NOTICE

This summary provides insight concerning the capabilities of automated credentialing systems. The list provides 15 potential capabilities that enhance the airport badging process. The TSA does not endorse any specific practice but rather offers this information to airport operators should it be of interest. This listing is provided in the interest of information exchange to enhance procedures for airport badge issue and processing. The U.S. Government assumes no liability for the contents or use. This listing does not create regulatory requirements or mandates of any kind. There are recommendations contained in this list that may prove beneficial in some airport badge issue office environments but not in others.

Automated Airport Badge/Credential System Best Practices

Automated badging/credentialing systems allow secure badges or credentials to be issued and renewed while enforcing the business rules/controls of the Airport Security Plan (ASP) and the Regulations and Security Directives (SD) issued by the Transportation Security Administration (TSA). A number of software companies have developed these automated systems because of their significant benefits, when compared with the error-prone manual systems that were instituted as near-term responses to the September 11, 2001 tragedy and subsequent threats to our Nations' airports. The following compilation of best practices for airport badging was prepared in August of 2012 with participation from leading airport credentialing automation companies.

1. Trusted Agent
   System should have the functionality to electronically manage Trusted Agent (TA) status to ensure that only authorized users are allowed to access and update badge holder information following requirements set forth in TSA Security Directive 1542-08G. These TA's are the staff members that enroll, update, and issue badges for the Airport.
   1.1. System should validate that the TA successfully completes the requisite TSA vetting processes.

1.2. System should maintain an audit trail that tracks which TA enrolled, modified and / or issued a credential to the applicant including the following details:

1.2.1. When and who collects and transmits information needed for Criminal History Record Check (CHRC) and Security Threat Assessment (STA).

1.2.2. When and who authorizes the issuance of the identification media.

1.2.3. When and who issues the identification media.

1.3. System should report on changes to TA status including new, updated or terminated TA's. This report is currently required by the local TSA Federal Security Director (FSD).

1.4. System should prevent the issuance of badges/credentials until all applicable procedures have been followed.

2. No Fly and Selectee Processing

System should have functionality to automate watchlist matching.

2.1. The system should perform data scrubbing required in SD1542-10G

2.2. System should record all changes to records by user and date.

2.3. System should provide flexible watchlist data report generation.

2.4. System should retrieve published derogatory data sets (i.e. TSA watchlist) automatically and on-demand. Note: Only authorized personnel of the airport that have proper security clearance are allowed to retrieve this information.

2.4.1. Retrieval of the information will happen no less that every 24 hours.

2.5. System should automatically compare each cardholder on record against the lists, using the procedures mandated in SD 1542-01-10F and log results of each comparison.

2.5.1. System should present watchlist data in a format that simplifies adjudication.

2.5.2. The same process will be used to compare records anytime a cardholder is added to or updated by the system.

2.5.3. Any cardholder records found with a positive match will create an immediate email notification to responsible Airport Security Administrators and warn the TA to notify the proper authorities.

2.5.4. Systems will prevent the issuance of a credential to an individual on the Selectee or Watch List.

2.5.5. System will automatically revoke a credential that has been issued when a person's name appears on the Selectee or Watch List.

3. Authorized to Work

The systems have business rules incorporated into the software to assure that an individual has met the criteria specified in SD 1542-08G prior to requesting CHRC or STA approval. Functionality to include but not limited to:

3.1. _ System should enforce the entry and verification of required I-9 documentation, including document numbers and expiration dates for:

3.1.1. Proof of US Citizenship (If not US Citizen must provide additional approved documentation)

3.1.2. Country of Birth (if outside US must require additional approved documentation)

4. <u>CHRC Processing</u>
   Systems should have the ability to interface with fingerprinting systems to retrieve data necessary to process 10 Prints to the Designated Aviation Channelers (DAC). All biographic data as well as NIST compliant information for the transmission is integrated to the LiveScan.
   4.1. System should automatically retrieve CHRC results and update those results into the cardholder record no less than every 12 hours.
   4.2. System should track resubmissions for Unclassified results, to avoid duplicate billings.

5. <u>STA Processing</u>
   Security Threat Assessment (STA) requirements for the TSA should be followed.
   5.1. System should track an individual using Unique Airport ID or Enrollment number. This ID will be used to assure that duplicate fees are not assessed for any person that may have more than one active badge at an Airport.
   5.2. System should collect, validate, and transmit biographical data required for STA processing as stated in SD 1542 08G to the Airport selected DAC.
   5.3. System should insure that all STA data is formatted properly:
      5.3.1. SSN
      5.3.2. Phone Numbers
      5.3.3. Alien Registration Number
   5.4. System should conform to the “Do Not Issue” requirements set forth in SD 1542 08G.
   5.5. System should process all STA results from their DAC using TSA approved protocols.
   5.6. System should provide a reconciliation tool that compares STA submissions and renewals for the DAC billings.

6. <u>Escorts</u>
   Systems should control the assignment of Escort privileges based on SD 1542 08G.

7. <u>Certifications</u>
   The systems should provide the functionality to store the following certifications:
   7.1. Privacy Act Notice Document Issued by the TSA (Electronic Signature of Cardholder)
   7.2. Authorization document for SSA(Social Security Administration) to release SSN to TSA (Electronic Signature of Cardholder)

8. <u>Signatory Authority, Training & Tracking:</u> Systems should be capable of managing authorized signatory transactions.

8.1. System should identify authorized signatories as part of the application process.

8.2. System should capture the authorized signatory's electronic signature during the application process.

8.2.1. The system should assure that only qualified signatories, for the applicants company, are available for selection during the application process.

8.2.2. System should track that training has been administered annually. If training or badge expires, the system should prevent the authorized signatory from processing applications.

8.2.3. System should track records associated with training to include date of completion, signature and printed name of the training administrator.

8.3. System should validate that the authorized signatory has successfully passed the STA & CHRC before qualifying as a signatory.

8.4. System should assure that all signatories have completed SIDA training before being assigned any signatory privileges.

9. <u>Training Requirement Tracking</u>

System should support the entry and tracking of training requirements, including:

9.1. Available Classes (SIDA, Movement, Non-Movement, Authorized Signatory, etc.)

9.2. Prerequisites for those classes

9.3. Airport approved trainers of the classes

9.4. Track Trainer Types

9.4.1. Master Trainer

9.4.2. Standard Trainer

10. <u>Cardholder Life Cycle Specifications</u>

System should manage cardholder life cycle including:

10.1. Assign and maintain cardholder expiration dates.

10.2. Track training requirements and results.

10.3. Maintain time limit for issuance after STA and CHRC Clearance

10.4. Renewal Processing

10.5. Revocation Processing

10.6. Lost or Damaged Replacement credential processing

10.7. Electronic record keeping for the minimum time required as mandated in SD1542-08G.

10.8. Biometric Verification prior to printing badge.

10.9. Comment tracking for each cardholder.

10.10. Automated systems provide complete audit trail of any changes made to cardholders.

11. <u>Automated Audit Procedures</u>

System should provide automated audit procedures in the following areas:

11.1. Collection and maintenance of binding documentation requiring any and all individuals that have been issued badges to immediately notify Airport Security Coordinator of lost, stolen, and/or terminated media.

11.2. Complete audit of all airport-issued badges at least once every 12 months, and not less than 10 % of the badges issued via random selection every 6 months.

11.2.1. Comparison of the current list of airport-issued badges against the lists maintained by the signatories to identify and resolve discrepancies.

11.2.2. All Audit information is retained for a minimum of 12 months.

11.2.3. Ensures that any access rights associated with media that cannot be verified are immediately deactivated or disabled.

12. Cardholder Accountability

System should provide recurring accountability reporting with automated notification when any area exceeds 4% unaccountability.

13. Concessionaire SIDA Access

System should report on concessionaire SIDA Access, specifically when it reaches key percentages (i.e. 25%).

14. Segregation of Duties

System should support and maintain the segregation of duties for the following roles:

14.1. Sponsors

14.2. Registrars

14.3. Adjudicators

14.4. Issuers

15. Visitor Management

System should create and issue visitor badges and manage the key activities including:

15.1. Issue temporary cards to visitors

15.2. Report Un-Returned Cards

15.3. Customize Badge Designs By Visitor Type

15.4. Visitors are scanned against No-Fly and Selectee list prior to issue

15.5. Report on Visitor badge issuance activity