

**REMARKS BY
FRANK E. MOSS
IDENTITY MATTERS LLC
WASHINGTON, DC
AT THE
WIRELESS ID SUMMIT
DARTMOUTH COLLEGE
APRIL 9, 2007**

GOOD AFTERNOON:

IT IS A REAL PLEASURE TO BE WITH YOU HERE IN HANOVER. I WANT TO TAKE THIS OPPORTUNITY TO THANK DAVID KOTZ (COATS) FOR PLANNING THIS MEETING. HE IS TRULY A BRAVE CONFERENCE ORGANIZER. HE ASKED ME TO SPEAK BASED ON MY EXPERIENCES OVER THE LAST FOUR YEARS WITH RFID WHEN I SERVED AS THE DEPUTY ASSISTANT SECRETARY FOR PASSPORT SERVICES AT THE U.S. DEPARTMENT OF STATE. HE PROBABLY DID NOT KNOW WHEN HE INVITED ME THAT I WAS AWARDED BY THE GROUP *CITIZENS AGAINST GOVERNMENT WASTE* THE TITLE OF "PORKER OF THE MONTH" (FEBRUARY 2006) FOR MY LEADERSHIP OF THE U.S. ELECTRONIC PASSPORT (E-PASSPORT) PROGRAM. ALSO, ONE OF THE COMMENTERS ON THE DEPARTMENT OF STATE'S RULEMAKING ON THE E-PASSPORT PROGRAM LABELLED ME "THE ANTI-CHRIST" AND ALSO WENT ON TO REPORT THAT ANYONE WHO HELPED ME MAKE THIS PROGRAM HAPPEN WOULD BE A "MINION OF THE ANTI-CHRIST" AND "THEIR NAME TOO WOULD BE REMOVED FROM THE BOOK OF LIFE". IF ANYONE WOULD LIKE TO LEAVE BEFORE I BEGIN DISCUSSING THE U.S. E-PASSPORT, I WON'T BE OFFENDED.

OKAY....LET'S START AT THE BEGINNING WITH A LITTLE BACKGROUND ON THE U.S. PASSPORT PROGRAM AND THEN I WILL SEGUE INTO A MORE COMPREHENSIVE EXPLANATION

OF HOW AND WHY WE USE RFID IN THE NEW GENERATION U.S. PASSPORT.

FIRST....THE U.S. PASSPORT PROGRAM. LET ME BEGIN WITH A QUESTION FOR THE AUDIENCE....HOW MANY OF YOU HAVE A U.S. PASSPORT? CURRENTLY, ONLY 28 PERCENT OF U.S. CITIZENS HAVE A PASSPORT. HOWEVER, THAT PERCENTAGE HAS MORE THAN DOUBLED IN THE LAST TEN YEARS AND THE DEPARTMENT OF STATE EXPECTS THAT IT WILL CONTINUE TO GROW IN THE FUTURE UNTIL AT LEAST 50 PERCENT OF THE POPULATION HAS A VALID PASSPORT. THE U.S. IS ALREADY THE WORLD'S LARGEST ISSUER OF PASSPORTS AND WILL ADJUDICATE ABOUT 17 MILLION PASSPORT APPLICATIONS THIS YEAR. THAT COMPARES TO ONLY 7 MILLION PER YEAR WHEN I ASSUMED THE POSITION OF MANAGING THE U.S. PASSPORT PROGRAM IN 2003. WHAT ACCOUNTS FOR THE CHANGE? SEVERAL THINGS THAT INCLUDE:

- INCREASED TRAVEL ABROAD, INCLUDING BY STUDENTS ON SEMESTER ABROAD PROGRAMS;**
- U.S. POPULATION GROWTH;**
- POST 9/11 POLICIES THAT INCENTIVIZED CITIZENSHIP;**
- AMERICANS USING PASSPORTS AS PORTABLE PROOF OF IDENTITY AND NATIONALITY FOR PURPOSES SUCH AS DOMESTIC AIR TRAVEL; AND,**
- THE WESTERN HEMISPHERE TRAVEL INITIATIVE THAT REQUIRES MORE FORMAL DOCUMENTATION FOR TRAVELERS RETURNING FROM CANADA, THE CARIBBEAN OR MEXICO.**

OKAY....NOW ON TO THE ISSUE OF THE U.S. ELECTRONIC OR E-PASSPORT THAT INCORPORATES RFID TECHNOLOGY. FIRST, WHAT DO I MEAN BY AN "E-PASSPORT"? THAT TERM MEANS A PASSPORT ISSUED BY ANY NATION AROUND THE WORLD THAT CONTAINS AN INTEGRATED CIRCUIT (I.C.) TO WHICH DATA ABOUT THE PASSPORT BEARER IS WRITTEN. DATA IS EXCHANGED BETWEEN THE I.C. AND THE PASSPORT READER IN A CONTACTLESS ENVIRONMENT USING RFID TECHNOLOGY. YOU CAN TELL EASILY IF YOUR PASSPORT IS

AN E-PASSPORT. THERE IS AN ICON ON THE BOTTOM OF THE FRONT COVER (SHOW SAMPLE) THAT IS USED BY NATIONS AROUND THE WORLD TO IDENTIFY “E-PASSPORTS”.

AN OBVIOUS QUESTION IS “WHY ARE NATIONS TAKING THE STEP OF INCLUDING RFID TECHNOLOGY IN PASSPORTS?” AS BACKGROUND, THE UNITED STATES, LIKE MANY NATIONS AROUND THE WORLD, TOOK A FUNDAMENTAL LOOK AT ITS BORDER SECURITY PRACTICES FOLLOWING THE EVENTS OF SEPTEMBER 11. THE U.S. IMPROVED ITS OPERATIONS IN MANY AREAS. FOR EXAMPLE, THE U.S. INTRODUCED MAJOR CHANGES TO ITS VISA PROCESSING SYSTEMS FOR PEOPLE SEEKING TO VISIT OR IMMIGRATE TO THE UNITED STATES.

AT THE SAME TIME, AN EFFORT UNDER THE AUSPICES OF THE INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO) HAD BEEN LAUNCHED TO IMPROVE PASSPORTS. THE CENTRAL GOAL OF THIS PROGRAM PRE-9/11 WAS TO HELP FACILITATE THE MOVEMENT OF TRAVELERS THROUGH AIRPORTS IN THE EXPECTATION THAT AIRCRAFT SUCH AS THE AIRBUS A-380 WOULD OVERWHELM CUSTOMS AND IMMIGRATION PROCESSING. IN HOPES OF MEETING THAT OBJECTIVE, CONSIDERABLE WORK WAS DONE IN THE LATE 1990’S TO IDENTITY TECHNOLOGIES THAT COULD HELP A PASSPORT EVOLVE FROM A PAPER-BASED “DUMB” DOCUMENT INTO ONE THAT COULD CONTAIN SOME LIMITED DATA STORAGE CAPACITY TO WHICH INFORMATION ABOUT THE TRAVELER COULD BE WRITTEN. IN THE POST 9/11 PERIOD, THE FOCUS OF ICAO’S EFFORTS, NOT SURPRISINGLY, BEGAN TO AIM AT WAYS OF ENSURING THAT ONLY THE PERSON TO WHOM A PASSPORT WAS ISSUED COULD ACTUALLY TRAVEL ON THAT DOCUMENT.

THE OUTCOME OF ICAO’S EFFORTS WAS THE ADOPTION IN 2003 OF A SERIES OF “SPECIFICATIONS” THAT ESTABLISHED HOW GOVERNMENTS WOULD INTRODUCE BIOMETRICS AND ELECTRONIC STORAGE CAPABILITIES, IF THEY SO DECIDED. THOSE SPECIFICATIONS ESTABLISHED THAT:

- 1) THE BASELINE BIOMETRIC WOULD BE A FACIAL IMAGE. NATIONS WOULD RELY UPON THE**

PHOTOGRAPH THAT HAS LONG BEEN INCLUDED IN PASSPORTS AS A BIOMETRIC IDENTIFIED. COUNTRIES COULD INCLUDE FINGERSCANS OR IRIS SCANS AS WELL, IF THEY PREFERRED.

- 2) THE DATA WOULD BE WRITTEN TO A CONTACTLESS INTEGRATED CIRCUIT (I.C.) WITH A STORAGE CAPACITY OF AT LEAST 32 KB. CONTACTLESS TECHNOLOGY WAS CHOSEN BASED ON CONSIDERATIONS OF RELIABILITY AND EASE OF USE FOR BOTH GOVERNMENTS AND TRAVELERS.**
- 3) THE DATA WRITTEN TO THE CHIP WOULD NOT BE ENCODED, CONSISTENT WITH THE GOAL OF GLOBAL INTEROPERABILITY.**
- 4) THE DATA TRANSMISSION PROTOCOLS WOULD BE THOSE ADOPTED BY THE INTERNATIONAL STANDARDS ORGANIZATION (ISO) IN ITS 14443 (A) OR (B) STANDARDS. THIS MEANS, MOST BASICALLY, THAT THE DISTANCE BETWEEN THE CHIP AND THE READER MUST BE LESS THAN 10 CENTIMETERS OWING TO CONSIDERATIONS OF SIGNAL STRENGTH AND FREQUENCY.**
- 5) THE I.C. WOULD OPERATE IN A "WORM"—WRITE ONCE, READ MANY—ENVIRONMENT. DATA WRITTEN TO THE CHIP CANNOT BE UPDATED AFTER THE PASSPORT IS ISSUED. THUS, AT THIS TIME, THERE IS NO CAPABILITY TO USE THE I.C. AS AN ELECTRONIC REPOSITORY FOR VISAS OR ENTRY AND EXIT DATA FROM PORTS OF ENTRY.**

LET ME IF I MAY TRANSLATE THOSE SPECIFICATIONS INTO WHAT THE UNITED STATES WRITES TO THE I.C. CONTAINED IN THE REAR COVER OF U.S. E-PASSPORTS. FIRST, THE UNITED STATES USES AN I.C. WITH 64KB OF STORAGE CAPACITY AND 8KB OF PROCESSOR POWER. THE CHIPS ARE MANUFACTURED BY EITHER INFINEON OR NXP, TWO OF THE WORLD LEADERS IN THIS TECHNOLOGY. THE DATA WRITTEN TO THE CHIP INCLUDES THE FULL FACIAL IMAGE OF THE PASSPORT BEARER AS WELL AS THE BIOGRAPHIC INFORMATION FOUND ON THE DATA PAGE OF THE U.S. PASSPORT. IN OTHER WORDS, THE RFID FEATURE OF THE

U.S. PASSPORT IS SIMPLY A COPY OF THE DATA PAGE. THAT DATA, IN TURN, IS SECURED TO THE I.C. USING PUBLIC KEY INFRASTRUCTURE (PKI) TECHNOLOGY. THE U.S. ELECTED TO USE THE 64 KB CHIP IN ORDER TO “FUTURE PROOF” THE U.S. E-PASSPORT IN THE EVENT THAT DECISIONS ARE MADE TO INCORPORATE ADDITIONAL BIOMETRIC FEATURES. LET ME ASSURE YOU THAT ANY SUCH CHANGE WOULD BE SUBJECT TO A FULL PUBLIC VETTING THROUGH THE FEDERAL RULEMAKING PROCESS.

AS I NOTED IN MY INTRODUCTORY COMMENTS, THE DEPARTMENT OF STATE ENGAGED IN A PUBLIC RULE-MAKING PROCESS AS IT DEVELOPED THE U.S. E-PASSPORT. THAT PROCESS HELPED THE STATE DEPARTMENT MAKE FUNDAMENTAL IMPROVEMENTS IN THE U.S. PASSPORT DESIGN. I WANT TO TAKE THIS OPPORTUNITY TO THANK ALL WHO PROVIDED COMMENTS ON THE TECHNICAL PROPOSALS, ESPECIALLY THE U.S. PRIVACY COMMUNITY. AS A RESULT OF THE COMMENTS STATE RECEIVED, IT:

- **STRENGTHENED PERSONAL PRIVACY PROTECTION BY INCLUDING ANTI-SKIMMING MATERIAL IN THE FRONT COVER THAT WRAPS AROUND ONTO A PORTION OF THE REAR COVER. THIS GREATLY COMPLICATES READING THE I.C. AS LONG AS THE BOOK IS CLOSED. THE U.S. IS THE ONLY NATION OF THE 30 OR SO WHO ISSUE E-PASSPORTS TO HAVE TAKEN THIS STEP.**
- **ADOPTED BASIC ACCESS CONTROL (BAC) TO MINIMIZE THE RISK OF EAVESDROPPING. BAC REQUIRES THAT THE MACHINE READABLE ZONE ON THE DATA PAGE BE READ ELECTRONICALLY TO GENERATE A KEY THAT UNLOCKS THE I.C. THIS, IN TURN, ALLOWS FOR AN ENCRYPTED COMMUNICATION SESSION BETWEEN THE I.C. AND THE CHIP READER.**
- **MITIGATED THE RISK THAT AN E-PASSPORT COULD BE USED TO “TRACK” THE BEARER AROUND THE WORLD BY TAKING ADVANTAGE OF THE COMPUTATIONAL POWER OF THE I.C. TO**

GENERATE A RANDOMIZED UNIQUE ID NUMBER EACH TIME A READER “INTERROGATES” THE I.C.

MOREOVER, THE UNITED STATES IS NOT DOING A NUMBER OF THINGS WITH ITS E-PASSPORTS DESIGN:

- **DOES NOT COLLECT FINGERSCANS FROM AMERICAN CITIZENS AS PART OF THE PASSPORT APPLICATION PROCESS, LET ALONE WRITE THOSE PRINTS IN AN ENCRYPTED STATUS TO THE CHIP. SOME NATIONS, ESPECIALLY IN THE EUROPEAN UNION, PLAN TO TAKE THIS STEP. THE U.S. HAS DECLINED TO DO SO OWING TO CONCERNS ABOUT THE FEASIBILITY OF PROTECTING FINGERSCANS BASED ON CURRENT ENCRYPTION TECHNOLOGY AND KEY MANAGEMENT PRACTICES.**
- **NOWHERE ON THE CHIP OR IN THE PASSPORT DOES STATE INCLUDE YOUR:**
 - **SOCIAL SECURITY NUMBER;**
 - **HOME ADDRESS;**
 - **BLOOD TYPE;**
 - **DNA;**
 - **CREDIT CARD INFORMATION;**
 - **TELEPHONE OR CELL NUMBERS; OR**
 - **ANY OTHER IDENTITY-RICH MATERIAL.**

I SHOULD ALSO NOTE THAT SOME OF THE CLAIMS MADE ABOUT THE SUSCEPTIBILITY OF E-PASSPORTS TO SKIMMING OR EAVESDROPPING ARE, IN MY OPINION, OVERSTATED. THE STATE DEPARTMENT RETAINED THE SERVICES OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) TO PERFORM COMPREHENSIVE AND INDEPENDENT TESTING OF BOTH THE DURABILITY AND SECURITY FEATURES OF THE U.S. E-PASSPORTS. EVEN IN A NIST LABORATORY SETTING WITH HIGHLY SENSITIVE EQUIPMENT, EXPERTS HAVE NOT BEEN ABLE TO EVEN ACTIVATE, LET ALONE EXCHANGE DATA, WITH THE I.C. FROM A DISTANCE OF MORE THAN A FEW FEET. MOREOVER, THE POWER REQUIREMENTS TO ACTIVATE THE CHIP GO UP SO QUICKLY—I BELIEVE THAT FIELD STRENGTH ATTENUATES

ACCORDING TO THE CUBE OF THE DISTANCE BETWEEN THE I.C. AND THE READER—THAT LONG RANGE COLLECTION IS IMPRACTICAL. AND, I MUST EMPHASIZE AGAIN THAT THE RISK MITIGATION STRATEGY OF ANTI-SKIMMING TECHNOLOGY PLUS BAC ADDRESSES THAT RISK.

I AM CONFIDENT THAT THE U.S. GOVERNMENT IS NOW ISSUING A SIGNIFICANTLY MORE SECURE U.S. E-PASSPORT THAN WAS ORIGINALLY PROPOSED. AND, I BELIEVE THE U.S. E-PASSPORT IS AT THE FOREFRONT OF INTERNATIONAL EFFORTS TO PRODUCE E-PASSPORTS THAT MINIMIZE THE RISK OF UNAUTHORIZED READING AND IDENTITY THEFT. IN FACT, AFTER INITIALLY BEING QUESTIONED BY MANY NATIONS AS TO WHY WE WERE GOING TO THE TROUBLE AND EXPENSE OF ADOPTING A “BELT AND SUSPENDERS”—THAT IS ANTI-SKIMMING MATERIAL PLUS BAC—SECURITY ARCHITECTURE, THE U.S. HAS NOW BEEN APPROACHED BY SEVERAL GOVERNMENTS INTERESTED IN CONSIDERING THIS APPROACH FOR THEIR OWN PASSPORTS.

I COULD SPEAK FOR MUCH LONGER ABOUT RFID IN U.S. TRAVEL DOCUMENTS. IN PARTICULAR, I COULD ADDRESS WHY THE U.S. USES PROXIMITY READ TECHNOLOGY IN ITS PASSPORTS, BUT APPEARS TO FAVOR VICINITY READ RFID FOR THE PROPOSED PASSPORT CARD. THAT IS THE CARD THAT THE STATE DEPARTMENT PLANS TO ISSUE AS PART OF THE IMPLEMENTATION OF THE LAND BORDER CROSSING AND SEA TRAVEL ELEMENTS OF THE WESTERN HEMISPHERE TRAVEL INITIATIVE. RATHER THAN DO THAT IN MY REMARKS, I WILL BE PLEASED TO ADDRESS THAT DURING THE Q&A SESSION IN DEFERENCE TO MY COLLEAGUES ON THE PANEL HAVING AN OPPORTUNITY TO DELIVER THEIR REMARKS.

THANK YOU FOR YOUR TIME AND ATTENTION AND I LOOK FORWARD TO YOUR QUESTIONS.