

In response to The Immigration and Naturalization Service's Request for Information regarding the "United States Entry Exit System"(EES), we are pleased to present the technology solutions offered by AuthX™.

AuthX™

Security Simplified

Contact:

Jeffrey C. Milanette
AuthX, Inc.
325 Kimball Ave.
Westfield, NJ 07090 USA

Tel. 908-789-3424
Fax. 908-789-9761
E-mail: jeffm@authx.com
Web: www.authx.com

The events of September 11th, as well as terrorist events prior and since, have often had a common thread, in that they involved fraudulent IDs in the planning and execution of these acts. As there are many millions of existing passports, and federal and locally issued IDs, the ability to easily migrate to highly secure documents that can be instantly verified anywhere at any time is crucial. Future IDs must be compatible with government and travel systems to provide a seamless system of security with a high level of process efficiency, regardless of network or database availability.

AuthX™¹ should become the primary document authentication component of the United States Entry/Exit System. No other system offers the same:

- Levels of security,
- Ability to be retrofit,
- Scalability,
- COTS deployment,
- Flexible Biometric Platform,
- Ease of use,
- Cost effectiveness and economic return,
- Ability to integrate with travel, transportation and law enforcement databases,
- Individual privacy protection.

AuthX™ technology is highly functional, resilient, fault tolerant, low cost and easily retrofitted to existing documents, making it an ideal medium for this use. Because AuthX™ integrates and links processes and transactions using existing infrastructure, minimal cost and time to deploy result. Additionally, processes are improved; boarding and border inspection tasks become automated, simplified and highly secure. Finally, the AuthX™ system architecture incorporates important provisions to secure and maintain the rights to personal privacy for the traveling public. The system is designed to work within the judicial oversight structure, so important to a free society.

¹ AuthX™ has Patents Pending on its System Architecture, core technologies, and its unique applications of those technologies.

AuthX™.

Enabling Technology: The AuthX™ software technology architecture offers a unique solution to the problems of identity verification and tracking. AuthX™ makes new or existing documents self-authenticating, while at the same time making them machine-readable and network enabled. AuthX™ is built on open systems platforms, enabling interoperability with existing government and transportation networks, systems, and databases. Able to function within a network, AuthX™ can also operate in a standalone mode, continuing to operate when networks or databases have failed or are otherwise unavailable. This allows AuthX to create and authenticate documents on battery-operated devices in remote or mobile locations. AuthX™ uses inexpensive COTS hardware, and the operator interface can be a full data PC display, or a simple, hand held pass-fail indicator. The AuthX unique document identifier will enable the linking of information across databases so as to facilitate production of overstay and ad hoc reports as necessary. AuthX™ uses a unique implementation of Public/Private Key encryption to create and read documents. This multi-level encryption utilizes a highly secure 2048 bit key with a state of the art the encryption algorithm. The result is an inexpensive document with the highest level of security.

AuthX™ can be retrofitted to virtually any document currently in use on U.S. borders, including passports, visas, government issued ID's, driver's licenses, etc. Because AuthX™ is designed to work with legacy systems, implementation, training and cultural adaptation by both travelers and transportation security personnel will be minimal. Since it is a software solution, AuthX™ will continually benefit from the evolutionary gains in image processing and computation speeds. Its scaleable architecture will allow for a phased rollout that will meet the challenge of legislatively mandated improvements.

The following presents an overview of the how AuthX™ secures photo ID documents and how AuthX™ is already being supported by the world's leading travel processing and distribution services company, Sabre Holdings. It also outlines some of the unique advantages of the AuthX™ System Architecture, and explains (with compelling reasons) why AuthX™ should be considered as the primary document authentication component of the United States Entry/Exit System.

The AuthX™ Self-Authenticating Photo ID System

Secure Document Creation and Retrofitting. AuthX™ provides a highly reliable and extremely secure means for creating new or retrofitting existing documents, which then become both machine readable and virtually impervious to counterfeiting or alteration. Utilizing AuthX™ enables all elements of a document including the photo, to become machine readable, and is not limited simply to MRZ text.

The process begins with an image of the document to be secured. The AuthX™ system scans the entire document, including the picture and the text. A grayscale template of the picture is created and encoded. Concurrently, the descriptive text identifying the person is recognized and also encoded. Finally, other information contained in the document is analyzed and encoded. These elements are securely encrypted and combined into an *authentication code* that is encapsulated in a machine-readable format, such as the two-dimensional PDF 417 barcode². Once the machine-readable authentication code is attached to the document, the authentication code becomes part of the document itself. Self-Authentication of the document can take place at any time by comparing the document with the information embedded in the

² PDF 417 is an open source standard bar code format selected by AAMVA and ICAO for driver licenses and passports. Other open standard bar code formats include DataMatrix and Aztec, both of which are significantly more compact and therefore have a significantly smaller footprint on the document.

authentication code. Removal or alteration of the bar code is immediately detected and will indicate the document has been tampered with.

The barcode serves only as a machine-readable envelope for the authentication code. Other envelope types such as optical character recognition (OCR), a magnetic-stripe and smart card can also contain the secure AuthX™ authentication code. AuthX™ is compatible with commonly used passport scanners and networks in place throughout the world today in border management and commercial transportation systems.

Document Authentication. Once a document has been created or retrofit with an AuthX™ authentication code, any tampering will be quickly detected when presented for verification. The authentication process uses a secure key to decrypt the authentication code. If the current scan of the document does not match the information encapsulated in the authentication code, any tampering will be detected, and the document will be immediately rejected. This will take place **regardless** of network or telecommunications availability. It is important to note that AuthX™ algorithms make allowances for real world wear and tear to which documents are subjected. Barcode encapsulation provides a high level of functionality combined with durability, low fragility and low cost. This makes AuthX™ technology an attractive alternative to the various chip technologies that have experienced issues with cost, fault tolerance, and electro-magnetic stability.

Sabre: The world's leading Global Distribution Systems (GDS). Sabre, the world's leading passenger processing and travel distribution firm, is working with AuthX™ to add greater document and information security to the services they provide. Sabre will use AuthX™ to enhance the travel experience by securely linking the identity of the traveler with itinerary and reservations, payment data, passport and visa information, ticketing and baggage details, hotel and car rental information, etc. This relationship will provide unique and value added interoperability with Sabre and the other Global Distribution Systems.

Auth X: Secure, Scalable, Interoperable

Unique Identifier. In securing a new or existing document, AuthX™ derives a unique document identifier from a number of metrics that contribute to the authentication code. The unique identifier is a character string that can be used in a variety of ways. In a networked database system, it can link multiple types of data by acting as a pointer to various data files stored in any number of databases. It can be used to track a document across jurisdictional boundaries, while at the same time protecting the privacy of the traveler.

Biometrics. In addition to creating the photo template, the AuthX™ system is designed to carry an additional biometric in the authentication code. This biometric can be obtained either when the document is created, or when an existing document is retrofit. A standard AuthX™ barcode can contain two fingerprint minutia templates suitable for 1:1 matching, however larger biometric templates can be carried on larger barcodes or alternate information envelopes. The AuthX™ system has the built-in flexibility to utilize any biometric in use now or in the future, including facial recognition, fingerprint, hand geometry, and iris recognition.

Public/ Private Key Security. AuthX™ utilizes a unique implementation of the Public/Private Key encryption. A second level of encryption utilizing a symmetrical key further enhances system performance. AuthX™ creates pairs of asymmetrical, non-reversible keys. One is used by issuers to create documents, and the other is used by all authorizing entities to read the document. Since the keys are NOT reversible, they are referred to as asymmetric keys.

The writing keys are held in a highly secure environment within the issuing agency. The AuthX™ system is designed to enable the agency issuing documents to create new write/read key pairs as needed. As new reading keys are generated, AuthX™ provides a Key Maintenance System to securely communicate with all of the installed scanning units and provide them with the latest reading keys. The intent is to permit all users the ability to validate any AuthX™ controlled document, so that all authorized agencies can validate all documents regardless of source. This creates a community of users across organizational entities, thus enabling cooperation and automated document tracking through the maze of existing systems and databases today.

Scalability. AuthX™ systems scalability is constrained only by the limitations of the databases with which it must interface. A single workstation can be used to both secure and authenticate documents, and because the authentication code data is so concise (typically under 100 bytes), network traffic concerns are minimized. Hardware availability concerns are also minimized because AuthX™ is designed to work with commercially available PC's, networks, scanners, and printers. This will allow AuthX™ to take advantage of gains in hardware performance and image processing technology as they occur.

Interoperability. AuthX™ was designed to be interoperable with existing systems. The AuthX™ software is written with the intent of fostering open systems thus permitting it to easily interface with a variety of legacy platforms and systems. New developments in mobile and fixed passport and image scanners, hardware and networks can be easily and quickly integrated into the system.

Optical Scanning Technology: The evolution of optical scanning technology has been dramatic and this trend continues. Improvements in general imaging technology and the introduction of the new CMOS imaging chips have lead to increased performance and substantial cost reductions. Other components of the scanner, including the processing chips and memory are also undergoing a revolution in price performance and package size. The result is that manufacturers are today designing smaller, inexpensive scanning devices that are portable, highly reliable, and fully integrated around powerful onboard processors.

Optical encoding and bar code technology is also changing rapidly. New forms of encoding information into an optical readable form are now offering extremely high information density that is far more reliable than what was used in the past. The AuthX system takes advantage of these developments and is designed to accommodate future advances in scanning hardware and optical encoding methodology. Optical scanning allows a document secured with AuthX to be inexpensive to create or retrofit on COTS hardware. The result is an extremely cost effective, highly secure photo identity document that is resistant to both mechanical and electromagnetic damage a document may be subjected to over its lifespan.

Overall System Architecture: Document Registry, Key Maintenance System, Picture Server

Document Registry. Each time an AuthX™ document is created, a derivative of the AuthX™ authentication code will be passed to the Document Registry Database for secure storage. This system maintains a comprehensive registry of ALL documents produced by ALL AuthX™ issuers. The document registry code is small, approximately 100 bytes, and enables a secondary level of verification that insures that a document has not been compromised. This system, maintained in a highly secure environment is essentially a registry of all issued documents, without any of the personal identifying information. This facilitates document tracking and searching of the photo templates to look for altered photos, while at the same time protecting the privacy of all document owners.

Key Maintenance System. AuthX™ supports universal document authentication through a feature called the Key Maintenance System. As new agencies and issuing authorities adopt the AuthX™ system, new reading keys will need to be distributed to allow universal readability. This feature will continue to update

all reading keys along with the information needed to locate photo and text information on these new user documents. When these updates are made, the Key Maintenance System will also provide biometric template reference updates, enabling the introduction of new biometric methods as they are established and implemented. An additional feature of the Key Maintenance System is that each time an update is installed the system will carry out a security audit to detect any intrusions, corruptions, or unauthorized insertions of keys.

This Key Maintenance System will prove extremely valuable to the EES. With a significant percentage of US visitors each year being from Visa Waiver countries, documents other than passports and visas will also have to be addressed by the EES. Drivers Licenses, corporate or students ID's etc. that have already been secured by AuthX™ will be machine-readable and trackable through the EES. This is a powerful architectural feature that leverages AuthX™'s retrofitability and low cost advantages.

Picture Server. This service will be provided to various law enforcement and government security agencies. As documents are secured by AuthX™ technology, the picture associated with the document is sent to the Picture Server. Pictures will reside on the server for a limited period of time before being archived. During this period, authorized law enforcement agencies will be able to search the database in accordance with their needs. The Picture Server database will allow any facial feature recognition algorithm to be used. An important design requirement for the picture server was that it guards the privacy of the public yet provides law enforcement with the information they need to maintain national security.

The privacy rights of individuals will be protected in that only the AuthX™ unique identifier will accompany the picture file. Once a match is obtained, the agency will apply the same judicial practices they follow in wiretap cases to secure the necessary court orders to access the person's identity, location, travel plans, or other available information from the issuing entity. This design architecture guarantees a high degree of personal privacy protection for the public and at the same time protects the various non-government agencies (such as travel GDS's or private industry issuers) from liability.

Mission Critical: The AuthX™ Workflow and Facilitating Timely Border Crossings

The AuthX™ Photo ID Systems provide three levels of document security:

1. The **Base Level** of security is a visual inspection of the AuthX™ enabled document. Because the AuthX™ document is machine-readable and highly secure, anyone contemplating altering the document runs the increased risk of the probability of detection. Thus tampering is discouraged and visual inspection of the document alone is likely to be more robust than with other photo identity documents.
2. The **Elevated Level** of security uses the AuthX™ barcode as a machine-readable "Digital Signature". At a point of entry, a device similar to a standard retail barcode reader would scan the AuthX™ barcode. This would collect the traveler's identity and biometric information, which is contained in the authentication code. This would also confirm that the document has been legitimately processed with AuthX™. The authentication code could be rapidly compared to any watch lists. The time and network infrastructure necessary to do this is minimal because the information needed to make the comparison is less than 100 bytes.
3. The **Highest Level** of security would come from taking each document and doing a complete "full document-full authentication" scan to confirm that the document has not been tampered with in any way. This would also fully authenticate the document and collect the traveler's identity information as

above. The time necessary to perform a full authentication of the document is a few seconds and this time interval is largely determined by the processing power of the scanning unit and processor on site.

Two Specific Issues Raised in the RFI

1. "The Program Office is particularly interested in industry comments on the gathering and processing of biometric identifier data without unduly delaying processing times at the border."

Utilizing AuthX™, biometric information (such as a fingerprint) would only have to be captured once, from that point on the biometric template would be securely contained in the document authentication code. In those cases where full ten finger impressions are captured by automated means, the two fingers used for 1:1 matching by the AuthX™ system can be processed and the minutia templates stored within the AuthX™ authentication code. As stated earlier, the AuthX™ system has the built in flexibility to utilize any biometric in use now or in the future, including facial recognition, fingerprint recognition, hand geometry, and iris recognition.

2. "... how might this issue be addressed as it relates to admitting several foreign nationals arriving at a land POE in one vehicle?"

If all the occupants of the vehicle have an acceptable form of ID that has been secured by AuthX™, the Border Official would only have to quickly scan each barcode using a hand held bar code reader. If only the digital signatures were collected, scanning 5 passports would take little longer than checking out 5 items from a supermarket. If a complete authentication was done on each identification, the time taken would be limited to the speed of the scanners and the processing speeds of the PC's (both of which will continue to improve over time.) Information collected with hand held scanners could be linked to a database by wireless methods, or stored for a period of time then downloaded to a database.

EES: The AuthX™ System Advantage

AuthX™ technology offers the best solution for migrating to an effective entry exit system.

- By enabling the EES to use existing documents where they exist (retrofitting);
- Enabling the use of the existing network and data infrastructure (Efficient data formats and design for interoperability);
- Enabling the linking of information across databases using a common unique document identifier and authentication code;
- Ensuring preservation of personal privacy while facilitating legitimate security inquiries by authorized agencies.

These advantages add up to outstanding price performance for the AuthX™ system.

AuthX™ Integration into the Border Management Process:

The AuthX™ System will serve equally well at **Land, Air, and Sea Points of Entry**, integrating into the Border Management process and playing a significant role at each step in the process.

1. The Pre-Entry Process:

Once the decision to issue a visa is made, it is created at a US Consulate abroad and will include the AuthX™ barcode. The barcode links the applicant's visa, biometric information and passport information in a single secure envelope. The Unique identifier and photo template created with this barcode will be transmitted and stored on the AuthX™ Document Registry. At the same time, a copy of the photo in a common format, will be sent to and stored on the AuthX™ Picture server. The Unique Identifier will then be transmitted, as a database pointer, to the EES system serving points of entry in the US in anticipation of the traveler's arrival. The advantage of this process is that existing foreign passports can then be brought into the AuthX™ system, and the data needed to integrate information from other systems is in a very concise package of less than 100 bytes. Consequently, background checks can be processed and sought individuals identified well in advance of the travel event.

Once the visa is complete and the travel reservation is booked, the AuthX™ unique identifier enables the linking of the GDS ticketing, travel and stay information, with the identity, photo and biometric data of the traveler. This information could then be accessed as required by the appropriate control authorities. With the time and destinations of travel known, the traveler's documents can be quickly scanned, authenticated and referenced to their ticketing as part of the check-in process. This process will also help automate I-94 forms, and link the form to the passport and the travel reservation record. This immediate verification of multiple aspects of the travel process will prove critical in eliminating reservation, ticket, document, and visa fraud. This will help reduce overstays, and unauthorized travel, saving the government and commercial stakeholders tens of millions of dollars a year.

2. The Entry Process: Upon arrival at any land, air or sea, point of entry, the visa/passport combination will be scanned (either as a complete, "full document-full authentication" scan, or as a quick "Digital Signature" barcode only scan). The travelers identity information will be collected, referenced back to a primary EES database, and begin the "clock" on their allotted stay time in the US.

At land border crossings where speed of commerce is an issue, the AuthX™ authentication code can be put into a RF or IR tag to enable machine readable rolling pre-clearance of cross border trucking. The driver and vehicle identification can further be linked to motor vehicle; DOT license and freight manifest information, thus automating the entire land border entry exit process.

Visa Waiver: Citizens of visa waiver countries could be required to have their passports secured by AuthX™ at the border crossing or port of entry. For travelers who do not require a passport, some form of trackable ID will be needed. AuthX™ can retrofit virtually any kind of document that contains a photo of the person and identifying text, and bring it under trackable control. Driver's licenses, existing laser cards, student, corporate or government ID's can all be retrofit and enabled to provide tracking information while the person is in the US. Once scanned, the identity document is processed in the same manner as the visa (described above).

3. The Stay Management Process: The interoperability with Sabre and other GDS's, permit visitors to be tracked through each stop on their travel itinerary, confirming that a traveler is where they are expected, when they are expected. This technological linking has the ability to become the information core of an EES stay management tracking process. Any ID required process, such as domestic travel, or car or truck rental, can interact with the appropriate systems to add to the management of the stay information. Additionally, aliens with student and H1B or similar work visas, could be required to have their ID's scanned, allowing for tracking and verification at the beginning and end of their student or employee status.

4. The Exit Process: Upon exiting, a simple scan of the AuthX™ barcode would quickly record who is departing, when they are departing, and whether they've overstayed their welcome. This data would be compared to the appropriate databases and reported on appropriately. Once again, the data gathered from this transaction is extremely concise and precise. The data demand network infrastructure is negligible and

can easily integrate with technology as limited as 2.4k modems, dial up telephone lines or present wireless (2G) transmission technology. In airline travel, utilizing AuthX™ during boarding will securely and accurately collect Exit information, minimizing the exit lane construction costs, time to implementation, and space issues.

Economic Considerations. AuthX™ technology and secured documents can provide significant economic benefits by its implementation. While Smart Cards and Laser Cards are currently costing the government several dollars each, AuthX can produce or retrofit secure ID's for a fraction of that cost. In the case of commercial airlines, INS fines and the cost of detention for "TWOVs" (traveling without visa) and "document destroyers", will save the industry in excess of \$158 Million dollars³ annually. Other residual effects will be felt in freeing assets of the federal court system by eliminating many of these cases, (and saving millions of tax dollars).

Conclusion: Significant improvements in border management and security have been legislatively mandated. Achieving these mandates will require securing and enabling passports, visas, and trusted traveler cards, as well as driver's licenses, transportation workers credentials, and other forms of identification. The search for appropriate technologies and solutions will need to consider the cost, process efficiency, and the amount of disruption that will be caused by migration. We believe that the ability of AuthX™ to cost effectively retrofit existing documents will prove critical in meeting the challenge of the mandated improvements. And the AuthX™ System Architecture, ease of use and privacy protection will prove driving factors in the success of the United States Entry/Exit System. We look forward to the opportunity to demonstrate the power and versatility of AuthX™.

About AuthX™ Inc. Headquartered in northern New Jersey, AuthX™ was founded in 1997. The company is a privately held, small business concern. The company has several patents pending on its core technologies and unique applications of that technology. AuthX™ has been successfully tested in both border management, and travel processing applications. The company currently has working relationships or technology partnerships with organizations such as, Sabre, Hewlett Packard, AT&T, American Management Services and BearingPoint. These and other partners have significant presence in the Washington DC area.

³ Information extracted from the Department of Justice Immigration and Naturalization National Fines Office Annual Report Fiscal Year 2001 Report. Collateral cost information derived from Lufthansa Systems NA, and represents average costs per incident.