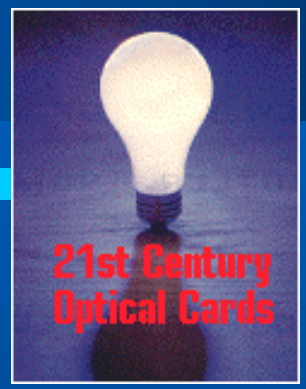
BSI2000, Inc.

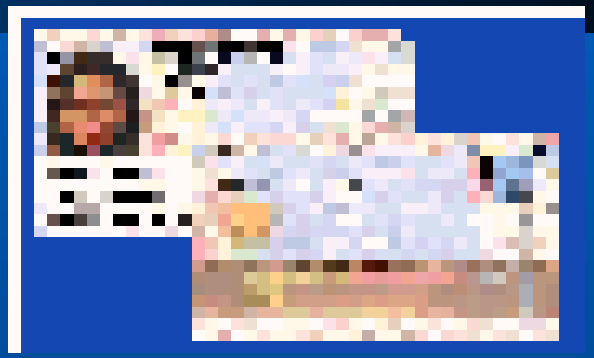


Trusted Optical Cards

Workshop on Storage and Processor Card-Based Technologies
National Institute of Standards and Technology (NIST) Gaithersburg, Maryland
Wednesday, July 9, 2002

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
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.**

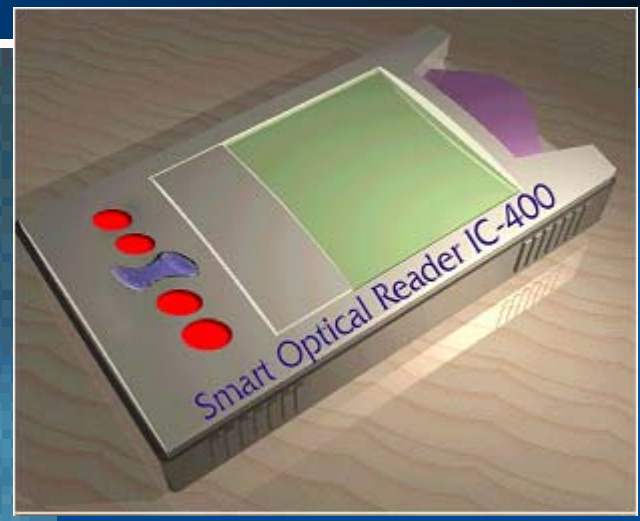
Border Projects Today.

- **USA/INS – *Green Card* (PRC)**
- **USA/INS – *Border Crossing***
- **Italian *National ID Card***
- **Canadian PRC – *Maple Leaf***
- **Saudi Arabian *National ID***

Why Optical Cards?

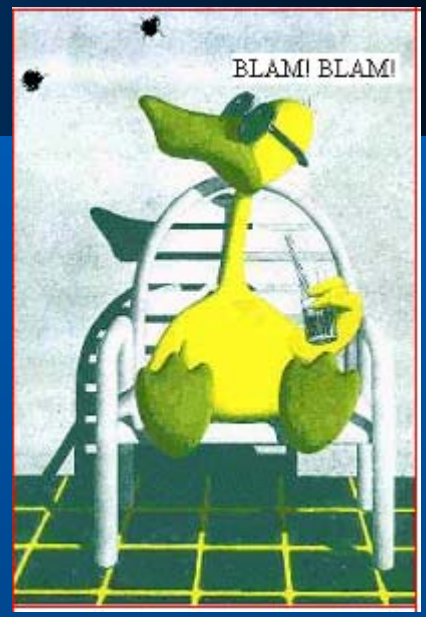
- ~1000x the Memory of Smart Card
- *Permanent Memory* – No Problems with Static
- *Highly Reliable* – 10 Yr Life in Harsh Env.
- Strong Identification – *Multiple Biometrics*
- *Off-Line Capability* -- Works ANYWHERE
- Complete *Audit Trail* on Card – 1000s of Transactions

Border Control System



- **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!

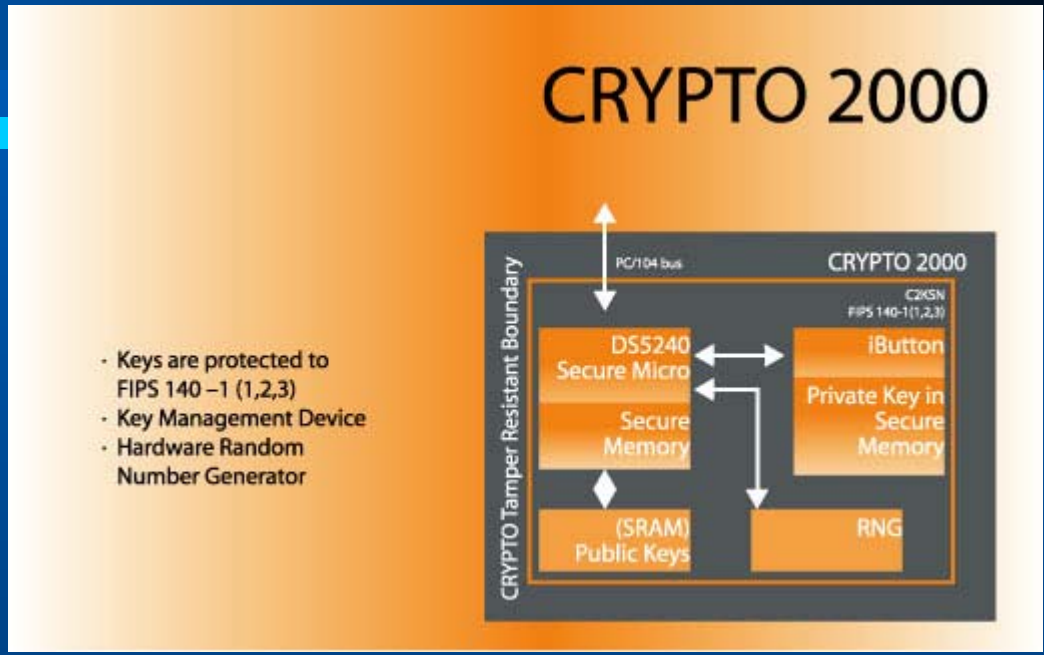
New Approach Needed!

- **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

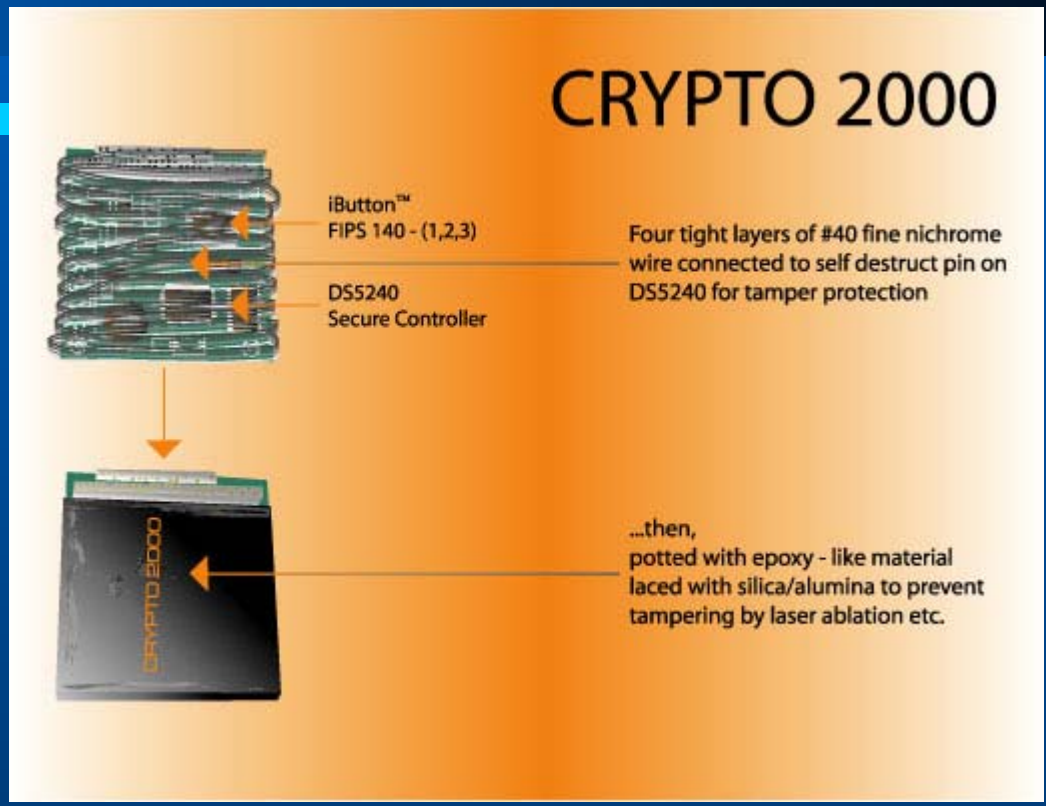
- **Combination of…**
- **…Standard Optical Card *Terminal Device***
- **…Special *Crypto Hardware* (Upgrade)**
- **…Standard *Crypto Software***
- **…the *SOCP Crypto Protocol.***

Crypto 2000™



- **Secure *Key Repository***
- **Secure *Key Management***
- **Cryptographically Secure *RNG***
- **Simple Plug-In Module**

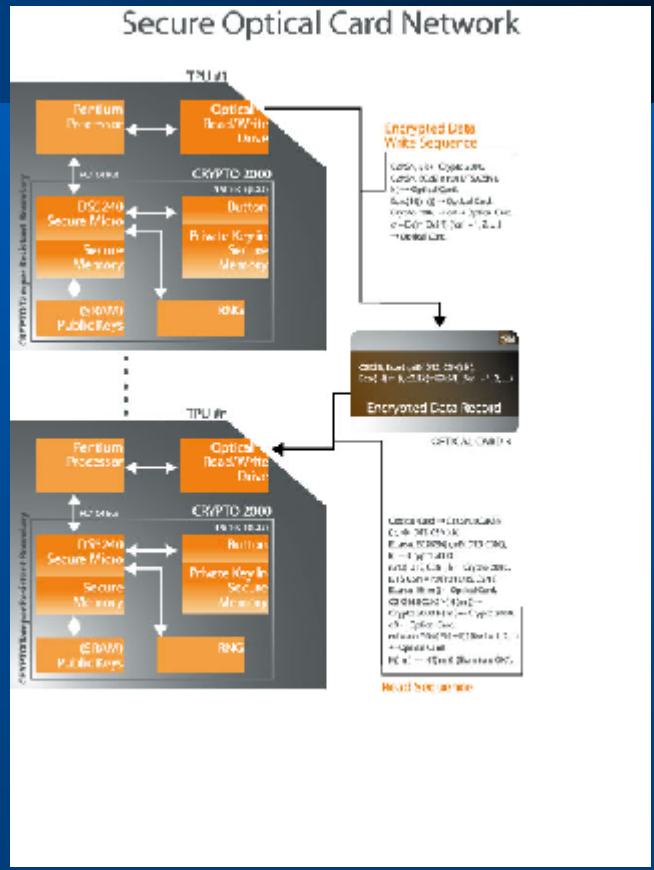
Tamper Resistance



- ***In-Box*** **Tamper Sensor**
- ***On-Chip*** **Tamper Sensor**
- ***Temperature Attack*** **Sensor**
- **…Attack Causes *Zeroization* of Battery Backed Up *SRAM*.**

Secure Optical Cards

- …any Number of Terminals
- …any Number of Cards…
- Record written to Card may only be Read by a Terminal in the Network.



Crypto Write Sequence

C2KSN, r, k ← Crypto 2000.

C2KSN, E_{C2K}(r, r ⊕(DTS, CSN), k) → Optical Card.

E_{C2K}(H(m)) → Optical Card.

Crypto 2000 → c_0 → Optical Card.

$c_i = E_k(m_i \oplus c_{i-1})$ (for i = 1, 2, …) → 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, $E_k(m_i \oplus c_{i-1})$ (for i = 1, 2, …)

Crypto Read Sequence

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

C2KSN, E_{C2KSN}(r, r⊕(DTS, CSN), k) ← Optical Card.

C2KSN, E_{C2KSN}(r, r⊕(DTS, CSN), k) → Crypto 2000.

r, r⊕(DTS, CSN), k ← Crypto 2000.

DTS, CSN = r⊕(r⊕(DTS, CSN))

E_{C2KSN}(H(m)) ← Optical Card.

C2KSN, E_{C2KSN}(H(m)) → Crypto 2000.

H(m) ← Crypto 2000.

c_0 ← Optical Card.

$c_i = m_i = c_{i-1} ⊕ D_k(E_k(m_i))$ (for i = 1, 2, …) ← Optical Card.

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

See "***Cryptographically Secure Transactions with Optical Cards***"

http://www.bsi2000.com/downloads.htm

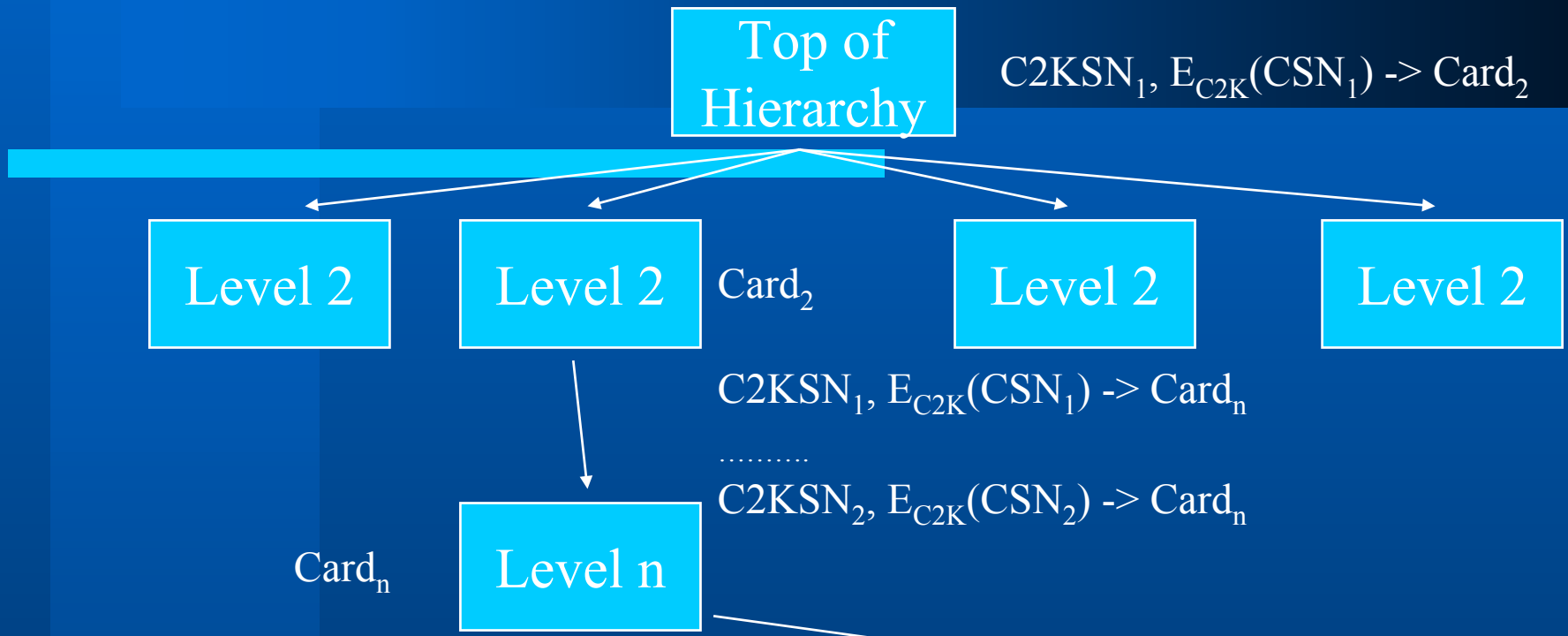
Trust Model…

Crypto 2000 provides Data Security…

…which is NOT Trust.

Trust: *"Firm reliance on the integrity, ability, or character of a person or thing."* – Random House College Dictionary.

Trust Model…



CARD is Trusted for this Specific Operation if the CSNk's can be Recovered through the Entire Chain.

Each Component of the Trust Chain Record was Written on the Specific Machines (specific Crypto 2000s).

www.bsi2000.com

jharper@bsi2000.com