

Considerations and Concepts

The Trusted Traveler Program

Improving Air Travel Security

Report to the United States General Accounting Office

September 3, 2002



TABLE OF CONTENTS

	Page
I. The Trusted Traveler Concept.....	3
II. Purpose.....	4
III. Technology Utilization	5
IV. Operational Implementation	8
V. Program Development Issues	12
VI. Pending Proposals	16
VII. Program Cost	17
VIII. Security Concerns	18
IX. Liability Concerns	19
X. Privacy Issues	20
XI. Experience	21
XII. Alternatives	22

I/O Software, Inc.

1533 Spruce Street

Riverside, CA 92507

(909) 222-7600

(909) 222-7601 FAX

www.iosoftware.com

I. THE TRUSTED TRAVELER CONCEPT

What are the main conceptual elements of the 'trusted traveler' program?

- The system is based on a voluntary pre-screening model that allows a thorough background screening against criminal or other relevant databases prior to the actual travel and without major time constraints or technical limitations.
- Travelers who are cleared through the background check are issued a card based ID that becomes available for future travel.
- The card confirms the initial pre-screening process and is presented similar to a certification. The data on the card must be strongly protected against tampering and forgery.
- The card securely stores a traveler's credentials such as biometrics, that allow for an unambiguous positive match between the traveler's identity and the card, and it gives the traveler control over personal and sensitive information.
- The trusted traveler concept extends the current structure of allowing only ticketed and screened passengers to the boarding gates, by separating passengers into higher risk and lower risk categories based on the availability of the card.
- A real-time revocation mechanism of any trusted traveler privileges allows for a quick response to potential security threats from card holders.
- Access via the card can be filtered by location, date and time, and other constraints.
- In person and on-site screening of trusted traveler card holders is not forgone, but can be streamlined based on the availability of a trusted traveler card.
- Valuable security personnel are freed up to screen travelers who are not participating in the trusted traveler program and who have not been pre-screened.

II. PURPOSE

What is the purpose of a trusted traveler program, what problems will it address, and why is this program needed?

- The introduction of a trusted traveler concept into the existing airport security infrastructure has the purpose of improving overall air travel security as well as streamlining the post 9/11 passenger screening process.
- The trusted traveler program is designed to enhance the existing in-person screening process at airports through the use of advanced authentication technology.
- By offering a filtering tool to security personnel, the system will save time and energy, allowing them to focus more attention on a thorough security screening process of more likely suspects.
- Being part of the trusted traveler program will save time for the passenger in various ways, increasing traveler convenience and acceptance of the check-in, boarding and traveling process.
- A properly implemented trusted traveler program will positively affect passenger confidence in the security screening process and overall air travel security, without raising privacy concerns.
- The system will significantly improve the security and convenience for all parties involved and increase cost efficiency of the air travel security framework.

III. TECHNOLOGY UTILIZATION

Is a successful implementation of a trusted traveler program dependent on deploying biometrics? What is the readiness/effectiveness of different biometric technologies, and which technologies are best suited for a trusted traveler program?

- The following three scenarios are generated with each level of technology deployed:
 - a) “Name only” via CAPPS - The question of a traveler’s true identity as well as the issue of identity fraud remains. Travelers can claim an identity based on an invalid ID. This is typically known as the “Which John?” problem.
 - b) “Card only” - While the card itself may be legitimate, the problem remains that the person presenting the card cannot be validated as the true card owner. The card might have been stolen, lost, or forged. This presents the “Is this John’s ID?” problem.
 - c) “Card plus biometrics” is the only way one can be reasonably sure that “This is John and his ID”. While different biometrics are generally associated with different levels of security, a biometric check can be used with great confidence to confirm that the individual presenting the card is also the legitimate card owner. The use of digital certificates (PKI) and encryption technologies protects the biometric data and prevents any data manipulation.
- Based on these scenarios and the fundamental rule that a system is only as secure as its weakest link, biometrics is considered an essential component of a trusted traveler program. Biometrics technology can be leveraged in two different areas:
 - a) Biometrics is used for background checking purposes. This is possibly the most controversial aspect of the program. By using the provided biometric information to check for criminal backgrounds using the FBI/AFIS/INS databases, it opens up the possibility that an applicant’s fingerprints could be added to such a database. At least initially, this level of background checks and data storage should be minimized and

applied to potentially critical applicants only. The architecture put into place, however, must already allow for a full integration with these databases in case a mandatory check becomes necessary.

- b) Biometrics is used for validating the appropriate ownership of the card presented at the airport. The trusted traveler program in its currently recommended implementation does not depend on a central data repository that would invite fraud or identity theft. Validated traveler credentials are managed and protected in a decentralized fashion, and the traveler's biometric data is stored on the card only. This approach addresses major privacy concerns as well as system cost considerations. However, with a decentralized storage mechanism in place, it is possible to add live-scan capability if it becomes necessary in the future.
- The following criteria must be considered when discussing the suitability and utilization of any biometric technology:
 - a) Security – How secure is the technology or the device itself? What is the expected 'False Acceptance Rate' (FAR) of a specific biometric technology? A high FAR will authenticate more unauthorized users and compromise security.
 - b) Maturity – How mature is the technology and what is the associated risk of failure? Can the technology/device be manufactured in the required quantities and has the technology proven itself to hold up in the "real world."
 - c) Time to Deployment – How quickly can a technology be adapted to meet the needs of the trusted traveler program? How complex is the deployment?
 - d) Technical limitations – How is performance affected by environmental factors and user errors? Can data easily be stored? The technology should be capable of limiting the passenger screening process to an acceptable level and not be affected by technical limitations such as data transfer.
 - e) Intrusiveness – Is technology readily accepted by travelers or will travelers feel constrained by the use of the technology?

- f) Cost – How cost efficient is the technology? Is there sufficient competition among technology providers? Will system cost have an unacceptable effect on the cost of air travel? What is the total cost of ownership (TCO) over the lifetime of the system? Typically, in systems like this, the full TCO is not taken into account where various proprietary components that may cost less early on, end up requiring considerable new investments when the system is upgraded.
 - g) Usage - The technology must be easily maintainable, convenient, relatively quick and user-friendly. What is the expected “False Reject Rate” (FRR) of a specific biometric technology? A high FRR will reject more legitimate users, thus lowering a card’s convenience and utility.
 - h) Flexibility - The technology must be interoperable, thereby enabling future technologies, applications and implementations. Newer, improved technologies will continue to become available. A system must not be tied or constrained to a specific device or technology.
 - i) Privacy – Does the technology intrude upon civil rights or liberties? Are individual rights and liberties exposed to risks?
- There is no single “best” biometric that provides all the answers and satisfy all the factors listed above, and one must be wary of any vendor claiming to “be the best” in this still relatively new industry. Considering all aspects, fingerprints currently have favorable tradeoffs, although that might change in the future.
 - As a result, the system needs to be developed independent of any particular technology and highly flexible in terms of policies, technologies and implementation. Overall infrastructure flexibility must be of major concern as policy and security needs will most likely change as the system is implemented and expanded. New policies, needs and technologies must be easy to implement to accommodate new circumstances, threats and counter technologies.
 - The ID card must include a mechanism to authenticate and confirm the integrity of both the card and its stored information, through the use of digital certificate (PKI) technology.

IV. OPERATIONAL IMPLEMENTATION

How would such a program actually work, operationally, in an airport, and how would it be integrated into existing check-in security procedures?

- The enrollment and trusted traveler ID creation process:
 - a) User data collection, registration and enrollment is performed through existing local infrastructure, preferably backed by a federal authority such as the U.S. Postal Service. An integration with the mechanism(s) currently employed to issue passports is conceivable.
 - b) User presents valid picture ID (i.e. passport, driver's license) and one other form of data confirming a physical mailing address (i.e., utility bill) prior to data collection.
 - c) Presented credentials are viewed and evaluated on site by trained personnel.
 - d) All necessary user data is collected and a biometrics is enrolled while witnessed by a Federal employee.
 - e) With current technology, the most likely initial biometrics is fingerprint. However, the system must be capable of supporting multiple biometric technologies, and provide integration of additional future technologies (iris, face, etc.).
 - f) Data is subjected to background checks with existing federal databases (i.e. FBI, INS, AFIS, NCIC, etc.). This is an optional feature.
 - g) Data integrity on card is secured through the implementation of digital certificates and public key infrastructure (PKI) methods.
 - h) The user does not receive the card immediately; allowing a thorough background check. The card is mailed to confirm physical address. This is an optional feature.
- The card used for the trusted traveler ID should not be based on traditional smart card technology. From a usability and acceptance standpoint, it is our experience

and opinion that the more modern contactless (wireless) smart cards would be advantageous in a number of ways:

- a) It is the same form factor and looks just like a regular credit card so the printable area is just as large.
 - b) There is no exposed chip to tamper. Tampering an enclosed card would be more evident.
 - c) There is no exposed chip that might be damaged accidentally.
 - d) The transmission speed is fast (<0.5 sec).
 - e) It is convenient to the user who doesn't necessarily want to "insert" a card into a reader (especially holding all their luggage).
 - f) In some cases, the hardware is cheaper.
 - g) The reader and card contacts do not wear out or become dirty.
- Once the card has been issued, the verification process uses the following check points:
 - a) Check-in counter: Card is presented by the traveler. The account is linked to the airline reservation and frequent flier system. Reservations, program memberships, traveler preferences, etc. can be accessed quickly and confirmed. Passenger and check-in luggage can be flagged. Business travelers may benefit from an optional lounge check-in.
 - b) Boarding pass check: Card is presented by the traveler to security personnel at the new boarding pass post-9/11 check point. Trusted traveler card holders are separated from other travelers and access a fast lane. Security personnel can optionally be equipped with portable card-check terminals. A simple kiosk with an optional turnstile can also expedite and automate this process. A passenger swipes the card and the kiosk checks whether the passenger has booked a valid flight for that day or within a specified time period. This automated process may be augmented with optional security personnel.
 - c) Metal detectors: There is no change compared to present status. Trusted traveler card holders are subject to standard screening at this point.

Optional fast lane may separate card holders for less invasive or expedited screening.

- d) Boarding Gate: Card+Biometric+Traveler are checked. This is considered the last line of defense and as such, is critical. The purpose of this check is to ensure that the passenger is the legitimate holder of the card, that the passenger is booked for that flight, and that the stored credentials are valid.
 - e) System has an optional interface that allows airlines to tie into existing systems providing passenger information for automatic check-in confirmation and frequent flier crediting.
- The different terminals used for the above steps do not perform a live scan against a central database. However, the system is equipped to download and implement lists of revoked cards via a Certificate Revocation List (CRL) mechanism at defined intervals. Intervals may change dynamically based on policy and/or the potential threat and level of necessity at any given moment.
 - A properly implemented system has to be able to deal with any of the following system failures modern at various check points since its not a matter of “if” failures will occur but “when”:
 - a) Stolen card – To make this scenario valid, one must make the assumption that the photo identification on the stolen card bears some resemblance to the illegal card holder. Most check points do not require a biometric check and the true card holder cannot be validated at those check points. If no action is taken, this could pose a potential security threat, at least to the point where the stored biometric data is checked. The legitimate card holder can be expected to report the loss, unlike a traditional identification card, it is possible to revoke such a card and disable it permanently. The proposed trusted traveler program, although decentralized, leverages a revocation mechanism. Ultimately, a stolen card does not have much utility at any biometric check point since the biometric data will not match the illegitimate holder of the card.
 - b) Forged or altered card - In this scenario, one assumes that the printable face of the card is altered to match the picture of the illegitimate user of

the card. This scenario also assumes that either the card was borrowed or stolen or that the card was created from “scratch”. Either way, technologies in the area of holographic printing can minimize the potential threat from such attacks. The contents of the IC chip itself can also be assumed unalterable to virtually all attackers, and at any card checking station, the cryptographic signatures would be flagged as invalid and immediately notify onsite security.

- c) Borrowed card - This scenario is similar to the stolen card scenario but it involves a collaborator. This problem exists with all forms of identification currently used for the screening process. Just like a stolen card, however, a borrowed card does not have much utility at any biometric check point since the biometric data will not match the illegitimate holder of the card, and will identify any illegitimate user.
- d) Intentionally mutilated card - The scenario is an attempt by the card holder to bypass the biometric check by presenting a seemingly valid but inexplicably damaged card. In this scenario, the worst case is to revert back to the existing methods of security check and deny any Trusted Traveler benefits. Situations such as this should automatically warrant an extensive security check.
- e) Terminal tampering - This scenario assumes the possibility of cooperative parties within the airport either physically swapping out a verification terminal or reprogramming it with a rogue or Trojan horse program. In this case, a properly designed application will utilize the existing public key infrastructure not only to validate card holders and the integrity of the card data, but to also verify the integrity of the terminal and the overall system. A security policy could also require a pre-boarding check of the terminal via a challenge/response card, and public key infrastructure to confirm the consistency of the device.
- f) Offline and intentionally disabled terminals - This assumes a scenario where verification terminals are broken, offline, disabled (intentionally or otherwise) and alternative terminals are not available. This issue will be less important as system components become more commonplace and portable emergency devices are available. Offline or disconnected

terminals are initially not an issue as CRLs (Certificate Revocation Lists) and other law enforcement data is only periodically downloaded and stored on the terminal device. Nevertheless, a security policy should monitor disconnects and automatically require the attendant to go back to manual or backup (status quo) security screening procedures.

- g) The issuing Certificate Authority (CA) is somehow compromised – This assumes that a normally secure CA (root or downstream) facility is compromised or tampered with. All certificates issued by that CA will be revoked and the CA will create a new root certificate. The ability to do this and the effort required along with the number of travelers affected depends on the CA deployment.
- Even in a worst case scenario, a compromise of a trusted traveler system will only result in reverting back to the existing method of security screening. It is important, however, that once a trusted traveler program becomes fully operational and integrated into the normal regime of air travel, the expectation of the traveling public will be raised to the point of expecting a certain level of reliability. When discussing the technical implementation, it is thus important to address issues of uptime, redundancy, and flexibility.

V. PROGRAM DEVELOPMENT ISSUES

What party should be responsible for developing, running, and financing the program? What should be the primary deployment parameters of a trusted traveler program? What are the main issues that should be resolved before such a program can be developed and implemented?

- Some components of the overall trusted traveler system should be funded, supported and structured by the federal government. Given that any tampering (or other fraudulent activity during enrollment or post enrollment) with the cards should have considerable penalties associated, card enrollment and issuance process should be ‘Federal’ in nature.

- A federal authority, TSA/FAA, should provide technology guidelines to the airports to ensure interoperability between the systems deployed. In doing so the authority needs to balance federal involvement, airport autonomy and common interests.
- Since airports are generally responsible for onsite security, deploying the physical devices at various check points should be within the airports' discretion, particularly if they see a need to reduce screening bottlenecks. This can be done by utilizing portable verification terminals. Momentary surges in traffic can be dynamically addressed.
- Airlines should be free to deploy automated check-in kiosks, lounge access, and “fast lane” expedited security checkpoints that take advantage of the card at their own expense.
- Driven by pressure from travelers, airlines and airports are expected to quickly deploy multiple trusted traveler checkpoints. Airlines and airports will most likely be pressured to also automate certain functions such as boarding, frequent flier crediting, lounge memberships, etc. At some point in time, it will be necessary for all major airports to install the system just to maintain competitiveness.
- Subsidies and passenger costs/fees (i.e. trusted traveler bonus miles, airport fees etc.) can also be considered but the dynamics are hard to quantify.
- The properly implemented trusted traveler system should address the needs of the following beneficiaries:
 - a) Airlines: Reduced delays in boarding will lead to higher customer satisfaction. Consistent form of legacy identification and faster reservation retrieval allows for quicker checks at check-in. There are also potential opportunities to cross reference frequent flier data, lounge information and other airline data. An efficient security upgrade system will also increase public confidence and readiness to travel.
 - b) Airports: Reduced boarding bottlenecks at various check points. Portable, stand-alone kiosks (with just Card or Card+Biometric) can be

deployed and located depending on various circumstances (holidays, group tours, etc.) and security needs (alert level changes).

- c) TSA: Reduced personnel needs due to efficiencies in filtering passengers into more granular “security risk” categories.
 - d) Passengers: Faster processing at various check points, minimally invasive checks, consolidated forms of identification (ID, frequent flier, lounge, credit card, etc.)
- The primary mission of the trusted traveler system should be to provide convenience to all stakeholders and provide an effective and efficient tool to enhance aviation security.
 - There are no major technical issues that need to be resolved in order for a trusted traveler system to be implemented, and a number of valid procedures have been proposed. However, the following technical and logistical issues should be discussed thoroughly and resolved prior to a coordinated large scale deployment:
 - a) Specialized cards and card readers, stand alone or integrated, will need to be designed, fabricated, distributed, and updated or otherwise maintained or replaced.
 - b) A proper distribution mechanism for card revocation lists will have to be established, maintained, and protected.
 - c) Consistent procedures for checking the authenticity of IDs and for verifying the presenter (with or without specialized equipment) would need to be established, promulgated, practiced, and audited.
 - d) Means to discover, report, verify, and authoritatively correct mistakes would need to be put in place.
 - e) A variety of security measures would need to be factored into all aspects of the system to be sure that it meets its objectives and is not vulnerable to things such as fraud or denial-of-service abuses that can result in privacy violations.
 - f) Implementation and setup of Certificate Authorities will determine the revocation mechanism and technical framework.

- There are also a number of political issues that need to be resolved prior to the implementation of a trusted traveler system:
 - a) What is the level of assumed security a trusted traveler card holder is granted at any given time? Although different security mechanisms can be put into place, it cannot be assumed that all program participants can be fully trusted without weakening the security structure. Acquiring and presenting a card simply increases the level of trust and streamlines screening, it does not completely eliminate the screening process and any other legitimate measure such as baggage check, metal detectors, and in person checking. Different levels of trust could possibly be tied to each participant.
 - b) How is the collected data used to profile travelers? The card can potentially store different types of data dynamically, and it is possible to further differentiate card holders by the various bits of data encoded based on past activities (boarding frequency, travel sites, travel habits).
 - c) How is the system integrated with existing databases, including airline tracking and reservation systems? The proposed system depends on a voluntary and decentralized system, without a direct traveler tracking mechanism. This approach currently presents the politically most acceptable balance of security and privacy. Without pre-empting future developments, it should be kept in mind that the system might require a more networked approach.
 - d) Should non-biometric data be shared with other applications, depending on the airlines, the airports or the card holders' consent?
- To define exact policy requirements and even technical requirements is beyond the scope of this document. However, a fundamental premise should be that the system must always be flexible enough to handle ever changing policies needs.

VI. PENDING PROPOSALS

Are there any specific proposals for implementing a trusted traveler program in the U.S.? What are the views of the proposals and how long would it take to implement such a program?

- The TSA and other federal agencies have been introduced to different trusted traveler proposals, including the proposal outlined in this document.
- The presented proposal allows for the independent and flexible development of policies that are separate from the underlying technology. It recommends the greatest possible flexibility regarding the choice of card, biometrics and any related technical implementation. It offers the ability to expedite initial deployment with existing technologies without the risk of being locked into a specific technology or the threat of political paralysis.
- Other proposals have been built on a pre-defined, proprietary and technologically limited infrastructure, and a trusted traveler implementation is wrapped around that technology.
- It is important to consider that the stakeholders' needs and the solution must drive the technology used. A system cannot be dictated by a proprietary and limited choice of authentication technologies. A trusted traveler system must be able to adapt to new and future authentication technologies as they are developed and become available, and even more so as security requirements and system needs change.
- The available technology, software and hardware, is already available and is not the gating issue for the launch of the proposed system. A similar infrastructure, based in its makeup on the trusted traveler system, has already been successfully deployed and performs within parameters. With the appropriate backing and the political support, it might only take a few months to work out policy and usage issues. An initial implementation could then relatively quickly be launched and a broad system deployment could be scheduled over the period of 12 to 24 months.

VII. PROGRAM COST

Are there any cost estimates for the implementation of such a program? If so, how much would such a program cost? If not, what specific items need to be accounted for in deriving such an estimate?

- There are currently no specific cost estimates, just overall cost considerations:
 - a) Card enrollment/issuance: Is the card issued by the government? Is there a participation fee or a customer enrollment fee?
 - b) System deployment and integration: Should the individual airports cover cost? Are there federal resources available?
 - c) Check-in terminal: The integration with existing check-in terminal is very inexpensive. Airlines should pay for these terminal upgrades.
 - d) Board pass check point: Very inexpensive. Airports should be able to decide on the level of deployment and should cover expenses.
 - e) Boarding gates: These are the most expensive components. Additional cost is estimated at a factor of 2 to 5 compared to traditional terminals. Airports should be responsible for the cost of these terminals since they are simply an extension of the screening process.
 - f) Portable confirmation devices (for law enforcement, airline/airport officials, etc.): These are very inexpensive and should be financed by the entity utilizing the devices.
 - g) All devices can utilize COTS technology and devices, and thus reduce system cost.
- A decentralized, card based and flexible solution as proposed will be far more cost efficient compared to a centralized and proprietary solution that requires a huge infrastructure. It also provides a suitable option of a deployment in phases.

VIII. SECURITY CONCERNS

What are the key security issues and concerns (sleeper cells, dupes, fake ID's) associated with a trusted traveler program and how might they be addressed?

- The existing system is not replaced by the trusted traveler program. The trusted traveler program is merely used to provide a tool to enhance and expand the existing systems, and make them more efficient. As such, it does not constitute a security risk.
- Sleeper cells: The cards themselves have the ability to store some flight information. Depending on the implementation, cards that were issued but have not been used for some time can still be required to go through the normal checking process. A trusted traveler system may in fact be used to optimize the screening process by looking out for specific usage patterns. (frequency of travel, clustering, ticket purchase, etc.) As stated above, a trusted traveler is not given routine access and boarding rights without appropriate on-site screening and the application of other security tools.
- Duplicates: The biometric information stored on the card will validate that the card presenter is the also the legitimate card holder, and the biometric data is protected by digital certificate technology. Duplicate cards will simply not pass biometric identity check, which is mandatory for at least one of the check points prior to boarding.
- Fakes: If done properly, the underlying technology, certificates and encryption would make it extraordinarily difficult, although not entirely impossible, to create fake cards. The necessary technology exists and is well established and proven. As with all security measures, it is a balance of necessary effort to crack the system and attempted reward that determines the validity of a system. A suspect who could potentially compromise the system and pass all other standard security screenings, will use far easier and cheaper means to illegally obtain access to a plane (by not having an ID, breaching the physical barriers etc.)
- A true security system/architecture in general, needs to address at the minimum, the following four requirements and components:

- a. Confidentiality – Trusted traveler card holders should feel comfortable that their travel habits and other personal information are kept confidential.
- b. Integrity – Both the card and the data stored on the card (i.e., biometric) needs to maintain a high level of integrity.
- c. Authentication – As outlined above, true, strong authentication is fundamental to the trusted traveler program. Authentication methods can be broken into three basic factors. “What you know” (PIN/password), “What you have” (keys, cards) and “What you are” (biometrics). Out of the three, biometrics is the only non-repudiated way to confirm a person’s identity. Incorporate a card (what you have) and you have a very strong two-factor authentication system.
- d. Authorization – The final component is based on making sure that once authenticated, a trusted traveler can benefit from the program while restricting high risk individuals. Many of these issues are policy based but ultimately need to work seamlessly with the components above.

IX. LIABILITY CONCERNS

What are the key liability issues associated with a trusted traveler program, and how can they be resolved?

- Who will be responsible for any damage caused by travelers enrolled in the program?
- There is realistically no increase in liability for program participants (i.e. airlines, airports).
- Expectations must be clarified and fully communicated to all the stakeholders. The trusted traveler program increases security; it does not eliminate the threat posed by potentially unsafe airline travelers.

X. PRIVACY ISSUES

What are the most important privacy and equity issues associated with implementing a trusted traveler program, and how can they be mitigated?

- Any system must balance security needs with the values of privacy and other civil liberties.
- Given the current proposal, the trusted traveler program participant is not giving up any new information and cannot be monitored beyond what the existing system already monitors.
- The proposal also suggests that any biometric user data is only stored on the card and only used to confirm the identity of the person who presents the card. The system does not require storage of biometric data offsite, or in a central database. Optionally, only applicants whose biometrics generates a match with existing databases (i.e. AFIS, INS) are noted. Travelers are absolutely free to join, refrain from joining, or even quit the program by destroying the card.
- Some of the existing information that the airlines, airports, the TSA, CAPPS, etc. already collect, process, and leverage (name, address, cities traveled, frequency of travel, etc.) may be required but is only presented in a more efficient and consolidated form for faster processing, and does not constitute a privacy concern.
- It must be considered that using technology to solve security issues in a public place such as an airport, compared to a workplace, imposes a low threshold with regard to violating individual rights. However, terrorists who are also passengers and as such are part of the general public, pose a major security risk. This conflict is not unsolvable and should not lead to paralysis, it is rather the responsibility of the federal agency such as the TSA to balance the security and privacy issues and support a program that takes this balance into account.
- The following constitutional issues might be raised in conjunction with a trusted traveler program:
 - a) Fourth Amendment: The Fourth Amendment regulates how and when authorities may engage in the search or seizure of a person or property.

The Fourth Amendment protects individual dignity and autonomy and a technology must not be used in a manner that infringes upon privacy or unreasonably singles out some individuals over others. The presented proposal does not single out individuals based on their ethnicity, religion or gender, but on an individual's willingness to submit to an offsite pre-screening process. As such, it is not more applicable to the trusted traveler program than the existing screening process.

- b) The Fifth and Fourteenth Amendments: The due process principle focuses upon the procedures used by government entities to determine whether a person should be subject to a particular legal restriction or requirement. Due process also attempts to balance the interests of government with those of the individual, for example the individual's right to travel. Due process remains a critical constitutional guarantee in the wake of September 11. Balancing the need for security against privacy of the individual requires technology deployment that is reasonably effective and accurate and that offers an easy upgrade path to improved authentication technologies as they become available.

XI. EXPERIENCE

Are you aware of any such programs in other countries? If so, how do they work? Are you aware of any cost estimate for programs in other countries? Are there any lessons to be learned from programs in other countries? If so, what are they?

- Although the technology is available and individual elements of the proposed program (i.e. biometric authentication, biometrics on card, digital certificates) have been tested and successfully deployed, there is currently no program with the same scope and sophistication in place. I/O Software has been in a front position involving a number of programs that leverage the technology proposed for the trusted traveler program.
- There is currently no program that would lend itself to a precise cost analysis since the implementation details and goals of other systems are fundamentally

different. However, since the program is based at least initially on available technology, cost can be estimated with reasonable certainty, based on the existing implementations and the required technologies.

- An important lesson that can be learned from ‘similar’ programs in the IT industry is the need for a flexible and scalable technology. An infrastructure such as the trusted traveler program is a considerable investment in terms of financial commitment, technology, public confidence and user acceptance. As a result, a trusted traveler system should not close the door on any technology and development that could enhance the program in the future.
- User acceptance, including usage for airports, airlines, as well as travelers, is the key for the success of a trusted traveler program unless it is mandated by the federal government.
- The presented proposal is mainly concerned with U.S. air travel, but, given the international nature of air travel, it might become important to extend a common architecture and card format to international frequent travelers.

XII. ALTERNATIVES

What possible alternatives are there to implementing a trusted traveler program? What does a trusted traveler program offer that other alternatives do not?

- There is really no equivalent alternative to a trusted traveler program such as the one we propose, particularly when considering security, privacy, convenience as well as cost.
- A massive deployment of additional screening mechanisms with conventional methods could increase security and address the convenience issues raised by travelers (i.e. check-in time), but it would increase cost considerably and would strain airport infrastructure considerably.
- Creating new and dedicated check-in facilities also raise concerns about cost and traveler acceptance. Such a security measure will involve substantial construction activities, massive disruption of travel, and it will create

considerable issues regarding airline participation, user acceptance and traveler convenience. Such projects will also not substantially alter or improve the critical screening process.

- Considering all aspects, the trusted traveler program is the most cost efficient and distinctly secure alternative. The increased level of security is achieved through the use of technology, not personnel and as such is easily scalable. Unlike other alternatives, the program supplies simple operational mechanism for focusing and streamlining the existing security screening process.