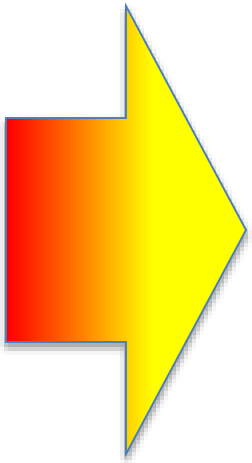
Thin film Secure Display Inlay: A revolutionary new Class of ID card

Mark Krawczewicz
Tocreo Labs
Annapolis, MD
mark.kraz@tocreo.com
410-562-9846

Conference Theme & This Talk

Passive Wireless Sensor Tag Workshop



Tocreo Labs

- ✓ Sensor
- ✓ No batteries
- ✓ No Scavenging Power
- ✓ No Wired Connection
- ✓ Inexpensive
- ✓ Easy to deploy

- ✓ Secure – Secure - Secure
  - ❖ Protects user's data, 2-way
- ✓ Display & Form factor
  - ❖ Thin- fit's within a ID card
- ✓ Broad Applications

Technology . . .

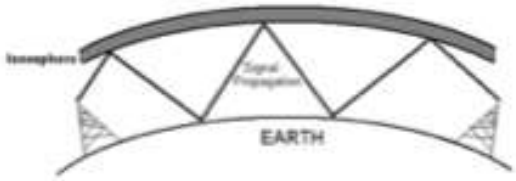
Developed a secure batteryless inlay with an embedded display to protect users data

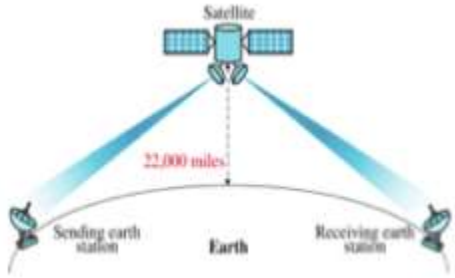
Unique combination of features have broad security Applications

Data Protection

Data-in-Motion

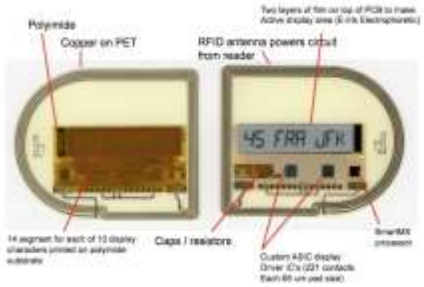
(wired or wireless)





Data-at-Rest

A Card Like No Other?



a. Dynamic Bi-State Display

a. Users Access -**day / hour / privileges / remaining balance** can be written to the display defining role or access period by access control station

b. Display can also show pending **authentication, cryptographic, transactional , or other security process**

c. **Visual Passport –** user carries **auditing** trail

b. Both an visual ID credential <u>and</u> a secure "Container" for data like photo, ID number, name, medical certificate, biometric, audit file, etc.

c. Extraordinarily secure – same security processor as in 250 million passports

d. Uses only reader power – will last indefinitely

e. Maintains the Chain of Trust - (Users can verify at one terminal and then at a later time, facility, or secured area, prove it} – **Virtual Fence**

f. Single card bridges physical & network access worlds

Q: Why Integrate a thin film display behind a trusted processor and memory in the card?

A: President Obama's Blackberry

Un-trusted Application display

SME PED- General Dynamic's Sectera

- Trusted display show visual evidence user is in secure voice or secure text mode
- Shows Security level of Call-ed party

What's Displayed!

The User's Privileges

✓ **Time** , **Date**, card holders **Role** or **Title**, **Validation period**, Flight number**dynamic security threat Level. . .**

Status of a Secure Process

✓Cryptographic, Biometric, Password, Payment transaction, Authentication from a trusted display . . .

Auditing List

✓Independent from network audit list, card can store and display medical, legal, document viewed, network, file access audits . . .

Role / Title credentials	Time stamped credentials	Secure Process		Audit Process
CONTRACTOR	13 JUNE 2011	VERIFIED	SECURE	Network
TSA AGENT	T 1300 – 1600	BIO -OK	ENCRYPT	Access
GND CREW	UA 1143	PIN-OK	VALID	payroll
FBI				

Security =  +  + 

User Authentication

Tocreo's security architecture (National Type 1 architecture) is modeled after DoD's

(Tocreo's architecture)

Security =  +  +  + 

User Authentication

and / or

Need all 3 keys to unlock

Applications of Technology

1. Labels for medicine, blood, containers
2. Mass Transit card
3. Coffee mug label
4. Micro payments, Student ID + meal plan
5. Cell phone payment credential
6. Battery label to show how many charges left
7. Reusable luggage tag and boarding pass
8. Retail Loyalty / rewards Cards
9. **Remote Login to Secure network Enclave**
10. Medical Records storage card
11. **Credential to unlock Mobile device (Phone, tablet)**
12. **Secure Access Control Badge (Aviation, trusted facility, sea ports, Government, etc)**

Security Applications

1. Unlock Mobile Phones, tablets, iPADs, etc.

1. Remote Login

1. Secure ID credential

Tocreo's forecast for a more secure Commercial mobile devices:

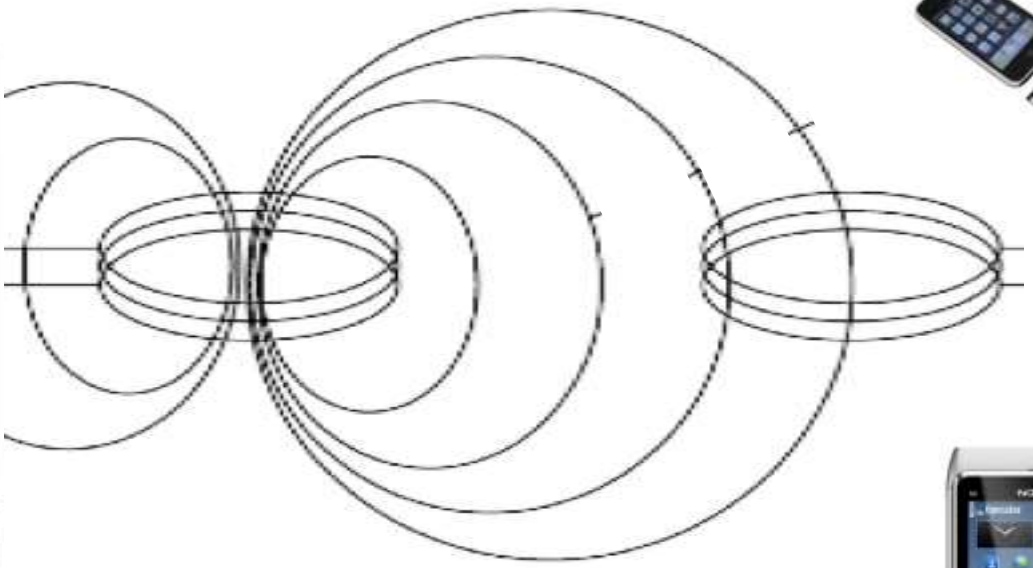
- Extremely Challenging to modify hardware - No Company can slow the "ocean" of mobile device hardware, interfaces, or power trends – everyone wants to live and work at the mobile beach

- Companies & Governments may have impact on redirecting the tide with secure OS, standards, & firmware

- Highest success will blend **secure design architecture** with winds of **manufacturing innovation** – **a Secure Display card to unlock commercial mobile device**

- **Solution balances** – low cost, convenience to customer, adaptability, & security

Tocreo's Mobile Solution



NFC

Power

Data

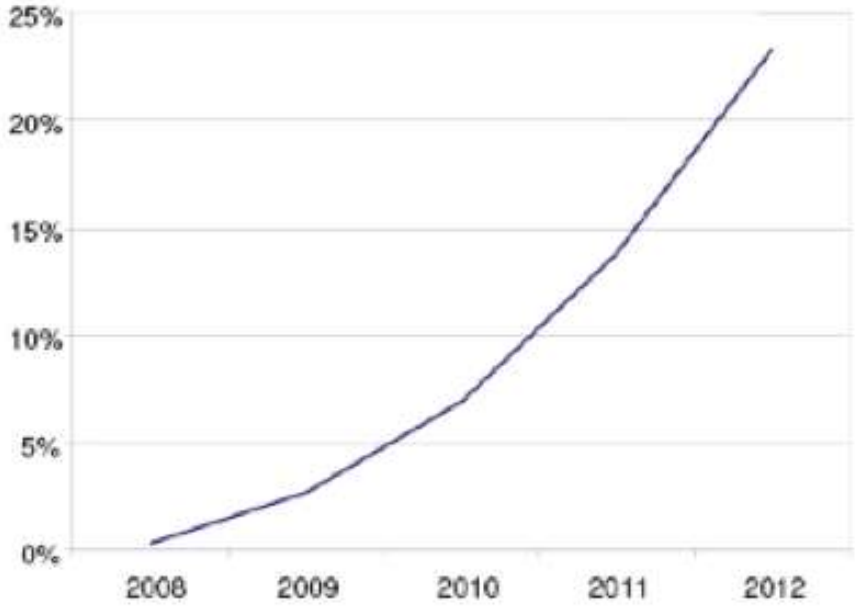
Execution within Card:

* Authentication,
* Secure Processes
* Crypto,
* Audit,
- Key split combination
- Cert / user biometric storage
- Data-at-Rest

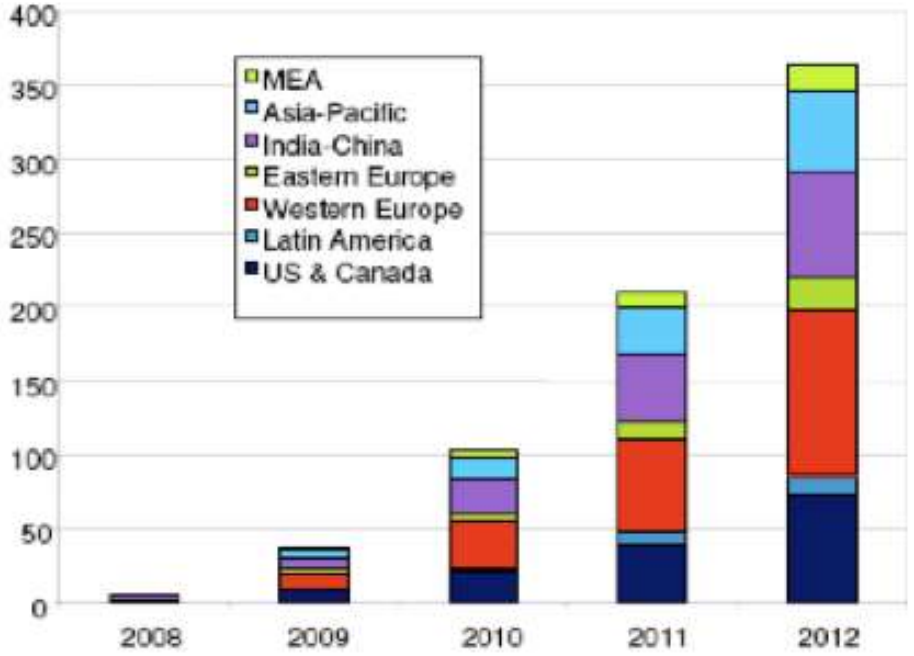
1.

Forecast for NFC enabled Handsets

Penetration of NFC in world handset sales (%)



NFC phone shipments (million)



- Ignited by support from key wireless players Nokia Corp. and Google Inc.,
- built-in NFC capability will rise to 220.1 million units in 2014
- Nokia said it will support NFC in all new smart phone models introduced in 2011
- the three largest U.S. mobile phone carriers—AT&T Wireless, Verizon Wireless and T-Mobile—have launched a joint venture known as ISIS that will develop a mobile payment system based on NFC
- according to Cult of Mac, Apple's doing more than just playing around with the technology--they've got big plans for NFC chips in the iPhone 5.

1.

Comparison NFC

	NFC	NFC benefits	Bluetooth	DASH-7 ISO 18000-7	Zigbee 102.15.4	uHF	Wi-Fi 102.11
Communications Mode	2-way	Safe, difficult to attack	2-way	1- way	2-way	1-way	2-way
Range (0 dBm)	< 10 cm	More immune to eavesdropping & intentional and unintentional interference	~10 m	250 m	75 m		25 m
Power	✓ Battery NOT Required	Inductive from reader Cards last indefinitely				✓ Battery NOT Required	
Nominal Data Rate	Up to 424 kbps		721 kbps	27.8 kbps	250 kbps	64-512bps	
Average power for (10) ten 256 kbyte messages / day	3DES – 7mA / 3ms block (2.5mW / u sec) **3DES = .16 uWatts** AES / EC = 15 uA / 2m sec (27 mW / 2 m sec) **AES / EC =0 .6uWatts**	All power coupled into from reader 60-80 mW	**50 *u*W**	**60 *u*W**	**414 *u*W**	**n/a**	**570 *u*W**
Cost	Low		Moderate	high	moderate	Low	Moderate
Mobile Infrastructure compatible		Low roll-out cost					

Common Cell Phone Interfaces

SMS

GPS

http://

Camera

Bluetooth

Access to PIM

2D Bar Code Capture

SIM HD

NFC / RFID

Interim for non- NFC Mobile Devices

Mobile Commerce – cell phones as payment mechanism?

(securing money rather then user data)

Why?

a. The Credit and Banking card industries will not move away from a form factor that has been adopted internationally for 60 years

b. Cell phones alone are not secure – big problem!

c. Other big players like Google, Apple, Facebook, & PayPal see the opportunity

‘Mobile wallet solutions are our top priority’ says PayPal boss

PayPal president Scott Thompson has revealed that moving the online payments service into the retail arena is now the company's top priority.

According to *The Wall Street Journal* Thompson said in an interview that the company's top priority "is to develop software that transforms mobile phones and other devices into 'digital wallets' that consumers can use to buy merchandise, keep coupons and store loyalty program data."

Security Applications

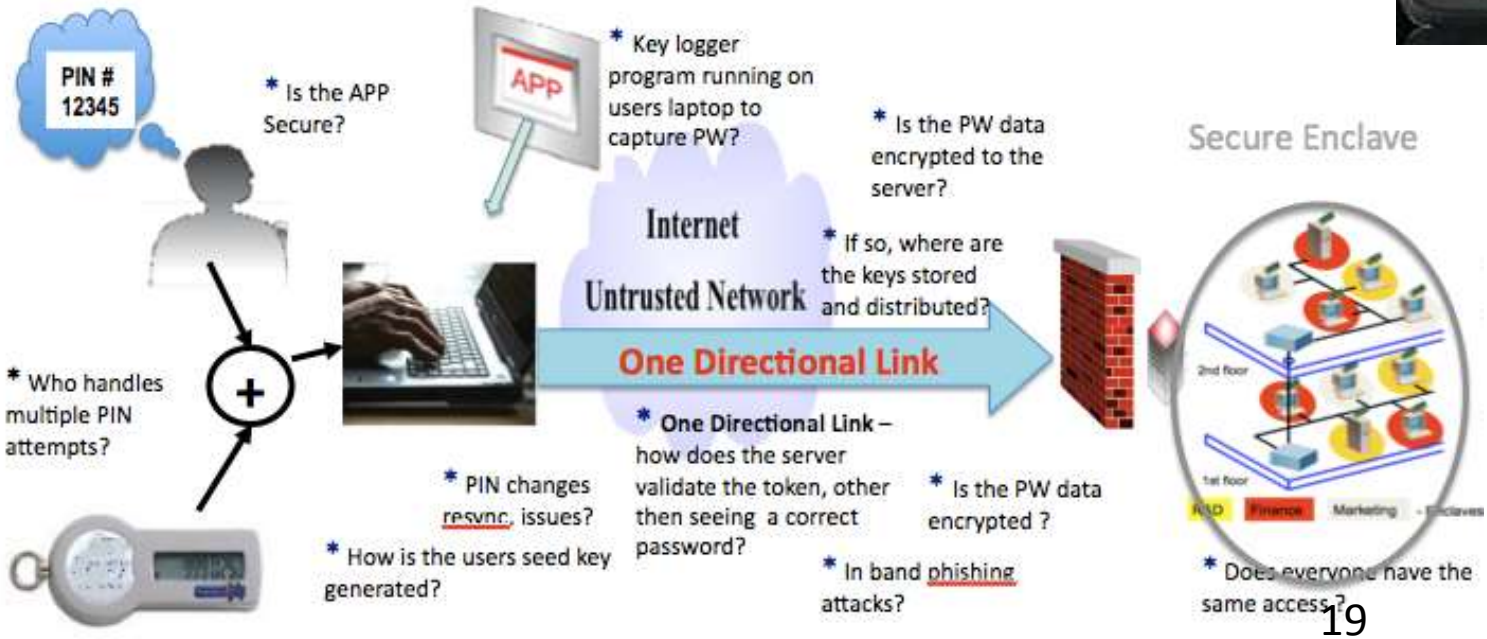
1. Unlock Mobile Phones, tablets, iPADs, etc.

1. Remote Login

1. Secure ID credential

2.

Some Commercial OTP for mobile and remote login applications



2.

Tocreos Remote Login Security Architecture

Steps

1. Card & Firewall mutually authenticate
2. 2 or 3 factor user authentication verifies user to card, unlocks users data on card
3. Set up secure (encrypted) channel to/from enclave firewall
4. After secure session, audit log stored on card memory & display

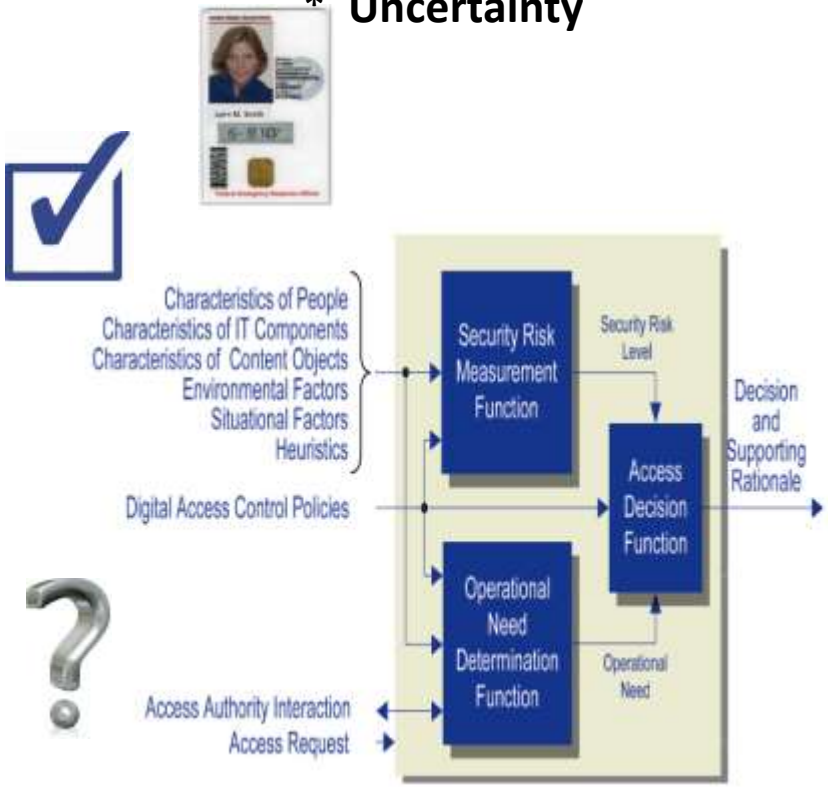
2.

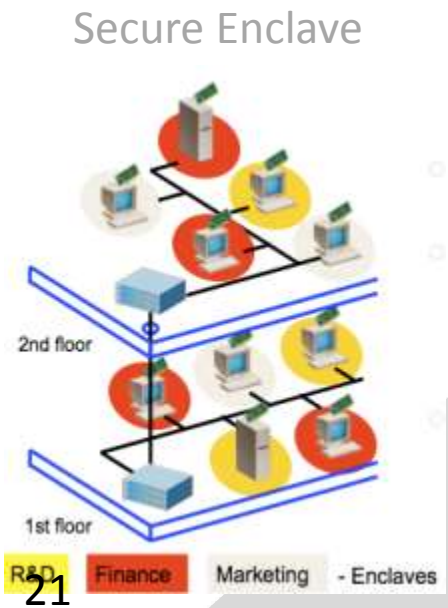
Risk Adaptable Access Control (RAdAC)

The network makes a decision of a user's privileges using factors such as;

* **Trust of person** requesting access
- Sensitivity of Information to be accessed
- Quality of protection that can be afforded the information

* **Role of the person**
* **History of access decisions**
* Environmental & situational factors
* Criticality of information to the operation
* **Uncertainty**





Security Applications

1. Mobile Phone & Device

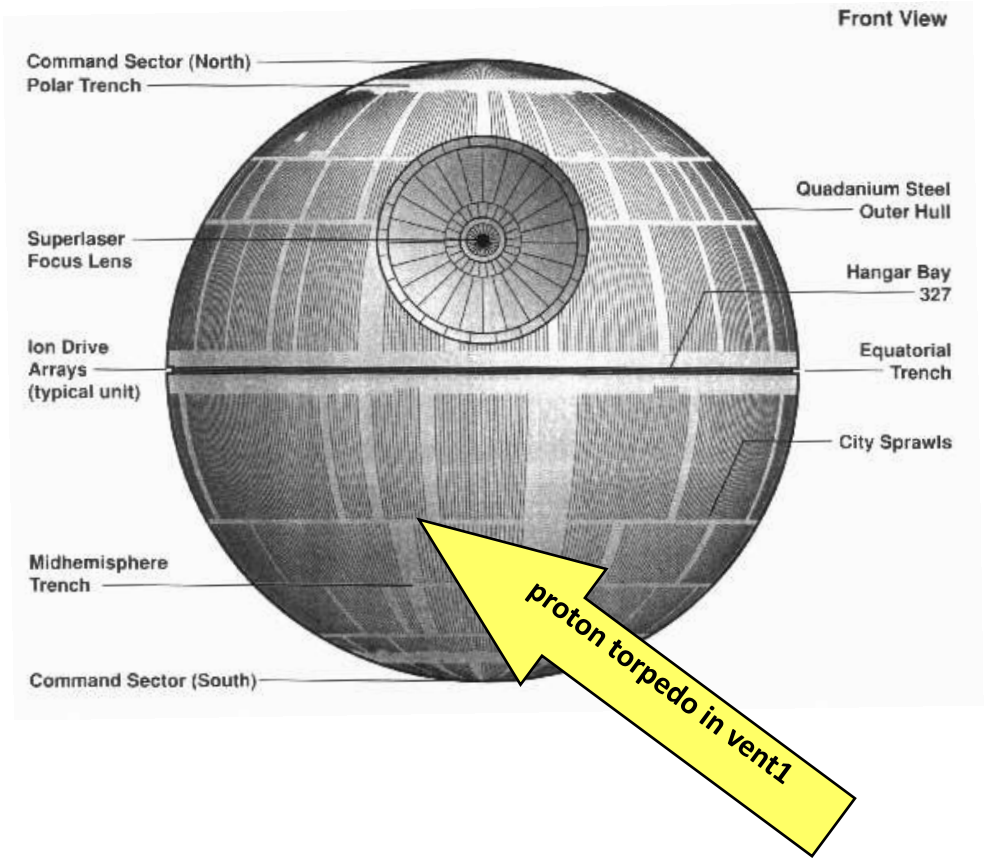
1. Remote Login

1. Secure ID credential

Protecting User's Credential Data

- Biometrics
- User Medical Information & data about drugs
- Roles & Responsibilities
- Dynamic Access Privileges
- Cryptographic variables
- User data
- Auditing information (electronic Passport)
- Single sign-on password

Protecting the Weakest Link

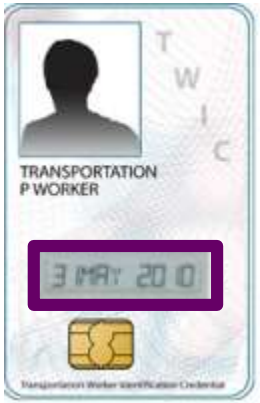


- Strength of cryptography relies on secrecy of key, not the algorithm
  - Do not create your own crypto algorithms
- It is not safe to assume that large key size will guarantee security
- If algorithm implemented improperly, can be broken or bypassed by attacker
  - Test implementations in laboratory first!

3.

Security - “It’s in the Details”

- On chip sensors
  - Under / Over Voltage
  - Under / Over Temperature
  - Under / Over Freq. Detector
  - Active Tamper grid
- Key Split algorithm
- Three factor user authentication
- Random Number Generator
- Secure Microprocessor

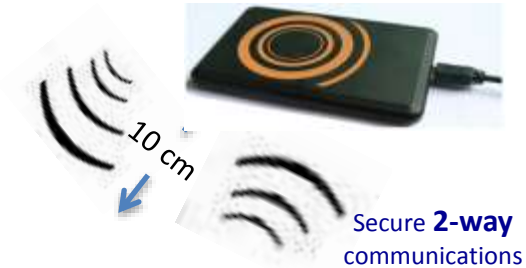


- Custom Low power RAM
- Differential Logic on Critical Paths
- Time Varying Process
- Opaque passive masking
- Tamper epoxies / new IC packaging technology
- Minimized I/O
- Other layout techniques
- Free running internal clock
- Critical Lines in Metal or Poly silicon
- Dynamic Address / data bus scrambling

Significantly More Secure Elegantly Simple

HF Reader

RF energy from HF reader powers up 3 chips & display

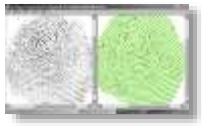


Secure **2-way** communications between reader & card

Secure Processor Memory

User Data memory

Display memory



- Digital photo
- biometric template

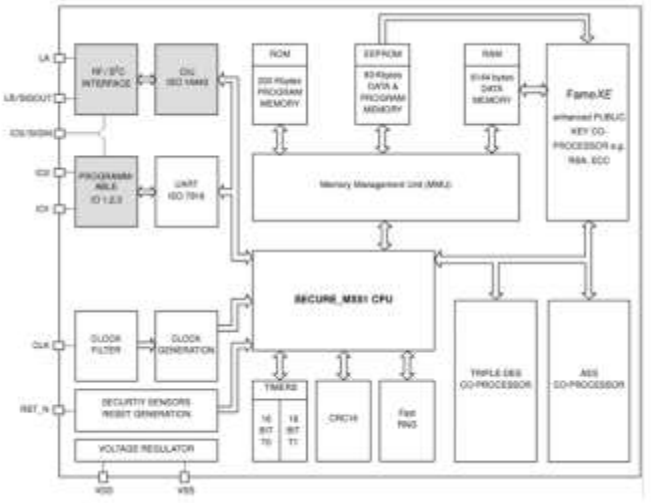
Doe, John G.
Pilot ID # 123-4567
Employee Status - Active
Flight Status – Active
Medical – Active

16 FEB 2011

J. SAMMON
UA 412
16 FEB 2011
JFK BWI
TIME 1730
MONDAY
VERIFIED

Baked – in SmartMX Security

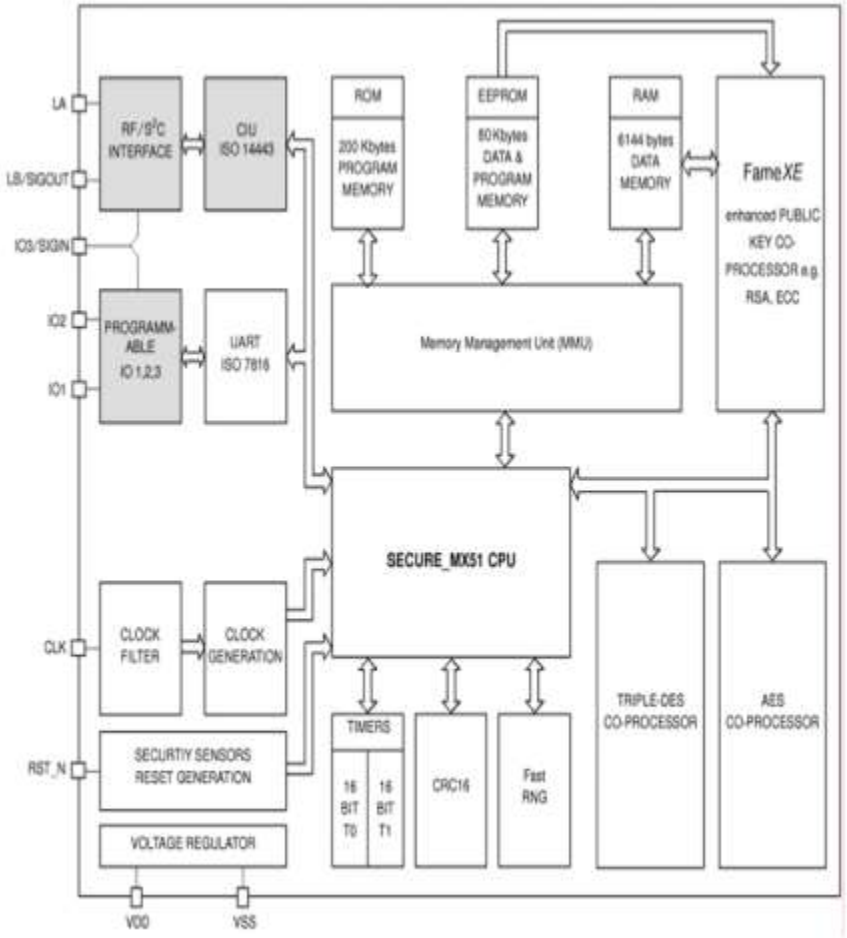
(to protect the user data, crypto key, firewall memory)



- SmartMX and its OS incorporate a range of both hardware and software-based security features as counter measures against attempted attacks,
- a very dense 5-metal-layer 0.14 µm technology
- active shielding methodology for optimum security results. SmartMX card ICs also features –
- beyond exception sensors for voltage, frequency, temperature
- dedicated countermeasures against Differential Failure Analysis, Single/Double Power Analysis and dangerous locally focused/well-timed laser light attacks .
- extremely resistant to any kind of physical analysis and forced malfunction during operation.
- A hardware memory management unit (Firewall) provides additional protection for PKI controllers.

- The SmartMX has achieved best-in-class Common Criteria EAL5+ certification on the basis of the rigorous BSI- -0002- 2001 Protection Profile (CC# BSI-DSZ-CC-0410-2007).
- 0.14 µm CMOS technology based on power saving,self timed asynchronous technology
- User keys (PIV application keys) can be zeroized using the delete mode of the PUT PIV KEY Command.Cryptographic
- Officer keys (Card Administrator keys and Application Provider keys) stored in non volatile memory are zeroized using a procedural overwrite.
- cryptographic keys (CSK and ASK) are stored in volatile memory and are zeroized upon termination of the session, i.e. when the secure channel is closed or when the module is powered off
- every keys and PINs are protected by a signature that is checked prior to every use of the keys or PINS.

SmartMX



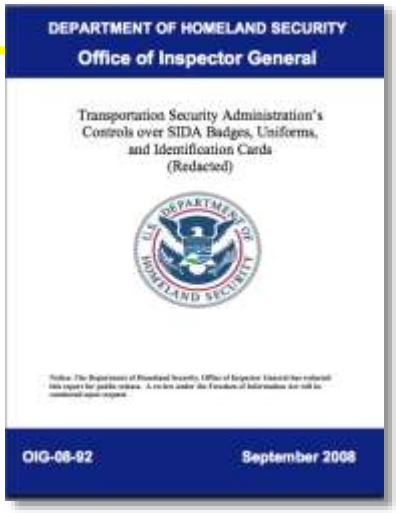
Algorithm ID	Algorithm - Modes	Reference	Key Size	Bits of Security	CAVP Cert. #
'00'	3 Key Triple DES – ECB	SP 800-78-2	192 bits	**112**	**698**
'01'	2 Key Triple DES – ECB	SP 800-78-2	128 bits	**80**	
'02'	2 Key Triple DES – CBC	SP 800-78-1[1]	128 bits	**80**	
'03'	3 Key Triple DES – ECB	SP 800-78-2	192 bits	**112**	
'04'	3 Key Triple DES – CBC	SP 800-78-1	192 bits	**112**	
'06'	RSA 1024 bit modulus	SP 800-78-2	1024 bits	**80**	**403**
'07'	RSA 2048 bit modulus	SP 800-78-2	2048 bits	**112**	
'08'	AES-128 – ECB	SP 800-78-2	128 bits	**128**	**840**
'09'	AES-128 – CBC	SP 800-78-1	128 bits	**128**	
'0A'	AES-192 – ECB	SP 800-78-2	192 bits	**192**	
'0B'	AES-192 – CBC	SP 800-78-1	192 bits	**192**	
'0C'	AES-256 – ECB	SP 800-78-2	256 bits	**256**	
'0D'	AES-256 – CBC	SP 800-78-1	256 bits	**256**	
'0E'	ECC: Curve P-224	SP 800-73[2]	NIST Curve P-224	**112**	**94**
'11'	ECC: Curve P-256	SP 800-78-2	NIST Curve P-256	**128**	
'14'	ECC: Curve P-384	SP 800-78-2	NIST Curve P-384	**192**	
N/A	RNG	FIPS 186-2	N/A	N/A	**480**
N/A	RSA Key Pair Generation	ANSI X9.31	1024 + 2048	N/A	**403**
N/A	ECC Key Pair Generation	FIPS 186-2	NIST Curves P224, P256, P384	N/A	**94**
N/A	SHS (SHA-1 only)	FIPS 180-3	N/A	N/A	**833**
N/A	Triple-DES MAC	Global Platform	128 bits	80	**698, vendor affirmed**
N/A	AES MAC	Global Platform	128 bits	128	**840, vendor affirmed**

Table 4: Supported Cryptographic Algorithm

Loss of **Static ID** Badges

5% rule – costly for airport!

- CrewPASS (53,000)
- SIDA (564,000)
- TSO (43,000 employees)
- air marshals (3000-4000)



- Prevent "Piggybacking" since expiration dates change each day / week / month on display

Dynamic ID Badges

3.

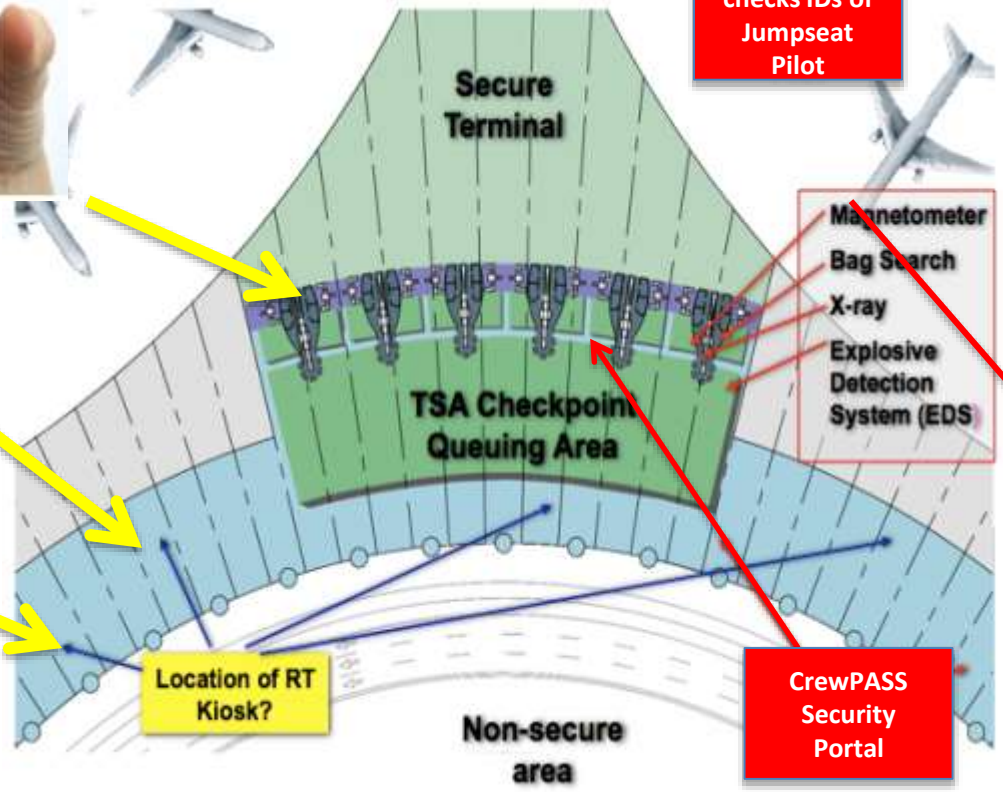
What about "Porous" Facilities like US Ports?

More fences, guards, check points, card readers, etc is not feasible or practical

Better Solution: A Card that can Display users Access period or Role Dynamically

3.

Air gap Examples – Registered Traveler & CrewPASS



- ✓ Airline ID card
- ✓ Medical certificate
- ✓ Pilot boarding pass

✓ The Display Card is a Dynamic Credential - providing "Visual evidence" to the TSA agent that the cardholder was pre-vetted, cryptographically, & biometrically authenticated at the kiosk on the insecure side of the airport.

✓ Maintains **chain of trust** between kiosk and TSA check point

3.

Network Integrators

- Encrypted Voice Application
- Speed, efficiency, convenient
- Secure Application Software
- Trusted Platform
- TPM / TMP
- Processor (with chip set extensions)

Secure, Low cost, scalable Solution

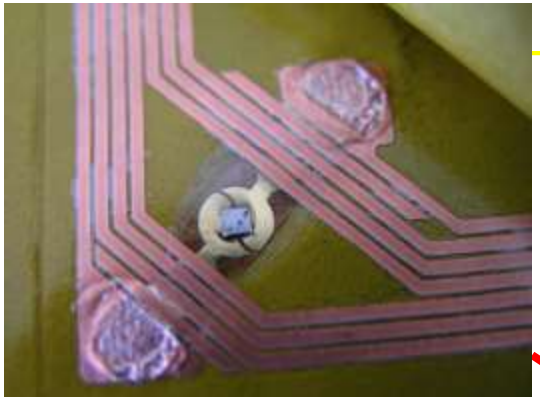
* Baseband Security (AJ - denial of service, relay attack proof)

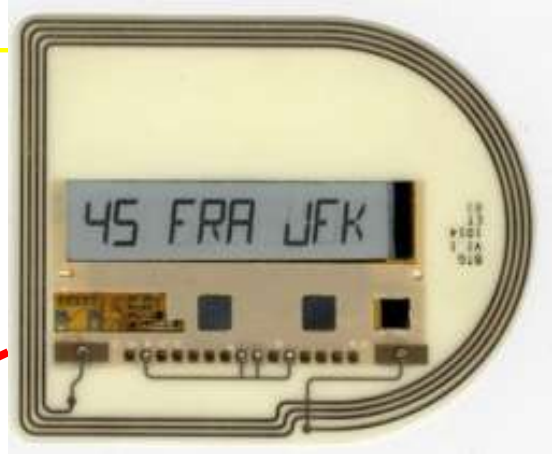
- Trusted display (status of security process and visual proof of auth process)
- Secure processor (with chip extensions)
- multi-factor authentication
- TMP (data at rest)
- OS support

Tocreo Labs

Inlay in Card

The Technology difference from a manufacturing perspective





Characteristics	RFID Inlay	Display Inlay	Failure Concern
Internal number of interconnects	**2**	**~520**	**Higher likelihood for interconnect failure**
Interconnect pad size	**20 mil sq.**	**.25 mil sq.**	**Larger pad provides more robust connection**
Inlay Thickness	15.7 mil	15.7 mil	Thicker is less robust mechanically
Substrate Material	PET / PVC	Polyimide / PET	Different expansion coefficients
Alignment accuracy required inlay to card window	3.1 mil	.4 mil	Auto placement tool accuracy
Max. manufacturing temp. of display	302 – 572 F 150 – 300 C	176 F 80 C	Excessive heat permanently damages plastic display
Max. manufacturing temp of inlay	302 – 572 F 150 – 300 C	176 F 80 C	Excessive heat permanently damages plastic display
Card operating temp.	-40 to +65 C -40 to +149 F	0 to +50 C 32 to +122 F	Slow display switching speed
Max. Mechanical stress	n/a	?	Damages electrical connection between IC's & PCB
Number of integrated Circuits (IC)	**1**	**3**	**Higher failure rate from mechanical & temp stress**
IC attachment process	Heat bar tab bonding	Flip chip / wirebond / additive deposition	Higher failure rate from mechanical & temp stress

Products

Technology

Unlock Cared for Mobile Device

Transit Card

Reusable luggage tag

Retail loyalty card

ID Access card
CAC / TWIC / PIV-201

E-battery label

Boarding pass

Medical Label

Mobile phone payment card

Stored Value card

Thin flexible display

No-battery circuit

Robust thin PCB

Thin IC packaging

Bi-state integrated display

Warm card encapsulation process

Unmatched security processor

The near "Perfect Storm"

Low Cost card

Multi-line display / active matrix

Card Switch to enable RFID antenna

Complete & Broad market acceptance

Summary

- We've developed an elegantly simple technology:
  - **On-card display – Extraordinary Security - Chain-of-Trust – batteryless**
- Applications
  - **Physical & Logical Access Control, Remote log-in, & Mobile Device Unlock**
- Huge Market
  - **need strategic partners for system integration in Aviation, Transit, National & Commercial network systems**

Questions?
Comments?