1/10/05

From: [redacted]
To: [redacted]

(b)(6)

(b)(6)

(b)(6)

Sent: Monday, January 10, 2005 3:55 PM
Attach: MOCK POE Test Findings.ppt
Subject: Mock POE Test Overview

I apologize for the first "blank" note you received. Intended to have the attached presentation from the Mock Port of Entry Test that was held the week of 29 NOV 04 included with that transmission.

Attached is an overview of the tests at Baltimore-Washington International airport. For those of you that participated or provided sample readers and/or e-passports/travel document samples, THANK YOU. We really appreciate your participation and/or contribution!

<<MOCK POE Test Findings.ppt>>
Hope you're all having a wonderful start to 2005!

Thanks,

[redacted]

(b)(6)

US-VISIT Program
Phone: [redacted]
Email: [redacted]

E-Passport Mock Port of Entry Test

November 29 thru December 2, 2004

Operational Impact on the Inspection Process

Homeland Security

International Organization for Standardization

5

Mock POE Purpose

- *The primary goal of this Mock Port of Entry (POE) test was to determine the operational impact of using new equipment capable of reading e-passports on the primary inspection process.*

Participating Nations

- United States Belgium
- Finland Sweden
- Essen Group (Germany, Netherlands, U.K.)
- Italy France
- Japan Singapore
- Australia New Zealand
- Canada Brunei
- Austria (provided sample passports only)

Homeland Security

International Organization for Standardization

Test Documents

- Sample Passports provided by manufacturers using consistent data for 13 test subjects (from nation of 'Utopia').
- National representatives with sample passports with their own data
  - United States
  - Australia
  - New Zealand
  - Sweden
  - France
  - Italy
  - Germany
  - Belgium
  - Japan
- Legacy travel documents used by test volunteers
  - Passports (multiple Nations)
  - Other US-issued Travel documents

Homeland Security

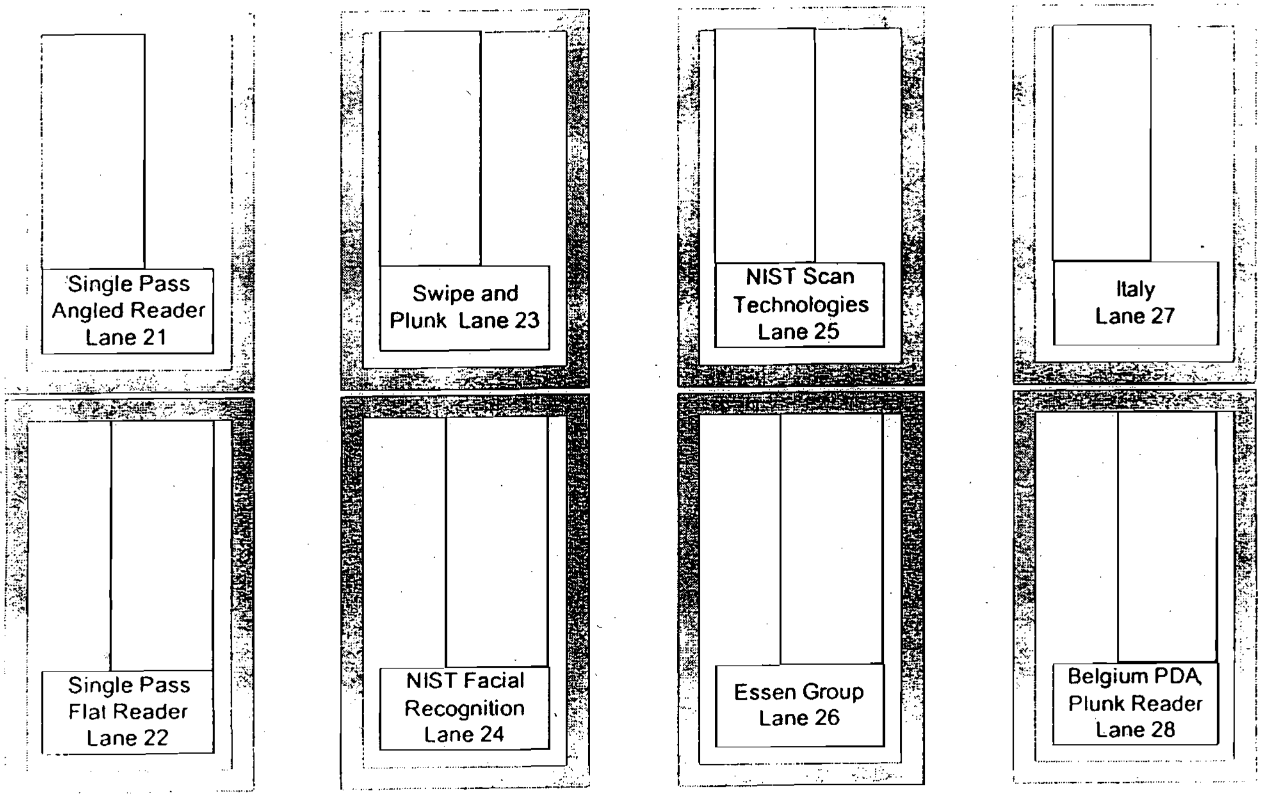
International Organization for Standardization

Technology Alternatives – Imaging

- Fixed camera triggered by inspector with facial matching algorithms comparing against data retrieved from chip
- Continuous video with facial matching algorithms comparing against data retrieved from chip
- Facial capture device operated by traveler to capture full frontal image
- Continuous video capturing 4 best images, performing facial image comparison against them

Note: The Mock POE test was not conceived as a formal biometric test. Accordingly the face camera providers were not asked to supply a face recognition capability. Although one elected to do so, the relevant goal of the session was to determine if images could be effectively collected that would be sufficient to allow good matching.

Technology by Lane



Single Pass Angled Reader Lane 21

Swipe and Plunk Lane 23

NIST Scan Technologies Lane 25

Italy Lane 27

Single Pass Flat Reader Lane 22

NIST Facial Recognition Lane 24

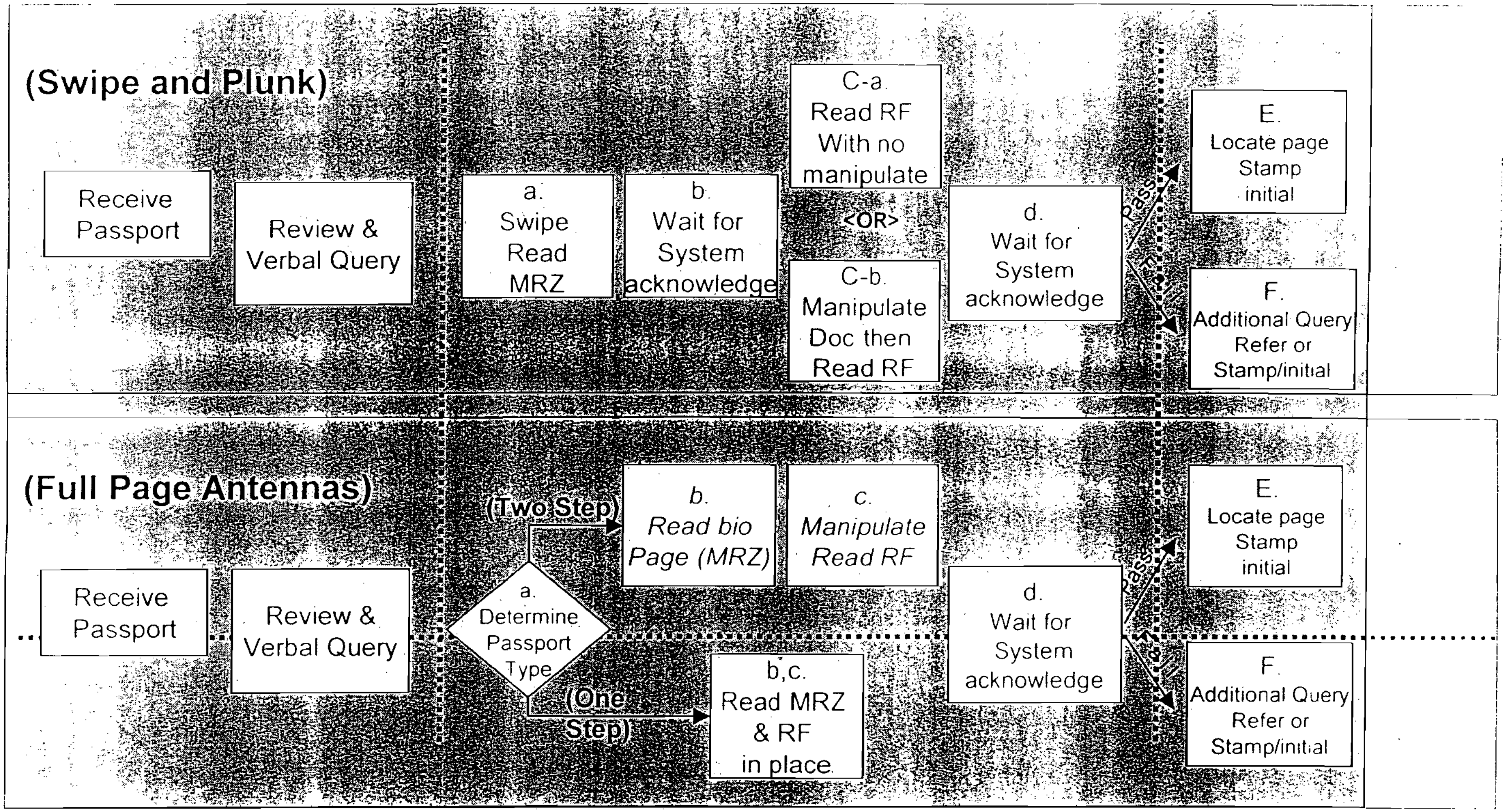
Essen Group Lane 26

Belgium PDA, Plunk Reader Lane 28

Homeland Security

International Organization for Standardization

Process



(Swipe and Plunk)

Receive Passport

Review & Verbal Query

a. Swipe Read MRZ

b. Wait for System acknowledge

C-a. Read RF With no manipulate

<OR>

C-b. Manipulate Doc then Read RF

d. Wait for System acknowledge

Pass

Fail

E. Locate page Stamp initial

F. Additional Query Refer or Stamp/initial

(Full Page Antennas)

Receive Passport

Review & Verbal Query

a. Determine Passport Type

(Two Step)

b. *Read bio Page (MRZ)*

c. *Manipulate Read RF*

(One Step)

b,c. Read MRZ & RF in place

d. Wait for System acknowledge

Pass

Fail

E. Locate page Stamp initial

F. Additional Query Refer or Stamp/initial

Homeland Security

International Organization for Standardization

Insight

If technology does not enhance or improve the existing process flow, new reader technology solutions will not be well received by the POE officer/inspector community.

Any solution implemented needs to be better than or equal to the current process, with minimal impact on the inspector.

Homeland Security

ISO International Organization for Standardization

Major Findings

- Insufficient power to read all variations of chips on many readers
- Inability to properly handle different chips read rates (424/848)
- Lack of use of digital signature verification in systems and only partial implementation of alternatives in others
- Most units required knowledge of where chip was in order to perform accurate read, required substantial manipulation of the passport.

Homeland
Security

ISO

International
Organization for
Standardization

Major Findings

- Readers require too much attention and time on the part of the inspector.
- Instructions on the reader distract the inspector, e.g. electronic displays.
- Lack of proper feedback to the inspector on WHEN to remove the passport.
- Footprint of the units interferes with inspector operations.
- Some readers required the inspector to hold the passport firmly against the unit in order to perform the read. This means the inspector is not able to perform other parts of the inspection.

Homeland Security

ISO International Organization for Standardization

Major Findings

- Full page readers have problems reading MRZs of worn or bent passports requiring inspector to press the passport firmly against the unit.
- Some full page readers required the inspector to read the MRZ and perform the chip read in separate movements.
- Correction of MRZ for Basic Access Control is subject to human error particularly when dealing with characters like zero and "O".
- Readers do not have consistency in handling type A and Type B chips.

Major Findings

- Electro Magnetic Interference (EMI) issues are still a factor (e.g. if two readers are too close to one another).
- Shielding of passports may make the chip unreadable when the data page is read on flat bed readers if the chip is on the other side of the shield from the data page. The plunk readers are required to have the book open instead of closed.
- Some systems could not handle legacy travel documents.
- Wide variation in speed of access and processing.
- Mobile unit proved highly successful.
- More research is needed on impact of stapling on e-passport.

Facial Image Acquisition

- Three different configurations used
  - Video using face finding via motion detection (2 versions)
  - Separate unit with traveler adjusting a mirror to see eyes
  - Still image triggered automatically by system
- Note: Existing US system has camera triggered by inspector and was at the port of entry. Still images already exist in the US-VISIT databases for this configuration.

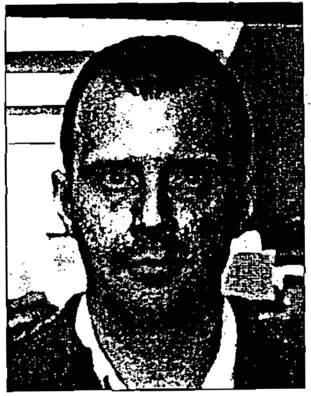
E-passport images from chip

Images retrieved from data page in e-passport

Images from live video systems

Images from self-adjusted unit

Image from still camera automatically activated by system



Homeland Security

ICAO • OACI • ИКАО

ISO International Organization for Standardization

Facial Capture - Findings

- Placement of camera critical
  - Recommend placement behind inspector.
  - System should be self-contained; no optical parts adjustable by officers.
  - Depth of field should extend from 8 inches on inspector's side to 2 feet beyond counter.
  - Special accommodations may be necessary for people in wheelchairs (standard fixed location cameras could not capture their faces with full-frontal pose).
- Illumination
  - Infra-red lighting should be built into the camera box.
  - Visible lighting must be examined on a location-by-location basis.

Homeland Security

International Organization for Standardization

Facial Capture - Findings

- Client application must display live and best-so-far image
- Officer must inspect images before final acceptance
- Automated quality control analysis of image may be helpful (e.g. verify image captured is specification compliant)
- Images scanned from e-passport data pages will probably not be reliably usable for automated comparison against image stored on the chip
- Compression/Decompression of images stored on some e-passports caused the image extracted to be of too poor a quality for automated facial comparison.
  - Images should be compressed only once in the process of creating the chip and must meet the guidelines of ICAO.

Homeland Security

ISO International Organization for Standardization

Additional Considerations

- Inspectors must keep their eyes on the traveler at all times
- The ‘feel’ of the passport has been a part of fraud detection and inspectors will require training on the new versions
- E-passports with anti-skimming technology embedded in them will require that the passport be open for reading. All types of readers will have to read the chip regardless of where it is located. (That is, on either ‘fold’ once the book is placed flat on the reader)

Homeland Security

ISO International Organization for Standardization

Next Steps

- Interoperability test in Japan during March is still very much needed
- Live test parameters will be refined based on findings of this mock port of entry session
- Refinements in readers necessary before nations can effectively integrate reading e-passports into existing inspection process
- ICAO / ISO development of a common set of core requirements to be presented to industry for 5 scenarios:
    1. Primary Inspection
    2. Mobile Inspection
    3. Self-service Kiosks
    4. Secondary / Document Investigation
    5. Production Quality Control

Homeland Security

ISO International Organization for Standardization

Technology Alternatives - Readers

- Full Page
  - Flat reader and flat antenna
  - Flat reader and angled Antenna
- Swipe and Plunk
  - Separate MRZ swipe and semi vertical reader
  - Separate MRZ swipe and slotted reader
- Simulated Swipe with Plunk
  - MRZ in data file with flat reader
- Mobile reader
  - PDA with reader attachment (no MRZ read)

Homeland
Security

International
Organization for
Standardization

From: [redacted] (b)(6)
To: [redacted] (b)(6)
Sent: Thursday, January 08, 2004 10:00 AM
Attach: VWP WG Meeting (6 JAN 04).xls; Inc 2 VWP WG Minutes (6 JAN 04).doc; Inc 2A CONOPS (5 JAN 04).doc; Increment 2 PMP (7 JAN 04) 98.mpp
Subject: VWP WG Meeting 6 JAN 04

All:

The attached files represent the VWP WG meeting held on 6 JAN 04 here at the US-VISIT office. The files include an MS Excel list of attendees, an MS Word file with the minute meetings, and a copy of the DRAFT Increment 2A Concept of Operatoins (CONOPS) for those of you that did not receive the initial DRAFT distributed with the meeting reminder/agenda. Also attached is an updated MS Project schedule file.

Please review and let me know if you have any questions or comments.

Thanks, and hope everyone can make it to the next meeting schedule for 27 JAN (Tuesday) at 1400 here at US-VISIT.

[redacted] (b)(6)

<<VWP WG Meeting (6 JAN 04).xls>> <<Inc 2 VWP WG Minutes (6 JAN 04).doc>> <<Inc 2A CONOPS (5 JAN 04).doc>> <<Increment 2 PMP (7 JAN 04) 98.mpp>>

US-VISIT Visa Waiver Working Group
Attendees 6 JAN 04

Name	Organization	Phone	E-mail	Initials
[redacted]	MITRE	[redacted]	[redacted]	
[redacted]	US CIS	[redacted]	[redacted]	
[redacted]	DOS (GDS)	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	NIST (West)	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	NIST	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	DOS (CA)	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	US CIS	[redacted]	[redacted]	
[redacted]	MITRE	[redacted]	[redacted]	
[redacted]	NBSP	[redacted]	[redacted]	
[redacted]	MITRE	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	US CIS	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	Prizum	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
(b)(6)		(b)(2)	(b)(6)	
		(b)(6)		

From:
To:
Cc: [redacted] (b)(6)

Sent: Friday, November 05, 2004 6:12 PM
Subject: Re: 2A: Brief Notes on NIST Test Scope

[redacted], thanks for writing this up. A couple of amendments / thoughts: (b)(6)
I don't yet have cameras, nor do I have their dimensions. These will be forthcoming.

Also I DO think some footprint / space issues may occur and that I suggest we accept them on the grounds that this is a mock test. I indicated that I think ultimately a formal requirements document would include spatial constraints of the final operational environment and these would be based on the findings of the BWI test.

Timestamping of ALL captured data will be sufficient to do post-test alignment of data recovered from passports and cameras.

[redacted] (b)(6)

Quoting [redacted]@accenture.com:

> Hi everyone,
>
> I spoke with [redacted] yesterday about the scope of NIST camera/picture (b)(6)
> quality and automated facial recognition (AFR) tests in parallel to our
> mock test. First of all these tests are outside our direct scope (they
> are NIST's), but they interact with our test.
>
>
>
> So basically NIST will be testing:
>
> - Five (5) cameras, one with the Essen Group (UK, Germany, (b)(6)
> Netherlands) including AFR. The other four (4) cameras [redacted] intends
> to set up in each of our four (4) lanes/booths connected to a separate
> laptop which he will bring for each lane. We will need to identify on
> set up (11/29) whether they'd encroach on the Officer's space, but we do (b)(6)
> not anticipate so ([redacted] has camera dimensions as well as the
> cameras')
>
> - There will be no integration between NIST's tests and ours.
>

> > which can be "feeded" with two pictures and returns an match score?
>
> No. I have commercial face recognition engines only - I
> cannot distribute them because
> of a license agreement. But I could send an API (.dll) which
>
> 1. has the proposed interface
> 2. reads two JPEG files - but just returns a random
> number! We would integrate the
> real face-rec system later.
> We have wrapped three different face systems in a
> single API and have been
> testing with it since January 2004. So it works. I
> can send the C++
> wrapper to you.

That would be great! The best way to do this would be providing a DLL with dummy functionality which can be exchanged in Baltimore by a dll with the real functionality.

> An alternative, of course, is can you send a golden reader
> to me at NIST?

The reader is no problem, the sources may be a little bit more complicated and I have to coordinate this with our customer.

I ask [redacted] or [redacted] what to do in this case. Meanwhile we preparate the golden reader for the process as described above.

(b)(6)

Regards

[redacted]

(b)(6)

From: [redacted] (b)(6)
To:
Sent: Wednesday, October 27, 2004 3:48 AM
Subject: Re: Summary of BWI Visit and Decisions

Hello [redacted]

> I was under the assumption (from [redacted]talking to [redacted] (b)(6)
>[redacted]) that you
> would come to the US to do some integration.

Yes, we do, but not before the Baltimore testing in the week November 29th (that's my understanding so far...)

> I'm not sure which option you prefer here:
> 1. Passport reader then camera.
> 2. Camera then passport reader.

I think first camera than passport reader. And taking the picture also starts the passport reading process.

> How about this sequence.
> 1. Visitor hands passport to operator.
> 2. Operator places passport on reader.
> 3. Operator instructs visitor to look at camera.
> 4. Operator clicks a GUI button. This initiates two
> independent actions:
> 1. Reader accesses chip.
> 2. Camera takes photograph.

The design of the Reader Tool at the moment only allows sequential actions. So the sequence would be:
4a. Request photograph from camera-api
4b. Camera returns handle to JPEG
4c. Access chip data
4c. Reader returns handle to JPEG

> 7. Recognition engine is called, returns match score.

> I agree. Some face rec system produce match scores on
> different ranges (not [0,1]).
> This implies a need for interpretation based on the
> impostor distribution.
> Small detail to be handled later.

That's ok. Range adaption is no problem. I'll be very happy when we are at this point :-)

> > - Can you provide us with the recognition engine and a C/C++ api,

> > which can be "feeded" with two pictures and returns an match score?
>
> No. I have commercial face recognition engines only - I
> cannot distribute them because
> of a license agreement. But I could send an API (.dll) which
>
> 1. has the proposed interface
> 2. reads two JPEG files - but just returns a random
> number! We would integrate the
> real face-rec system later.
> We have wrapped three different face systems in a
> single API and have been
> testing with it since January 2004. So it works. I
> can send the C++
> wrapper to you.

That would be great! The best way to do this would be providing a DLL with dummy functionality which can be exchanged in Baltimore by a dll with the real functionality.

> An alternative, of course, is can you send a golden reader
> to me at NIST?

The reader is no problem, the sources may be a little bit more complicated and I have to coordinate this with our customer.

I ask [redacted] or [redacted], what to do in this case. Meanwhile we preparate the golden reader for the process as described above. (b)(6)

Regards

[redacted] (b)(6)

Projektbereichsleiter Security Applications (NL Essen)
Security Networks AG Tel [redacted] (b)(6)
Im Teelbruch 116 Fax : [redacted]
45219 Essen E-Mail: [redacted]

1072/04

From:
To:

(b)(6)

(b)(6)

Sent: Saturday, October 02, 2004 10:59 PM
Attach: Task Force One.doc
Subject: ICAO/WG3 Task Force One

Greetings

At the ICAO New Technologies Work Group (NTWG) meeting in Tokyo last month, the =ecision was made to allow the three ad hoc task forces, created at last =uly's London meeting, to dissolve. Related to that, the NTWG directed =SO/SC17/WG3 to create the organizational framework and process to carry out the work =ssociated with advising and serving the needs of the NTWG in all matters including =he development and maintenance of the full suite of 9303. These matters =ere addressed at the WG3 meetings immediately following NTWG and were held =n Kyoto. In brief summary, Task Force One was designated as the entity through which these =TWG responsibilities would be carried out. The attachment outlines the terms =f reference as approved at Kyoto.

In =/span>Kyoto, we decided that Task Force One would have a meeting in the =/span>United States on November 30 and =/span>December 1, =004. This message constitutes the calling notice for that meeting. Note that those =ates coincide with the Mock POE activities to be conducted at =altimore-Washington International Airport (BWI). The Task Force meeting will be held at or =ear the BWI airport.

At this point I intend to cover a wide range of issues, =ncluding:

- Organization and procedure =f TF1
- Pending matters from TAG =nd related
- Contactless chip =nteroperability/Annex K/other Biometric Deployment TR issues
- LDS =[redacted], project =ditor) (b)(6)
- PKI =[redacted] project editor)
- Biometrics [redacted], lead)
- Country-specific initiatives/updates/plans
- Outlook and =ision
- System integrity =nhancements

This distribution list is a compendium that I =ave constructed based on related sessions over the past year or so. If you =ee an omission, please pass the message on and let me know you have done so. I welcome any additional agenda items you care to submit for =onsideration. Lodging and logistical details will be available shortly. Please let me know =u>no later than October 17 if you would like to attend. As always, =ttendance may be limited due to capacity of facilities. I will request that this announcement be posted to the NTWG and WG3 web sites. I look forward to =ery productive meetings. Best wishes.

[redacted] (b)(6)

[redacted] (b)(6)

e-mail: =/span>=st1:PersonName>jetlag10@earthlink.net=o:p>

[redacted]

Principal

[redacted] (b)(6)

Fall =ill Associates, LLC

Task Force One/Interoperability--Responsibilities and Issues

1. What is the definition of the terms of reference?
   - Short Term
   - Long Term
   - Continuing

2. What are the deliverables?
   - Draft technical reports and revisions of current documents
   - FAQ statements, e.g., clarifications, amplifications, interpretations
   - Updates, e.g., CanMorSyd
   - All of the above to constitute "Supplement—9303"

3. Mechanisms and procedures
   - Reviewing documents extant
   - Modifying/updating/identifying areas for rewrite and revision
   - Drafting documents
   - Sanctioning recommendations to NTWG to publish/distribute our products
   - Managed distribution lists to communicate and activate various activities
     - Drafting
     - Reviewing
     - Approval

4. Specific work items at this time
   - Defined information gathering and exchange framework
   - PKI version 2/coordinated by TF5
   - LDS version 2
     - Update capability
   - Biometric Deployment TR harmonization/oversight/revision/communicating
     - Monitoring and review of SC37/incorporation into 9303 as appropriate
   - e-Visas
   - Vision
   - Simplify!
   - Simplify!!
   - Simplify!!!

10/01/04

From: [redacted] (b)(6)
To:

(b)(6)

US – VISIT PROGRAM
OFFICE OF THE CHIEF STRATEGIST
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

2 page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Title 5, United States Code, (U.S.C.) Section 552 (FOIA)					**Title 5, U.S.C. Section 552a(PA)**	
		(b)(1)		(b)(7)(D)		(d)(5)
		(b)(2)		(b)(7)(E)		(j)(2)
		(b)(3)		(b)(7)(F)		(k)(1)
		(b)(4)		(b)(8)		(k)(2)
		(b)(5)		(b)(9)		(k)(3)
X		(b)(6)				(k)(4)
		(b)(7)(A)				(k)(5)
		(b)(7)(B)				(k)(6)
		(b)(7)(C)				(k)(7)

Documents originated with (an) other Government agency(ies). These documents were referred to that agency for review and direct response to you.

__pages contain information furnished by (an) other Government agency (ies). You will be advised by the FOIA Office to the releasability of this information.

_______pages have not been provided to you at this time because a final release determination has not been made. You will be advised as to the disposition at a later date.

For your information

Page(s) 2-3 of a 5 page email is being withheld in its entirety under FOIA exemption b(6).

(b)(6)

Sent: Friday, October 01, 2004 11:33 AM
Attach: READERQS.DOC
Subject: ICAO Mock POE Clarification Note

Hello, all.

The purpose of this e-mail is to clarify a few issues that have been raised following the initial ICAO Mock Port of Entry (POE) Test notice that went out two weeks ago.

This test will be different than the one that was hosted by DHS US-VISIT in Morgantown, West Virginia, the last week of July. The ICAO Mock POE Test will be an operational and process exercise (versus the interoperability focus that was exercised in West Virginia's test). The one like feature of this event and the one in July is that there will be no results publicized and no decisional impacts will come of this exercise. We want to reiterate the focus will be on operability and processes, not on the technology.

We are very pleased to have received so many responses from those of you that will be providing sample passports, readers and Application Program Interfaces (APIs). As a friendly reminder, we request those be sent by 15 OCT 04. Please send to:

Attn: [redacted] (b)(6)
DHS US-VISIT Program Office
1616 North Fort Myer Drive, 18th Floor
Arlington, Virginia 22209
USA

Please use my phone number for shipping reference: +1 (202) [redacted] (b)(2)

Though it was not spelled out in the initial notice for this test, actual participants will be limited only to governments and representatives of their authorized staff. This is not an open, public, vendor participation event. Though we do ask that those of you sending readers and APIs provide a point of contact (POC) name and contact information should there be any difficulties integrating your unit with our workstations. As for those who are providing sample e-Passports, please identify the specifics of your samples (e.g. chip type, passive/active, BAC, antenna size, etc.).

Also, please be advised that whatever products you ship to us by 15 OCT 04 will be the actual items used during the test the week of 29 NOV. The Governments may or may not use all products sent.

In addition, for your review, the attached file below answers some of the questions received to date.

Thank you again and again for such an overwhelming response and willingness to participate. We look forward to receiving your products by October 15th.

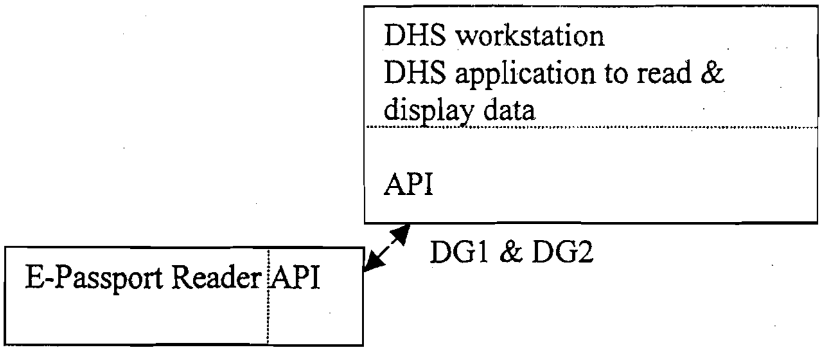
Thank you, and have a great weekend!

[redacted]

[redacted]
US-VISIT Program
Phone: [redacted]
Email: [redacted]@dhs.gov (b)(2)

<<READERQS.DOC>>

System Configuration



Communication channel

We are open to your design (USB ,serial, etc.)

Data transfer and processing

We would need your DLL (API) for the workstation.

You don't need to actually emulate an MRZ reader -- just let us know the how your API is constituted so we can read the MRZ data and the picture from the chip. We don't need you to do anything specific with the picture display as long as we can receive the picture data through the API.

e-Passport

We are interested in having some samples that meet the ICAO LDS so that we can test the operations (not the performance of any particular reader). A solution with an inlay attached to a regular passport is acceptable.

We will be able to provide the digital pictures of the volunteers, if you can produce any samples. We have about 15 volunteers, but we don't expect any one vendor to be able to provide that number of samples. Please let us know what you feel is realistic (anything is appreciated!)

What we expect of the e-passport is simply something where we can test the process of reading it. The printed page will be important to compare the MRZ data in the chip with the printed data page. The e-passport should be encoded according to ICAO specification so that we can retrieve the information and (hopefully) perform facial recognition.

Extra PC

We don't need you to provide a PC -- just the reader & API.

E-Passport Mock Port of Entry Test

November 29 thru December 2, 2004

Operational Impact on the Inspection Process

Homeland Security

International Organization for Standardization

See previous slides under message 01/10/05 (pages 4-22_

e-Passports Interoperability Test Session
July 27-29
Morgantown, West Virginia, USA

Hosted by the
United States Department of Homeland Security (DHS), US-VISIT Program
At the Facilities of the
National Biometric Security Project (NBSP)

Summary:

This session provided an opportunity for organizations involved in the production of e-Passports and in the development of equipment to access the information from e-Passports to come together in a non-competitive environment in order to work towards establishing interoperability of their products. Approximately 130 persons from 18 nations, representing over 50 organizations were present. Chip and passport integrators provided 128 prototype samples for use in testing chip and passport readers. By the end of the session, the technical staff of the participating organizations was able to establish basic interoperability for a broad set of prototype e-Passports and readers.

Background:

The International Civil Aviation Organization (ICAO) approved a set of technical documents that define e-Passports at its Technical Advisory Group (TAG) meeting in May 2004. An e-Passport consists of a standard passport that conforms to the existing passport guidelines set by ICAO, such as inclusion of a machine-readable zone (MRZ) and a photograph on the data page, but also includes a contactless integrated circuit (IC) chip that is encoded with biometric and biographic information. ICAO adopted standards for the contact-less chip and for biometric data that were established by the International Standards Organization (ISO). The ISO standards were written to establish a certain level of conformity in the marketplace, but also allow for multiple types of applications. ICAO had the task of selecting the various options in the ISO standards that were applicable to its needs and specifying specific approaches to areas not covered in the ISO standards. After a series of joint ICAO/ISO meetings, culminating in a meeting held June 17, 2004 in London, most of the apparent technical issues and specifications were resolved. At that meeting, the DHS representative offered to host a testing session in July for manufacturers and integrators to come together and test whether their interpretations of the standards were, indeed, similar and would allow for interoperability (the ability to have an e-Passport produced for one nation read by readers produced by other companies and placed at various locations around the world, and for the readers to read all of the e-Passports presented to it). Australia also offered to host a session in late August 2004.

DHS utilized the mail lists from the ICAO e-Passports task force and from the ISO Working Group that co-chaired the London meeting to invite participants to the testing session. The e-mail received broad circulation and resulted in several groups expressing a desire to participate.

Session Format:

Chip and e-Passport manufacturers brought samples of their products that were encoded with the 'Silver Data Set.' This data set contained information conforming to the 'Logical Data Structure' (LDS) as defined by ICAO. In this manner, a similar set of encoded samples could be tested. The Silver Data Set was developed by the 'Essen Group' which is formed by representatives from the Netherlands, Germany and the United Kingdom. Participants were also encouraged to provide variants from the Silver Data Set that included different (authorized) methods of storing the photograph (JPEG 2000) and also that represented Basic Access Control and Active Authentication, as well as samples encoded as 'non-passports' to test the effects of multiple chips in the read range.

The US-VISIT/NBSP team logged-in all of the chip and passport samples brought to the session. They maintained strict control of the samples at all times, enforcing a check-in/check-out procedure. Passport reader manufacturers could request samples for testing their units . If the vendor had problems reading or using the sample, the reader vendor and the chip/passport manufacturer could get together to resolve issues uncovered during the test. E-Passport manufacturers could also bring their samples around to the reader manufacturers to ensure that their samples were tested on all of the units. Each passport reader manufacturer had a separate work area in the NBSP laboratory. The layout allowed representatives from the participating companies to work together and discuss issues freely and openly.

Independent test teams chaired by professors from West Virginia University were made available to the participating groups to record results. This process made it possible to discern any common pattern to the testing or detect unresolved interoperability issues. The chair of the testing session assured all of the participants that the summaries would be presented in a manner that did not 'rank' the results. Companies would not be specifically identified in the published results -- only the technical and procedural issues would be covered. This agreement, established at the beginning, greatly increased the spirit of cooperation, and this report will maintain that approach to anonymity in the test analyses.

US-VISIT requested that the National Institute of Standards (NIST) bring equipment to the test sessions such that they could demonstrate eavesdropping and jamming with the prototype readers brought to the session. This is not an interoperability issue, but is a usability issue. This capability served to familiarize the manufacturing community with the problems that will be faced by users of their equipment in certain environments.

While testing was occurring, the organizers held four discussion periods to allow the exchange of ideas:

- Durability
- Ergonomics
- Skimming and Eavesdropping
- System Fallback Procedures

A 'Discussion of Interim Results' of the testing and a final wrap-up session ensured that the principal issues raised by the testing were discussed in a broad forum.

Results:

The Host of the Session stressed in his opening remarks that the purpose of the event was *NOT* to re-write or revise ICAO documents. If issues arose during the testing, they would be addressed by stating a 'recommended interpretation' of the ICAO documents in order to ensure maximum interoperability. That is the approach that is followed here. The following four issues were raised by participants:

Issue 01: File Select Command (7816-4 read short)

Description: Two valid alternative read sequences are supported within reader applications: select by file identifier (SID) and read short."7816-4 is a tool box of available commands, there is a need for an instruction sequences be defined". Note: There is a limited address space (five bits, 31) for file identifiers in the LDS. Select command supports three options (AID, p1, p2).

Reference: LDS, v. 1.7, table A1 (section 11.1), Annex K (K.15)

Recommended clarification to LDS table A1, section 11.1 for interoperable implementation:

Select Application:
The first 7816 instruction is "select application", with the code 00A4 04 0C 07 A0 00 00 02 47 10 01. Every machine-readable travel document (MRTD) application supports the select command. Reference ISO 7816-4 (table 5, section 5.1.3) for complete return codes.

Select File:
The MRTD supports both methods (select file and read short). Readers support at least one of the two methods. The file identifier and short file is mandatory for the [card] operating system, but optional for reader.

Read binary:
Le must be one byte, and must be encoded per 7816-4.

Other: The clause "*by the reader*" is understood as implied in the LDS anywhere that 'select file' is stated as optional.

1.5 A/m has been observed to be too low for some chips. Manufacturing variances must be accounted for, yet balanced against the desire to operate at low field strength (for efficiency reasons and to reduce the risk of skimming). Also, reader manufacturers require clarification of how the field strength is measured and calibrated (loaded versus unloaded).

Recommended interpretation for interoperable implementation:
To ensure maximum interoperability, a card is recommended to operate between 3 to 7.5 A/m. However, 1.5 A/m is within the standard. The lower target level of 3 is to account for card variances that may result in lower actual values. The measurement of the field shall be according to ISO 10373. Ideally, the ISO 10373 field measurement card must be adapted to include ID-1 size (passport document). Until such time, the field strength shall be measured according to ISO 10373.

A related issue for consideration is to provide a mechanism for the reader to dynamically vary field strength, for example when there are multiple cards in the field.

Issue 03: PC/SC & device application programming interface (API)

Description and Background: There are no normative specifications for APIs between reader and host. PC/SC recommended, but is acknowledged to be incomplete. Issue is being addressed within ICAO (Annex K).

Reference: Annex K (K.19)
Recommended interpretation for interoperable implementation: As mentioned in Annex K, a new PC/SC standard for contactless cards is forthcoming. Until such time the existing standard, PC/SC 2.0, shall be used as an interface between chip reader and host.

Issue 04: 5ms delay after field reset

Description and Background: Per ISO standard, the reader request must wait 5ms prior to read after a field reset; however, Type A cards may require (and request) an extended initialization period.

Recommended interpretation for interoperable implementation: The card reply shall be within 20 ms.

Note: The above statement reflects the recommendations of those present, however, conflicts with existing standards. ISO allowance for cards to request additional time is pending.
Related note: Common exceptions in ISO standards are desired to provide readers the opportunity to provide more optimal reads as well as more robust recovery and retry behavior.
The following observations were made:

In accordance with ISO/IEC 14443-3:2001 and latest clarifications in pending amendments, an e-Passport shall answer a Request command from a reader (either REQA or REQB, depending on e-Passport type) in each of the following test cases:

Test case 1: the passport reader continuously idles for a passport by alternating REQA and REQB commands, the start of one being 5 ms after the end of the other and vice versa.

Test case 2: with the e-Passport placed in the operating volume, the passport reader activates the RF field, then sends a single REQA 5 ms after this activation and then sends a single REQB 5 ms after the end of the REQA.

Test case 3: with the e-Passport placed in the operating volume, the passport reader activates the RF field, then sends a single REQB 5 ms after this activation and then sends a single REQA 5 ms after the end of the REQB.

Clarifications issued prior to the meeting:

1. *Regarding the contents of the SOD as presented in the Silver sample :*

> *The last 128 bytes represents a digital signature .*
> *Please clarify the content of the data to be signed.*

Answer 1:

The PKI report describes the syntax of the SOD-File.

The hashes of the present DGs are encoded in an ASN.1-Syntax which is again encoded in a "Signed Data" structure. The hash of these Signed Attributes is signed using RSA/DSA/ECDSA. See "TECHNICAL REPORT PKI for Machine Readable Travel Documents offering ICC Read-Only Access Version - 1.0 Date - April 21, 2004"

The signature in the EF.SOD conforms with PKCS1 SignatureFormat. It has the format 01 || PS || 00 || T where T is a DigestInfo structure. The length of this format is exactly the modulus length and PS is used to fill it with FF to that length. The DigestInfo contains the used hash algorithm (SHA-1) and the calculated hash value.

The hash value is calculated to conform to the RFC3369 Cryptographic Message Syntax. This means that the signature is calculated over the DER encoding of the signedAttrs of the SignerInfo structure. In the case of EF.SOD, the signedAttrs contain only the minimum required attributes, content type and message digest. The content type is the eContentType of the encapContentInfo of the SignedData structure (i.e. 1.2.528.1.1006.1.20.1). The message-digest contains the calculated hash value (SHA-1) of the value of the eContent of the encapContentInfo of the SignedData structure (i.e. the DER encoding of the LDSSecurityObject as defined in the ICAO TR PKI). The LDSSecurityObject contains the hash values (SHA-1) of all available DataGroups, in case of the Silver Data set, DG1 and DG2. These hash-values are calculated over the complete contents of the DataGroup.

2. Referring to ver 1.7 Appendix 2 to Annex A pg 65
Subheading: Examples for ISO 7816 usage with LDS:
The first row in the table after the heading has "0A 00 00 02 47 10 01" for the data column and "Select Issuer Application" in the remarks column.
This evidently suggests that the Issuer Application AID (Application ID) is "0A 00 00 02 47 10 01"

However, in other sections in the documentation (ver 1.7), the Issuer Application AID is stated as "A0 00 00 02 47 10 01". Refer to Figure A.1 (page 52), Figure A.13 (page 46).

Answer 2: This is a typo that should be corrected. A0 00 00 02 47 10 01 is the correct AID.

3. The ICAO website has LDS v1.7 published. However the 'silver' reference data that you sent is based on LDS v1.6 (as designated in the EF.COM) Should we then assume that LDS v1.6 or v1.7 testing will be performed?

The main impact will be the Selection of Master File command. There is a difference between LDS v1.6 (page 61) and LDS v1.7 (page 63).

Also, with regard to DG1 data elements 03 (Name of holder) and 12 (optional data), LDS v1.7 has varying sizes for ID-1, ID-2 or ID-3 sized documents. LDS v 1.6 specified it as static sizing. If we are only testing passports with inlays, then it should not be a problem (same size); however, I am assuming there will be others bringing prototypes in card (ID-1) format.

Answer 3:

The editorial syntax for V1.7, page 63 is misleading.

The correct syntax is either
'00' 'A4' '00' '0C' Empty Empty Empty

Or

'00' 'A4' '00' '0C' Empty Empty MaxRet

The difference between the commands is: The first one just returns 0x9000 in case of success, the second one returns the File Control Parameters of the selected file (see LDS 1.x, x<5)

ISO Compliant cards have to support both commands and reading software should be written in a way that additional return information does not kick it out..

ISO Compliant cards should work with both commands, but it has to be a valid command, not the one described in V1.7 (see above). By the way: for reading EF.COM to detect the LDS Version, you already may have used the select command. Iit does not make sense to change the behavior of the software depending on the LDS –Version.

For the second part of question 3: For now LDS only considers passports (part 1 ICAO Doc 9303). Of course, visa and other documents have different length in the MRZ fields and lines, which is standardized by Doc 9303. In any case, the length of the MRZ should be FIXED as in LDS 1.7. Which FIXED LENGTH to be used should be governed by Doc 9303 corresponding to document type. In all cases, LDS and optical personalization should correspond. This has to be amended in the LDS TR (eventually).
Version 1.6 is the reference, used in the silver data set (there was no version 1.7 at that time of its preparation).

Fixed/not fixed: DG1 contains exactly the complete MRZ as it is printed (visible) on the document.

General:

While enormous amounts of time and effort have been expended going over the documents carefully to correct typos, there may well be other typos that will become apparent as we begin to implement. These will be corrected at some point in the future when sufficient time has passed that we can be certain all necessary changes have been caught. We should make every effort to move to LDS 1.7 as now published on the ICAO web site, recognizing the 'anomalies' in it such as have been pointed out here.

www.icao.int/mrtd/download/technical.cfm

Panel Discussion Summaries:

Forum 1: Durability

How confident are we that the inlay will be functional for the full 10 year life expectancy of the e-Passport? Will physical aging of the polymeric inlays cause a problem several years from now?

Many ISO tests are derived from tests on smart card/credit card type products that typically last three-five years. Are the tests that we are considering really going to be able to predict successful behavior over the 10 year life span? Accelerated aging tests may be performed, but only a real ten-year test will adequately address this issue.

What are the likely mechanisms of document failure, and do the proposed ISO standards adequately address these mechanisms?

The authors of the proposed ISO standard posted that document on the LAN available to all participants at the testing session and asked for direct feedback. This document addresses broad topic areas, including environment and wear.

Forum 2: Ergonomics

The principal purpose of this session was to highlight that not all technical solutions to reading e-Passports may be practical. Several potential uses of e-Passport readers were discussed:

- Port-of-entry
    - Direct inspection of the e-Passport by the inspector and placement in/on the reader by the inspector
    - Facilitated inspection systems with the traveler placing the e-Passport on a reader incorporated into a biometric-based inspection kiosk
    - Staged inspection with the travelers placing the e-Passport on a reader located prior to the inspection booth
- e-Passport issuance
    - Quality control during production at the production facility
    - 'Self-service' units available to persons picking up their e-Passport and wishing to verify the contents of the IC chip
- Government service
    - Verification of identity based on biometrics in the e-Passport when the holder requests certain services, such as welfare payments
- Private industry
    - Banking facilities using kiosks equipped with e-Passport readers

Each of these situations has a slightly different set of requirements relating to ergonomics. However, some common threads emerged:

- Units should have a status indicator (on/off)

- For units requiring placement of the e-Passport on/in the reader by the holder, the instructions must be clear, either printed in the local language(s) or symbolic
- The unit should be accessible by a wide range of people (short / tall / in wheelchair, etc.)
- The size of the unit is more important in certain applications than others
    - Limited space is available on inspection counters in ports-of-entry
    - The view of the inspector must remain unobstructed
- Inspection applications should not require substantial interaction from the inspector in order to retrieve the relevant information from the e-Passport
- The physical motions associated with the use of the e-Passport reader must be intuitive and easy to perform (no contortions or awkward positioning of the arm, hand or body)
- For systems integrated with biometric capture devices, they must be designed to ensure usability by a wide range of persons (physical characteristics)

Forum 3: Skimming and Eavesdropping

The National Institute of Standards and Technology provided a test capability that illustrated the susceptibility of many chip readers to detection of their electronic signals. NIST personnel examined several units, with the result that signals could for some units be picked up by a coil antenna about 20 meters away. The initial results indicated that the signals could have been picked up even an order of magnitude further away. However, the tests also indicated that the housing of the readers dramatically affected results -- reducing the range where the signal could be detected to less than a meter. For these tests, NIST was able to detect the actual bit transfer rate and capture the signal itself. It should be noted that it was very difficult to detect the signal from some readers.

This is not an interoperability problem, and may not be a problem for all applications. For certain uses, if protection against eavesdropping is required, the area of use can be shielded. Other applications may require a reader unit with a housing that substantially diminishes the possibility of electronic eavesdropping.

Readers were also tested to see if there was interference when two readers were located in close proximity to each other. NIST found that some readers had unrecoverable errors when located as close as 30 cm to another reader. Other readers performed without errors when a second reader was only 5 cm away.

NIST did not demonstrate actual 'skimming' of data from a passport sample at this session. That would involve activating the chip, and retrieving data from it that then could be fed to an analysis program. This is an area for future testing.

NIST conducted tests on selected units to determine susceptibility to jamming. Namely, whether an outside electronic signal can interfere with the reading process from the chip, or could it stop the read / chip access process of the reader. Current indications are that it is possible to jam or disrupt the signal.

Forum 4: System Fallback Procedures/Processes

Points of Failure

1) Passport chip failure –
    a. Chip -
    b. Antenna connection
    c. Antenna itself -

Discussion –

- It is immaterial how the passport fails (either it works or not)
- It may be possible to reconnect the antenna (secondary inspection or forensic lab). What type of equipment in the field is required in secondary inspection? Probably not practical in secondary inspection to correct.
- The passport is the property of the issuing State. The State should be aware of the instances of the problems with passport failure. The State's lab will be responsible for disseminating the information about the failures.
- The receiving States should maintain logs of the failures and relay that information to the issuing States
    - Record possible sources of error
    - Report to issuing States
    - There are practical considerations regarding how much information States can collect about the failure rates

2) Interference
    a. Items in passport (e.g. visas)
    b. Individual interference (shielding) - metal insert

Discussion –

- Inspection process is affected by the presence of shields, pouches, covers, pockets, etc..
- Individuals can intentionally interfere with the passport RF signal by putting metal etc into the cover.
- Does the presence of metallic threads in the passport affect the reading of the passport?
- Some technologies exist that have randomly distributed RF activated dipoles into the paper which could react with the reading of the passport
- Holograms can also interfere with the read (ones with electronic capabilities). Ones that were submitted for testing had no effect on the read
- Metallic stamps of the seal of the nation?
- Staples from the visas?

3) Misread of MRZ causing basic authentication error – 5% failure has been noted under certain circumstances
    a. Aging

b. Ink blots
c. Dirt

Discussion –

- Need to have an override capability to open the chip with access control. Correction mechanism is required
- The inspectors must know what to correct to open the chip.
- The passport reader needs to have some kind of data entry to correct the MRZ.
- Swipe readers must somehow transmit information to RF device to open up the chip.

4) Reader failures
   a. Malfunction of device
   b. Logic problem
   c. Jamming
   d. Accidental Unplugging
   e. Electrical spikes
   f. Short circuits
   g. Transmission out fails

Discussion -

- Device malfunction - Does there need to be a self-check mechanism on the device?
  a. This may not be practical.
  b. The inspector may use a test document to check the system.
- Logical problem – how do we make sure we have upgrades that the logic still works. Who checks the logic? We need a conformance document or regression testing capability. National testing a function of acceptance testing and the procurement process.
- Accidental unplugging - This is covered under SOP and standard device feedback, LEDs, and status indicators. The status indicator needs to be separate from the power and connectivity indicators.
- Electrical spikes – Do we need surge protector inside/outside device? Recommend surge protection outside the device. The units should be FCC and C-compliant and international regulatory requirements should withstand most common electrical conditions
- Transmission out fails – information out to external databases, etc. Cables must be checked.

Human Error – we must ensure ease of use and have clear procedures.
Insider Attacks – How do we be sure the reader hasn't been tampered to provide a set output. The diversity of passport reader manufacturers limits the possibility that all readers would be attacked in the same manner. How do countries without an independent testing authority ensure the integrity of the unit?

An e-Passport is an aid to the inspection process not a replacement for human inspection.

Media attacks or other critics of the system may ultimately cause States to stop trusting the e-Passport solution.

Recommendations for Follow-up Work:

This was the first opportunity for such a diverse group of players in the e-Passport arena to come together and test their equipment and products. Almost universally, the participants requested more test sessions, thus underscoring the importance of this event. Comments stated during the summary session included:

- The ad-hoc and anonymous nature of the forum was desirable
- Reader manufacturers may not want to work with PKI issues
- More specific and detailed tests and test procedures would be helpful in future sessions (including explanation of reason for each test)
- Availability of a large number and variety of chips/passports was essential for the success of the tests
- Next tests should stress basic access control and active authentication. Some vendors felt that there needed to be more explanation of these mechanisms and development of a 'standard reference' prior to the next testing session
- The momentum gained by this session should not be lost. A regular series of tests should be scheduled
- Lack of U.S. and Australian data samples was regrettable (Sponsor's note: This was deliberate, as explained in earlier correspondence which stated "since there are active tenders for passports in Australia and the U.S., no representatives from groups associated with those contract actions will be at the testing sessions. I am hosting this session and will not be part of the U.S. Department of State passport contract selection panel (nor for any other nation)."
- Establishment of an independent group to test chips / passports / readers as they are developed or modified would be beneficial to both the industry and to potential customers.

The timing of the sessions was raised as important. The next session is scheduled to be held by Australia Customs in Sydney, Australia on August 25-26 2004. While many felt that this was too soon to prepare, the statement was also made that if a Government calls such a session, the manufacturers would come and participate. Several persons expressed the hope that another session would occur around October. It was noted that the Australian test was scheduled to occur just before the ICAO New Technologies Working Group meeting so that results could be presented there.

The testing format used in this session was relatively free form, but still provided some structure by using the Silver Data Set. Some participants expressed the desire for a modified data set to be used for future testing. The comments focused primarily on the data signing procedures. The collaborative testing environment employed at this session to verify product operability and interoperability was universally praised, and such a format was recommended for future sessions. Some participants requested that groups that have been working on specific problems or encountered 'difficult' issues be encouraged to make presentations -- rather than having a 'round table' format. However, others expressed that the 'round table' was probably the best approach.

Some participants felt that if the e-Passports had been marked with the location of the antenna, it would have made testing much more meaningful, since reader manufacturers would know what layouts that they were having problems with. The tests conducted at this session did move the e-Passport into varying positions relative to the reader (e.g. 2, 5, 10 cm above, or off-center); however, the passport reader manufacturers had to then find out the antenna details from the e-Passport manufacturer.

Many participants were interested in the NIST findings concerning eavesdropping and jamming. Their reaction indicated the strong desire to expand the tests from pure interoperability to 'usability' issues. This would also encompass ergonomic aspects of passport readers. Several speakers pointed out that these readers would not only be used in port-of-entry inspections but also potentially in the provision of other government services and in banks, also with other organizations with a need to establish the identity of an individual. The technical and operational requirements of readers in those situations may very well be different from those encountered at ports-of-entry.

US-VISIT will be hosting a multi-national mock port-of-entry test session in November 2004. That session is planned for governmental representatives in order to determine the optimum ways to integrate the e-Passport capability into inspection environments. That will be followed by an international 'live' test of reading e-Passports at selected ports-of-entry, planned to start in February 2005.

53

(b)(6)

(b)(6)
(b)(2)

(b)(6)

43	[redacted]	Nisko Projects Electronics & Comm.	Israel	[redacted]	[redacted]
44	[redacted]	Smartrac Technology	USA	[redacted]	[redacted]
45	[redacted]	NIST	USA	[redacted]	[redacted]
46	[redacted]	Cubic Corporation	USA	[redacted]	[redacted]
47	[redacted]	NBSP	USA	[redacted]	[redacted]
48	[redacted]	PCS Security	Singapore	[redacted]	[redacted]
49	[redacted]	3M-AIT	Canada	[redacted]	[redacted]
50	[redacted]	NIST	USA	[redacted]	[redacted]
51	[redacted]	Immigration & Checkpoints Authority	Singapore	[redacted]	[redacted]
52	[redacted]	Austrian State Printing House	Austria	[redacted]	[redacted]
53	[redacted]	Oberthur Card Systems	France	[redacted]	[redacted]
54	[redacted]	NBSP	USA	[redacted]	[redacted]
55	[redacted]	Smiths Heimann	Germany	[redacted]	[redacted]
56	[redacted]	Security Printing & Systems	UK	[redacted]	[redacted]
57	[redacted]	Panasonic	Japan	[redacted]	[redacted]
58	[redacted]	Aware, Inc.	USA	[redacted]	[redacted]
59	[redacted]	IRIS Corporation	Malaysia	[redacted]	[redacted]
60	[redacted]	Canadian Passport Office	Canada	[redacted]	[redacted]
61	[redacted]	Feig Electronic GmbH	Germany (USA)	[redacted]	[redacted]
62	[redacted]	OTI	Israel	[redacted]	[redacted]
63	[redacted]	Axalto	France	[redacted]	[redacted]
64	[redacted]	3M Company	USA	[redacted]	[redacted]
65	[redacted]	ACG Identification Tech	Austria	[redacted]	[redacted]
66	[redacted]	Fall Hill Associates. LLC	USA	[redacted]	[redacted]
67	[redacted]	SDU Identification	Netherlands	[redacted]	[redacted]
68	[redacted]	Panasonic	Japan	[redacted]	[redacted]
69	[redacted]	Sharp	Japan	[redacted]	[redacted]
70	[redacted]	IRIS Corporation	Malaysia	[redacted]	[redacted]
71	[redacted]	ACG Identification Tech	Austria	[redacted]	[redacted]
72	[redacted]	SNP SPrint Pte Ltd	Singapore	[redacted]	[redacted]
73	[redacted]	Smartrac Technology	Germany	[redacted]	[redacted]
74	[redacted]	NBSP	USA	[redacted]	[redacted]
75	[redacted]	ASK	France	[redacted]	[redacted]
76	[redacted]	OTI	Israel	[redacted]	[redacted]
77	[redacted]	3M-AIT	Canada	[redacted]	[redacted]
78	[redacted]	PCS Security	Singapore	[redacted]	[redacted]
79	[redacted]	ASK	France	[redacted]	[redacted]
80	[redacted]	ASK	France	[redacted]	[redacted]
81	[redacted]	IRIS Corporation	Malaysia	[redacted]	[redacted]
82	[redacted]	Bundesdruckerei GmbH	Germany	[redacted]	[redacted]
83	[redacted]	NEC Solutions Asia Pacific	Singapore	[redacted]	[redacted]
84	[redacted]	Cubic Defense Applications	USA	[redacted]	[redacted]
85	[redacted]	Gemplus	Canada	[redacted]	[redacted]
86	[redacted]	GEP S.p.A	Italy	[redacted]	[redacted]
87	[redacted]	Mitre	USA	[redacted]	[redacted]
88	[redacted]	NBSP	USA	[redacted]	[redacted]
89	[redacted]	Scsquare Ltd., SC2	Israel	[redacted]	[redacted]

(b)(6)

54

e-Passport/Biometric Test 27-29 July 2004

Attendees List

(b)(6) (b)(2) (b)(6) (b)(6)

#	Name	Org	Country	Phone	E-Mail
1	[redacted]	AssureTec Systems Inc.	USA	[redacted]	[redacted]
2	[redacted]	Francis Charles Oberthur Fiduciaire	France	[redacted]	[redacted]
3	[redacted]	Oberthur Card Systems	France	[redacted]	[redacted]
4	[redacted]	Datacard	USA	[redacted]	[redacted]
5	[redacted]	Canadian Bank Note Company, Ltd	Canada	[redacted]	[redacted]
6	[redacted]	Gemplus	France	[redacted]	[redacted]
7	[redacted]	Integrated Engineering	Netherlands	[redacted]	[redacted]
8	[redacted]	Aware, Inc.	USA	[redacted]	[redacted]
9	[redacted]	Giesecke & Devrient	Germany	[redacted]	[redacted]
10	[redacted]	Security Printing & Systems	UK	[redacted]	[redacted]
11	[redacted]	Gemplus	USA	[redacted]	[redacted]
12	[redacted]	Thomas & Herberg Consulting LLC	USA	[redacted]	[redacted]
13	[redacted]	Axalto	France	[redacted]	[redacted]
14	[redacted]	Bundesdruckerei GmbH	Germany	[redacted]	[redacted]
15	[redacted]	Ministerie van Binnenlandse Zaken	Netherlands	[redacted]	[redacted]
16	[redacted]	NBSP	USA	[redacted]	[redacted]
17	[redacted]	Infineon Technologies	USA	[redacted]	[redacted]
18	[redacted]	Gemplus	USA	[redacted]	[redacted]
19	[redacted]	US Department of Defense	USA	[redacted]	[redacted]
20	[redacted]	Oberthur Card Systems	USA	[redacted]	[redacted]
21	[redacted]	UK Passport Service	UK	[redacted]	[redacted]
22	[redacted]	Imaging Automation	USA	[redacted]	[redacted]
23	[redacted]	Oberthur Card Systems	France	[redacted]	[redacted]
24	[redacted]	Mitre	USA	[redacted]	[redacted]
25	[redacted]	IRIS Corporation	Malaysia	[redacted]	[redacted]
26	[redacted]	Giesecke & Devrient	USA	[redacted]	[redacted]
27	[redacted]	WVU Faculty	USA	[redacted]	[redacted]
28	[redacted]	Immigration & Checkpoints Authority	Singapore	[redacted]	[redacted]
29	[redacted]	Infineon Technologies	USA	[redacted]	[redacted]
30	[redacted]	Mitre	USA	[redacted]	[redacted]
31	[redacted]	ACG Identification GmbH	USA	[redacted]	[redacted]
32	[redacted]	Northrop Grumman Corp	USA	[redacted]	[redacted]
33	[redacted]	Embassy of Belgium	Belgium (USA)	[redacted]	[redacted]
34	[redacted]	Dynjab Technologies	Australia	[redacted]	[redacted]
35	[redacted]	Philips Semiconductors	USA	[redacted]	[redacted]
36	[redacted]	Smartrac Technology	Thailand	[redacted]	[redacted]
37	[redacted]	Axalto	USA	[redacted]	[redacted]
38	[redacted]	Ascom SA	France	[redacted]	[redacted]
39	[redacted]	UK Immigration Service - Home Office	UK	[redacted]	[redacted]
40	[redacted]	Dynjab Technologies	Australia	[redacted]	[redacted]
41	[redacted]	BSI	Germany	[redacted]	[redacted]

55

(b)(6) (b)(2) (b)(6)

90	[redacted]	Sharp	Singapore	[redacted]	[redacted]
91	[redacted]	BFC	USA	[redacted]	[redacted]
92	[redacted]	SCM Microsystems	USA	[redacted]	[redacted]
93	[redacted]	SAIC	USA	[redacted]	[redacted]
94	[redacted]	Bearingpoint	USA	[redacted]	[redacted]
95	[redacted]	SCM Microsystems	India	[redacted]	[redacted]
96	[redacted]	Imaging Automation	USA	[redacted]	[redacted]
97	[redacted]	NBSP	USA	[redacted]	[redacted]
98	[redacted]	Bundesdruckerei GmbH	Germany	[redacted]	[redacted]
99	[redacted]	Setec	Finland	[redacted]	[redacted]
100	[redacted]	WVU Faculty	USA	[redacted]	[redacted]
101	[redacted]	NBSP	USA	[redacted]	[redacted]
102	[redacted]	NIST	USA	[redacted]	[redacted]
103	[redacted]	Sharp	Japan	[redacted]	[redacted]
104	[redacted]	Ministry of Foreign Affairs	Japan	[redacted]	[redacted]
105	[redacted]	Mitre	USA	[redacted]	[redacted]
106	[redacted]	ST Microelectronics	France	[redacted]	[redacted]
107	[redacted]	Axalto	France	[redacted]	[redacted]
108	[redacted]	Axalto	USA	[redacted]	[redacted]
109	[redacted]	DHS US-VISIT	USA	[redacted]	[redacted]
110	[redacted]	NBSP	USA	[redacted]	[redacted]
111	[redacted]	PCS Security	Singapore	[redacted]	[redacted]
112	[redacted]	NIST	USA	[redacted]	[redacted]
113	[redacted]	Secunet	Germany	[redacted]	[redacted]
114	[redacted]	Ascom	France	[redacted]	[redacted]
115	[redacted]	Panasonic	Japan	[redacted]	[redacted]
116	[redacted]	Italy Interno	Italy	[redacted]	[redacted]
117	[redacted]	Secunet	Germany	[redacted]	[redacted]
118	[redacted]	AssureTec Systems Inc.	USA	[redacted]	[redacted]
119	[redacted]	Lasercard	USA	[redacted]	[redacted]
120	[redacted]	Imaging Automation	USA	[redacted]	[redacted]
121	[redacted]	Sharp	Japan	[redacted]	[redacted]
122	[redacted]	Scsquare Ltd., SC2	Israel	[redacted]	[redacted]
123	[redacted]	BEC	USA	[redacted]	[redacted]
124	[redacted]	Sharp	USA	[redacted]	[redacted]
125	[redacted]	NBSP	USA	[redacted]	[redacted]
126	[redacted]	Infineon Technologies	USA	[redacted]	[redacted]
127	[redacted]	DHS US-VISIT	USA	[redacted]	[redacted]
128	[redacted]	Canadian Bank Note Company, Ltd	Canada	[redacted]	[redacted]
129	[redacted]	Oce North America	USA	[redacted]	[redacted]
130	[redacted]	Giesecke & Devrient	USA	[redacted]	[redacted]
131	[redacted]	Integrated Engineering	Netherlands	[redacted]	[redacted]
132	[redacted]	WVU Faculty	USA	[redacted]	[redacted]
133	[redacted]	ACG Identification GmbH	Germany	[redacted]	[redacted]
134	[redacted]	Inside Contactless	France	[redacted]	[redacted]
135	[redacted]	Italy IPZS	Italy	[redacted]	[redacted]
136	[redacted]	SCM Microsystems	India	[redacted]	[redacted]

(b)(6)

137	[redacted]	Smiths Heimann	Germany	[redacted]	[redacted]	
138	[redacted]	DHS US-VISIT	USA	[redacted]	[redacted]	
139	[redacted]	BFC	USA	[redacted]	[redacted]	
140	[redacted]	Sharp	Japan	[redacted]	[redacted]	
141	[redacted]	NEC Solutions Asia Pacific	Singapore	[redacted]	[redacted]	
142	[redacted]	NBSP	USA	[redacted]	[redacted]	
143	[redacted]	WVU	USA	[redacted]	[redacted]	
144	[redacted]	OTI	Israel	[redacted]	[redacted]	

(b)(6) (b)(6) (b)(6)

X-Sieve: CMU Sieve 2.2
From: "[redacted] (b)(6)

(b)(6)

US – VISIT PROGRAM
OFFICE OF THE CHIEF STRATEGIST
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

_1_ page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

	Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Title 5, United States Code, (U.S.C.) Section 552 (FOIA)						**Title 5, U.S.C. Section 552a(PA)**
		(b)(1)		(b)(7)(D)		(d)(5)
		(b)(2)		(b)(7)(E)		(j)(2)
		(b)(3)		(b)(7)(F)		(k)(1)
		(b)(4)		(b)(8)		(k)(2)
		(b)(5)		(b)(9)		(k)(3)
X		(b)(6)				(k)(4)
		(b)(7)(A)				(k)(5)
		(b)(7)(B)				(k)(6)
		(b)(7)(C)				(k)(7)

		Documents originated with (an) other Government agency(ies). These documents were referred to that agency for review and direct response to you.

__pages contain information furnished by (an) other Government agency (ies). You will be advised by the FOIA Office to the releasability of this information.

______pages have not been provided to you at this time because a final release determination has not been made. You will be advised as to the disposition at a later date.

For your information

Page 2 of a 6 page email is being withheld in its entirety under FOIA exemption b(6).

(b)(6)

[redacted]

Subject: Updates - Interoperability Tests
Date: Fri, 23 Jul 2004 11:11:03 -0400
X-Mailer: Internet Mail Service (5.5.2657.72)
X-MailScanner:
X-MailScanner-From: [redacted]@dhs.gov

To all:

I have received a few questions that I would like to answer for you (as best I can) before next week. I forwarded these questions to some experts in the Netherlands, U.S. and Germany who provided me with the following:

1. Regarding the contents of the SOD as presented in the Silver sample :

> The last 128 bytes represents a digital signature .
> Please clarify the content of the data to be signed.

Answer 1:

The PKI-report describes the syntax of the SOD-File.

The hashes of the present DGs are encoded in an ASN.1-Syntax which is again encoded in a "Signed Data" structure. The hash of these Signed Attributes is signed using RSA/DSA/ECDSA.... See "TECHNICAL REPORT PKI for Machine Readable Travel Documents offering ICC Read-Only Access Version - 1.0 Date - April 21, 2004"

The signature in the EF.SOD conforms with PKCS1 SignatureFormat. It has the format 01 || PS || 00 || T where T is a DigestInfo structure. The length of this format is exactly the modulus length and PS is used to fill it with FF to that length. The DigestInfo contains the used hash algorithm (SHA-1) and the calculated hash value.

The hash value is calculated to conform to the RFC3369 Cryptographic Message Syntax.
This means that the signature is calculated over the DER-encoding of the signedAttrs of the SignerInfo structure. In the case of EF.SOD, the signedAttrs contain only the minimum required attributes, content-type and message-digest. The content-type is the eContentType of the encapContentInfo of the SignedData structure (i.e. 1.2.528.1.1006.1.20.1). The message-digest contains the calculated hash-value (SHA-1) of the value of the eContent of the encapContentInfo of the SignedData structure (i.e. the DER-encoding of the LDSSecurityObject as defined in the ICAO TR PKI).
The LDSSecurityObject contains the hash-values (SHA-1) of all available DataGroups, in case of the Silver Data set, DG1 and DG2. These hash-values are calculated over the complete contents of the DataGroup.

2. Referring to ver 1.7 Appendix 2 to Annex A pg 65
Subheading: Examples for ISO 7816 usage with LDS:
The first row in the table after the heading has
"0A 00 00 02 47 10 01" for the data column and "Select Issuer Application"
in the remarks column.
This evidently suggests that the Issuer Application AID (Application ID) is
"0A 00 00 02 47 10 01"

However in other sections in the documentation (ver 1.7), the Issuer Application AID is stated as "A0 00 00 02 47 10 01". Refer to pg 52 Fig A.1, pg 46 A.13.

Answer 2: This is a typo that should be corrected.
A0 00 00 02 47 10 01 is the correct AID.

3. The ICAO website has LDS v1.7 published. However the 'silver' reference data that you sent is based on LDS v1.6 (as designated in the EF.COM) Should we then assume that LDS v1.6 or v1.7 testing will be performed?

The main impact will be the Selection of Master File command. There is a difference between LDS v1.6 (p. 61) and v1.7 (page 63).

Also, with regard to DG1 data elements 03 (Name of holder) and 12 (optional data), LDS v1.7 has varying sizes for ID-1, ID-2 or ID-3 sized documents. v 1.6 specified it as static sizing. If we are only testing passports with inlays, then it should not be a problem (same size) however I am assuming there will be others bringing prototypes in card (ID-1) format.

Answer 3:

The editorial syntax for V1.7, page 63 is misleading.

The correct syntax is either
'00' 'A4' '00' '0C' Empty Empty Empty

Or

'00' 'A4' '00' '0C' Empty Empty MaxRet

The difference between the commands is: The first one just returns 0x9000 in case of success, the second one returns the File Control Parameters of the selected file (see LDS 1.x, x<5)

ISO-Compliant cards even have to support both
commands and reading software should be written in a way that additional return information does not kick it out....

ISO-Compliant cards should work with both commands (but it has to be a valid command, not that one described in V1.7 (see above)). By the way: for reading EF.COM to detect the LDS-Version, you already may have used the select command So it does not make sense to change the behavior of the software depending on the LDS-Version....

For the second part of question 3: For now LDS only considers passports (part 1 ICAO Doc 9303). Of course, visa and other documents have different length in the MRZ fields and lines, which is standardized by Doc 9303. In any case, as in LDS 1.6/1.7, the length of the MRZ should be FIXED as in LDS 1.7, BUT which FIXED LENGTH to be used should be governed by Doc 9303 corresponding to document type. In all cases, LDS and optical personalization should correspond. This has to be amended in the LDS TR (eventually).
Version 1.6 is the reference, used in the silver data set (there was no version 1.7 at that time of its preparation).

Fixed/not fixed: DG1 contains exactly the complete MRZ as it is printed (visible) on the document.

General:

While enormous amounts of time and effort have been expended going over the documents carefully to correct typos, there may well be other typos that will become apparent as we begin to implement. These will be corrected at some point in the future when sufficient time has passed that we can be certain all necessary changes have been caught. We should make every effort to move to LDS 1.7 as now published on the ICAO web site, recognizing the 'anomalies' in it such as have been pointed out here.

www.icao.int/mrtd/download/technical.cfm

On another point, since there are active tenders for passports in Australia and the U.S., no representatives from groups associated with those contract actions will be at the testing sessions. I am hosting this session and will not be part of the U.S. Department of State passport contract selection panel (nor for any other nation).

We want these sessions to be an opportunity for groups to openly exchange information on interoperability issues. This will not be a marketing event or a competition in any sense.
We will summarize the findings in ways that will be focused on technical issues and their resolutions, not the 'relative performance' of any participating group.

Thanks,

<<...OLE_Obj...>>

<<[redacted](E-mail).vcf>>

(b)(6)

[redacted](E-mail).vcf

From: [redacted] (b)(6)
To

(b)(6)

Sent: Thursday, July 15, 2004 4:51 PM
Attach: e-Passports Lab Test 27-29 JUL 04 Regime-Schedule (15 JUL 04).doc
Subject: e-Passport Test Regime and Schedule

All:

Please see the attached file that includes the updated test regime and schedule for the upcoming e-Passports interoperability test in Morgantown, West Virginia, 27-29 July 2004.

Please forward to those folks attending the testing for whom I did not have an e-mail address.

Thanks. See you on the 27th!

[redacted]

<<e-Passports Lab Test 27-29 JUL 04 Regime-Schedule (15 JUL 04).doc>>

[redacted]
US-VISIT Program
Phone: [redacted]
Email: [redacted]

(b)(6)

Testing Regime

Each passport reader company will be provided with a list of e-passport types available for test. The conference room in the laboratory will be where each vendor can pick up the passports for testing. Each vendor is encouraged to test all of the 'Silver Standard' samples first. These will be of both types A and B.

Space will be available in the laboratory for those companies wishing to use it. Vendors may also perform their own tests privately.

Once a company has had time to verify their systems with the passport samples, they can schedule a conference room and test team who will oversee the testing and log the results. The test teams are comprised of persons not affiliated with any vendor of passports or readers.

There will also be an area set aside in a separate computer room where equipment and staff will be present to perform eavesdropping, skimming, and jamming tests. To schedule a conference room or the computer room please contact the NBSP/DHS test coordinators.

For groups bringing IC chips, please provide a binary representation of the LDS encoding on another storage medium as generated by your software. This will allow examination of the LDS interpretation by different groups to ensure the same information is encoded by all vendors, given identical input.

Part 1 - Functional Testing

The first day will be focused on basic functionality. Each chip will be tested with the following information collected:

- Detect whether chip is readable
    - Read chip at 1-10 cm from reader
        - Direct contact (standard passport)
        - In Passport Folder
        - In Traveler Neck Wallet
    - Read chip at >10 cm (should not be able to read chip)
    - Display chip header information (ATS/ATR/UID)
    - Indicate orientation (1-8) of chip and MRZ in passport (if applicable)
    - If required, how many repositioning attempts were made before the chip was read?
- Read Silver Data Set (Common, Data Group 1 and Data Group 2). Note: DG1 and DG2 information should be displayed even if the digital signature does not match.
    - How long did it take from placement of passport on reader to display of information?
        - How long did it take to display Silver Data Set DG1
        - How long did it take to display Silver Data Set DG2

    - Did the Data Group 1 data match the Silver data?
    - Did the photograph (Data Group 2) get retrieved and displayed properly (compared against the input Silver photo)?
    - Did the Digital Signature verify properly?
        - Data Group 1
        - Data Group 2
- What is the claimed transmission speed (KBPS) for the data retrieval and what is the speed claim based on?
- What is the power level for data retrieval?
- How long does it take to reset the system for the next read?

Part 2 – Additional Testing

The second and third days will be devoted to further testing. Vendors may proceed at their own pace. THIS IS NOT A COMPETITION.

Optional Test – Eavesdropping/Skimming/Jamming

The vendors will be encouraged to have their units tested for eavesdropping, skimming, and jamming. A special test area will be provided where a loop antenna, and measuring devices will be placed to detect transmissions between the chip and the reader.

The effect of placing the readers near other equipment typical of an inspection area will also be tested.

- Will readers near each other interfere with each other?
- What is the minimum separation required for the systems to work properly?
- What happens when the read is interrupted before completion?

Optional Test –Stored Image Test (DG2)

Additional e-passports with images that deviate from the 'Silver' Data Group 2 will be provided to include:

- A variant of JPEG storage (Note: although digital signature will not verify for DG2, photo must be displayed)
- Multiple variants of JPEG 2000 storage options
- Variant with extra Data Groups
- SHA-256 hashing with different digital signature than Silver Data Set

Optional Test – Multiple Chip/Code Tests

In order to detect whether the reader can decipher a passport from other chips, the readers will be tested with chips that have codes other than 'P' in the MRZ for document type. For Part 2, they will be tested individually. (A reader may be presented with a 'normal' passport' that contains an e-visa).

As in Part 1, timing, power levels, and accuracy of data retrieval will be recorded for the following:

- e-Passports including active authentication
  - Test with correct MRZ
  - Test with incorrect MRZ (not matching chip data)
- e-passports including Basic Access Control
  - Test the Basic Access Control with a 'correct' MRZ
  - Test the Basic Access Control with an 'incorrect' MRZ
  - Test the capability to make manual correction of the MRZ (in case it is misread)
- e-passports without either active authentication or Basic Access Control, but with a photo larger than 32K in DG2 (pending availability of test chips)

Inlays that are encoded as visas will be available for insertion into e-passports. These will be of both types A and B. For testing purposes, it is assumed that the only difference between e-visa and e-passport chips will be the "V" vs. "P" indication in the MRZ. In order to standardize these tests, there will be two stages

1) e-passport with 1 e-visa
   a. e-passport type A, e-visa type A
   b. e-passport type B, e-visa type A
   c. e-passport type A, e-visa type B
   d. e-passport type B, e-visa type B
2) e-passport with 2 e-visas
   a. (a) Above with 2nd e-visa type A
   b. (a) Above with 2nd e-visa type B
   c. (b) Above with 2nd e-visa type A
   d. (b) Above with 2nd e-visa type B
   e. (c) Above with 2nd e-visa type A
   f. (c) Above with 2nd e-visa type B
   g. (d) Above with 2nd e-visa type A
   h. (d) Above with 2nd e-visa type B

Vendors can test their units using different power levels and various combinations of e-passport / e-visas available at the test center.

SCHEDULE

July 27

8:30	Registration	All	HOTEL	
9:00	Welcome and Description of Tests	[redacted]	HOTEL	(b)(6)
9:30	Description of Passport Samples Description of chip orientation in passports	Govt Reps	HOTEL	
10:00	Setup of Equipment and Begin Testing	Vendors	NBSP	
12:00	Lunch	All	______	
13:00	Testing - Part 1 (Continued)	All	NBSP	
14:30	Summary of Part 1 Interim Results	All	NBSP	
15:00	Testing - Part 1 (Continued)	All	NBSP	

July 28

8:00	Testing (Continued)	All	NBSP
11:00	Discussion of Interim Test Results	All	NBSP
12:00	Lunch	All	______
13:00	Testing (Continued)	Vendors	NBSP
Special Sessions (Discussion)		Government/Vendors	HOTEL
13:00	Forum A: Durability Tests and Results		
14:45	Break		
15:15	Forum B: Ergonomics of Inspection Systems		

July 29

8:00	Testing (Continued)	Vendors	NBSP
Special Sessions (Continued)		Government/Vendors	HOTEL
8:00	Forum A: Skimming and Eavesdropping		
9:45	Break		
10:15	Forum B: System Fallback Procedures / Processes		
12:00	Lunch	ALL	______
13:00	Presentation of Results of Testing	ALL	HOTEL
14:00	Discussion of next steps	ALL	HOTEL
15:00	Adjourn		

NOTE: Special Sessions are available to government and vendors. Vendors can continue laboratory testing at NBSP during these sessions.

6/29/04

From: [redacted]
To:
Sent: Tuesday, June 29, 2004 11:59 AM
Attach: e-Passport Test.ppt; Directions to The Radisson.doc
Subject: Fwd: e-passport Testing

(b)(6)

[redacted]

Are you going to this? Will you be setting up the face verification demo?
thanks

>X-Sieve: CMU Sieve 2.2
>Subject: e-passport Testing
>Date: Tue, 29 Jun 2004 09:49:42 -0400
>X-MS-Has-Attach: yes
>X-MS-TNEF-Correlator:
>Thread-Topic: e-passport Testing
>Thread-Index: AcRd35c5HEPG+21jQMuStcQGpZU6RAAADxFA
From: [redacted]
>To: [redacted]
>
>X-OriginalArrivalTime: 29 Jun 2004 13:49:44.0056 (UTC)
>FILETIME=[EEE91780:01C45DDF]
>X-MailScanner:
>X-MailScanner-From: [redacted]@dhs.gov
>
>FYI.................[redacted]
>
>-----Original Message-----
From: [redacted]
>Sent: Tuesday, June 29, 2004 9:54 AM
>To: '[redacted]

(b)(6)

(b)(6)

[redacted]

(b)(6)

>Subject: e-passport Testing
>
>As was announced at the special ICAO e-passports Task Force and ISO WG8
>session in London (June 17), we will be sponsoring a test in July. The
>attached file (e-passport Test.ppt)describes the general goals of the
>tests
>as presented on the 17th.
>
>The sessions will be hosted by the U.S. Department of Homeland Security
>on
>July 27-29 at the National Biometrics Security Project laboratory in
>Morgantown, West Virginia. This is 1 hour south of Pittsburgh,
>Pennsylvania, USA. A map and directions is included as an attachment to
>this message (Directions to the Radisson.doc). A block of rooms has
>been

>held at the Radisson Hotel for the nights of July 26, 27 and 28. Please
>refer to "NBSP" when making your reservations.
>
>We actively encourage technicians to take part in these tests. This is
>NOT
>a competition, but rather an exercise to exchange information and to
>ensure
>interoperability. At the London meeting, 4 passport reader
>manufacturers
>stated that they will participate, and some others indicated that they
>also
>might be ready by that date. In addition, we expect passport samples
>from
>passport manufacturers and from some nations. The German, Dutch and
>British
>Governments have been working closely together on the issues of
>interoperability. They will provide a 'reference' set of readers,
>reading
>applications and sample documents, giving the participants the
>opportunity
>to test against it. AWARE, Inc. will have a software system at the
>sessions
>that can display and present the information in the Logical Data
>Structure
>(LDS).
>
>There will be separate areas provided for each passport reader
>manufacturer
>to set up and work with / modify (if necessary) their product during the
>testing.
>
>Chip reader manufacturers and passport manufacturers who will not be
>able to
>attend the session are nonetheless encouraged to ship prototype units to
>NBSP with instructions on how to set up the units and operate them. The
>units should arrive at NBSP by 22 July. The shipping address is:
>
> NBSP [redacted]
> 150 Clay Street, [redacted] (b)(2)
> Morgantown, WV 26501 USA
>
>Note: Although not the prime focus of the tests, a team from the
>National
>Institute of Standards (NIST) will bring a PC-based application that
>(without addressing proper systems integration) will accept whatever
>image
>is recovered from a passport, and an image from a live camera, and will
>render a verification decision. This is not a 'facial verification
>test'
>but will be performed to demonstrate what will be involved in inspection
>systems once the data is retrieved from the passport.

>
>Another team from NIST will be available to perform tests on
>eavesdropping.
>They will set up a loop antenna, amplifier, and oscilloscope to detect
>information being exchanged between the reader and the passport. They
>will
>attempt this at varying distances. An attempt will also be made to
>determine if the exchange can be 'jammed' (intentionally or
>unintentionally). This is important in order for inspection agencies to
>take
>corrective measures in the design of their inspection areas, should it
>be
>necessary.
>
>Although not specifically mentioned in the test outline presented in
>London,
>Part 1 testing will also include passive authentication. For
>participants
>wishing to create chips / passports with standard reference DG1, DG2 and
>signature data sets, please let me know (via e-mail) and I will forward
>those data files to you.
>
>A rough schedule for the tests is as follows:
>
>July 27
>   9:00   Welcome and Description of Tests   [redacted] US   (b)(6)
>DHS
>   9:30   Setup of Equipment   Passport
>Reader Companies
>   10:00   Description of Passport Samples
>Participating Nations and
>
>Passport Manufacturers
>   11:00 Testing - Part 1   All
>   12:30 Lunch   All
>   1:30   Testing - Part 1 Continued   All
>   2:30   Summary of Part 1 Interim Results   All
>   3:00   Testing - Part 1 Continued   All
>   Analysis of Data retrieved from chips
>   (Comparison to supplied DG1 and DG2)
>
>
>July 28
>
>   9:00   Continuation of Tests (Parts 2 & 3 if possible) All
>   11:00 Discussion of Interim Test Results
>All
>   12:00 Lunch
>   1:00 Continuation of Testing
>Non-Government
>   Special Sessions

>Government
> Forum A: Durability Tests and Results
> Forum B: Ergonomics of Inspection Systems with new
>Equipment
>
>July 29
> 9:00 Continuation of Tests (Parts 2 & 3 if possible)
>Non-Government
> Special Sessions
>Government
> Forum A: Skimming and Eavesdropping
> Forum B: System Fallback Procedures / Processes
> 12:00 Lunch
> 1:00 Presentation of Final Results of Testing
> 2:30 Discussion of Sydney Tests (Week of August 23) and next
>steps
> 3:30 Adjourn
>
>
>I look forward very much to seeing you at the test session. If you
>could
>please send me a response (and copy [redacted]
>indicating
>that you are participating, (and the number of people coming), I would
>greatly appreciate it.
>
[redacted]
>US-VISIT, U.S. Department of Homeland Security
>
[redacted] (b)(6)
>
>
>
>

[redacted] (b)(6)
Information Access Division
Information Technology Laboratory
National Institute of Standards & Technology
Bldg 225, [redacted] (b)(2)
100 Bureau Drive, STOP 8940
Gaithersburg, MD 20899-8940
Tel: [redacted] Email: [redacted] (b)(6)
Fax: [redacted] http://www.itl.nist.gov/iad

e-Passport Test

West Virginia, USA – July 27-29

Sydney, Australia – week of August 23

Test Objectives

- Part 1
  - – 1) Detect whether chip(s) in read range
    - Test chip inlay in front cover, inside page and back cover
  - – 2) Detect type of chip (A or B)
  - – 3) Retrieve Data Group 1, Data Group 2 with 15-20 K Photo (at 424 KBPS)
- Part 2
  - – 1) Detect if the chip a passport, visa or other
  - – 2) Detect if the chip uses Basic Access Control (BAC)
  - – 3) Retrieve Data Groups 1 & 2 using BAC
  - – 4) Retrieve Photo > 32K

Test Objectives (continued)

- Part 3
  - 1) Detect how many chips are in range
  - 2) Detect how many are A and B and how many are passport, visa and/or other
  - 3) Determine (test) impact of different power levels and chip(s)

  - Note: testing assumption: 1 passport chip, with 2 visa chips

Passport Reader “Style”

- Closed Passport (if coupled with a ‘swipe’ MRZ reader
- Full page reader: Two Styles
  - Flat (read chip on either page)
  - 90 degrees, with data page read on top (chip may be on either page)

Call for Participation

- Governments
  - Samples of e-passport prototypes
- Chip Vendors
  - Working samples encoded with DG1, DG2 to be supplied by testers
- Reader Manufacturers
  - Prototype working readers
  - Technicians should attend testing sessions

Contacts

- [redacted] (b)(6)
  - U.S. Department of Homeland Security
  - [redacted] (b)(6)
- [redacted]
  - Passports Australia
  - [redacted] (b)(6)

Process

- e-Mail [redacted] (b)(6) & [redacted] (b)(6) by June 30
  - Company name
  - Point of contact name / e-mail / phone number
  - Describe what will be provided by your group to test and number of people to attend and whether it will be for one or both sessions

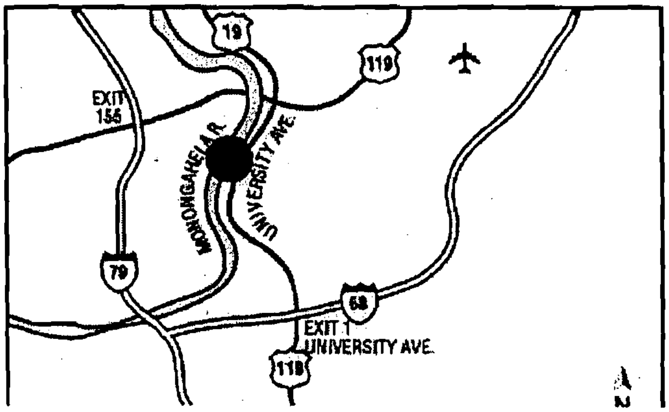
Directions to The Radisson Hotel at Waterfront Place
Two Waterfront Place – Morgantown, WV 304-296-1700
Map Available on line at www.radisson.com/morgantownwv

From the Pittsburgh Airport
- Take 60 East towards Pittsburgh
- Take I-79 South
- Merge onto I-68 East toward CUMBERLAND
- Take the US-119 exit- EXIT NUMBER 1- toward UNIVERSITY AVE./ DOWNTOWN
- Turn LEFT off of the exit ramp
- Travel towards downtown Morgantown going through 3 stop lights
- The Radisson is on the LEFT at the 4th stop light

Coming North on I-79:
- Merge onto I-68 East toward CUMBERLAND
- Take the US-119 exit- EXIT NUMBER 1- toward UNIVERSITY AVE./ DOWNTOWN
- Turn LEFT off of the exit ramp
- Travel towards downtown Morgantown going through 3 stop lights
- The Radisson is on the LEFT at the 4th stop light

Coming West on I-68:
- Take the US-119 exit- EXIT NUMBER 1- toward UNIVERSITY AVE./ DOWNTOWN
- Turn LEFT off the exit ramp
- Travel towards downtown Morgantown going through 3 stop lights
- The Radisson is on the LEFT at the 4th stop light

From Washington DC
- Take I-270 and merge onto I-70.
- Merge onto I-68 W via Exit 1A on the left toward Cumberland, MD
- Take Exit 1 on I-68
- Turn left onto 119
- Continue for 3.3 miles
- Radisson at Waterfront is located on Left



From: [redacted]
To:
Cc:

(b)(6)

Sent: Friday, June 25, 2004 10:33 AM
Attach: e-Passport Test.ppt
Subject: RE: Dates for July testing

Up in Montreal, I mentioned that we would have to move the large test to =he 27th, and that it was being coordinated/finalized at the 5-nation confere=ce being held in Williamsburg the following Monday. I'm sorry if I didn't ma=e it crystal clear and left you with the impression that the test would sti=l be around the 16th. Mea Culpa.

I just talked with [redacted] on the phone. I told him that we can work togethe= (2 nations) prior to the 27th and go through tests jointly. In fact, I would welcome that wholeheartedly. We can do it at any date that is convenient with you - such as the 16th. (Selfishly, it might help the U.=. prepare more efficiently for the tests on the 27th-29th). I'm planning t= start the detailed test schedule, etc. I don't have a formal test plan worked up yet. I wanted to see how the meeting in London went before developing it (and even if the tests would be possible).

(b)(6)

The test for passport or visa will be important, especially since the EU =s actively considering chip visas. The important thing is to be able to re=d the passport chip if the field contains 'other type' chips/antennas. The effect of antennas and their orientations could be a major factor. Howev=r, the multiple-chip-in-range tests are a later stage: after retrieval of t=e data. A standard DG1 and DG2 will be provided to the vendors (by Terry i= an e-mail in the next couple of days) so that we can retrieve 'standard' information. We will have test equipment in place to ensure that the dat= being read is correct (even if the reader may not decipher it properly) (oscilliscopes, etc.) Given that the data is retrievabale, NIST is bring=ng facial recognition setups to work with the information. Unfortunately w= will have to repeat a lot of the Canberra tests, since the manufacturers indicated that they still were not able to fully deal with the probalems that we have highlighted. Hopefully after the London meeting, their questions were fully resolved.

We would also like to be able to detect RF emissions during transmission (eavesdropping). These items were not outlined in the presentation in London, since the focus there was to get the developers to have chips /

readers that will work interoperably and be able to handle the LDS.

We will have a team of testers from NBSP, NIST, and representatives from participating governments. The manufacturers technicians will be able to work on their units during the session to improve performance / resolve issues.

We will have samples from several nations at the test and will run them a=l through the various configurations. I'm a little confused by the 'differ=nt technical solutions' reference that you have (do you mean Basic Access Control?) We definitely have to test that -- but we can only get there once we're assured that the architecture works without that feature being implemented. We have to do in in steps. BAC is part of the testing procedure.

The "Golden Solution" is imperative. I'd like to work with you on this. I've been looking at a product http://www.aware.com/products/compression/icaopack.html See what you thi=k about using it as part of the tests.

Now that I'm back and can focus a bit, we need to get caught up. One thi=g I want to stress, is that we can do tests together at any time that is convienient. Unfortunately the 27-29 dates work out for several nations =nd the passport reader vendors didn't believe that they would have anything ready sooner.

The "reference implementation" that you talk about is IMPERATIVE. I agre= with you 110%. I hope that I can focus on it now that I'm back in town a=d can 'pick your brain' on what we need for it [redacted] brain will also nee= to be 'picked') (b)(6)

[redacted] seemed to like to the idea of a bi-lateral test still occurring aroun= the 16th. Do you concur?

[redacted] (b)(6)

-----Original Message-----
From: [redacted] (b)(6)
Sent: Friday, June 25, 2004 9:00 AM
To: [redacted]
Cc: [redacted] (b)(6)
Subject: AW: Dates for July testing

Dear [redacted] (b)(6)

I am a little confused from your e-mail and the attached presentation.

1. When was the schedule revised by whom? In Montreal we agreed on anothe= date and we do not even talked about the Sydney meeting. Did I missed something?

2. In my understanding the detection if a chip is for passport, visa,...=is not covered by the last ICAO Plenary resolutions, ICAO TR on LDS and PKI.=We (UK, NL and D) provided Terry with some comments. (Slide 2)

(b)(6)

3. Testing readers/chips/... without having a technical spec/mutual agree= implementation (Reference Implemantation) is worthless. Because against w=at do you want to test? (Slide 2, 3 and 4)

4. Will the same testing in be done West Virginia and in Sydney? To be honest, I miss a little a structure/roadmap, because the presented testpl=n is simillar to one for the 'Canberra Testing'. I am expecting similar results - See 3. And in my personal view, in this case it is doubtful tha= Germany will take part, because we will not achieve any progress.

5. Who will be the testers? (Slide 5)

6. In my understanding the major goal of the 'July Testing' in West Virgi=ia should be, to achieve a mutual agreed technical solution for reading the different national LDS and PKI solutions. This technical solution could t=en be used as a 'Golden Solution' to test different readers/chips/... in Sydney.

7. I wonder a little what is more important, to be able to read the different national technical solutions or to test readers/chips/...?

Looking forward to your reply.

[redacted]; 06.25.04

-----Ursprüngliche Nachricht-----
Von: [redacted]
[redacted], 24. Juni 2004 21:11
[redacted]
Cc: [redacted]
Betreff: RE: Dates for July testing
Wichtigkeit: Hoch

(b)(6)

The schedule was revised a while ago to be July 27-29 in West Virginia. =t the London ICAO e-passports task force / ISO WG3 meeting last Thursday, [redacted] also announced the test in the week of August 23 in Sydney. The attached file is what was presented at the meeting. Four reader manufacturers committed to coming, and we will have sample passports from=a few nations ready. Chip vendors will also likely provide samples. I thi=k that most of the technical questions of manufacturers were answered at th= London meeting. (I don't remember seeing you or Axel at it, however).

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, June 24, 2004 4:41 AM
To: [redacted]
Cc: [redacted]
Subject: Dates for July testing

(b)(6)

Dear [redacted]

as [redacted] already wrote:

In order to plan our travel schedule we need for the upcoming consultations with the DHS side a reliable time schedule.

Follwing the talks between secretaries Ridge (US) and Schily (D), a high ranking German delegation from our ministry of the interior plans to visit the DHS in Washington on July 15/16 in order to discuss and present the German advances in the field of biometric MRTDs (passports and visa).

Ideally, we would start our technical consultations in West Virginia (with technicians, programmers) Monday 12 or Tuesday 13 in order to refer to those results on July 15/16 in the official meeting in Washington.

The second best possibility would be to start with the official meeting in Washington July 15/16 and let the technical consultations in West Virginia follow, starting Monday, July 19.

We have a lot of pressure on those dates, so could you please get back to me today by phone (best mobile) to confirm those dates? I'll try to call you as well.

Mit freundlichen Grüßen,

[redacted]

(b)(6)

[redacted]
Bundeskriminalamt
65173 Wiesbaden

(b)(6)

[redacted]
Email: mailto:

e-Passport Test

West Virginia, USA – July 27-29
Sydney, Australia – week of August 23

Test Objectives

- Part 1
  - 1) Detect whether chip(s) in read range
    - Test chip inlay in front cover, inside page and back cover
  - 2) Detect type of chip (A or B)
  - 3) Retrieve Data Group 1, Data Group 2 with 15-20 K Photo (at 424 KBPS)
- Part 2
  - 1) Detect if the chip a passport, visa or other
  - 2) Detect if the chip uses Basic Access Control (BAC)
  - 3) Retrieve Data Groups 1 & 2 using BAC
  - 4) Retrieve Photo > 32K

Test Objectives (continued)

- Part 3
  - 1) Detect how many chips are in range
  - 2) Detect how many are A and B and how many are passport, visa and/or other
  - 3) Determine (test) impact of different power levels and chip(s)

  - Note: testing assumption: 1 passport chip, with 2 visa chips

Passport Reader "Style"

- Closed Passport (if coupled with a 'swipe' MRZ reader
- Full page reader: Two Styles
  - Flat (read chip on either page)
  - 90 degrees, with data page read on top (chip may be on either page)

Call for Participation

- Governments
  - Samples of e-passport prototypes
- Chip Vendors
  - Working samples encoded with DG1, DG2 to be supplied by testers
- Reader Manufacturers
  - Prototype working readers
  - Technicians may attend testing sessions

Contacts

- [redacted] (b)(6)
  - U.S. Department of Homeland Security
  - [redacted] (b)(6)
- [redacted]
  - Passports Australia
  - [redacted] (b)(6)

Process

- e-Mail [redacted] & [redacted] by June 30
  (b)(6) (b)(6)
  - Company name
  - Point of contact name / e-mail / phone number
  - Describe what will be provided by your group to test and number of people to attend and whether it will be for one or both sessions

few nations ready. Chip vendors will also likely provide samples. I thi=k that most of the technical questions of manufacturers were answered at th= London meeting. (I don't remember seeing you or Axel at it, however).

[redacted] (b)(6)

-----Original Message-----
From: [redacted] (b)(6)
Sent: Thursday, June 24, 2004 4:41 AM
To: [redacted]
Cc: [redacted]
Subject: Dates for July testing

[redacted] (b)(6)

as [redacted] already wrote:

In order to plan our travel schedule we need for the upcoming consultations with the DHS side a reliable time schedule.

Follwing the talks between secretaries Ridge (US) and Schily (D), a high ranking German delegation from our ministry of the interior plans to visit the DHS in Washington on July 15/16 in order to discuss and present the German advances in the field of biometric MRTDs (passports and visa).

Ideally, we would start our technical consultations in West Virginia (with technicians, programmers) Monday 12 or Tuesday 13 in order to refer to those results on July 15/16 in the official meeting in Washington.

The second best possibility would be to start with the official meeting in Washington July 15/16 and let the technical consultations in West Virginia follow, starting Monday, July 19.

We have a lot of pressure on those dates, so could you please get back to me today by phone (best mobile) to confirm those dates? I'll try to call you as well.

Mit freundlichen Grüßen,

[redacted] (b)(6)

[redacted] (b)(6)

Email: [redacted]

From: [redacted] (b)(6)
To:
Cc: [redacted]
Sent: Thursday, June 24, 2004 2:54 PM
Subject: RE: Upcoming e-passports tests

Great!

[redacted] (b)(6)

-----Original Message-----
From: [redacted] (b)(6)
Sent: Wednesday, June 23, 2004 5:11 PM
To: [redacted]
Subject: Re: Upcoming e-passports tests

Hi [redacted] (b)(6)

For the first POE tests I can easily bring a PC-based application to the party that (without addressing proper systems integration) will accept whatever image is recovered from a passport, and an image from whatever live camera is used, and will render a verification decision. I'd use one or more vendors' SDKs inside this application.

[redacted] (b)(6)

Quoting [redacted] (b)(6)

> Well -- I'm finally back!
>
> As you (hopefully) know, ICAO approved the Logical Data Structure (LDS)
and
> the PKI schema for e-passports at its meeting in Montreal during May.
This
> was followed by a joint meeting of the e-passports task force from ICAO
and
> WG8 from the International Standards Organization (ISO). That meeting
> occurred in London last Thursday. The purpose was to bring together
> national government representatives, chip manufacturers, passport
> manufacturers and passport reader manufacturers and resolve any final
> questions that they have on the technical aspects of implementing
> e-passports and developing the readers to work with them. I believe that
> the meeting was successful in that regard. I should have a copy of the
> questions and answers raised at that meeting in the next day or so. I
will
> forward them to you immediately.

>
> One important outcome of the meeting was that we publicized the plans for
> the Morgantown, West Virginia (at the National Biometrics Security project
> laboratories) and Sydney tests. I wrote the attachment to this e-mail
> during the meeting there. [redacted] (of Australia - who chaired the
> London meeting) and I both presented it to the representatives. We have
> commitments from at least 4 passport reader vendors to participate, and
> possibly other will come as well. We will have a few chip venders
bringing
> their samples, as well as prototype passports from the US, Germany,
> Australia, NZ, and Belgium. The focus of this test will be to get the
chips
> read and the data properly retrieved. I would like to see the details on
> what tests that NIST-WEST has worked up. We need to order whatever
> equipment is needed to perform those tests and have it ready in time.
Also
> -- during the tests, we will want to have enough space for the
technicians
> from the various groups to work if they discover problems with their
> implementations. We will want to be able to test the readers separately,
> without having one vendor see the work going on with his competitors.
Also
> - we will need to ensure an adequate number of rooms at the hotel for
> people and get a good rate for them. I will work on an agenda, with some
> time for nations to brief about their testing work done to date and the
> status of their passport development/production. The West Virginia tests
> will allow manufacturers to 'iron out' their problems with interaction
from
> us. This will be followed a month later by a test during the week of
August
> 23 in Sydney, Australia. Following that session, the vendors should be
able
> to finalize their products and the nations should be able to proceed with
> their plans for passport production and reader specifications.
>
> We will conduct a 'mock port of entry' test during November. For this
test,
> we will set up an inspection booth and run several people through. We
will
> also include imposters in the tests. We want to find the best
'ergonomics'
> for the layout and develop processes and procedures that will work. It is
> important to remember that the e-passport system, at this point, will be a
> stand-alone unit. We will not be integrating it with IBIS or anything
else
> during these tests.
>
> Following the November tests, we will prepare for the live tests. These
> will be conducted at LAX (Terminal 4 for Qantas; other terminals (?) such
as
> Terminal 2 for Air NZ), IAD, Sydney (Australia), and possibly Brisbane

(b)(6)

> (Australia) and Frankfurt (Germany). These tests will run until about
May.
> We should have passports issued to citizens of the US, Australia, NZ, and
> Belgium by the time of the tests. Germany and the Netherlands may also be
> able to issue a limited number of passports by that time. The first test
> participants from the US will be official passport holders, and probably
> airline crew. The US DOS may issue passports free of charge (for limited
> duration) to air crew who would be willing to participate in the test.
> Australia will start issuing their passports to QANTAS crew. I have not
> confirmed yet whether Denmark and Finland will have their passports
issued
> by that time. In order to meet the likely October 26, 2005 deadline for
> having the capability to deal with e-passports at ALL ports of entry, we
> will need to start installing reader units in June at about the rate of 25
> POEs a week! We need to pull together a team to plan for the tests
> (US-VISIT Increment Management?) -- which lanes to use (i.e. can we use
the
> INSPASS referral lane as a 'carrot' for the test participants?); how to
> train the staff for the tests; how to collect and analyze the data from
the
> test, etc.
>
> For all of the upcoming tests, it is important that our team involve
people
> who have 'real life' experience on the front line with Inspections, as
well
> as people involved in Standard Operating Procedures, technical testing,
etc.
> (US-VISIT Mission Ops, CBP-OFO, ...)
>
> It will be an exciting next few months, and I look forward to the it all.
I
> hope that you do, too!
>
> Thanks,
>
[redacted] (b)(6)
>
> <<e-Passport Test.ppt>>
>

From:
To: [redacted]

(b)(6)

Sent: Wednesday, June 23, 2004 3:27 PM
Attach: e-Passport Test.ppt
Subject: Upcoming e-passports tests

Well -- I'm finally back!

As you (hopefully) know, ICAO approved the Logical Data Structure (LDS) and the PKI schema for e-passports at its meeting in Montreal during May. This was followed by a joint meeting of the e-passports task force from ICAO and WGS from the International Standards Organization (ISO). That meeting occurred in London last Thursday. The purpose was to bring together national government representatives, chip manufacturers, passport manufacturers and passport reader manufacturers and resolve any final questions that they have on the technical aspects of implementing e-passports and developing the readers to work with them. I believe that the meeting was successful in that regard. I should have a copy of the questions and answers raised at that meeting in the next day or so. I will forward them to you immediately.

One important outcome of the meeting was that we publicized the plans for the Morgantown, West Virginia (at the National Biometrics Security project laboratories) and Sydney tests. I wrote the attachment to this e-mail during the meeting there. [redacted] (of Australia - who chaired the London meeting) and I both presented it to the representatives. We have commitments from at least 4 passport reader vendors to participate, and possibly other will come as well. We will have a few chip venders bringing their samples, as well as prototype passports from the US, Germany, Australia, NZ, and Belgium. The focus of this test will be to get the chips read and the data properly retrieved. I would like to see the details on what tests that NIST-WEST has worked up. We need to order whatever equipment is needed to perform those tests and have it ready in time. Also -- during the tests, we will want to have enough space for the technicians from the various groups to work if they discover problems with their implementations. We will want to be able to test the readers separately, (b)(6) without having one vendor see the work going on with his competitors. Also - we will need to ensure an adequate number of rooms at the hotel for people and get a good rate for them. I will work on an agenda, with some time for nations to brief about their testing work done to date and the status of their passport development/production. The West Virginia tests will allow manufacturers to 'iron out' their problems with interaction from us. This will be followed a month later by a test during the week of August 23 in Sydney, Australia. Following that session, the vendors should be able to finalize their products and the nations should be able to proceed with their plans for passport production and reader specifications.

We will conduct a 'mock port of entry' test during November. For this test, we will set up an inspection booth and run several people through. We will also include imposters in the tests. We want to find the best 'ergonomics' for the layout and develop processes and procedures that will work. It is important to remember that the e-passport system, at this point, will be a stand-alone unit. We will not be integrating it with IBIS or anything else during these tests.

Following the November tests, we will prepare for the live tests. These will be conducted at LAX (Terminal 4 for Qantas; other terminals (?) such as Terminal 2 for Air NZ), IAD, Sydney (Australia), and possibly Brisbane (Australia) and Frankfurt (Germany). These tests will run until about May. We should have passports issued to citizens of the US, Australia, NZ, and Belgium by the time of the tests. Germany and the Netherlands may also be able to issue a limited number of passports by that time. The first test participants from the US will be official passport holders, and probably airline crew. The US DOS may issue passports free of charge (for limited duration) to air crew who would be willing to participate in the test. Australia will start issuing their passports to QANTAS crew. I have not confirmed yet whether Denmark and Finland will have their passports issued by that time. In order to meet the likely October 26, 2005 deadline for having the capability to deal with e-passports at ALL ports of entry, we will need to start installing reader units in June at about the rate of 25 POEs a week! We need to pull together a team to plan for the tests (US-VISIT Increment Management?) -- which lanes to use (i.e. can we use the INSPASS referral lane as a 'carrot' for the test participants?); how to train the staff for the tests; how to collect and analyze the data from the test, etc.

For all of the upcoming tests, it is important that our team involve people who have 'real life' experience on the front line with Inspections, as well as people involved in Standard Operating Procedures, technical testing, etc. (US-VISIT Mission Ops, CBP-OFO, ...)

It will be an exciting next few months, and I look forward to the it all. I hope that you do, too!

Thanks,

[redacted] (b)(6)

<<e-Passport Test.ppt>>

e-Passport Test

West Virginia, USA – July 27-29

Sydney, Australia – week of August 23

See slide presentation
after 6/29/04 5-page message
(pages 74-80)

From: [redacted]
To: [redacted] (b)(6)

Subject: Final Standards (Zipped File)
Date: Fri, 30 Apr 2004 16:40:23 -0400
X-Mailer: Internet Mail Service (5.5.2657.72)
X-Scanned-By: milter-spamc/0.10.108 (franklin-node1 [132.163.128.81]);
Fri, 30 Apr 2004 14:38:08 %z
X-Spam-Flag: NO
X-Spam-Status: NO, hits=1.30 required=5.00
X-MailScanner-SpamScore: s

All:

Attached is the zipped file consisting of the final standards to
date. Am
going ahead and sending this separate from anything else as it is
HUGE!
Hope I don't clog anybody's pipes getting this to you!

More to follow in other notes. Thanks for participating today!

Hope you all have a great weekend!

[redacted]<<TAG 15.zip>>

[redacted] (b)(6)
DHS US-VISIT Program
Phone: [redacted]
Email:

TAG 15.zip

From: [redacted]
To:

(b)(6)

Sent: Tuesday, January 20, 2004 5:16 PM
Attach: Expectations for contactless reader.doc
Subject: FW: e-Passports - Expectations for Contactless Readers

This is the set of guidelines for the Australia test on Feb. 5, 6. I will be atttending along with [redacted] from the DOS. I think we will gain a lot of information from that as to how to proceed with our work here.

(b)(6)

Brad

-----Original Message-----
From: [redacted]

(b)(6)

Sent: Thursday, January 15, 2004 10:25 PM
To: [redacted]

(b)(6)

US – VISIT PROGRAM
OFFICE OF THE CHIEF STRATEGIST
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

_1page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

	Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Title 5, United States Code, (U.S.C.) Section 552 (FOIA)					Title 5, U.S.C. Section 552a(PA)	
		(b)(1)		(b)(7)(D)		(d)(5)
		(b)(2)		(b)(7)(E)		(j)(2)
		(b)(3)		(b)(7)(F)		(k)(1)
		(b)(4)		(b)(8)		(k)(2)
		(b)(5)		(b)(9)		(k)(3)
X		(b)(6)				(k)(4)
		(b)(7)(A)				(k)(5)
		(b)(7)(B)				(k)(6)
		(b)(7)(C)				(k)(7)
		Documents originated with (an) other Government agency(ies). These documents were referred to that agency for review and direct response to you.				

_pages contain information furnished by (an) other Government agency (ies). You will be advised by the FOIA Office to the releasability of this information.

______pages have not been provided to you at this time because a final release determinatiqn has not been made. You will be advised as to the disposition at a later date.

For your information

Page 2 of a three page email is being withheld in its entirety under FOIA exemption b(6).

[redacted]
Subject: e-Passports - Expectations for Contactless Readers

Hello All,

[redacted] has asked me to send this attachment to everyone on the mailing list from the ICAO/NTWG e-Passports Task Force meeting he chaired in Glasgow last September.

b(6)

The document is self-explanatory, but please reply by return email with any questions.

Regards
[redacted]
Passports Australia

(See attached file: Expectations for contactless reader.doc)

BACKGROUND

On 5th-6th February 2004, the Australian Department of Foreign Affairs & Trade – Passports Branch will be conducting a series of tests of different contactless chips, readers and writers.

The aim is to identify the readers/writers in the marketplace and their effectiveness at reading contactless chips on which data has been written in accordance with the ICAO blueprints for deployment of biometrics in passports – in particular ISO 14443 Type A/B and the Logical Data Structure specified by ICAO for formatting of passport electronic data.

You are invited to provide any of the following:

- Contactless chip(s) of capacity >= 32 Kilobytes in either credit card format or embedded within sample passports
- Chip writers and Chip readers (which can be combo devices) on their own and/or combined with passport MRZ readers

The testing will be informal and on a "good faith" basis. The objective is simply to see how well contactless chips and reader/writers "plug and play".

We will pay for return of any equipment sent.

It is likely representatives of other Governments besides Australia will participate in this informal testing exercise.

Delivery address for equipment/packages is to

[redacted]
Passports Branch
The RG Casey Building
BARTON ACT 2600 AUSTRALIA

For all shipments please advise by email the courier, date sent and the airway bill consignment number to

[redacted] (b)(6)

Shipments should be sent as soon as possible to avoid any possible hold-ups in Customs.

EXPECTATIONS FOR CONTACTLESS READER/WRITERS

Hardware and Interface

- Must conform to ISO 14443. Must read both Type A and Type B. Must write either Type A or Type B or preferably either Type.
- Must read at a distance of up to 2cm
- Device drivers for Microsoft Windows 2000 or XP.
- Conformance to Windows PC/SC standard - Highly Desirable.
- Connection – USB 1.1 or 2.0 preferable. Serial or parallel will be accepted.
- Able to handle extended length in the ISO 7816-4 READ BINARY command
- Reader must be capable of accepting ID3 size cards/passport books
- Form Factor – Flat Bed Scanner is preferable to Slot

Software

Minimum

- Application that will show presence/absence of chip
- Display results from ATR (Serial number etc)
- Data rate of 106kbps\
- Read cards with 32 Kilobytes (or more) of data
- Supply of demonstration software to write and read (in a format of your choice)
- Supply of at least one demonstration contactless card (preferably >= 32K but lower will be accepted)
- Must support commands SELECT FILE, READ BINARY
- Should support commands GET CHALLENGE, EXTERNAL AUTHENTICATE, PSO_MSE, PSO_CDS

Desirable

- Supply of demonstration software to read data from a card structured in ICAO LDS version 1.0 format or later.
- Display the data on Screen by LDS Data Group
- Display reading speed for each DG and for overall data
- Data rate of 212kbps, 424kbps or greater

Documentation

- Any special instructions, observations or questions you may have
- For Readers manufacturers - list of cards/manufacturers you believe your reader works with – and those you believe it does not work with
- For chip manufacturers - list of readers (make and model) you believe your reader works with – and those you believe it does not work with

From: [redacted] (b)(6)
To:

Cc:

Sent: Monday, December 22, 2003 4:19 PM
Attach: Inrement2A_Team Mtg (22 DEC 03).ppt
Subject: Inc 2A Overview

All,

Attached is the Increment 2A Overview briefing updated after last week's meetings, reviews and comments.

Please let me know if you have any questions or comments.

<<Inrement2A_Team Mtg (22 DEC 03).ppt>>

[redacted] (b)(6)

US-VISIT Increment 2A Overview

United States

Visitor and Immigrant Status Indicator Technology

Homeland
Security

US-VISIT Program

Purpose:

- **To collect, maintain, and share information, including biometric identifiers, on foreign nationals, through a dynamic system to determine whether the individual:**
  - Should be prohibited from entering the U.S.
  - Can receive, extend, change, or adjust immigration status
  - Has overstayed or otherwise violated the terms of their admission
  - Should be apprehended or detained for law enforcement action
  - Needs special protection/attention (i.e., refugees)

US-VISIT Program (Continued)

Goals:

- Enhance the security of our citizens and visitors
- Expedite legitimate travel and trade
- Ensure the integrity of the immigration system
- Safeguard the personal privacy of our visitors
- Protect the environment

US-VISIT Implementation Requirements

Increment 1 – 12/31/03

- Air & Sea

Increment 2A – 10/26/04

- Air, Sea & Land (Read biometrically enabled documents)

Increment 2B – 12/31/04

- Land

Increment 3 – 12/31/05

- Increment 2B extended capability to remaining land POEs

Increment 4 – End Vision

- Single Interface and System Modernization

US-VISIT Increment 2A

Mission:

- To acquire and deploy document readers with the capability to read Integrated Circuit (IC) chips on biometrically enabled travel documents that are compliant with International Civil Aviation Organization (ICAO) standards and use biometric verification techniques as part of the identity checking process.

Legislative Requirements - 10/26/04

- All Visa Waiver Program (VWP) countries must issue biometrically enabled travel documents following ICAO standards
  - Since the VWP is a reciprocal program, the Department of State (DOS) will also be placing Integrated Circuit (IC) chips, including biometric and biographic (e.g. name, DOB, address) data into U.S. passports following ICAO standards
  - *ICAO 9303 Logical Data Structure (LDS) mandates digital facial biometric*
  - *ICAO 9303 LDS permits fingerprint and iris biometrics as optional*
- United States air, sea, and land Ports of Entry (POEs) must deploy the capability to read biometric travel documents

Changes at POEs - Aliens

- Visa waiver travelers having IC chip passports issued after 10/26/04 have a biometric check performed.
- Visa waiver travelers having a passport issued after 10/26/04 that do not include an IC chip may require having their photo and fingerprints registered by US-VISIT as being done for visa holders (per policy draft 12/03/03)
- *Visa Waiver travelers with passports issued prior to 10/26/04 have no changes in their processing.*
- Re-entry permits & refugee travel documents issued by the U.S. during FY05 will include IC chips containing biometric data used for verification.

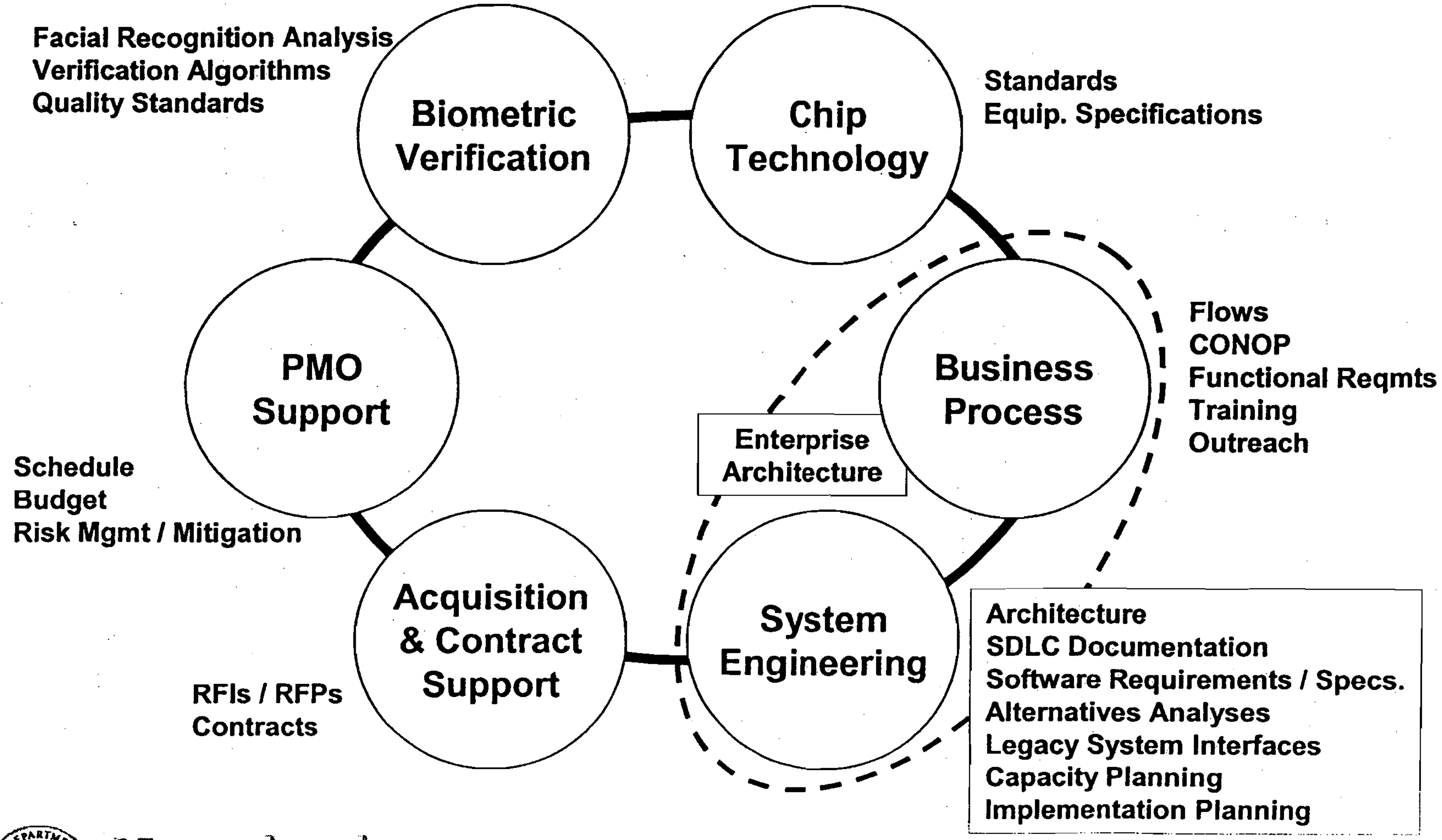
115

Preparation Responsibilities

- *Biometrics Evaluation Team*
  - *Finalize International Standards for IC Passports*
  - *Determine VWP nation eligibility criteria*
  - *Establish national and international working arrangements*
  - *Determine test and evaluation methodology*
  - *Acquire test samples (chips, passports, readers) and facial recognition systems*
  - *Perform laboratory tests*
  - *Perform mock POE tests*
  - *Develop specifications for workstations and hardware / software acquisitions / modifications / upgrades*
- Joint Biometrics Evaluation / Implementation Teams
  - Acquire and install units for live tests
  - Perform live test and provide feedback for final design
- Implementation Team
  - Acquire and install full operational capability at all POEs (OCTOBER 26, 2004)

116

Increment 2A Activity Areas



Biometric Verification

Facial Recognition Analysis
Verification Algorithms
Quality Standards

Chip Technology

Standards
Equip. Specifications

Business Process

Flows
CONOP
Functional Reqmts
Training
Outreach

Enterprise Architecture

System Engineering

Architecture
SDLC Documentation
Software Requirements / Specs.
Alternatives Analyses
Legacy System Interfaces
Capacity Planning
Implementation Planning

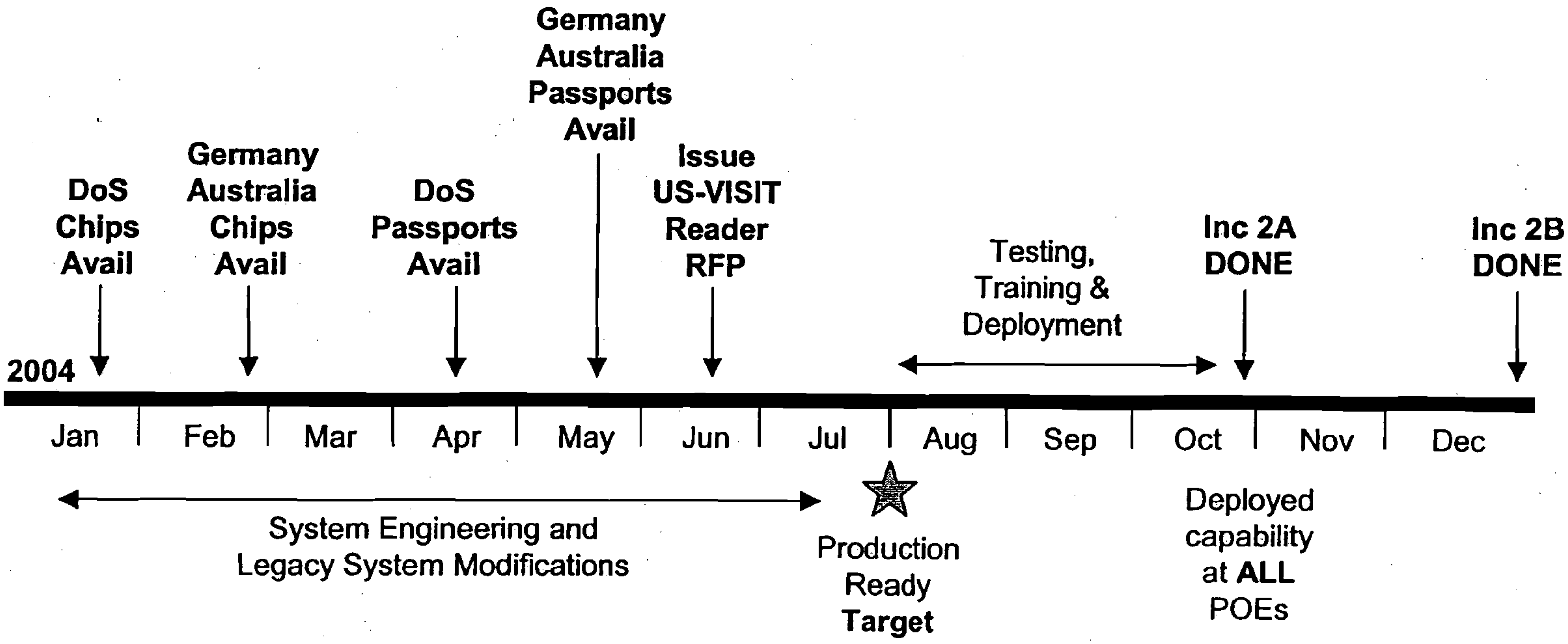
Acquisition & Contract Support

RFIs / RFPs
Contracts

PMO Support

Schedule
Budget
Risk Mgmt / Mitigation

Increment 2A Timeframes


2004
DoS Chips Avail
Germany Australia Chips Avail
DoS Passports Avail
Germany Australia Passports Avail
Issue US-VISIT Reader RFP
Testing, Training & Deployment
Inc 2A DONE
Inc 2B DONE
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
System Engineering and Legacy System Modifications
Production Ready **Target**
Deployed capability at **ALL** POEs

Possible Implementation Levels

- Level 0 – Read Chip, Take picture, Perform Verification
- Level 1 – Level 0 plus Examine Digital Signature
- Level 2 – Level 1 plus Compare Printed Picture to Stored Picture and MRZ data to Stored MRZ data
- Level 3 – Level 2 plus fixed watch list check
- Level 4 – Level 3 but with dynamic watch list

119

Stand-Alone Alternative

- Kiosk – VW traveler places passport on kiosk reader and has photo taken with facial recognition performed in kiosk. Results from the kiosk forwarded to inspector in booth. Place in queue or before one designated lane
- System placed at inspection booth (not a kiosk) – Inspector directs VW traveler on usage and can view results
  - Level 0 – Feasible
  - Level 1 – Feasible; Requires periodic updates of digital signature tables
  - Level 2 – Feasible; Requires periodic updates of digital signature tables; Requires full page reader
  - Level 3 – Feasible; Requires periodic updates of digital signature tables and fixed facial watch list data
  - Level 4 - Infeasible

Integrated Upgrade Alternative

- Link results of passport/chip reader to inspector's workstation and IBIS
- Design could be either kiosk or countertop units
  - Level 0 – Feasible
  - Level 1 – Feasible; Requires periodic updates of digital signature tables
  - Level 2 – Feasible; Requires periodic updates of digital signature tables; Requires full page reader
  - Level 3 – Feasible; Requires periodic updates of digital signature tables and fixed facial watch list data
  - Level 4 - Feasible; Allows possibility of linkage to TTIC data

Status – Biometrics Evaluation Team

- US-VISIT established a program with Department of State and US CIS to test the new U.S. travel documents
  - Sample chips to be provided by DOS in January 2004
  - Sample passports to be provided by DOS in April 2004
  - Sample travel documents to be provided by ÇIS (Date to be determined)
- US-VISIT established joint testing programs with Germany, New Zealand, Australia, Japan, and the Netherlands, and has initiated a separate biometric vulnerability research effort with the UK
  - Sample chips to be provided by Germany & Australia in February 2004
  - Sample passports to be provided by Germany & Australia in May 2004
- Laboratory will be ready in January 2004 at NBSP
- Agreements reached on data and data formats for passport chips (US-VISIT participation in ICAO, ISO, and M1 working groups)
- DOS Request for Proposals is on the street for new U.S. passports with IC chips

Status (Continued)

- PEC contractor brought on board to prepare schedules and track project (funded)
- Bi-weekly status meetings underway for Increment 2a team
- Monthly coordination meetings with DOS underway (DOS invited to Increment 2a team meetings)
- US-VISIT invited to participate in DOS RFP evaluation

US-VISIT Increment 2A

Next Steps:

- Establish laboratory and mock POEs (entry & exit)
- Review photos captured in Increment 1 to determine suitability for facial recognition
- Test and evaluate facial recognition systems in mock POEs – proceed with procurement action
- Test and evaluate chips, both before and after embedded in passports
- Refine specifications for the full page/chip passport reader for procurement action
- Modify existing software systems as required
- Define new standard operating procedures & training for Inspectors
- Install, test, and evaluate new system

Technology Implications for Increment 2A

- Facial Recognition Technology
  - Technology and vendors are still emerging
  - Numerous issues with performing analysis based upon photo capture in “real world” situations (e.g., poorly lit POE lanes)
- Passport Readers
  - 14443 Chip Reader for ICAO LDS will be slow (estimates at 7 seconds)
  - Format factor and inspector processing necessitate integrated device for both full page scanning and chip reading
- Systems Engineering
  - Numerous stakeholders and organizations supporting this effort
  - Many technical decisions have operational considerations
  - Standards and standard operating procedures are in flux (e.g., ICAO Digital Certificate processing)
- Interfaces with Inspector
  - Screen modification to reflect results of biometric verification and checks of MRZ and printed photo against data stored on chip

Technology – Facial Recognition

- Tests were performed by NIST & DARPA (FRVT 2002).
    - Top vendors: Cognitec (Germany) & Identix (US)
    - Tests by NIST: Improved accuracy by combining results of the two vendor algorithms
- *One-to-one comparisons for VERIFICATION is what is required by law.*
    - False Rejection and False Acceptance rates very low <1% based on good quality comparison pictures like those in passports and with good lighting on the subject for the live image
    - One-to-one comparison used for identity verification and document fraud detection
- For a one-to-many (~10,000) comparison with a 1% false hit rate test results are approximately 52% accurate.
- For a one-to-few comparison (~100) with a 1% false hit rate test results are approximately 75% (Watch list).
    - In order to achieve rejection rates <1% must limit candidate gallery to about 100 images
    - If watch list implemented, must have a dynamic generation of the watch list suited to the traveler type (RESEARCH AREA not expected for October 2004 implementation)
- The statistics improve with multiple systems or multiple images (or both).

126

Preparation – Facial Recognition

- Examine enrollment photos from IDENT: IMAGE QUALITY TEST (already funded)
  - Photos from IDENT cross-matched with IBIS data to provide an input tape to NIST with images tagged by POE, lane, date & time
  - Determine if photos can be successfully processed in a test environment at NIST using the facial recognition algorithms validated by FRVT2002 (Cognitec & IDENTIX)
  - Examine problems by location of photo image
    - Determine changes in lighting, background, and/or positioning to get images usable in facial recognition
    - Determine if current cameras need replacement for Increment 2a
  - Document changes as input to Increment 2a implementation / facility modifications
- Laboratory Preparation (already funded)
  - NIST to specify parameters for 1-1 verification settings in facial algorithms based on policy input from US-VISIT (target rejection levels)
  - NIST to develop process to merge recognition algorithms with the highest scores from FRVT 2002

Technology – Passport Readers

- Existing Technology
  - Swipe readers at POEs to get MRZ data
  - Full page readers incorporated in exit kiosk design extracts MRZ data and performs some fraud analysis
  - Chip readers are commercially available for 14443 chips
- Requirement: For certain VWP nations the MRZ is the key used to open the chip so that biometric data can be extracted from the chip and used for a live comparison against the biometric sample collected from the traveler
- Need: Integrate capability to perform a full-page read and access the chip using proximity readers
  - Full page readers offer capability to do more extensive fraud detection
    - Compare printed photo to photo stored on the chip to detect photo substitution
    - Examine holograms and security features of passports (magnetic threads, etc.) that should be present on authentic passports
- Current Status: At least 2 passport reader manufacturers have developed prototype full page / chip readers for the new passport formats

Technology – Passport Readers

- Chip Readibility Testing
  - NIST is preparing a test protocol on chip read testing (already funded)
  - Utilize the test protocol at NBSP's laboratory to evaluate the prototype chips and passports provided by DOS, US CIS, Japan, Germany, Australia, Netherlands, UK, New Zealand using readily available devices (funded by NSA to NBSP)
- Integrated Passport Reader Evaluation
  - Issue RFI to passport reader manufacturers
  - Examine results of Australian demonstration in February 2004 (major vendors invited to participate)
  - Get first samples of passport and chip readers from the vendors
    - **PURCHASE vs. COOPERATIVE DEVELOPMENT DECISION NEEDED HERE**
    - **DECISION ON HOW TO PROVIDE FEEDBACK TO INDUSTRY TO FURTHER DEVELOP THEIR DEVICE(S)**
  - Evaluate samples against operational concept at test laboratory in NBSP
  - Finalize operational and technical specifications for procurement action in June 2004

From: [redacted] (b)(6)
To:

Cc:

Sent: Monday, December 22, 2003 1:30 PM
Attach: VWP WG Meeting (16 DEC 03).xls; Inc 2 VWP WG Minutes (16 DEC).doc; Increment 2 PMP (19 DEC 03) P98 mpp
Subject: VWP WG Meeting 16 DEC 03

<'--[if gte =so 9]><![endif]-->
All

Attached are the =esults of last week's Visa Waiver Program (VWP) Working Group (WG) meeting (16 DEC =3). The files include the meeting attendees list, notes, and an =pdated project schedule.

Please let me know if =ou have any questions.

Hope you and yours =ave a safe, happy holiday season!

[redacted] (b)(6)

[redacted]	MITRE	[redacted]	[redacted]	[redacted]
[redacted]	NIST	[redacted]	[redacted]	[redacted]
[redacted]	DHS US-VISIT	[redacted]		[redacted]
[redacted]	NIST	[redacted]	[redacted]	[redacted]
[redacted]	DHS US-VISIT	[redacted]		[redacted]
[redacted]	DHS US-VISIT	[redacted]	[redacted]	[redacted]
[redacted]	US CIS	[redacted]	[redacted]	[redacted]
[redacted]	DHS US-VISIT	[redacted]		[redacted]
[redacted]	MITRE	[redacted]		[redacted]
[redacted]	NBSP	[redacted]	[redacted]	[redacted]
[redacted]	MITRE	[redacted]		[redacted]
[redacted]	DHS US-VISIT	[redacted]		[redacted]
[redacted]	DHS US-VISIT	[redacted]	[redacted]	[redacted]
[redacted]	DHS US-VISIT	[redacted]	[redacted]	[redacted]
[redacted]	DHS US-VISIT	[redacted]	[redacted]	[redacted]
(b)(6)		(b)(6)	(b)(2)	(b)(6)

US – VISIT PROGRAM
OFFICE OF THE CHIEF STRATEGIST
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

3 page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Title 5, United States Code, (U.S.C.) Section 552 (FOIA)					Title 5 U.S.C. Section 552a(PA)	
		(b)(1)		(b)(7)(D)		(d)(5)
		(b)(2)		(b)(7)(E)		(j)(2)
		(b)(3)		(b)(7)(F)		(k)(1)
		(b)(4)		(b)(8)		(k)(2)
X		(b)(5)		(b)(9)		(k)(3)
		(b)(6)				(k)(4)
		(b)(7)(A)				(k)(5)
		(b)(7)(B)				(k)(6)
		(b)(7)(C)				(k)(7)
		Documents originated with (an) other Government agency(ies). These documents were referred to that agency for review and direct response to you.				

_pages contain information furnished by (an) other Government agency (ies). You will be advised by the FOIA Office to the releasability of this information.

_______pages have not been provided to you at this time because a final release determination has not been made. You will be advised as to the disposition at a later date.

For your information

DRAFT copy of the Visa Waiver Program (VWP) meeting notes (3 pages) are being withheld in their entirety, at this location in the file under FOIA exemption b(5).

US – VISIT PROGRAM
OFFICE OF THE CHIEF STRATEGIST
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

2 page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Title 5, United States Code, (U.S.C.) Section 552 (FOIA)

Title 5, U.S.C. Section 552a(PA)

		(b)(1)		(b)(7)(D)		(d)(5)
		(b)(2)		(b)(7)(E)		(j)(2)
		(b)(3)		(b)(7)(F)		(k)(1)
		(b)(4)		(b)(8)		(k)(2)
X		(b)(5)		(b)(9)		(k)(3)
		(b)(6)				(k)(4)
		(b)(7)(A)				(k)(5)
		(b)(7)(B)				(k)(6)
		(b)(7)(C)				(k)(7)

Documents originated with (an) other Government agency(ies). These documents were referred to that agency for review and direct response to you.

_pages contain information furnished by (an) other Government agency (ies). You will be advised by the FOIA Office to the releasability of this information.

_______pages have not been provided to you at this time because a final release determination has not been made. You will be advised as to the disposition at a later date.

For your information

DRAFT copy of the Increment 2 Visa Waiver Program (VWP)outline (2 pages) are being withheld in their entirety, at this location in the file under FOIA exemption b(5).

From: [redacted]
To:
Cc:

(b)(6)

Sent: Thursday, December 11, 2003 11:46 AM
Attach: VWP WG Meeting 2 DEC 03.xls; Inc 2 VWP Meeting (2 DEC) Mod 10 DEC 03.doc; Increment 2 VWP PMP (10 DEC 03).mpp; Diplomatic Note VWP.doc
Subject: FW: VWP WG Meeting 2 DEC 03

All,

This is just a friendly reminder of the Visa Waiver Program meeting next Tuesday, 16 DEC. We have the US-VISIT conference room, #5910, here in Rosslyn reserved from 1400-1600 for this meeting.

I had mistakingly stated in the last paragraph of the meeting notes from 2 DEC that this would be held on 17 DEC, it will NOT, this meeting is separate from the 17th meeting with DOS. The red-lined/updated meeting notes are attached along with an updated schedule file dated 10 DEC 03 (which reflects the updates received from State milestone slide and a few additional tasks status updates).

Please reply to this note if you do not wish to be included on these distributions/list(s).

Thanks, and see you on the 16th!

[redacted] (b)(6)

> -----Original Message----- (b)(6)
> From: [redacted]
> Sent: Wednesday, December 03, 2003 9:09 AM
> To: [redacted] (b)(6)

nd Meeting

2-Dec-03
Attendees List

Name	Organization	Phone	E-mail	Initials
[redacted]	NBSP	[redacted]	[redacted]	
[redacted]	MITRE	[redacted]	[redacted]	
[redacted]	MITRE	[redacted]	[redacted]	
[redacted]	NIST	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	MITRE	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	MITRE	[redacted]	[redacted]	
[redacted]	NBSP	[redacted]	[redacted]	
[redacted]	NBSP	[redacted]	[redacted]	
[redacted]	MITRE	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	
[redacted]	DHS US-VISIT	[redacted]	[redacted]	

(b)(6)

(b)(2)
(b)(6)

(b)(6)

US – VISIT PROGRAM
OFFICE OF THE CHIEF STRATEGIST
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

2 page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

	Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Title 5, United States Code, (U.S.C.) Section 552 (FOIA)					Title 5, U.S.C. Section 552a(PA)	
		(b)(1)		(b)(7)(D)		(d)(5)
		(b)(2)		(b)(7)(E)		(j)(2)
		(b)(3)		(b)(7)(F)		(k)(1)
		(b)(4)		(b)(8)		(k)(2)
X		(b)(5)		(b)(9)		(k)(3)
		(b)(6)				(k)(4)
		(b)(7)(A)				(k)(5)
		(b)(7)(B)				(k)(6)
		(b)(7)(C)				(k)(7)
		Documents originated with (an) other Government agency(ies). These documents were referred to that agency for review and direct response to you.				

pages contain information furnished by (an) other Government agency (ies). You will be advised by the FOIA Office to the releasability of this information.

______pages have not been provided to you at this time because a final release determination has not been made. You will be advised as to the disposition at a later date.

For your information

DRAFT copy of the Visa Waiver Program (VWP) meeting notes (2 pages) are being withheld in their entirety at this location in the file under FOIA exemption b5.

US – VISIT PROGRAM
OFFICE OF THE CHIEF STRATEGIST
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

3 page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

	Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.					
Title 5, United States Code, (U.S.C.) Section 552 (FOIA)					Title 5, U.S.C. Section 552a(PA)	
		(b)(1)		(b)(7)(D)		(d)(5)
		(b)(2)		(b)(7)(E)		(j)(2)
		(b)(3)		(b)(7)(F)		(k)(1)
		(b)(4)		(b)(8)		(k)(2)
X		(b)(5)		(b)(9)		(k)(3)
		(b)(6)				(k)(4)
		(b)(7)(A)				(k)(5)
		(b)(7)(B)				(k)(6)
		(b)(7)(C)				(k)(7)
		Documents originated with (an) other Government agency(ies). These documents were referred to that agency for review and direct response to you.				

pages contain information furnished by (an) other Government agency (ies). You will be advised by the FOIA Office to the releasability of this information.

_______pages have not been provided to you at this time because a final release determination has not been made. You will be advised as to the disposition at a later date.

For your information

DRAFT copy of the Increment 2 Visa Waiver Program (VWP) outline (3 pages) are being withheld in their entirety at this location in the file under FOIA exemption b5.

US – VISIT PROGRAM
OFFICE OF THE CHIEF STRATEGIST
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

_page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

	Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.					
Title 5, United States Code, (U.S.C.) Section 552 (FOIA)					**Title 5, U.S.C. Section 552a(PA)**	
		(b)(1)		(b)(7)(D)		(d)(5)
		(b)(2)		(b)(7)(E)		(j)(2)
		(b)(3)		(b)(7)(F)		(k)(1)
		(b)(4)		(b)(8)		(k)(2)
		(b)(5)		(b)(9)		(k)(3)
		(b)(6)				(k)(4)
		(b)(7)(A)				(k)(5)
		(b)(7)(B)				(k)(6)
		(b)(7)(C)				(k)(7)
✓		Documents originated with (an) other Government agency(ies). These documents were referred to that agency for review and direct response to you.				

3 pages contain information furnished by (an) other Government agency (ies). You will be advised by the FOIA Office to the releasability of this information.

______pages have not been provided to you at this time because a final release determination has not been made. You will be advised as to the disposition at a later date.

For your information

Three page document did not originate with the US-VISIT Program. This document originated with the Department of State (DOS) and we are referring it to DOS for review, release determination and a direct response to you regarding disposition.

From: [redacted]
To:

Cc:
Sent: Wednesday, December 10, 2003 12:13 PM
Subject: FW: ICAO-NTWG Glasgow 17-18 September 2003 - Presentation Material - Amendment

(b)(6)

Gentlemen:

[redacted] asked that I forward you the following e-mail and URL with posted results and/or presentations from the SEP 03 Glasgow meeting. (b)(6)

Hope this information is useful.

[redacted] (b)(6)

-----Original Message-----
From: [redacted]
Sent: Monday, December 01, 2003 7:00 PM
To: [redacted]

(b)(6)

138

US – VISIT PROGRAM
OFFICE OF THE CHIEF STRATEGIST
FREEDOM OF INFORMATION ACT/PRIVACY ACT DELETED PAGE INFORMATION SHEET

_1_ page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

□ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Title 5, United States Code, (U.S.C.) Section 552 (FOIA)					Title 5, U.S.C. Section 552a(PA)	
		(b)(1)		(b)(7)(D)		(d)(5)
		(b)(2)		(b)(7)(E)		(j)(2)
		(b)(3)		(b)(7)(F)		(k)(1)
		(b)(4)		(b)(8)		(k)(2)
		(b)(5)		(b)(9)		(k)(3)
X		(b)(6)				(k)(4)
		(b)(7)(A)				(k)(5)
		(b)(7)(B)				(k)(6)
		(b)(7)(C)				(k)(7)

□ Documents originated with (an) other Government agency(ies). These documents were referred to that agency for review and direct response to you.

pages contain information furnished by (an) other Government agency (ies). You will be advised by the FOIA Office to the releasability of this information.

______pages have not been provided to you at this time because a final release determination has not been made. You will be advised as to the disposition at a later date.

For your information

Page 2 of 4 is being withheld in its entirety at this location in the file.

- Amendment

All, My apologies, in the original email I omitted to give you the Userid for ICAO-NTWG. It is include below.

All,

[redacted] of ICAO-NTWG e-Passports Task Force is pleased to announce that presentation material from Glasgow is now available. (b)(6)

We apologise for the delay with distribution but commitments since the conference have been extremely heavy. In addition we wanted to ensure the material was presented in a professional way.

To access the information go to:

www.eitslondon.org

Note: Link no longer operable!

[redacted] (b)(6)

[redacted] (b)(6)

Every effort has been made to ensure the presentations are displayed as they were supplied. If that is not the case please advise the originator of this email. All documents are presented in pdf format and it was necessary to convert some from mpp, this was to enhance the security of the document from manipulation.

If you no longer wish to be on the distribution list for NTWG e-Passport material or have received this email in error please advise the originator then delete the email.

If on the other hand you are aware of others that are not on the distribution list and would wish to contribute to the NTWG e-Passport project please ask them to email the originator.

Regards
[redacted] (b)(6)
Passports Australia

Note: Page 4 of 4 was blank

Mock Port of Entry Operational Simulation: e-Passports

An international simulation of inspection processing for e-Passports will occur at the Baltimore-Washington International Airport the week of November 29, 2004. This session will examine the impact of using new equipment to read the e-Passports during primary inspection at a port of entry. This process will allow Government personnel associated with inspection processes in several nations to assess how to best integrate the e-Passport reader capabilities into their current operations. This is NOT an evaluation of readers or an interoperability test, but is focused on operational and ergonomic aspects of reading and using the data acquired from e-Passports.

The e-Passport samples will be encoded according to the specifications of the International Civil Aviation Organization (ICAO) and will be provided by several passport manufacturers. Volunteers will be provided these 'dummy' passports with their pictures encoded on the chips. Volunteers will also be asked to provide older pictures of themselves to simulate the effect of aging. The volunteers will act as travelers proceeding through a primary inspections process -- allowing the Government personnel to determine the impact of handling e-Passports under a variety of operational scenarios. Organizations willing and able to provide sample e-Passports encoded with the volunteers' data and pictures should respond by September 30 and indicate the time necessary to prepare such samples.

Please note that this is not a solicitation for purchase or evaluation of any product. Passport readers in several configurations will be required. The readers should be capable of reading both Type A and Type B ISO 14443 compliant integrated circuit chips. Ability to handle chips encoded with Basic Access Control is advantageous but not required, since it will allow operational assessment of the process to correct the MRZ for opening the chip, should it be misread. It is requested that passport reader manufacturers respond by September 30 if they are able to provide a sample reader. To assess the impact of integrating e-Passport readers into an inspection system, we will need to have a description of the output data stream (API, if developed). This description should be provided in the September 30 response. A sample reader must be provided by October 15 in order to ensure that the integration is operational prior to the sessions.

Organizations with systems that can be integrated with passport readers to perform facial recognition against the stored biometric data on the e-Passport are encouraged to provide a description of their system by September 30 and a list of passport readers with which their system has been integrated.

Government organizations wishing to participate in and/or observe these simulations should respond by October 15 with a list of persons attending. If possible, these individuals should send ICAO-compliant photographs so that they can be included in the pool of 'volunteer travelers.'

All responses should be sent to:

(b)(6)

FAQ – ICAO PKI

Frequently Asked Questions – ICAO MRTD PKI Initiative

V 0.2 January 12, 2004

1. *What is the objective of the ICAO PKI initiative?*

The ICAO PKI initiative is intended to provide standards and a simple international infrastructure to support digital signatures applied to Machine Readable Passports (MRPs) and other Machine Readable Travel Documents (MRTDs). These digital signatures are particularly intended to permit authentication of basic data, as contained in the Machine Readable Zone (MRZ) of the passport, plus digitized biometric measurements and other data, that are stored by the issuing country in advanced document storage devices such as Integrated Circuit Chips (ICCs) contained within the MRP or MRTD. In this way the computer-readable data so stored can be determined to be genuine (issued undeniably by the issuing State) and unchanged, and so acts as a further security measure to ensure the authenticity of the MRP or MRTD.

2. *How will the ICAO PKI initiative operate?*

Each country will install a basic PKI infrastructure for the sole purpose of applying digital signatures to passports and other MRTDs it issues. These digital signatures will be used in accordance with ICAO international standards regarding algorithms, key lengths, hashing methods, key lifetimes, and other standards and practices. Each country will have only a limited number of keys in use for signing purposes at any time, and these will change on a regular basis.

Each country will establish at least two levels of keys: a "Country Signing Key" and a "Document Signing Key". The former is a high-level key used to validate (sign) the certificates for its Document Signing Keys. The Document Signing (private) Key is used to sign the data it stores on the each MRTD issued, and the Document Signing (public) Key is used by other countries to validate the data received in a document through validation of the digital signature.

Country Signing Keys will be fairly static and the public portions of those keys will be securely shared country-to-country by diplomatic or other out-of-band secure means. Document Signing (public) Keys will be shared with all countries and with airlines and other users primarily by means of an ICAO Public Key Directory (PKD), which will serve as a repository of all such keys. Document Signing Keys will change frequently, not less than every 3 months, and countries may have several such keys in use at any time.

3. *Why do Document Signing Keys change every three months, and how many of these keys can a country use for signing at any time?*

The number of Document Signing Keys in use for signing by any country at any time, and the signing lifetime of these keys, is really determined by balancing two factors: limiting the number of MRPs and MRTDs issued and signed by each key, and limiting the number of keys that must be managed by the PKD and every country's border system. Signing too many documents with the same key exposes more passports to the event of a compromise of that key, whereas the use of excessive numbers of keys makes the international task of key management very burdensome.

ICAO recommends therefore that countries not use the same key for more than several hundred thousand documents although there is no rationale for fixing this number to precise levels. In addition each such key should change every three months (maximum), even if the number of documents signed is limited. It is up to each State to determine what works best for them given their document issuance counts and other factors; for example, the use different issuing locations may also be part of their decision process.

4. *How will States and other users obtain up to date public keys of all other States from the ICAO Public Key Directory?*

The PKD will not be designed or implemented for active on-line key confirmation for every passport encountered at every border post in the world. Rather States will be expected to download the entire copy of the PKD, estimated to be <25MB, on a regular basis and store it internally in their border management systems. In this way data stored on MRPs and MRTDs encountered can readily be authenticated from the appropriate issuing country Document Signing (public) Keys contained in the certificates stored in the PKD data.

If an MRTD is encountered with a key not recognized in the PKD copy currently stored by a country, implying that PKD updates may have been missed, occasional requests for certificate information can be made of the Directory on-line. The design response for these requests will be minutes vs. seconds, at most.

The PKD will be set up under X.500 protocol, and communications with the PKD shall be via LDAP over SSL. Each download of the entire PKD is recommended to be via a "Shadow-LDAP" function, which should simplify implementation for each country.

The certificate for the Document Signing Key used with any passport or MRTD will also often be contained within the MRTD itself as well as in the PKD, although this is optional. These certificates are signed by the Country Signing Key of the issuing State, the public key of which the receiving country is aware of (exchanged through diplomatic means). As a result the receiving country may opt in some cases to accept a new key without ICAO PKD reference; however the existence of the certificate on the PKD provides the additional operational security desired by the ICAO community. The PKD is also the only key reference for airlines and other legitimate users.

5. *How will ICAO operate the certificate update process for the PKD?*

Countries will regularly provide new Document Signing certificate information to the ICAO PKD, again using the LDAP X.500 protocol. It is essential that ICAO exercise some due diligence over the process on behalf of member States. Since LDAP is a direct-update protocol, where the X.500 directory is immediately altered by changes forwarded, this will be managed by ICAO through the setup of a separate PKD "Write Directory" where all proposed certificate updates are sent. Once ICAO has examined the changes, and exercised other due diligence such as checking the IP address of the sender, the update information will be copied into the PKD "Read Directory" which is the PKD available for download by each nation.

6. *Who will be able to access the ICAO Public Key Directory?*

The PKD will be a totally open and Internet-enabled resource, available to any and all who wish to access it (for read-only). Its LDAP protocol will not make it readily apparent to casual Internet browsers and so traffic is not expected to be excessive because of this. The lack of user sign-up protocols will lead to simplification of implementation, and broader security through the ready availability of its certificate services to airlines and others who wish to use it to authenticate documents.

7. *Will the ICAO PKI use standard X.509 certificates?*

There are two X.509 certificates that may be stored on the MRP or MRTD, the mandatory one called the "Document Certificate" which contains the digital signature for the data contained, and the optional "Document Signing (CA) Certificate", containing the public part of the Document Signing Key used to sign the document and signed by the Country Signing Key.

The Document Signing Key (CA) Certificate is a standard X.509 certificate with no optional extensions. The Document Certificate, however, has unique extensions that contain to the (SHA) hash results of each LDS Data Group contained in the advanced storage area (ICC). This Document Certificate is signed by the Document Signing Key. The reason for this approach is that it simplifies document validation by not requiring that all LDS Data Groups be read to validate the data with a single digital signature; once the hash results of all Data Groups are validated (in the Document Certificate) the receiving country can then trust the individual hash results for the Data Groups of interest to it.

8. *What encryption algorithms are used in the ICAO PKI?*

DSA, RSA, and ECDSA are all permitted encryption algorithms for use in the ICAO PKI initiative. None are recommended as the default; it is up to individual States to determine which best suits their needs.

9. *What hashing algorithms will be used in the ICAO PKI?*

SHA-1, SHA-256, SAH-384, and SHA-512 are all permitted hashing algorithms. ICAO recommends the use of appropriate SHA algorithms consistent with good PKI practice; the availability of longer encryption keys may therefore result in country selection of other than SHA-1 for its purposes.

10. *What are the recommended key lengths and key lifetimes?*

In determining appropriate key lengths ICAO had to consider the length of time that many MRPs and MRTDs remain valid; in many cases passports are valid for a period of 10 years. In view of this key lengths must be such that they are not likely to be compromised through brute force efforts in that time period.

Although there are no definitive answers to these cryptographic questions, ICAO has adopted the following key lengths as being sufficiently robust based on current expertise in this area.

Algorithm	**Country Signing Key**	**Document Signing Key**
RSA	n=3,072	n=2,048
DSA	p=3,072, q=256	p=2,048, q=224
ECDSA	f=256	f=224

Key lifetimes are defined in the following manner:

Document Signing Key lifetime = (the length of time it is used to sign documents) + (the longest validity period of any document signed using it).

Country Signing Key lifetime = (the length of time it is used to sign Document Signing Key certificates) + (the longest lifetime or latest future expiry date of a

Document Signing Key certificate signed by it).

For example, if a Document Signing Key is used for three months to sign 10-year validity passports, then the lifetime of that key is 10 years plus 3 months. Similarly if a Country Signing Key is used for 3 years to issue Document Signing Key certificates that will be used for 3 months for signing of 10-year validity passports, then the lifetime of that Country Signing Key is 3 years plus 10 years plus 3 months.

11. *Will ICAO sign anything with its own keys?*

ICAO will not sign any certificates stored on the PKD, nor sign any PKD certificate downloads with countries so as to not give the false impression that it is in any way acting as a CA. As such there is no need for non-standard certificates to include an ICAO signature that is not a CA-like signature. ICAO will develop certain data statistics, such as record counts by nation, overall sizes, and similar data integrity controls corresponding to the current updated PKD. Transmission of these statistical and audit control values, and other communications, if by email, may be signed by ICAO using its current signing key; however all communications of certificates, CRLs, and PKD downloads, will only use the ICAO key to generate appropriate session keys for SSL-based communications.

12. *Does the ICAO PKI use CRL's, and if so how will they operate?*

CRL's will be used in the ICAO infrastructure. However CRLs are really only necessary for key compromise events, although "good practice" involves the posting of a CRL list, even if null, on a periodic basis. The recommended period for CRL issuance is between 48 hours, if the CRL is event based (resulting from a key compromise), and 90 days for a complete CRL list from each country.

CRL's required by compromise events will be primarily shared between and amongst countries by urgent messaging, and is the responsibility of the country with the compromised key. The ICAO PKD will serve as the secondary CRL Distribution Point for such CRL's and as the primary CRL distribution point for the complete set of CRL's in existence for each country at any time.

CRLs will be issued only for active revocation of signing keys and will not be issued for regular keys and certificates after their usage period for signing is over (3 months maximum); the validity dates on each certificate will specify the valid signing date range of the contained key but the documents signed by that key will remain valid for a long time (10 years + 3 months?). As such these certificates will remain on the Directory for a long period of time. Each receiving nation must check the issuing date of the MRTDs it encounters against the appropriate PKD certificate in use at the time of issuance in order to ascertain that the key used to sign it was valid at that time. Such certificates will only be removed from the PKD as a result of some positive action by the issuing country to do so. A CRL might be appropriate for this purpose, or some other mechanism might have been devised over the next 5-10 years to clean up the Directory files without the need for CRL issuance and indefinite CRL storage. At present non-null CRL's are only to be used for real key compromise events.

CRL's will not be issued on the MRTDs of departing travelers. Event-based CRLs will only be shared bilaterally and through the ICAO PKD.

13. *What happens if a country's Document Signing Key is compromised?*

When a compromise of a Document Signing Key is detected, the country must immediately issue a revocation, to be communicated to (all) other countries, and to ICAO PKD, within 48 hours maximum.

All documents signed by that key will then not be able to be validated using their digital signatures, and so these document must thereafter be inspected on first principles. This may result in significant delay and difficulty for the bearer if the world by then has increasingly come to rely upon the encoded data, with biometric, and the digital signature to verify the authenticity of the document and the bearer.

14. *What happens if a Country Signing Key is compromised?*

Compromise of a Country Signing Key is a disastrous event for that country. In effect, revoking that key invalidates all of the MRTD signatures applied by any Document Signing Keys whose certificates were issued by that Country Signing Key. Nothing can be done to restore confidence in those past documents – e.g. by issuing new certificates for those Document Signing Keys – since it will not be known if any such Document Signing Key certificates were improperly issued and used in the first place.

To issue new documents the country basically must start over: generate a new Country Signing Key, share it via diplomatic means with other countries, convince those countries that it's key management practices are now more secure, begin to issue Document Signing Key certificates, post these with the ICAO PKD, and begin to sign passports and MRTDs with these new keys.

15. *Will the chip serial number be part of the certificate extensions?*

The chip serial number may be stored by a country in the LDS, probably in Data Group 13. However this is intended for use by that country alone, as it is not normally a requirement for international interoperability. This is due to differences between manufacturers and their numbering standards. The serial number is normally only used for protection before and during the data load process in each country.

ICAO will not set any standards at this time for use and management of chip serial number in the LDS or in any certificate extension.

16. *How can the chip be authenticated as the proper one originally encoded by the issuing country?*

The ICAO PKI also utilizes an optional lower layer of key pair, called the Active Authentication Key pair, which is a document-specific key pair generated at the time of chip data loading. This key pair is entirely contained on the chip, the private portion within the chip's secure memory, and the public portion in the Document Certificate (also containing the LDS Data Group hash values) that is signed by the country's Document Signing Key. An inspection station may opt to use these keys along with a hash value taken from the MRZ to verify that the chip is genuine and belongs to this MRTD.

These Active Authentication Keys are document-specific and are not subject to international distribution, control, or CRL reporting. They also do not restrict the storage and retrieval of open data from the chip without chip authentication.

17. *What mechanisms are used to protect the privacy of the data on the MRTD ICC?*

The main implementation of advanced technologies involves the use of RF ICCs, namely computer chips that are readable by contactless RF communications. Transfers of data between chip and reader are considered very safe by ICAO, with little negative impact should the data somehow be captured or skimmed. In any case only the basic data as contained in the MRZ, and the digitized photo as it appears on the data page are recommended to be stored as "open" or unencrypted data. Other personal data, including fingerprint and iris data, are considered private and will be encrypted for private usage by the issuing country.

However some countries believe that even relatively public data (MRZ plus photo) can be skimmed under certain circumstances and cannot be allowed by their internal privacy policies. This skimming is believed to be feasible by listening in on communications between the chip and reader at the border point, even though this would not present any copying or forgery opportunities because of the integrity of the digital signatures.

Nonetheless to guard against this, some States may choose to implement an active access technique. The method proposed involves the use of the chip External

Authenticate command using a key derived from the MRZ (which therefore must be read from the data page, hence proving that the passport bearer proffered the document for reading). Once the authentication challenge is accepted data is transmitted using session keys that are set up between the MRTD chip and the reader.

This active access process makes reading the chip data impossible without the access test, even if the data is stored as open data; i.e. unencrypted. Active Access should not be confused with the Active Authentication process, which only validates the chip and always permits open chip data access regardless.

18. *How will other biometrics such as fingerprint and iris-scan be accommodated?*

Other biometric measurements (fingerprint, iris) are considered sensitive for privacy purposes by ICAO and many member States, and as such cannot be made available in open format, even with active access control, for other nations to read. As such, these biometric measurements are recommended to be stored in encrypted form by each nation wishing to do so.

However ICAO encourages the usage of such biometrics. The "New Orleans Resolution" adopted by ICAO/TAG in March 3003, states:

ICAO TAG-MRTD/NTWG recognizes that Member States currently and will continue to utilize the facial image as the primary identifier for MRTDs and as such endorses the use of standardized digitally-stored facial images as the globally interoperable biometric to support facial recognition technologies for machine assisted identity verification with machine-readable travel documents.

ICAO TAG-MRTD/NTWG further recognizes that in addition to the use of a digitally stored facial image, Member States can use standardized digitally-stored fingerprint and/or iris images as additional globally interoperable biometrics in support of machine assisted verification and/or identification.

As a result it is anticipated that some countries will capture and store these biometrics for their own purposes and for special purposes in conjunction with partner nations in private bilateral or n-lateral schemes. This information can be shared through special arrangements for private key sharing, or through the encryption of the same data multiple times using a public Document Key of each intended receiving country. In this way the biometric data can be protected but read by those countries that are partners with the issuing country in sharing this data.

19. *Will the ICAO Public Key Directory be ready in 2004 and how much will countries pay for its setup and on-going operation?*

The ICAO PKD is intended for implementation by October 2004. All funding of PKD implementation and operations is to be achieved through annual membership or participation fees from countries that are issuing documents with digital signatures in accordance with ICAO international practice.

The ICAO PKD will be an open and accessible facility. Airlines and other users who require steady access to the PKD will be encouraged to download copies of the PKD on a regular basis, just like the border inspection agencies of member States. It may not be possible to charge airlines and other users for this service given the open Internet architecture of the PKD; however there are clear security benefits in security for all nations in encouraging airlines and other agencies to use the PKD to validate digital signatures and documents.

Exact fee structures and rates have not been finalized at this time.