAIC's integration of automated KYC, real-time revocation capabilities, and compliance with Transport Canada's stringent guidelines demonstrates its potential to redefine how airports approach restricted area access. Together, WACC, Baseline, and Equans can drive forward this groundbreaking project, delivering an operational solution that ensures safety, accountability, and future-proofing for the aviation industry worldwide. Let's join forces to lead this transformative journey in airport security innovation.