

# PHILIPS

## Identification at the Land Borders: Technology and Policy Challenges

Jim Sheire  
Philips Washington Office  
Manager, Government Programs  
04/20/2006

# Current and Future Programs

## **Current**

- FAST Lane
- Nexus
- INS/ Green Cards

## **Future**

- I-94 Visa Pilot (EPCGlobal item ID standard)
- ePassport (ISO 14443 personal ID standard)
- WHTI/ PASS Card (Currently under review)

# Operational Challenge

- Primary challenge facing DHS (US-VISIT, CBP) is improving border security yet not slowing down crossing speeds
- ePassport initially designated the ID credential for land borders, but this was withdrawn after loud protests from industry, tourism and travel, and other groups that would be negatively impacted by the time it takes to thoroughly verify identity
- Often, when presenting US-VISIT with technology solutions, they have a code phrase: “Does not meet operational requirements;”
- Translation: “DHS does not want to deal with the political firestorm of increased wait times that result from improved ID verification comparable to that at air and sea ports, federal facilities, etc.”

# DHS/ CBP Consider Alternatives to ISO Personal ID Standards

- The “operational requirements” thus led DHS to look at other RF-based solutions
- US-VISIT program utilizes large-scale databases on foreign visitors, where sensitive data resides, including biometric scans; databases are connected via networks to ports of entry, as well as to law enforcement databases
- US-VISIT launched an I-94 visa pilot project employing long-range UHF RFID technology (EPCglobal supply chain standards) to record when foreign visa holders exited the country
- Nexus program at Canadian border also employs UHF-based personal ID credentials

# Western Hemispheric Travel Initiative and the PASS Card

- When tasked to develop a non-ePassport solution to the land borders, US-VISIT and CBP thus developed a new approach that combined the perceived long-range read and speed capabilities of UHF-based credentials with large scale centralized databases

# UHF PASS Card Operation

- As Mr. Williams described on day one of this conference, a car at the land border pulls up to a “yellow line” under a UHF antenna portal thirty feet out from a Customs kiosk
- Card holders will be required to remove their UHF credentials from planned “protective sleeves” and place them on the dashboard or held against their windows (as in Nexus)
- Data on the pre-screened card holder(s) is then downloaded via always-on broadband computer network connection and loaded on the computer screen of the Customs officer

# UHF PASS Card Operation

- The car pulls up, and the Customs officer performs the visual identification and other security checks of the passengers based on database information
- Any anti-counterfeiting features on the card (as there are none on the chip) would be on the card itself, such as holograms or other printed features
- High-speed exit is then recorded by large-scale antenna arrays similar to that employed in the I-94 pilots
- Summary: this process is envisioned to be substantially faster and superior from a privacy and “operational” perspective than an ISO 14443 approach

## Full Disclosure

- Philips Semiconductors designs and manufacturers a full range of RFID products across all frequencies, including 13.56 Mhz ISO 14443 contactless smart card ICs and a full range of UHF products, including EPCGlobal Generation 2 UHF chips designed for supply chain logistics applications



# The Paradigm Shift This Represents

- The PASS card program as envisioned by US-VISIT represents a fundamental departure from the ISO 14443 secure personal ID standard and the personal ID verification model adopted by the PIV, ePassport, transportation, financial, and countless other contactless card programs
- Rejected is the very notion that a smart card IC securely stores information for the purposes of identity verification, not dependent on large databases and always-on computer networks, intelligently authorizing itself to a reader (and vice-versa) while simultaneously providing strong anti-counterfeiting features
- The proposed PASS card is instead a commodity “dumb card” with minimal security or privacy features on the chip, containing a static unique identifier that serves as a database pointer, and that relies for border security exclusively on human verification of identity backed by extensive back-end IT infrastructure and lower-security printed anti-counterfeiting features

## And Why Is This Being Considered?

- ISO-based alternatives don't (remember the code phrase) “meet operational requirements”
- Another paradigm shift here, in US-VISIT's defense, is the need for high-speed identity verification
- Politically, it has become necessary to compromise on security and privacy for convenience and trade facilitation
- It remains to be seen whether U.S. citizens and privacy groups will accept a long-range, static UID based ID credential, with or without an easily misplaced “protective sleeve”

## Alternative: ISO 14443 Credential with a “Database Pointer”

- An alternative might be an ISO 14443-based credential with solid security and privacy features such as a random temporary ID and an encrypted secure channel that securely communicates a database pointer to a road-side reader, allowing DHS to maintain it’s “yellow-line, database lookup” model while providing far superior (and faster) anti-counterfeiting capabilities and protecting cardholder privacy
- Such a credential (a single card or multiple cards presented to a reader) would have a read speed of a fraction of a second
- CBP apparently wishes to avoid travelers from having to roll down their windows and present cards to a reader at the necessary 3-5 inches, believing this to add unnecessary seconds to the process promised by the

# But Is UHF Faster in the Real-World Environment?

- Let's review the real-world operation of the proposed UHF card again. The steps are:
  - remove the card from wallets/backpacks/suitcases
  - remove it from the protective sleeve
  - place the card on the dashboard and against windows
  - wait for 100% read rates from the proposed UHF “portals” and clearance from the customs officer to pull up
  - wait again while the customs officer reviews the driver and passengers and information on the screen
  - wait again as customs officer collects cards of passengers missed by the portal
  - possibly wait again while the customs officer reviews the hologram or watermark, perhaps even under an additional UV scanner or other piece of equipment

# How Does This Compare to ISO 14443?

- Privacy “enhancing” faraday sleeve unnecessary due to authentication and limited read-range
- Time required to remove UHF card from sleeve and hold on dashboard/window likely comparable to time required to roll down window and present ISO 14443 card to reader
- Cards presented to road-side ISO 14443 reader would enjoy higher read-rates (pilot test results and report on the I-94 visa UHF pilot that could address this, as Mr. Williams said Tuesday, are apparently not being reviewed prior to a decision)
- On-chip anti-counterfeiting (digital signature) features far more secure and vastly faster than human verification of digital watermarks or other printed features

## Solution: Compare ISO 14443 and EPCglobal UHF Side-by-Side

- The solution might be to test the technologies side-by-side against a defined set of operational requirements (read-speed, per car transaction times, etc.)
- Also compare security and privacy features to ensure that the program addresses the legitimate privacy concerns we saw articulated in the development of the ePassport and in countless state legislatures

# Potential Risks

- The risk I believe DHS and the State Department run is that a long-range, low security EPCglobal based solution will encounter a firestorm of protest from the privacy groups, threatening not just the WHTI program itself, but myriad other contactless smart card applications (privacy groups, as we learned yesterday in the policy session, lump RFID and contactless smart card together, as does media)
- EPCglobal Gen 2 UHF is a superb technology, designed for high performance in supply chain logistics, presenting no privacy concerns when employed for that purpose (in warehouses, store-rooms, etc.). The UHF frequency itself could hypothetically be used to gain advantages in read-range in a PASS card, but a new standard might be required that adds basic security and privacy features

# Conclusions

- Philips, as a vendor of both UHF and ISO 14443 solutions, strongly urges DHS and DoS to stick with a tried and true **standards-based** approach
- The globally accepted ISO 14443 personal ID standard is based on years of experience in secure personal identification
- Conduct a real-world environment test of the technologies; Philips suggests that transaction times and performance of an ISO 14443 solution at the border would be very comparable to the perceived performance of a UHF-based solution, while addressing security and privacy concerns



**Thank You!**

**Jim Sheire  
Philips Electronics  
(202) 962-8566  
James.sheire@philips.com**