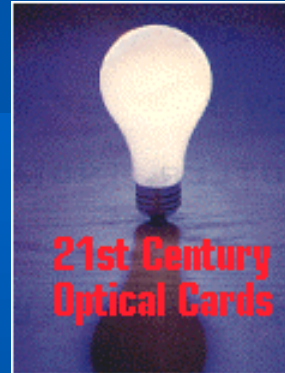


# BSI2000, Inc.



## *Securing Borders and Airports with Optical Cards*

CardTech/SecurTech 2003 – My 14, 2003

By Jack Harper, BSI2000, Inc.

12600 West Colfax Avenue, Suite B.410 Lakewood, Colorado 80215 USA

303.231.9095 303.231.9002 (fax)

[www.bsi2000.com](http://www.bsi2000.com)

[jharper@bsi2000.com](mailto:jharper@bsi2000.com)

# What are *Optical Cards*?...

**Card that you carry in your  
*Wallet or Purse***



**Same Size and Shape as *Credit Card***

**Holds Four Megabytes of Digital Data –  
that's *1,500 Typewritten Pages***

**~20-Million in Use in N.A. by 2004.**

# Border Projects Today.

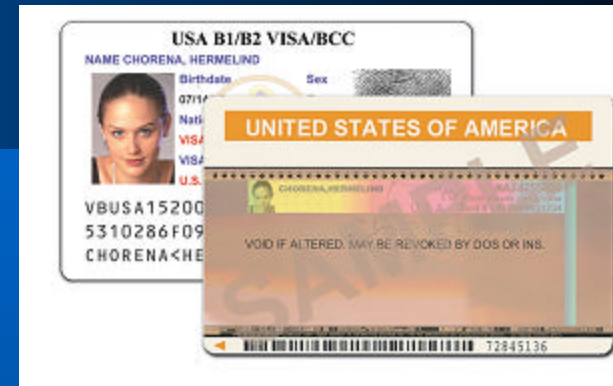
USA/INS – *Green Card (PRC)*

USA/INS – *Border Crossing*

*Italian National ID Card*

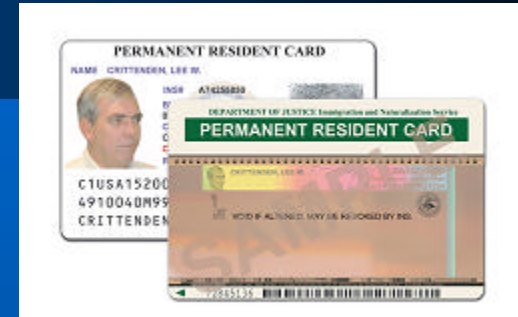
*Canadian PRC – Maple Leaf*

*Saudi Arabian National ID*



# Why Optical Cards?

~1000x the Memory of Smart Card



*Permanent Memory* – No Problems with Static

*Highly Reliable* – 10 Yr Life in Harsh Env.

**Strong Identification** – *Multiple Biometrics*

*Off-Line Capability* -- Works ANYWHERE

**Complete Audit Trail on Card** – 1000s of Transactions

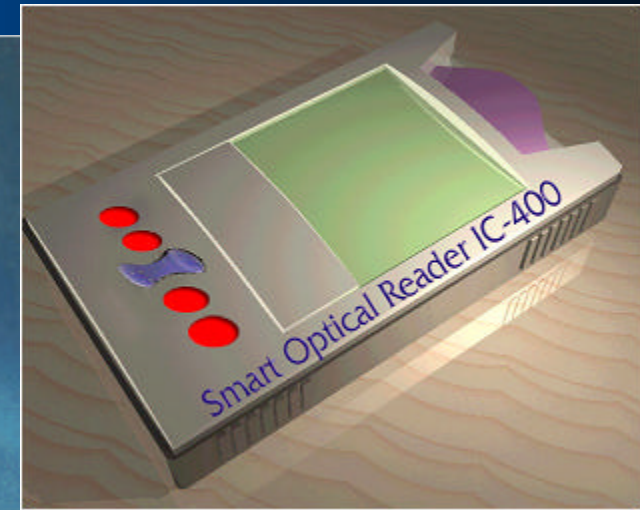
# Border Control System

**Carta d'Identita**

Nome: GIUBLE, VANESSA  
Comune che emette il documento: ROMA  
Comune di nascita: MILANO  
Data di nascita: 04/19/09  
Sesso: F  
Estremi alto: 12345  
Statura (cm): 175  
Comune di residenza: ROMA  
Indirizzo: P.ZZA GIUSEPPE VERDI 10  
Data emissione documento: 25.02.10  
Data scadenza documento: 25.02.10  
Codice fiscale: R2SMROS2R10H501Z

*Vanessa Giuble*

Stampare Ok



Card Production Systems – *Information Spectrum, Inc.*

Integrated Card Terminals – *BSI2000, Inc.*

Hand Held Readers – *LaserCard Systems Corp.*



# *Data Security* – Optical Cards

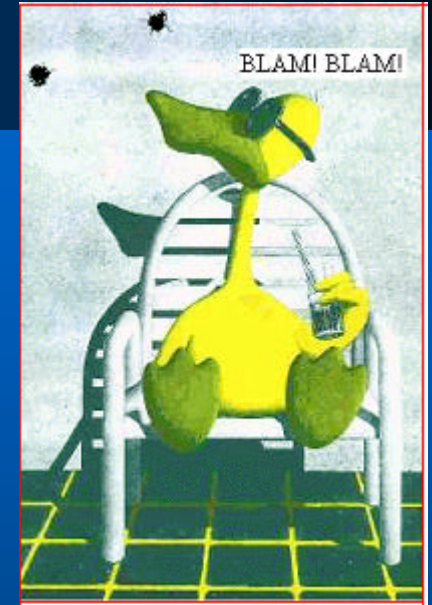
Where Do you Keep the Secret Key????

Past Solutions – Keep it *in the Software...*

Past Solutions -- *...in the Microcode...*

Past Solutions -- *...Use a Home-Grown Keyless  
Crypto...*

*..Obfuscate the Key...*



**All are BAD!**

# *New Approach Needed!*

Cryptographically Secure!

**Credibly Secure!**

*Tough Nut (Keys!) Certified to  
FIPS 140-1 (1, 2, 3).*

**Enable Standard *Public Key Crypto.***

**Resistant to *Rubber Hose* Cryptanalysis.**

**Prevent Cloned Cards, Records, Fraud, etc.....**

**Affordable!**



# Secure Optical Card Protocol - SOCP

Combination of...

...Standard Optical Card *Terminal Device*

...Special *Crypto Hardware* (Upgrade)

...Standard *Crypto Software*

...the *SOCP Crypto Protocol*.



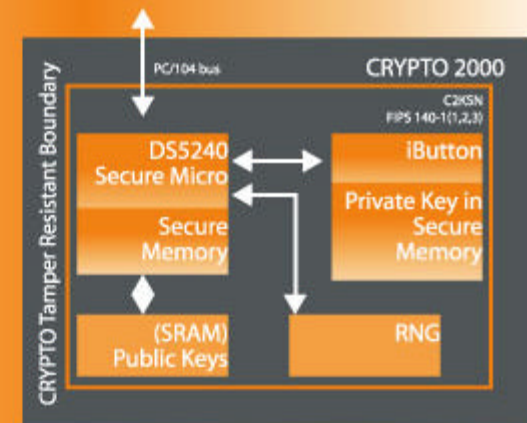


# Crypto 2000™



- Keys are protected to FIPS 140-1 (1,2,3)
- Key Management Device
- Hardware Random Number Generator

## CRYPTO 2000



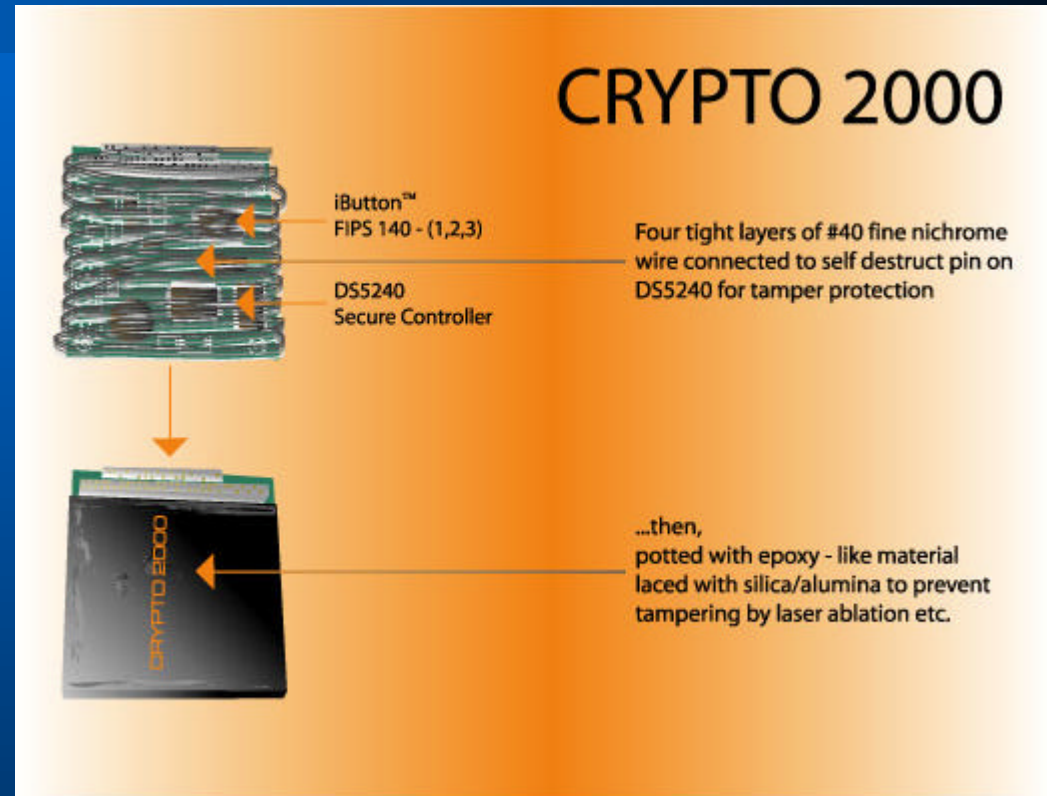
**Secure Key Repository**

**Secure Key Management**

**Cryptographically Secure RNG**

**Simple Plug-In Module**

# Tamper Resistance



*In-Box Tamper Sensor*

*On-Chip Tamper Sensor*

*Temperature Attack Sensor*

*...Attack Causes Zeroization of Battery Backed Up SRAM.*



# Crypto Write Sequence

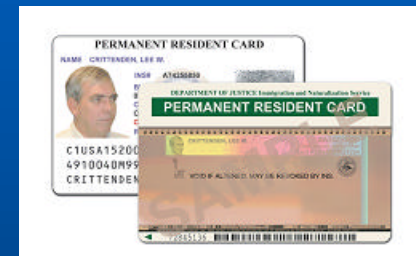
$C2KSN, r, k \in \text{Crypto 2000}.$

$C2KSN, E_{C2K}(r, r? (DTS, CSN), k) \in \text{Optical Card}.$

$E_{C2K}(H(m)) \in \text{Optical Card}.$

$\text{Crypto 2000} \in c_0 \in \text{Optical Card}.$

$c_i = E_k(m_i? c_{i-1})$  (for  $i = 1, 2, \dots$ )  $\in \text{Optical Card}.$



Therefore, the complete secure record for the plaintext  $m$  is written to the optical card as:

$C2KSN, E_{C2K}(r, r? (DTS, CSN), k), E_{C2K}(H(m)), c_0, E_k(m_i? c_{i-1})$  (for  $i = 1, 2, \dots$ )

# Crypto Read Sequence



The complete secure record read sequence to recover the plaintext  $m$  is:

$C2KSN, E_{C2KSN}(r, r? (DTS, CSN), k) \not\Leftarrow$  Optical Card.

$C2KSN, E_{C2KSN}(r, r? (DTS, CSN), k) \not\Leftarrow$  Crypto 2000.

$r, r? (DTS, CSN), k \not\Leftarrow$  Crypto 2000.

$DTS, CSN = r? (r? (DTS, CSN))$

$E_{C2KSN}(H(m)) \not\Leftarrow$  Optical Card.

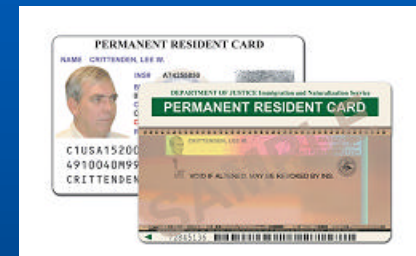
$C2KSN, E_{C2KSN}(H(m)) \not\Leftarrow$  Crypto 2000.

$H(m) \not\Leftarrow$  Crypto 2000.

$c_0 \not\Leftarrow$  Optical Card.

$c_i = m_i = c_{i-1} ? D_k(E_k(m_i))$  (for  $i = 1, 2, \dots$ )  $\not\Leftarrow$  Optical Card.

$H(m) == H?(m)?$  (Signature OK?).



# Conclusions

It is now possible to build *Cryptographically Secure Optical Card Systems*.

Security with **Crypto 2000/SOCP** is *Better than that provided by Smart Cards*.

The Secure Repository that protects keys is *Certified to Federal NIST FIPS 140-1 (Levels 1, 2, 3)*.

Designed to *protect new card systems* and to also *elevate the security of older legacy systems* to **FIPS 140-1 (1, 2, 3)**.



Please see the paper *Cryptographically Secure Transactions with Optical Cards* for details.

*See Crypto 2000 at the BSI2000 Booth.*

[www.bsi2000.com](http://www.bsi2000.com)

*jharper@bsi2000.com*