



Airside is dedicated to ensuring your privacy and we want you to be familiar with how we collect, use, and disclose personal information. We engaged independent data privacy risk management provider TrustArc™ to review and document the data flows and practices described in this datasheet.

The purpose of this document is to provide users of the Mobile Passport App with the information needed to assess the impact of Mobile Passport on their overall privacy posture by detailing how personal information may be collected, processed, and stored.

1.0 Product Summary

The Mobile Passport application enables U.S. and Canadian passport holders to submit passport information and answers regarding travel entry to U.S. Customs and Border Protection (CBP) on a mobile device, then access designated Mobile Passport Control lanes upon arrival in the United States. Mobile Passport Control lanes are operated by CBP in the U.S. Federal Inspection Services (FIS) area.

Mobile Passport was designed to reduce the associated administrative and operating functions carried out by CBP, increase the quality of inspections, streamline the traveler's inspection process, and shorten overall entry wait times (as compared to traditional primary processing).

The app can be downloaded for free from the Apple App Store and Google Play Store and used immediately; use of the app does not require a background check, interview, or pre-approval. Users may opt to purchase an in-app upgrade to an annual or monthly Mobile Passport *plus* subscription.

2.0 Information Collected and Processed

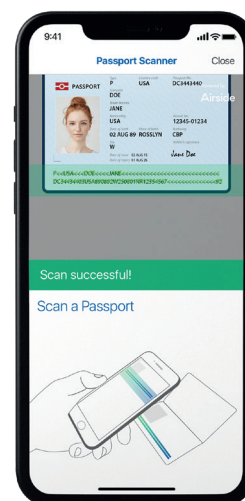
The Mobile Passport App is a mobile automation program; the data collected on the app is the same data collected on Automated Passport Control (APC) program kiosks operated by CBP. The kinds of data collected are: (1) photograph (i.e. selfie); (2) valid U.S. or Canadian passport information; and (3) answers to questions verifying biographic and flight information. Only passport information and answers to questions verifying biographic and flight information are transmitted to CBP.

The Mobile Passport App enables group submissions of passport information for people residing at the same address, allowing group answers to questions verifying biographic and flight information.

2.1 Photographs

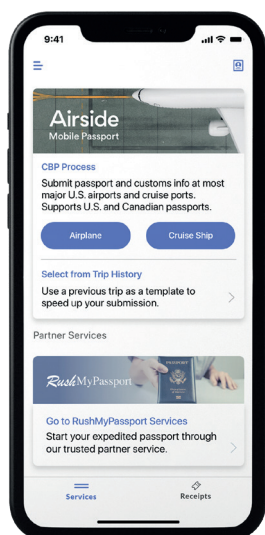
Mobile Passport *plus* subscribers may opt to use the document scanner to add passport information to the app. However, the passport photo will not be collected in the app as it is not included in the passport's MRZ (Machine-Readable Zone) code.

Selfies collected on the app are not included in the transmission to CBP. The selfie of the respective passport holder will be shown on the app adjacent to the QR code receipt, which serves to help the CBP officer visually identify the QR code belonging to each passport holder in a group submission. Mobile Passport *plus* subscribers may opt to save their selfie(s) on their encrypted device.



2.2 Partner Services

Users will find a tile on the home screen of the Mobile Passport App, offering a direct link to RushMyPassport online application services. RushMyPassport is provided by Expedited Travel and facilitates online application services for new or renewed U.S. passports with the U.S. Department of State.



The RushMyPassport application process does not take place within the Mobile Passport App. Users of the Mobile Passport App may select the link on the home screen of the app to RushMyPassport online services, wherein they will leave the app to start an online application.

Mobile Passport *plus* subscribers who have opted to save their U.S. passport on the app will receive an in-app notification when their passport is within six months of the expiration date. This notification includes a link to leave the app to start an application directly through RushMyPassport online services. No data collected on the Mobile Passport App is shared with RushMyPassport or Expedited Travel.

3.0 Information Retained

Users who choose to submit passport information and answers regarding travel entry to CBP for review on the Mobile Passport App will receive an encrypted Quick Response (QR) code receipt on the app that will expire from the app four (4) hours after submission.

All information collected on the free version of the Mobile Passport App will also expire from the app four (4) hours after submission.

Mobile Passport *plus* subscribers have the option to store their selfie, passport information, and/or history of previous trips on their encrypted device. With Mobile Passport *plus*, data is only retained on the encrypted device for the duration of auto-renewing subscription unless deleted from the app.

CBP has a reporting process, Advanced Passenger Information System (APIS), for travelers entering the United States. Consistent with existing policies for advance passenger information, CBP maintains information in their system; use of the Mobile Passport App means the record will include passport information and answers regarding travel entry to the United States. Any other methods used during entry, such as taking a photo during the interview, are at the discretion of local CBP officials at that particular time and are not related to the Mobile Passport App.

Airside keeps transaction records (which do not contain any personal information) to be used only for audit purposes.

4.0 Access to Data and User Privacy Options

Users of the Mobile Passport App own and control their encrypted data on their device. The Mobile Passport App does not share personal information with third parties (other than CBP) and does not operate a virtual system or central database to store personal information. Users consent to share passport information and answers to the questions prior to transmission to CBP.

At any time, users may delete data from the app or uninstall the app from the device. Uninstalling the Mobile Passport App from the device will automatically delete any saved data.

5.0 Security, Operations and Management

Robust encryption and security technology is embedded in every aspect of the Mobile Passport App, from front-end applications and software development kits (SDKs) to transmissions of highly-protected data.



Users use a 4-digit PIN or TouchID or FaceID to unlock the app. Personal information is collected on the app and transmitted securely to CBP for review.



Airside networks and devices are designed, deployed, and operated in a manner that provides proper levels of protection for data being accessed and transported. Mechanisms are also in place to alert network operators and administrators of possible incidents including denial of service attacks, improper access, virus infections, and malware.

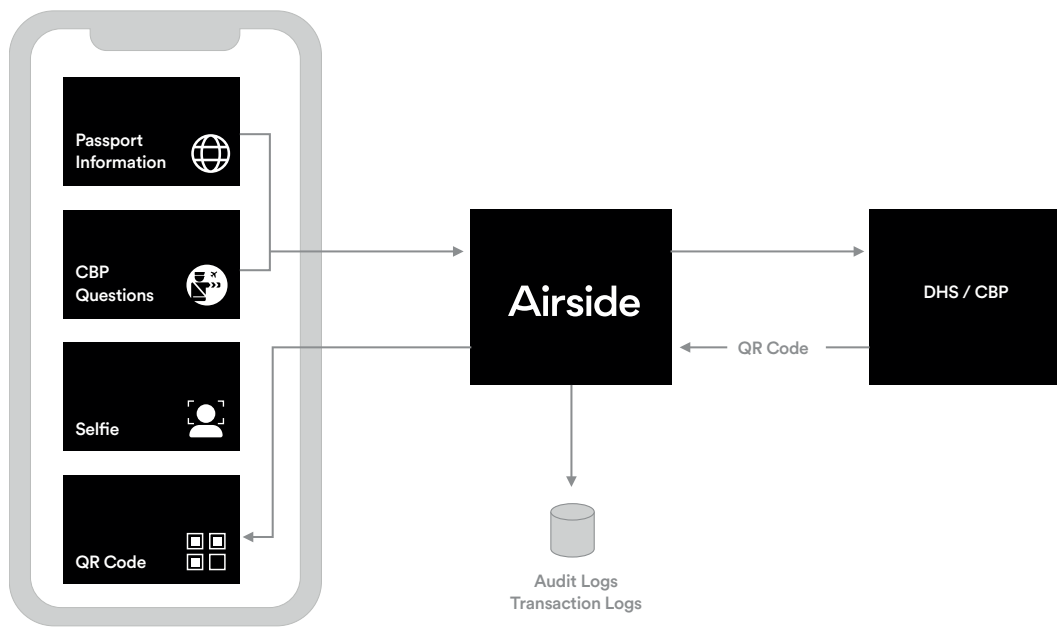


6.0 Software Development and Change Control

Airside's software development life-cycle includes protection testing and validation at each stage, where appropriate. All testing data is anonymized or sanitized to prevent the leakage of customer, company, or client information. Production data is not used during testing.

All change and maintenance processes include testing and validation that security vulnerabilities have not been introduced into the software. This includes checks for malware, back doors, and violation of access rules.

7.0 Dataflow Map



8.0 External Links/Resources

Mobile Passport Website: <https://www.mobilepassport.us/>

Mobile Passport FAQs: <https://www.mobilepassport.us/faq/>

Mobile Passport Privacy Policy: <https://www.mobilepassport.us/privacy/>

Mobile Passport App Terms of Service: <https://airsidemobile.com/terms-of-use-apps>

RushMyPassport Services in Mobile Passport: <https://mobilepassport.rushmypassport.com>

9.0 About This Datasheet

The Mobile Passport App is designed and developed by the company, Airside Mobile Inc. Airside builds innovative digital identity products for individuals and businesses with privacy-by-design and leading-edge security as its guiding principles.

Airside works closely with Airports Council International-North America (ACI-NA) and the U.S. Customs and Border Protection (CBP) to provide the Mobile Passport Control service.

The information contained herein is based upon document reviews and interviews with relevant subject matter experts involved in the development and operation of the services described. The discovery process relied upon the good faith accuracy of the information provided; TrustArc has not undertaken an independent audit and does not certify the information contained in this datasheet. However, the information contained herein was believed to be accurate and complete as of the time this datasheet was first published. Please note that the information provided with this paper, concerning technical or professional subject matters, is for general awareness only, may be subject to change, and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.