Secure RFID for Trusting Devices and Data

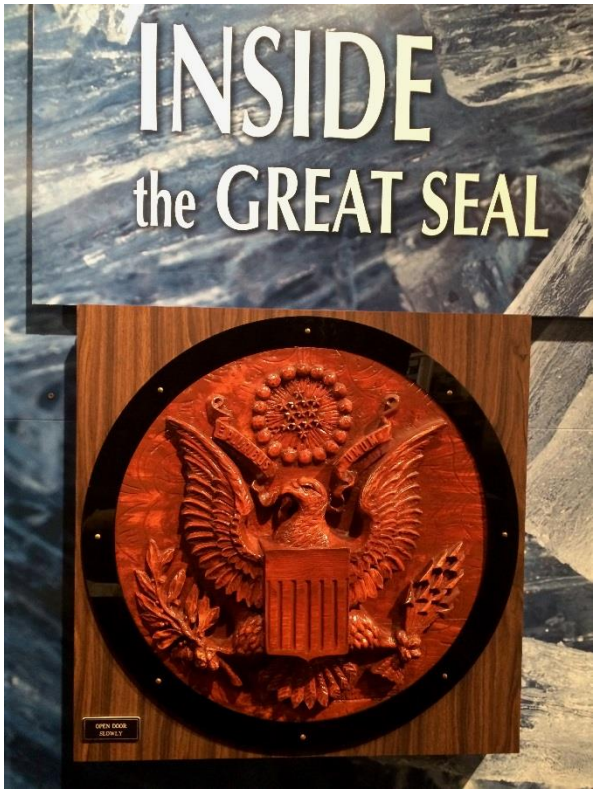
Dr. René Martinez
Engineering Fellow
Safety and Productivity Solutions

Honeywell

Legacy of RF, RFID, and Security

Honeywell

- RF is a shared medium and needs security
- Basis of RFID technology is backscatter modulation and is not a source of RF energy; makes information from RFID intrinsically more difficult to detect



Presentation Outline

Honeywell

- Context and Background
  - Focus
  - Deterrence mechanisms
- Incursions and Problems
  - Privacy
  - Cloning
- Deterrence and Solutions
  - Standards
  - Protocols
  - Key management

Secure RFID for Trusting Devices and Data

Honeywell

- **Trust**
  - Derives from “True”, as in "real, genuine, not counterfeit" from 14th century
  - Derives from trees, as in "firm, solid, steadfast” from Proto Indo-European
- **Secure**
  - Private to prevent unauthorized reading or writing of data
  - Secure to prevent unauthorized listening
  - Authentic to ensure the data is valid
- **Cryptographic Secure UHF RFID**
  - Cryptography has well established mechanisms for “Secure” and “Trust”
  - High performance UHF (distance and speed) has previously limited implementation of cryptography in UHF RFID
  - *Focus of presentation is Cryptographic Secure UHF RFID*

UHF RFID Mechanisms for Deterrence

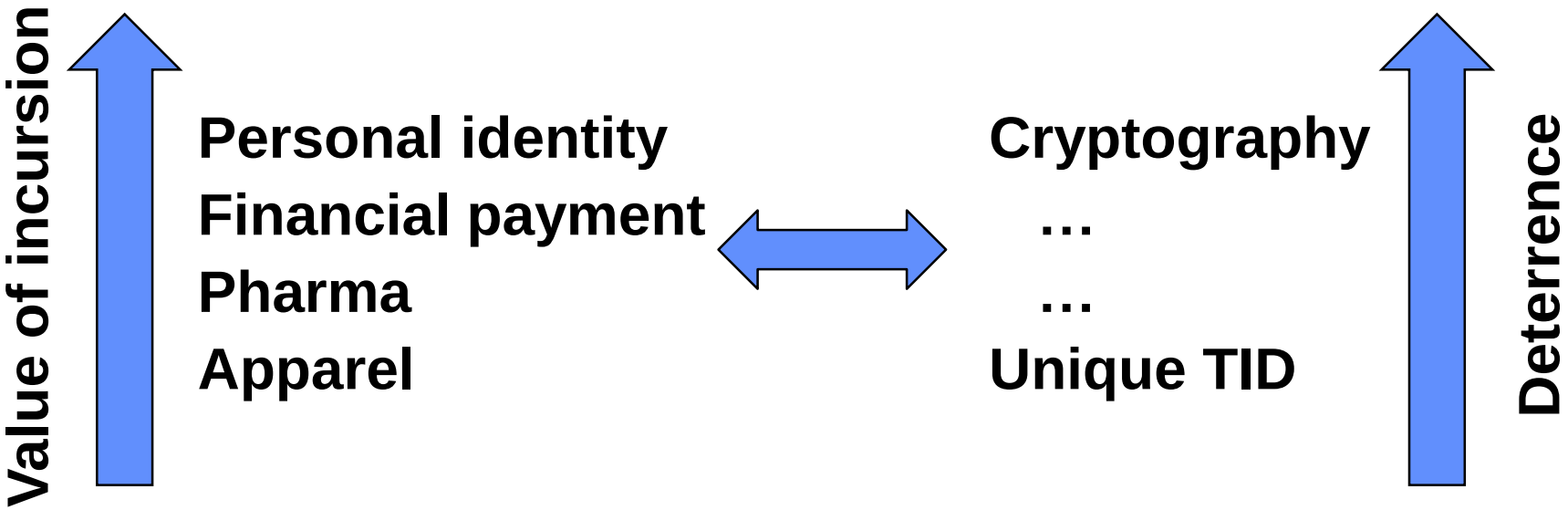
Honeywell

- **Unique Tag Identifier (TID)**
  - Unique TID in tag is a read-only serial number programmed by IC manufacturers
  - Offers basic protection that tag is unique, but…
  - No defenses against emulators
  - No defenses against IC manufacturers with writeable TID
  - Privacy issue since unique TID is NIST PII
- **Password Protection**
  - Uses Access password to read Kill password, but..
  - 32bit password space is small
  - Limits speed performance with several reader/tag packets
  - Eavesdropping on “secret” cover code from tag isn’t difficult, and XOR for hiding password is easily reversed
- **Secure RFID**
  - Uses established and accepted cryptographic algorithms to implement security

Deterrence and Value of Incursion

Honeywell

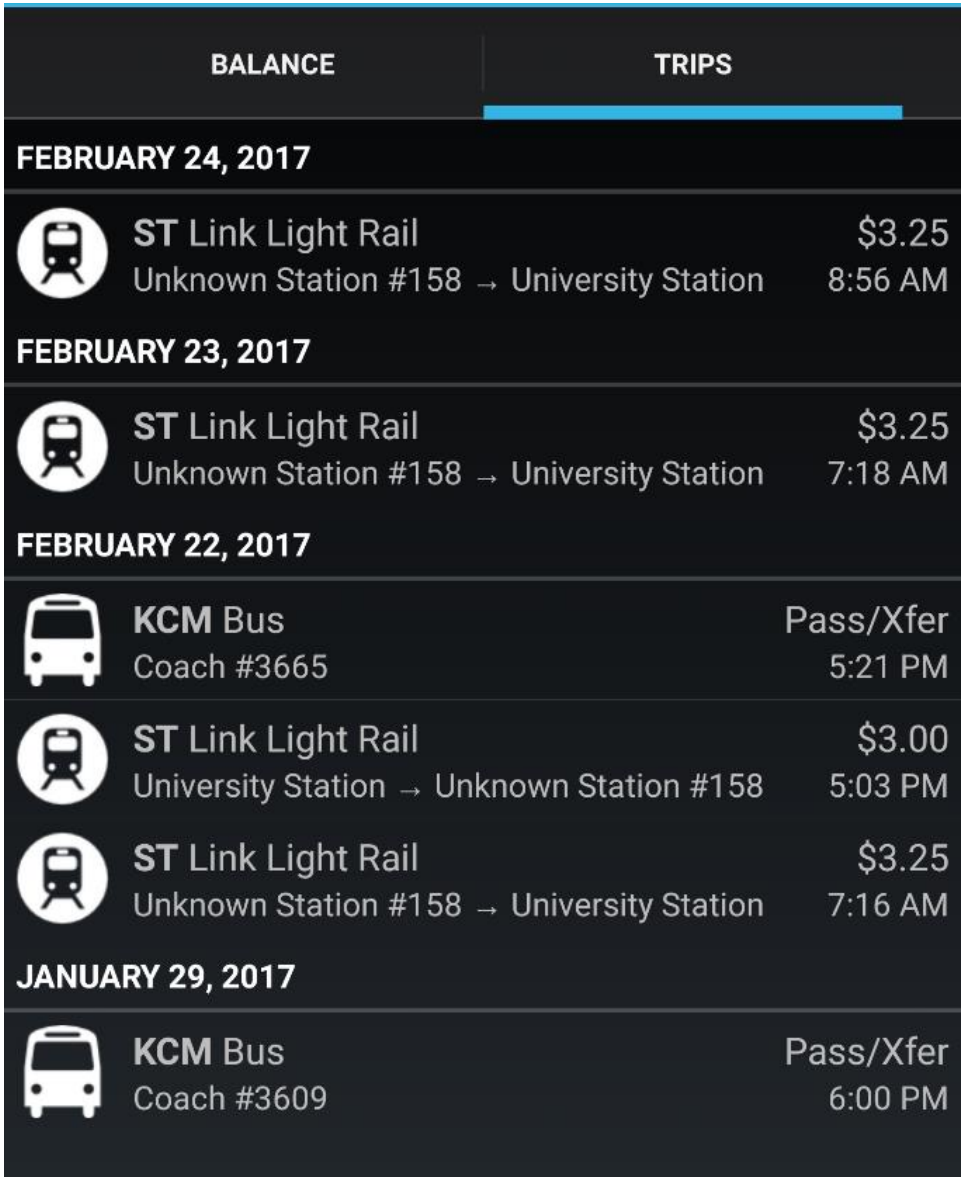
- **Deterrence should exceed value of incursion**



Incursions and Problems
(White hat hacking)

HF RFID Mass Transit Tracking

Honeywell



Skimming Electronic Toll Tags

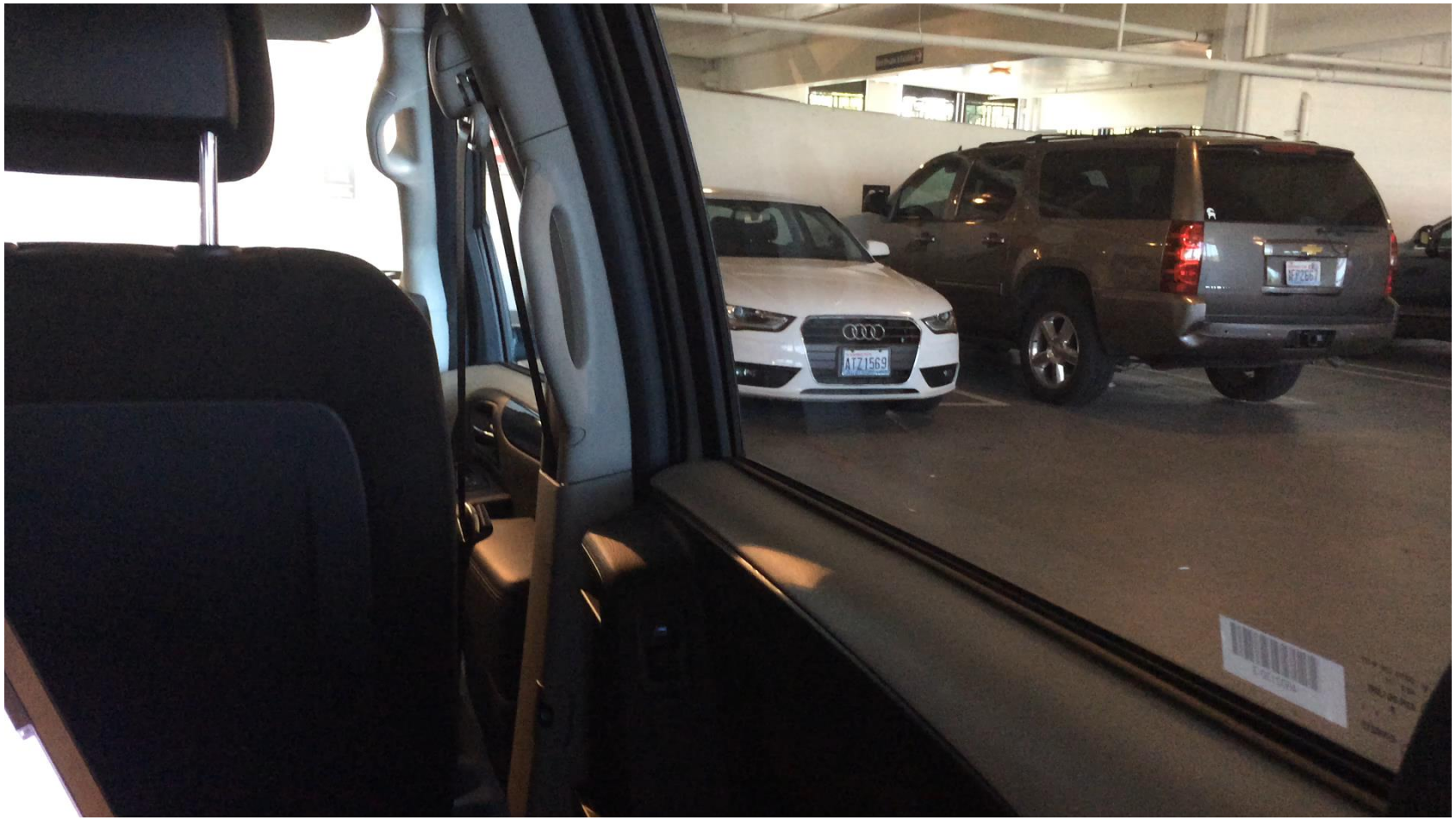
Honeywell

Skimming tags at highway ramp

Skimming tags at parking lot

Skimming Tags in Parking Lot

Honeywell



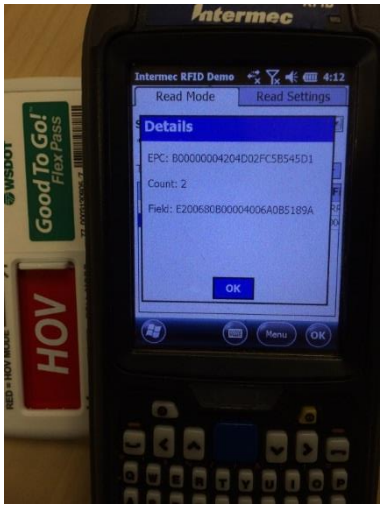
Cloning of Electronic Toll Tag

Honeywell

Financial Transaction with Cloned Tag

Honeywell

- **Authentic EPC/TID tag data duplicated into clone tag (tag emulator)**
- **Use clone to pay for toll**



Tag Mode	Tag contents			Pass ID			
				Prefix		Account	
	Bank 1 (UII/EPC)	Bank 2 (TID)	Bar code	Dec	Hex	Decimal	Hex
Toll	B00000001204D02FC5B50DB8	E200680B00004006A0B5884F	77 0003130805 7	77	4D	003130805	02FC5B5
HOV	B00000004204D02FC5B545D1	E200680B00004006A0B5189A	77 0003130805 7	77	4D	003130805	02FC5B5

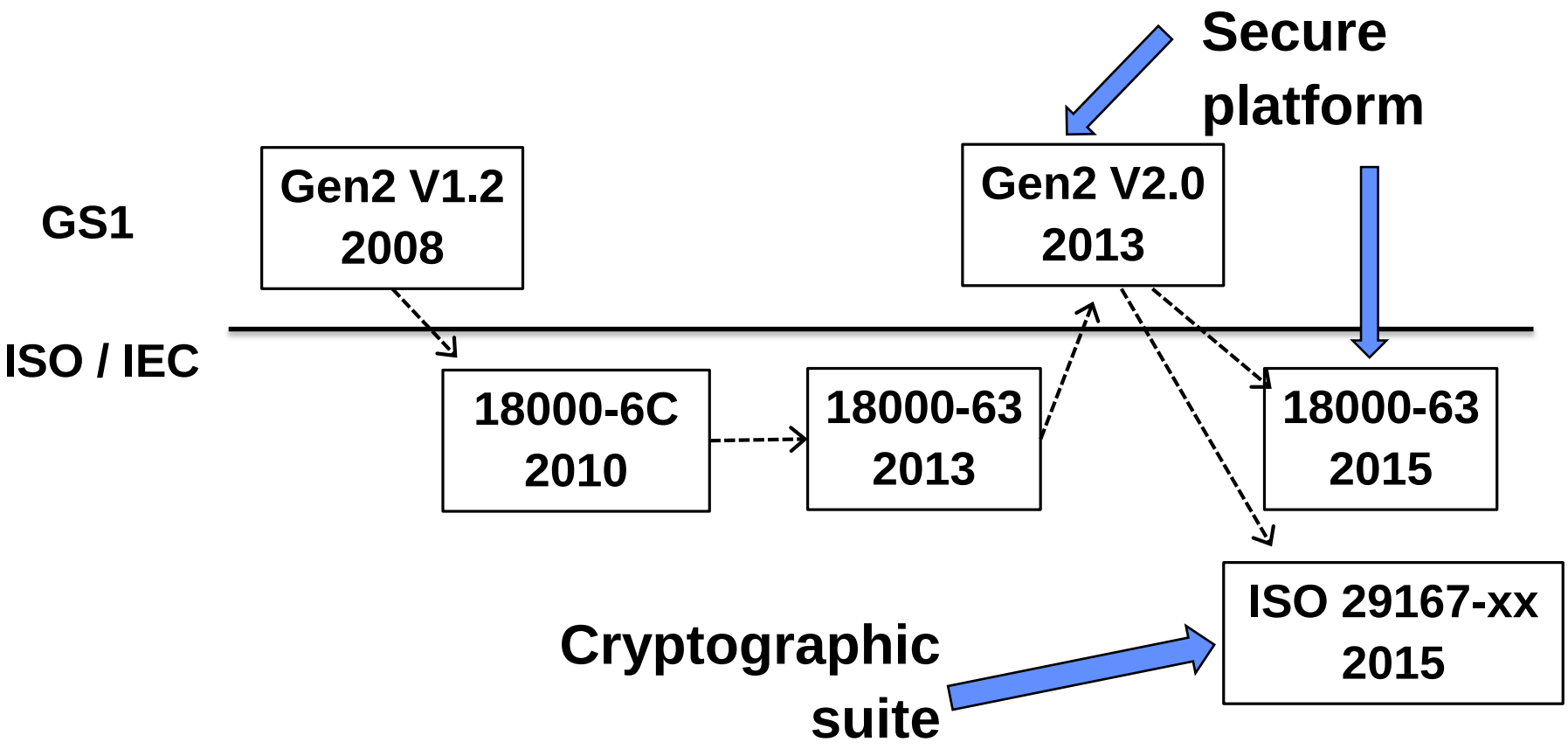
Transaction	Posted Date	Pass ID	Lic[illegible]	Location	Lane	Directio	Amount
11/13/2015 14:58:53	11/13/2015 16:04:58	77-00031 30805		SR 520 Bridge East	520E-520EB-01	East	-$3.10

Deterrence and Solutions (Standards and Protocols)

Secure UHF RFID Standards in 2015

Honeywell

- Platform for cryptographic suites in 2013 and 2015
- First cryptographic suite in 2015
- Secure UHF RFID needs 18000-63 *and* 29167



Security Commands in ISO 18000-63 / Gen2v2

Honeywell

Gen2v2 / ISO 18000-63 commands	Common use	Required	Optional
Untraceable	Hiding serialized public tag data	✗	✓
Authenticate	Secure reading and writing of data, usually for ≤128bits of memory	✗	✓
ReadBuffer	Recovery from crypto data errors	✗	✓
Challenge	Parallel processing of cryptographic operation saves time; 25% for two tags, and 50% for three tags	✗	✓
AuthComm	Authenticated transactions >128bits of data with stream cypher	✗	✓
SecureComm	Encrypted transactions for >128bits of data with stream cypher [1] *Authcomm can also encrypt data*	✗	✓ [1]
KeyUpdate	Secure update of keys in-the-field [2] *Authenticate write could update key*	✗	✓ [2]

AES Crypto suite ISO 29167-10: 2015 and 2017

Honeywell

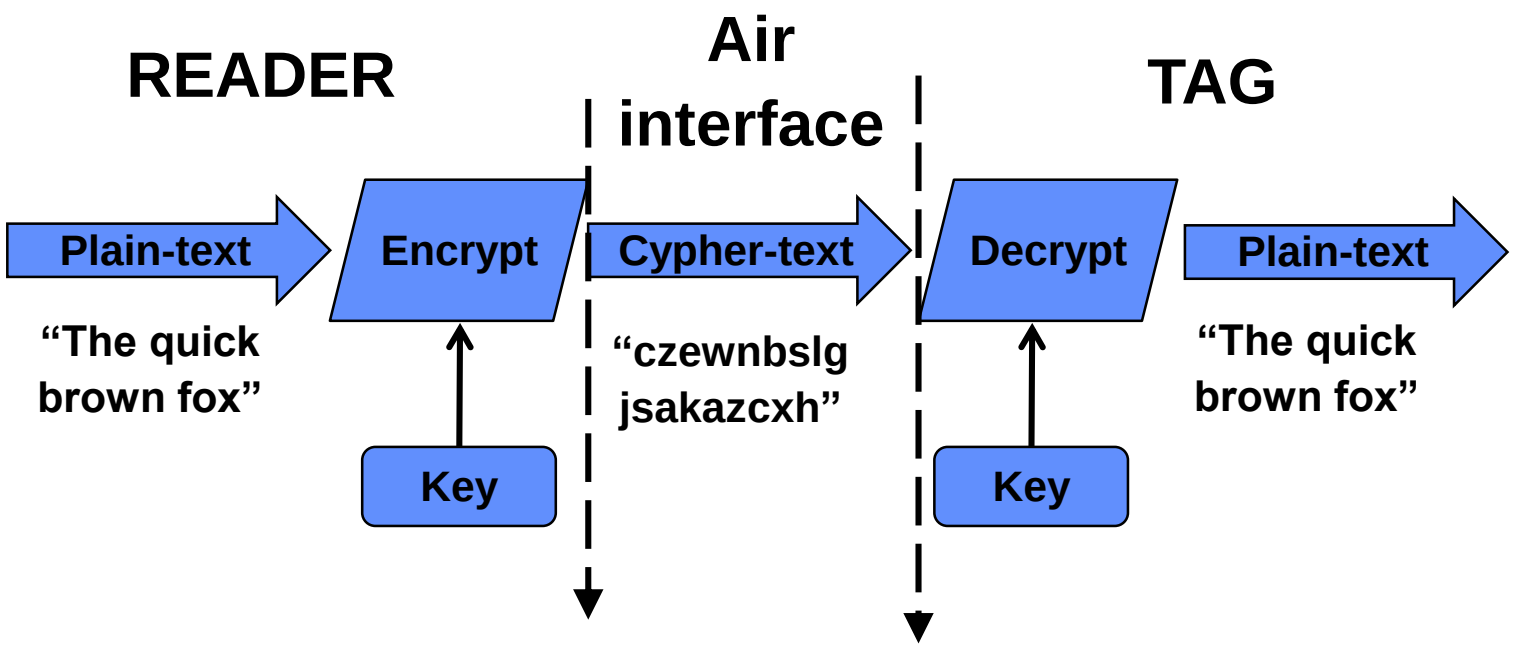
29167-10 Method	Common use	Conformance requirement	In 2015 version	In 2017 version
TAM1	*Authenticate tag* – often combined with public plaintext identification	Mandatory	✓	✓
TAM2	*Secure encrypted read* – authentication of tag with private cyphertext identification	Mandatory	✓	✓ [1]
IAM1/2 or MAM1/2	*Secure change to tag* – modification to tag by authenticated reader	Optional	×	✓
IAM1/3	*Secure encrypted write* – write encrypted data to tag by authenticated reader	Optional	×	✓

[1] Version 2017 adds additional TAM2 format to prevent man-in-the-middle attack that corrupts read data (e.g. private identifier) in the 2015 version.

Example of Encrypting Data

Honeywell

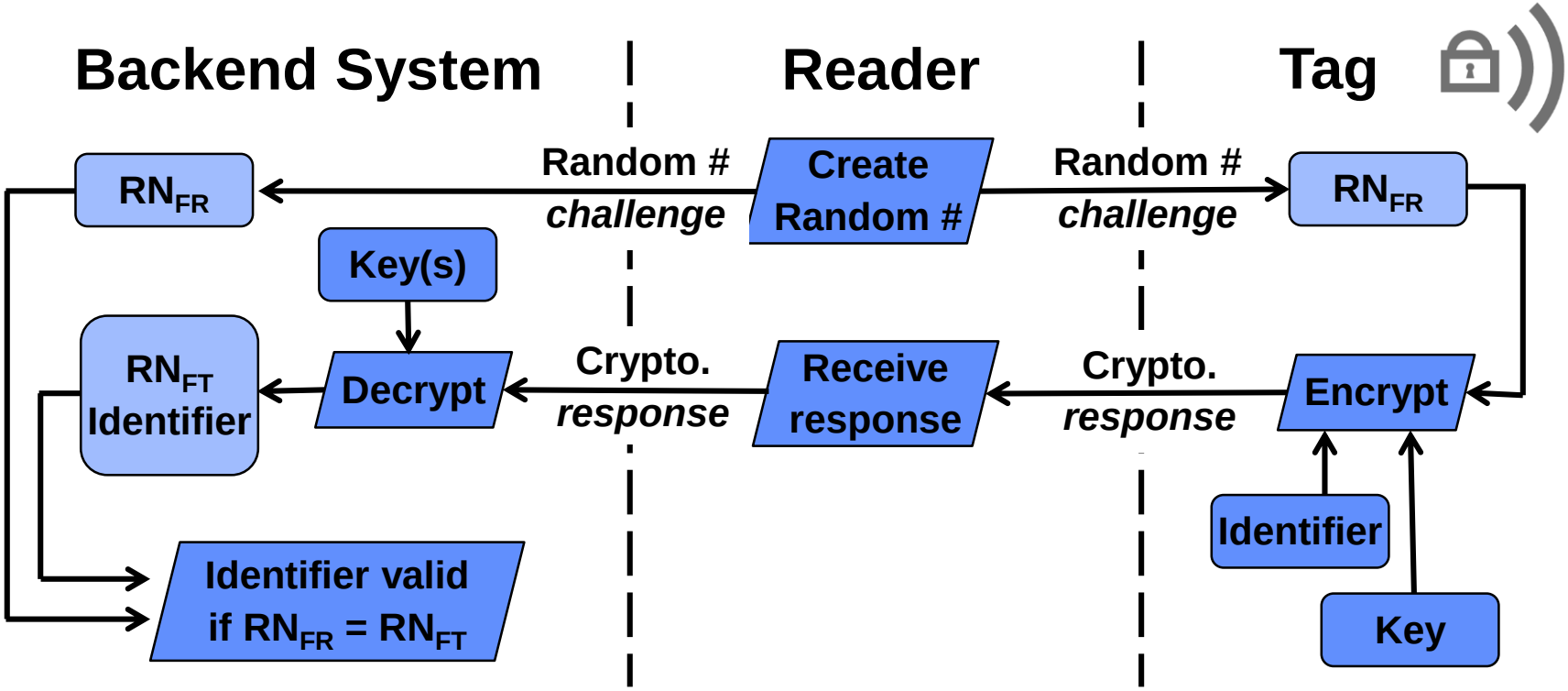
- Reader encrypts plain-text data, sends “cypher-text”, tag receives and decrypts cypher-text
- Plain-text data can be information or a random number “challenge”



Anonymous Identification with TAM2

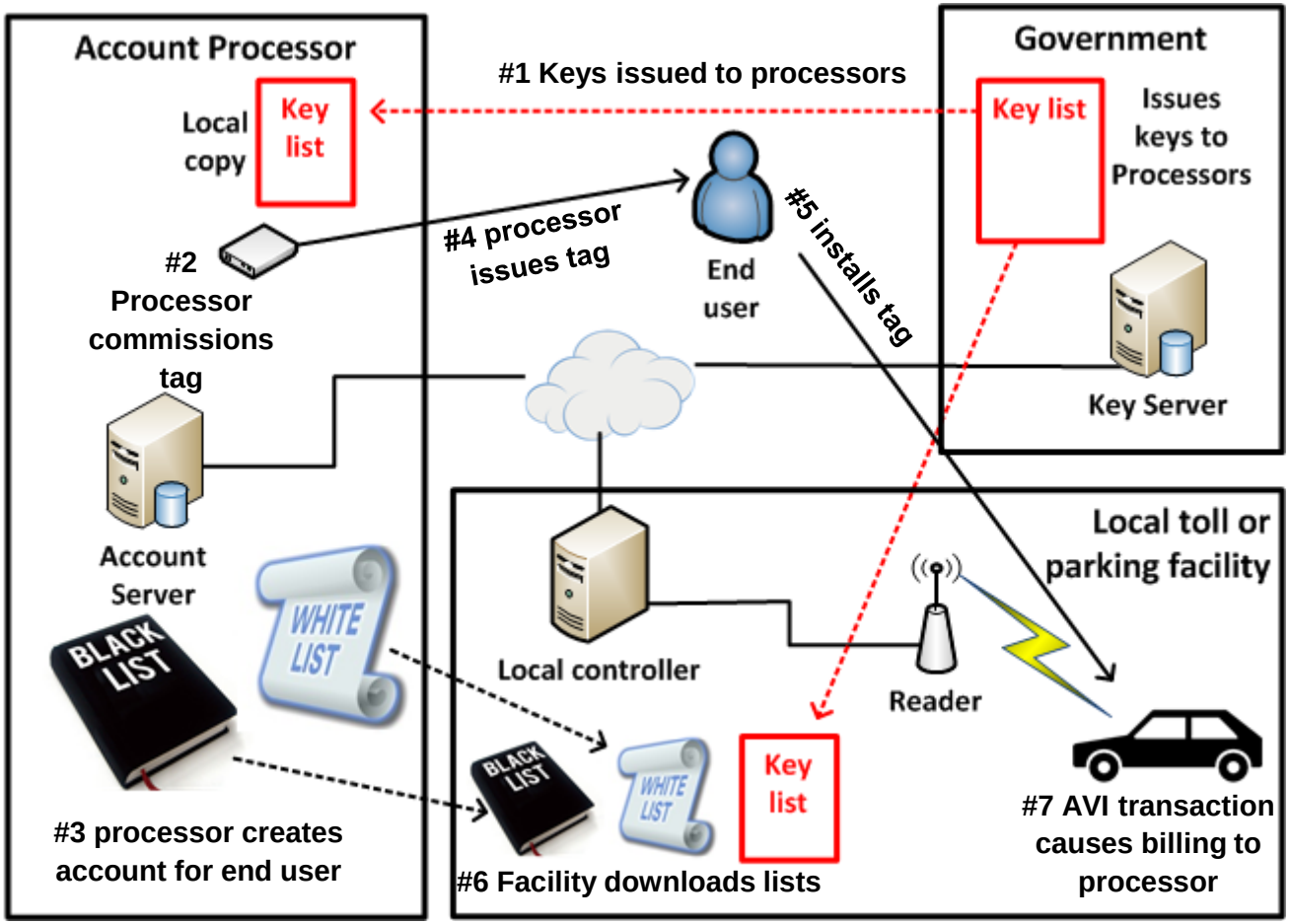
Honeywell

- Tag loaded with Unique Identifier and Key
- Backend system loaded with Key(s)
- Reader functions as intermediate between tag and backend system
- Backend system decrypts tag's cryptographic response to extract and verify identifier



Key and Account Management

Honeywell



Secure UHF RFID in Vehicle Track Tests

Honeywell

Conclusions

Honeywell

- RF and RFID is a shared medium
  → use security when viable
- Security is viable with UHF RFID
  - Standards exist
  - Implementations exist
- Enforce Privacy
  → no unique plain-text identifiers
- Encrypt and Authenticate Data
  → consider talented adversaries

Thank you