

# Encrypted Dynamic Privacy for RFID

Dr. Steve Barry

703-983-3409 • [sbarry@mitre.org](mailto:sbarry@mitre.org)

CEM IR&D

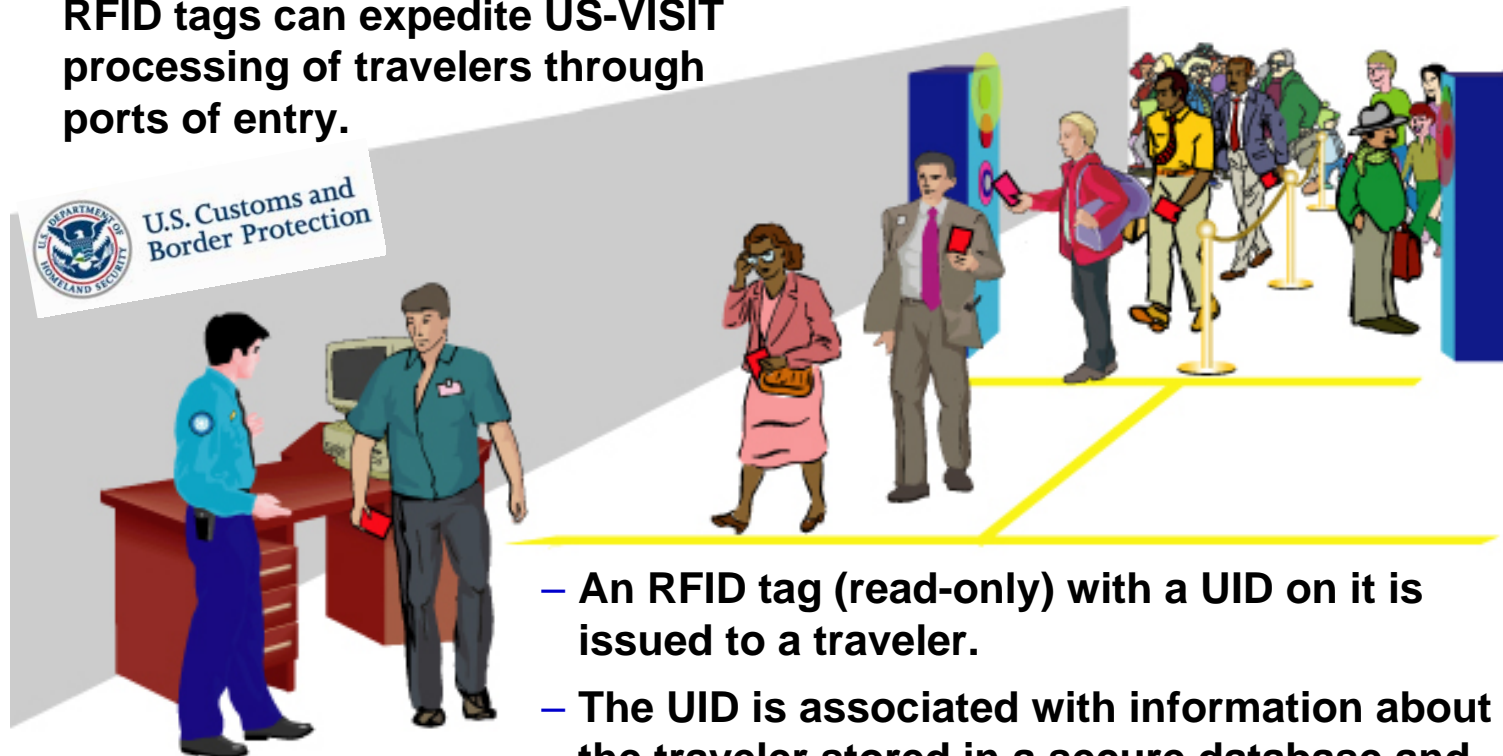
 MITRE  
Technology  
Program

# Problem

- RFID tags may be used to speed processing of travelers at ports of entry.
- A tag is sensed about 15–30 ft. from the entry point and traveler data is pre-fetched to speed processing when the traveler reaches the CBP officer.
- Since the unique ID number (UID) is transmitted “in the clear,” it may be interpreted as a “nickname” for the traveler and may be overheard by a third party.
- Third-party observers might be able to associate personal information with the UID.
- Concerns over this scenario motivates an approach that eliminates the association of a static ID number with the activities of a person.

# Background

RFID tags can expedite US-VISIT processing of travelers through ports of entry.



- An RFID tag (read-only) with a UID on it is issued to a traveler.
- The UID is associated with information about the traveler stored in a secure database and compared with information presented by the traveler.

# Objective

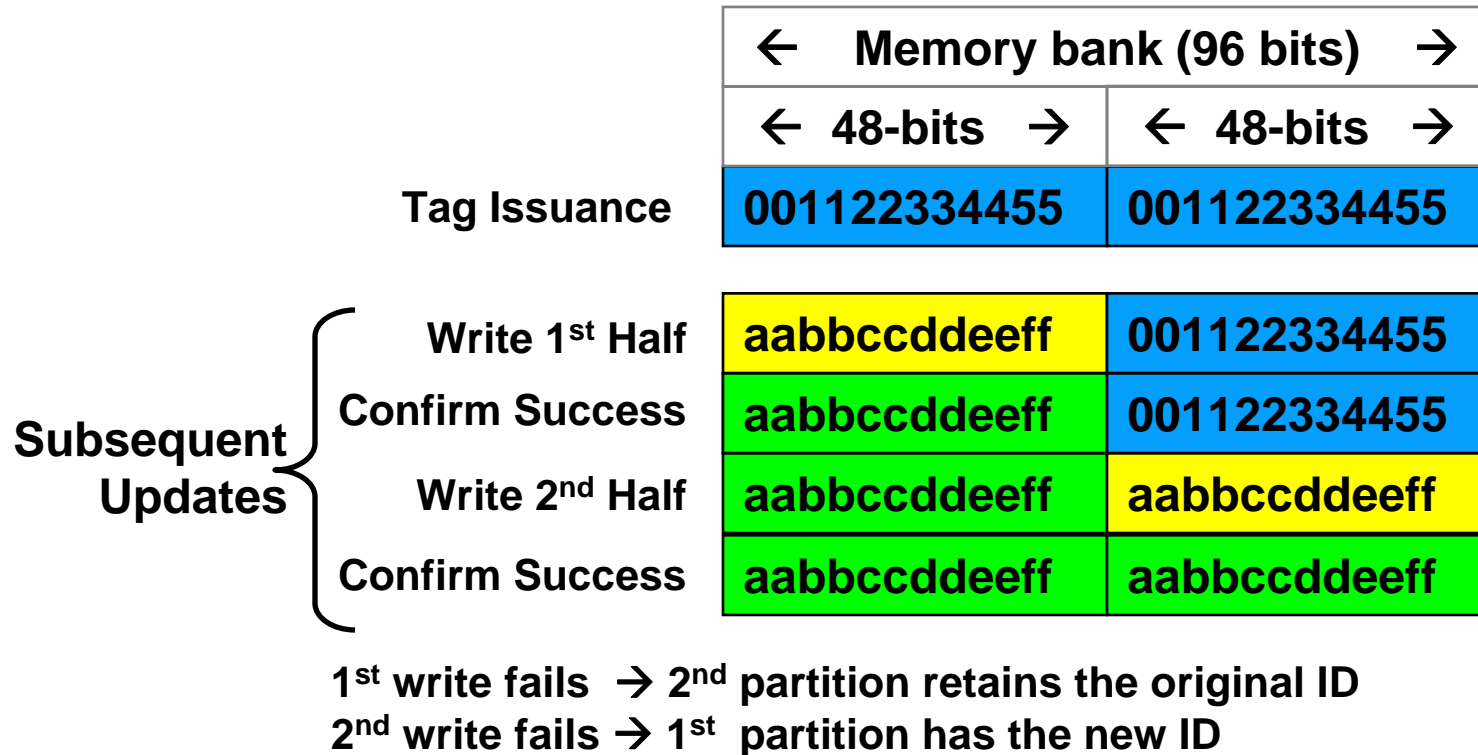
- **Develop a method to preserve identity information while changing the observable data on the tag**
  - Develop the required database schema needed to handle tag personalization and history
  - Implement a method to change the data on the tag without breaking the association between the tag and the traveler
  - Implement reliable reading and writing of data to standard tags using standards-based hardware
  - Identify and mitigate reliability failure modes inherent in RFID communications when physical tag control is not possible
  - Evaluate security and eavesdropping protections
- **Identify and measure aspects of performance**
  - Document factors that affect performance and reliability
  - Determine maximum transactions per second, evaluate reliability of transactions

# Activities

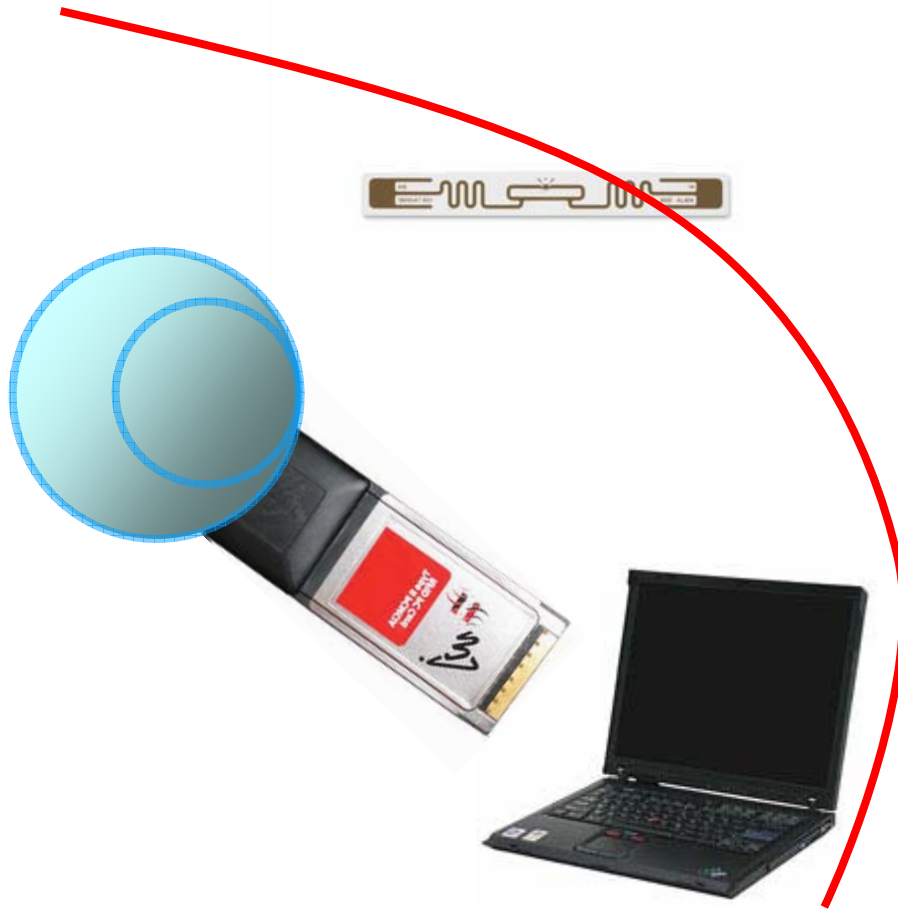
- **Acquire equipment:**
  - Laptop computer
  - Tag reader
  - Standard tags
  - Development software
- **Implement capability**
- **Collect performance metrics**
- **Demonstrate the capability to US-VISIT, other Government sponsors; transfer technology to sponsor organizations**

# Highlight

- 2-stage write of mirrored ID prevents unrecoverable corruption
- Guarantees we can keep on-tag data and database in sync



# Demonstration



**Encrypted Dynamic Privacy**

File View Help

CDM Port: CDM1 [Connect] [Offline] [Start Reading Tags]

Settings: Antenna: A B, Tx Power (dBm): 0, Tag Persist Time: 2 seconds, Refresh (ms): 300, Class 0, Class 1, Gen 2

Last Tag Information: Tag ID: n/a, Owner: n/a

Tag History

Tag ID (unencrypted)	Owner	Crypto Slot	In Range?

**Inventory Management**

Tag ID (unencrypted)	Owner	Last Read	Times Read	Last Written	Times Written	Crypto Slot
07322863E366842E...	New User	n/a	0	11/13/2006 4:0...	1	8
16440677974091D8...	Finkle, Fred	n/a	0	11/13/2006 3:3...	1	0
379D8505A3046664...	Bany, Steve	n/a	0	11/13/2006 1:3...	1	9
379D8505A3046664...	Bob	n/a	0	11/13/2006 1:3...	1	6
4420154E46D04EF4...	Rivers, Bob	n/a	0	11/13/2006 1:4...	1	7
54B04E6381E18E55...	House, Paul	n/a	0	11/13/2006 1:4...	1	6
D2BE90E32D7548...	Newer User	n/a	0	11/13/2006 4:0...	1	6

Personalize New Tag: Tag ID: <auto generated>, Owner: [ ]

Populate Cryptographic Slots: Number of Slots: 16

Warning! This will invalidate existing tags and cryptographic slots!

Slot	Key
0	D37917936CB6269767C8CD22A5C8...
1	98B8387053DC8565E5670D4A0A1F...
2	7846A3D894F7851E885EF7B47E854...
3	96451958A973DD90B2A5F90C39DC...

[No Tag in Range] [Assign] [Populate] [Done]

# Impacts

- **Support major Government initiatives that use RFID (e.g., WHTI, TWIC, NEXUS)**
- **Applicable to any technology capable of reading and writing data that as used to address the object**
- **Provides an effective, standards-compliant, and inexpensive solution to privacy concerns with Government use of RFID to identify people**

# Future Plans

- **Improved performance:**
  - Increase read-write rate by 10x
  - Increase effective working range
  - Document enhancements to security, privacy
  - Prepare implementation notes for hand-off to sponsor organizations
- **Implement with stationary equipment**
- **Conduct performance testing**
  - Database transactions/sec.
  - Tags/sec. in field