Privacy Impact Assessment

for the

Travel Document Checker Automation - Digital Identity Technology Pilots

DHS Reference No. DHS/TSA/PIA-051

January 14, 2022

Homeland Security

Abstract

The Transportation Security Administration (TSA) requires that aviation passengers verify their identity at TSA checkpoints. Typically, this is accomplished by the presentation of a physical identity document (ID) to the Travel Document Checker Officer. TSA is exploring the acceptance of digital IDs (a digital representation of a passenger's physical ID on a digital device) to provide passengers with a secure, efficient, and touchless experience. TSA is building on prior efforts that use Credential Authentication Technology (CAT) with Camera and 1:1 facial verification technology (CAT-2[1]), by incorporating a digital ID reader to process digital IDs and matching the information on the digital ID against a live photo taken at the checkpoint and passenger information provided through the Secure Flight program[2] before traveling. TSA is partnering and sharing information with the DHS Science & Technology Directorate (S&T) to evaluate system performance when using digital IDs. This Privacy Impact Assessment (PIA) is conducted pursuant to Section 222 of the Homeland Security Act to address privacy risks in the use of digital IDs in the identity verification[3] process at the checkpoint.

Introduction

TSA's mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. TSA aviation authorities extend to all passengers, regardless of citizenship, for both domestic and international flights, as well as individuals seeking to enter the sterile area of airports.[4] As part of its effort to secure aviation transportation, TSA confirms passenger identities before granting access to airport sterile areas. To improve the security, speed, and efficiency of TSA's checkpoint identity verification process, TSA is exploring the use of biometric matching technologies,[5] with a focus on facial verification as the primary means of identity verification for aviation security screening.[6] TSA expects that facial verification may permit TSA personnel to improve airport security and expedite checkpoint

[1] CAT-2 has previously been referred to in TSA Privacy Impact Assessments as CAT-C (CAT with a camera). CAT-2 has the capability for the passenger to self-initiate a transaction.
[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR SECURE FLIGHT, DHS/TSA/PIA-018, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.
[3] Federal Information Processing Standard (FIPS) 201 defines identity verification as the process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those credentials previously proven and stored in… [a] system and associated with the identity being claimed.
[4] "Sterile areas" are portions of airports that provide passengers access to boarding aircraft and to which the access generally, is controlled by TSA, or by an aircraft operator or a foreign air carrier through the screening of persons and property (49 CFR Part 1540.5).
[5] DHS defines biometrics as "unique physical characteristics, such as fingerprints, that can be used for automated recognition." *See* https://www.dhs.gov/biometrics.
[6] *See* TSA Biometrics Roadmap for Aviation Security & the Passenger Experience (September 2018), *available at* https://www.tsa.gov.

security processes.

In a previous proof of concept,[7] TSA tested CAT-2 for identity verification at the checkpoint. CAT-2 authenticated the physical ID presented by the passenger, collected the photo image and biographic information of the passenger from the physical ID, and captured the passenger's live facial image to biometrically compare with and authenticate[8] the passenger's photo on their ID. Additionally, a connection was established between CAT-2 and TSA's Secure Flight program to consolidate the passenger's vetting status, ID authentication result, and 1:1 facial verification result. The Travel Document Checker Officer conducted resolution procedures as necessary and directed passengers to the appropriate screening lane. TSA is now building upon this previous proof of concept by testing the efficacy of using digital IDs at the checkpoint to confirm passenger identity.

Digital Identities

A digital ID is an ID that is hosted on a digital platform — oftentimes a user's mobile device — owned and managed by an issuing authority as noted in Figure 1. A mobile driver's license is one example of a digital ID credential — specifically, it is a digital representation of the information contained on a state-issued physical ID, stored on or accessed through a mobile device. It is not simply a digital photo of a physical driver's license taken by a user and saved to their personal mobile device, nor a replacement for a physical ID — rather, it is complementary.

[7] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR TRAVEL DOCUMENT CHECKER AUTOMATION USING FACIAL RECOGNITION, DHS/TSA/PIA-046(b), *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[8] According to Federal Information Processing Standards Publication 190 (FIPS PUB 190) biometric authentication is the measurement of a unique biological feature used to verify the claimed identity of an individual through automated means. The biometric authentication mechanism will strive to measure a unique biological feature to the degree that only one person may be authenticated as a specific user.

For illustrative purposes, using a mobile driver's license as an example, a state Department of Motor Vehicles enrolls a user, capturing and storing the appropriate data in digital form. That state Department of Motor Vehicles is the issuing authority that will process the user's request to receive a mobile driver's license. Once approved, the Department of Motor Vehicles securely issues the mobile driver's license onto the user's mobile device. When the user arrives at the checkpoint, the user will present their mobile driver's license to the Travel Document Checker and a secure channel will be established to access the traveler's driver's license information. TSA will only request access to the relevant data for identity verification at the checkpoint. The user consents to release this data, and TSA validates that the information is authentic and signed by the issuing Department of Motor Vehicles. During validation and authentication, the only information TSA receives is the necessary public key[9] from the Department of Motor Vehicles to decrypt and authenticate mobile driver's license information provided by the mobile device. TSA does not contact the Department of Motor Vehicles for an individual's information.

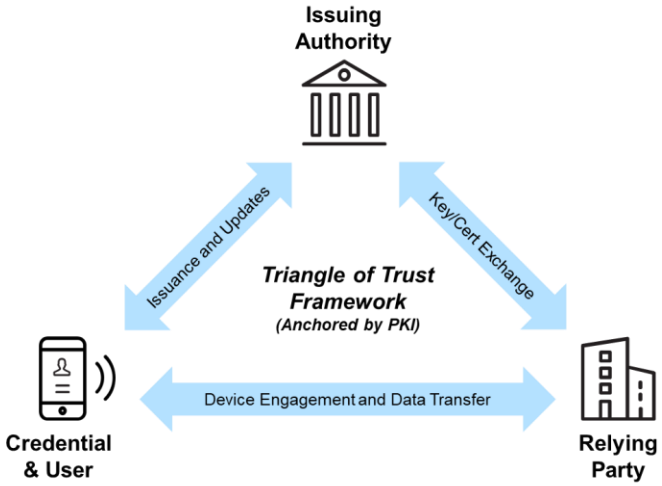

Figure 1. Triangle of Trust Framework

Digital IDs will enable passengers to seamlessly and securely transmit identity information from their mobile device (e.g., smartphones, smart watches, tablets) at the TSA checkpoint. TSA will notify passengers what data is transmitted from the mobile device to TSA and that their data will only be used for identity verification purposes, and during testing, shared with S&T for performance evaluation and analysis. Once a passenger's identity is successfully verified, they will be directed to the appropriate screening lane.

CAT-2 Process for Digital IDs

Public adoption and use of digital IDs are rapidly increasing, and TSA expects this trend to continue and that passengers will want to use their digital IDs at TSA checkpoints. TSA will pilot the integration of digital ID authentication capability with CAT-2 to process digital information to verify a passenger's identity. The passenger will go through the same process as

[9] NIST SP 800-57 Part 1 Rev. 5 defines public key as a cryptographic key used with a public-key cryptographic algorithm that is uniquely associated with an entity and that may be made public. In an asymmetric-key (public-key) cryptosystem, the public key has a corresponding private key. The public key may be known by anyone and, depending on the algorithm, may be used, for example, to: 1. Verify a digital signature that was generated using the corresponding private key, 2. Encrypt keys that can be decrypted using the corresponding private key, or 3. Compute a shared secret during a key-agreement transaction.

previous CAT-2 pilots, except that they will present a digital ID instead of a physical ID. Passengers may self-initiate their own digital ID verification on the CAT-2 digital reader without handing their mobile device to the Transportation Security Officer performing the Travel Document Checker functions as seen in Figure 2 below. This configuration was developed specifically to minimize physical interaction between passengers and Transportation Security Officer at Travel Document Checker stations.

A passenger initiates a digital ID transaction with CAT-2 by tapping their mobile device against the CAT-2 digital reader or by scanning a barcode on their mobile device. Once an encrypted wireless connection is established between CAT-2 and the mobile device, or the scanned barcode has been collected, CAT-2 will request the passenger's name, gender, date of birth, and photo.[10] The passenger will see an alert on their mobile device with a summary of the data to be sent to TSA and will be asked for their consent to send their information to TSA for identity verification purposes. After the passenger provides consent, CAT-2 is able to access the digital ID by unlocking the mobile application. The passenger's data is sent from the digital ID on the passenger's device to CAT-2 over the secure, encrypted wireless connection.

TSA will authenticate the digital ID using the public key certificate provided by the issuing authority (e.g., Department of Motor Vehicles). The name, gender, and date of birth from the digital ID will be compared within CAT-2 to information provided by Secure Flight.[11] The CAT-2 device will then display the passenger's biometric match and digital ID authentication results, as well as their Secure Flight information including screening instructions for the Travel Document Checker Officer to review. It will also display the live facial image of the passenger obtained at the checkpoint and the passenger's photo from the digital ID.[12] This process allows the Travel Document Checker Officer to cross-check the biographic information from the passenger's digital ID directly against the passenger's Secure Flight information to ensure that the data is the same, verifying the passenger should be at that airport that day and ensuring the passenger receives the appropriate level of screening. Finally, the Travel Document Checker Officer will conduct any necessary resolution procedures and direct passengers to the appropriate screening lane.

[10] In addition to the passenger's name, gender, date of birth, and photo, CAT-2 will also request the date of issue, date of expiration, issuing authority, document number, and REAL ID status consistent with the information required from a physical ID. A live photo is also captured at checkpoints for face matching with the digital ID photo.
[11] Secure Flight is a risk-based passenger prescreening program that enhances security by identifying low and high-risk passengers before they arrive at the airport by matching their names against trusted traveler lists and watchlists.
[12] At this point, the CAT-2 automatically will have verified the live face against the digital ID photo using the facial matching algorithm. TSA displays the live photo and digital ID photo to the Travel Document Checker Officer to allow the human to be the final and independent arbitrator of any security decision. This is exactly how it works with physical ID's today with CAT-2.

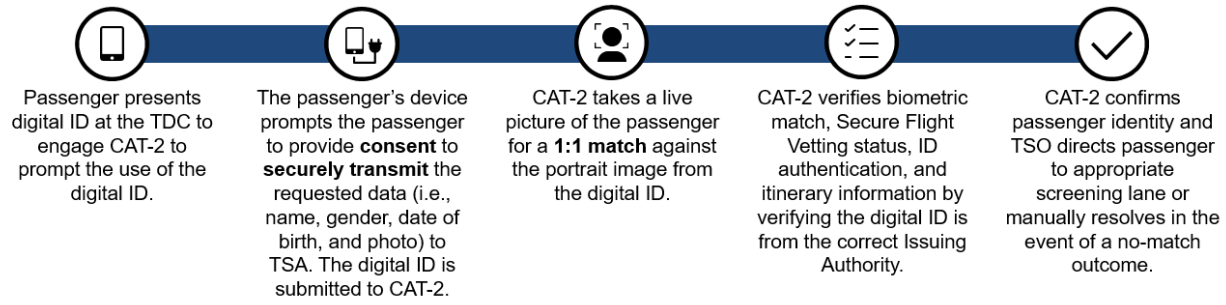

Figure 2. Digital ID Passenger Journey

The passenger's personally identifiable information (PII) will be used solely for identity verification purposes, in the same manner that biographic information from physical IDs is used. Additionally, during testing, this passenger information will be shared with S&T to evaluate system performance when using digital IDs.

Signs will be posted providing passengers with notice of CAT-2 with digital ID reader, along with the option to opt to participate. If a passenger opts not to participate, the Travel Document Checker Officer will direct them to a different lane for standard identify verification using physical ID. TSA's public website will be updated, as appropriate, to reflect all pilot programs conducted under this Privacy Impact Assessment.[13]

Data Retention During Routine Operations

Identifying data provided by the passenger to the booking agent or airline is held in TSA's Secure Flight system and is then sent to CAT-2 through TSA's Security Technology Infrastructure Program[14] in preparation for the passenger's arrival at the checkpoint, the data is then used to help verify the passenger's identity. The passenger will present their digital ID and take a live photo. Digital ID information is matched against the Secure Flight passenger data provided before arriving at the checkpoint. During routine screening operations, TSA will delete the Secure Flight passenger data stored on CAT-2 within 24 hours of the original flight departure time. Each passenger's personally identifiable information that is collected from the digital ID device along with the live photo will be overwritten when the next passenger scan occurs or when the Travel Document Checker Officer logs off the CAT-2 device, whichever occurs first.[15]

Data Retention for Test Purposes During the Pilot

During the pilot, Secure Flight passenger data, digital ID passenger data, and live photos

[13] *See* Biometrics Technology, *available at* https://www.tsa.gov/biometrics-technology.
[14] Security Technology Infrastructure Program is a suite of TSA applications that provide equipment connectivity, data collection, and data reporting.
[15] As an additional safeguard, the CAT-2 is configured to automatically log off if there has been 30 minutes of inactivity, which will delete the last passenger's personally identifiable information.

taken will be shared with S&T for subsequent analysis. TSA may also collect data other than personally identifiable information that will be used for performance evaluation and provided to S&T for analysis.[16] TSA will evaluate system performance as well as test new algorithms and software changes in an operational setting. In order to support system improvements, TSA may from time to time configure a small number of CAT-2 devices to retain passenger data from the digital ID device and the live photo for a short period.[17] Passenger data captured by CAT-2 from the passenger's digital ID as well as their live photo will be collected by TSA and retained for subsequent qualitative and quantitative analysis by TSA and S&T. The test data will be obscured to the greatest extent possible and will be stored on a removable TSA-owned encrypted hard drive attached to the CAT-2 device. TSA personnel will remove the encrypted hard drive and securely transfer it to S&T personnel. Exchanging the hard drives will help to minimize any potential corrupted data and will allow S&T to start qualitative and quantitative analysis before testing concludes.[18] S&T will not use the data provided by TSA for any other purpose, including operational uses within DHS. S&T will delete the data no later than 24 months following receipt in accordance with a Memorandum of Understanding.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[19] articulates concepts regarding how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[20]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[21] The Fair Information Practice

[16] The other data that will be sent to S&T is date of issue, date of expiration, issuing authority, document number, and REAL ID status.
[17] TSA may also collect other data that will be used and shared with S&T for performance evaluation such as the departure airport code, the date and time of the transaction, the date and time of travel, the serial number of the biometric device, system configuration, and biometric capture quality metrics, match result metrics.
[18] For further information about S&T's role in previous CAT-2 efforts, s*ee* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR TRAVEL DOCUMENT CHECKER AUTOMATION USING FACIAL RECOGNITION, DHS/TSA/PIA-046(a), *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.
[19] 5 U.S.C. § 552a.
[20] 6 U.S.C. § 142(a)(2).
[21] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.

Principles account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[22] and the Homeland Security Act of 2002, Section 222.[23] This Privacy Impact Assessment examines the privacy impact of the use of biometric technology and digital IDs as it relates to the Fair Information Practice Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

TSA will post signs close to the queue at airports implementing this technology to provide notice to passengers. Signs will provide travelers information regarding the procedures for participating, as well as instructions if they choose not to participate. Importantly, the digital ID process requires the individual to initiate the data transfer from their mobile device. The passenger will be reminded by a posted sign at the CAT-2 machine that confirming to share information from their digital ID devise is consenting to share it with TSA for identity verification and S&T for performance evaluation and analysis. If a passenger chooses not to participate, they will still be required to undergo the standard identity verification process. Information about the CAT-2 pilot as well as other biometric technology pilots are available on TSA's website. In addition, this privacy impact assessment provides notice by publication on the publicly available DHS website.

Privacy Risk: There is a risk that passengers will not know their digital ID and live photo are being captured by TSA for identity verification.

Mitigation: This risk is mitigated. The process for getting the passenger's digital ID and taking the live photo is completely transparent and obvious. It requires the passenger's active participation to physically swipe "confirm" on their digital device and to pose for the photo in front of the camera. In addition, this privacy impact assessment, along with signs posted close to the CAT-2 device and public communications materials, will inform members of the public about the procedures for participating and that TSA will take their photo and attempt to match the facial image with the image from their digital ID. Posted signs and public communications materials will also inform members of the public that they may choose standard identity verification procedures if they do not wish to participate in this CAT-2 pilot. Additionally, TSA's publicly available

[22] 44 U.S.C. § 3501 note.
[23] 6 U.S.C. § 142.

website contains information on all pilot programs, and is consistently updated with all relevant information for members of the public.[24]

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Signs in close proximity to the queue will provide notice to passengers about how to participate. Passengers will scan a barcode on their mobile device or tap their mobile device to the CAT-2 digital ID reader. The CAT-2 device will provide a signed public key certificate to the mobile device and request relevant data for ID verification at the checkpoint. The passenger will review and consent to share the requested data to the CAT-2 device. The CAT-2 device will then initiate a face photo capture. The CAT-2 device will display results for face matching, ID authentication, Secure Flight passenger data, and itinerary information to the Travel Document Checker Officer. The Travel Document Checker Officer will direct passengers to the appropriate screening lane and conduct any resolution procedures as necessary. All passengers proceeding through the dedicated queue will have the option to decline having their photo taken and can request manual identity verification by a Travel Document Checker Officer.

Through the Secure Flight program, TSA collects certain information from U.S. aircraft operators and foreign air carriers to identify and prevent known or suspected terrorists from boarding aircraft or accessing airport sterile areas. Individuals grant consent to the use of their Secure Flight information during the airline ticket purchase process for security purposes and to generate an appropriate boarding pass instruction. Linking Secure Flight to CAT-2 permits TSA to verify the content of the ID against the data contained in Secure Flight that generated the boarding pass instruction.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The Aviation and Transportation Security Act, Pub. L. 107-71, provides TSA with broad authority for securing aviation transportation and specifically authorizes TSA to test new technology and equipment.[25] In the Aviation and Transportation Security Act, Congress gave TSA specific authority to use biometric and other technologies to prevent persons who may pose a

[24] *See* Biometrics Technology, *available at* https://www.tsa.gov/biometrics-technology.
[25] 49 U.S.C. § 114(f)(8), (9).

danger to aviation safety or security from boarding an aircraft.[26] TSA has authority to establish pilot programs to test new technology to ensure safety and security for airports, including biometric technology that ensures only authorized access to secure areas.[27] TSA also has authority to strengthen access control points by deploying biometric or similar technologies to ensure security of passengers and aircraft.[28] In this pilot, the principal purpose of using passengers' personally identifiable information is to perform identity verification and assess critical operational and technological components of CAT-2. The personally identifiable information that is passed to CAT-2 from the digital ID will not be treated any differently than personally identifiable information that is gathered from physical IDs. Finally, the TSA Modernization Act required a report that includes specific assessments regarding the impacts of the use of biometric technology by TSA, as well as U.S. Customs and Border Protection.[29]

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

TSA will collect only the personally identifiable information directly relevant and necessary to perform identity verification, and to assess critical operational and technological components of CAT-2. TSA will only collect facial images and biographic information from passengers who opt to participate. This data will be provided to S&T pursuant to a Memorandum of Understanding. S&T will delete the data no later than 24 months following receipt in accordance with the approved TSA record retention schedule for security technology (NI-560-04-14, Item 2).

TSA uses the same information from a passenger's digital ID that it uses from a physical ID to verify identity at a checkpoint. TSA will only have access to passenger personally identifiable information that the issuing authority and the passenger have agreed to provide through the issuing authority's public key, which decrypts and authenticates the digital ID. Furthermore, TSA will minimize the collection of personally identifiable information by limiting the amount of Secure Flight data passed to CAT-2 devices, and only the local Secure Flight data for a specific airport will be passed to the CAT-2 devices at that airport. TSA will further minimize the amount of information stored in Security Technology Infrastructure Program by transmitting only a subset of Secure Flight information, specifically the passenger's name, gender, and date of birth, as self-reported by the passenger when making their reservation, plus Secure Flight screening status,

[26] Pub. L. 107-71, § 109(a)(7) (November 19, 2001) (codified at 49 U.S.C. § 114 note).
[27] 49 U.S.C. § 44903(c)(2)(3).
[28] 49 U.S.C. § 44903(g)(2)(G); 49 U.S.C. § 114(f)(8).
[29] TSA Modernization Act, Pub. L. 115-254, § 1919(c) (October 5, 2018).

reservation control number, and flight itinerary[30] from the Secure Flight to Security Technology Infrastructure Program.[31] Security Technology Infrastructure Program will then send the data, received from Secure Flight, to the CAT-2 device. Consistent with current CAT procedures,[32] only the Secure Flight data for passengers scheduled to fly from a specific airport will be sent to CAT-2 devices at that airport. The name, gender, date of birth, and other data will be sent back, through Security Technology Infrastructure Program, to Secure Flight to compare against the self-reported data provided by the passenger.

Privacy Risk: There is a risk that TSA may retain passenger information that is not required for the completion of the identity verification process.

Mitigation: This risk is mitigated. When a passenger initiates a digital ID transaction, CAT-2 will request only the data fields (name, gender, date of birth, and ID photo) necessary for identity verification at the checkpoint. The passenger will review the data fields requested and either reject or consent to the data transfer. The use of a digital ID with CAT-2 provides passengers with greater transparency into their transactions. It also allows TSA to request and see only the information that is necessary for identity verification at the checkpoint, further minimizing the data exchange in comparison with using physical IDs.

Privacy Risk: There is a risk that TSA may retain passenger information longer than is necessary.

Mitigation: This risk is mitigated. In accordance with current CAT procedures,[33] personally identifiable information from Secure Flight will be retained for no longer than 24 hours after the flight departure time to accommodate passengers that may require rescreening due to security events or when they decide to leave the airport sterile area for various reasons prior to their flight. Images will be retained until the next transaction is processed or when the Travel Document Checker Officer logs off the system. System auto logoff is set at 30 minutes of

[30] Flight itinerary data will be used to assist Security Technology Infrastructure Program in distributing information destined for CAT/Boarding Pass Scanning System (BPSS) devices to the correct airport.
[31] Secure Flight data used for CAT/Boarding Pass Scanning System purposes do not include passport information, redress, Known Traveler number, record sequence number, record type, passenger update indicator, and traveler reference number. More information on the Secure Flight program may be found in previously published PIAs *available at*, http://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.
[32] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR CREDENTIAL AUTHENTICATION TECHNOLOGY/BOARDING PASS SCANNING SYSTEM, DHS/TSA/PIA-024(b), *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.
[33] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR CREDENTIAL AUTHENTICATION TECHNOLOGY/BOARDING PASS SCANNING SYSTEM, DHS/TSA/PIA-024(b), *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

inactivity. Personally identifiable information sent back to Secure Flight will follow Secure Flight's retention policy.

S&T will delete the data no later than 24 months following receipt in accordance with the approved TSA record retention schedule for security technology (NI-560-04-14, Item 2) and the Memorandum of Understanding between TSA and S&T.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Information read from CAT-2 will be used for the purposes specified in the notice, airport signs, TSA's website, and this Privacy Impact Assessment: to verify identity, test CAT-2 functionality, determine CAT-2's ability to accurately compare a passenger's facial image on their digital ID with the passenger's photo taken at the checkpoint, and incorporate passenger Secure Flight data. The data generated on CAT-2 devices is not used for any purpose other than as discussed in this Privacy Impact Assessment or the previous Privacy Impact Assessments addressing CAT devices with Secure Flight connectivity.

It is the passenger who initiates the sharing of personally identifiable information with TSA upon engaging the CAT-2 reader. The passenger sees what personally identifiable information will be transmitted to CAT-2 and then consents to having it sent to CAT-2 for identity verification at the checkpoint. The passenger has complete control over the initiation of the transfer of personally identifiable information from their mobile device.

Personally identifiable information temporarily stored on CAT-2 will be shared with S&T for evaluation of system performance when using digital IDs. Information in Secure Flight is shared in accordance with the Privacy Act, 5 U.S.C. § 552a, and per the Routine Uses set forth in DHS/TSA-019 Secure Flight Records.[34]

TSA is committed to protecting passenger privacy and justifying the public's trust as it seeks to improve security and the passenger experience through its exploration of new identity verification technology. TSA will be providing terminal authentication as a service to all partners who are developing digital IDs to be accepted at the TSA checkpoint and wish to implement terminal authentication in their solution. Terminal authentication is encouraged, but not required, for a digital ID to interact with CAT-2. CAT-2 will send the necessary information for a digital ID to authenticate with CAT-2 at every transaction, but it is ultimately the digital ID developer's decision to support terminal authentication for their solution. Terminal authentication will prove to the passenger's device that it is communicating with and sending the passenger's information

[34] DHS/TSA-019 Secure Flight Records, 80 Fed. Reg. 233 (January 5, 2015).

to an authentic TSA reader. As a result, passengers will have full transparency into the data that TSA is requesting, what the data will be used for, and if the data will be saved. After reviewing this information, the passenger may accept and transfer their information, or decline and choose to go through the standard identity verification process.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

The personally identifiable information electronically obtained from Secure Flight for CAT-2 purposes is the same information that individuals present to a Transportation Security Officer during the physical ID verification process. When CAT-2 reads a digital ID, TSA obtains the passenger's name, gender, and date of birth from the digital ID. An image of the passenger from the digital ID is presented to the Transportation Security Officer. Digital identities will be signed and encrypted by the issuing authority, and TSA will have the issuing authority's public key to decrypt and verify the authenticity of the digital ID. The comparison of information between Secure Flight and CAT-2 via Security Technology Infrastructure Program, as well as certificate validation of the digital ID provides TSA with greater assurance that the digital ID is not fraudulent and has not been altered. The comparison ensures data accuracy by providing near real-time updates from Secure Flight to the CAT-2 device, which enhances transportation security.

If name mismatches occur, CAT-2 will display a list of Secure Flight data on passengers with similar attributes (e.g., the same date of birth, gender, last name, and/or first name) that are scheduled to travel on the same day at the assigned airport in order to compare data and resolve name mismatches. If the comparison identifies a fraudulent digital ID, TSA will investigate and may retain information on the incident within the Performance and Results Information System (PARIS).[35] CAT-2 prohibits name-based searches or retrieving additional personally identifiable information. TSA does not store or maintain any additional personally identifiable information displayed on the screen of the CAT-2 unit.

Privacy Risk: There is a risk that inaccurate information could be sent to the CAT-2 device.

Mitigation: This risk is mitigated. TSA obtains the information directly from a trusted TSA data source using secure data transmission techniques described further in Section 7,

[35] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR TRANSPORTAION SECURITY ADMINISTRATION PERFORMANCE AND RESULTS INFORMATION SYSTEM, DHS/TSA/PIA-038, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

Principle of Security. Additionally, if any issues arise during the process, the Travel Document Checker Officer will conduct resolution procedures as necessary.

Privacy Risk: There is a risk that TSA's cameras will be unable to capture images of a high enough quality to produce accurate matches, resulting in TSA's inability to confirm passenger identities.

Mitigation: This risk is mitigated. If CAT-2 is unable to match a passenger's photo, or experiences any error during the process, the Travel Document Checker Officer will screen the passenger according to the normal manual process.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Authorized users of CAT-2 will be limited to the TSA personnel staffing the device. Close accountability of the CAT-2 device and its removable drives will always be maintained. The CAT-2 device will be physically locked when not in use, and there will be access control to the CAT-2 computer including requiring login with an active Personal Identity Verification (PIV) card. In the unlikely event a CAT-2 device is tampered with or damaged, it is programmed to automatically delete all of its data. TSA secures passenger personally identifiable information against risk of loss and unauthorized access or use through a variety of information technology technical and administrative safeguards.

Digital IDs offer additional privacy and security benefits to passengers over physical IDs. Digital IDs transparently transmit only the necessary information requested by the relying party—rather than sharing all data elements found on the ID—and require users to consent to the data transfer. Additionally, digital IDs do not display any personally identifiable information when it is not in use. All digital ID data is encrypted both at rest and during transfer, and all transactions with digital IDs occur through encrypted secure channels. Finally, terminal authentication is an additional security feature that enables the user to confirm that the digital ID is communicating with an authentic CAT-2 device, if it is implemented by the digital ID's developers.

Privacy Risk: There is a privacy risk of exposing the CAT-2 unit and related data transmissions to unauthorized access.

Mitigation: This risk is mitigated. TSA employs mandatory federal data encryption standards (in accordance with Federal Information Processing Standard (FIPS) 140-3 and 197 as applicable) for all data in transit and at rest. Additionally, the CAT-2 system requires authorized users to log into the system with a TSA-issued Personal Identity Verification card to access the system for screening activities. The system also uses auto-logoff capabilities.

Privacy Risk: There is a risk that employees without a need-to-know the information in the performance of official duties may receive access to Secure Flight data.

Mitigation: This risk is mitigated. CAT-2 will only display biometric matching results, ID authentication results, and Secure Flight information to the Transportation Security Officer operating the device or supervisors summoned to resolve passenger identity document and/or boarding pass validation matters. Additionally, TSA will adhere to Secure Flight security safeguards outlined in previously published privacy impact assessments, which include administrative and technical controls to protect information against unauthorized disclosure, use, modification, or destruction.

Privacy Risk: There is a risk that passenger personally identifiable information on display monitors will be visible to other passengers.

Mitigation: This risk is mitigated. TSA positions CAT-2 monitors away from passengers to help prevent members of the public from viewing the information.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

TSA personnel operating Secure Flight, Security Technology Infrastructure Program, and CAT-2 are trained in systems operation protocols. Moreover, personnel receive training on how to protect passenger privacy.

TSA personnel are assigned roles for accessing the system based on their function. The system administrator grants access to authorized users based on the principles of need-to-know, least privilege, and separation of duties. The Information System Security Officer (ISSO) confirms policy compliance and manages the activation or deactivation of accounts and privileges as required or when expired.

System user access for Secure Flight, Security Technology Infrastructure Program, and CAT-2 can be analyzed and audited by the system owner and Information System Security Officer to ensure that data and reports are accessed only by individuals with a need-to-know and for authorized purposes.

All TSA and contractor personnel are required to comply with DHS/TSA privacy policies. Access controls are currently in place (including technological controls) to ensure only authorized personnel may access CAT-2. The program manager may audit the examination, maintenance, destruction, and usage activities to ensure they are used as described and that privacy and security protections are followed.

Conclusion

TSA is expanding upon the previous CAT program by exploring the integration of a digital ID authentication capability for CAT-2 to receive digital identity information at the airport travel document checkpoint to verify a person's identity, thereby providing increased privacy protections to passengers while increasing security and operational effectiveness at the checkpoint.

Contact Official

Jason Lim
Identity Management Capability Manager TSA Biometrics
Transportation Security Administration
Jason.Lim@tsa.dhs.gov

Responsible Official

Peter Pietra
Privacy Officer
Transportation Security Administration
TSAprivacy@tsa.dhs.gov

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717