

# CardLogix



*Empower Your Vision*

# Points of Discussion

- Company Overview
- Security Mechanism Basics
- General Strategies
- Transparency
- Chains of Trust
- Hardware Barriers
- Card & System Architectures
- PKI & Signing



# CardLogix Corporate Overview

---

- Founded in 1994
- Manufacturing Started 1998
- ISO 9001/2000 UL Certified Quality Manufacturing Facility
- 500 + customers in 33 countries
- Security By Design Methodologies
- Multiple patents granted and pending in hardware and software design
- Privately Held



# Security Mechanism Basics

## *The Elements Of Data Security*

Hardware, including servers, redundant mass storage devices, communication channels and lines, hardware tokens (smart cards) and remotely located devices (e.g., thin clients or Internet appliances) serving as interfaces between users and computers

Software, including operating systems, database management systems, communication and security application programs

Data, including databases containing customer - related information.

Personnel, to act as originators and/or users of the data; professional personnel, clerical staff, administrative personnel, and computer staff



# Security Mechanism Basics

- Confidentiality/Cryptography
- Data Integrity
- Authentication
- Non-Repudiation
- Authorization and Delegation
- Auditing and Logging
- Management



# Confidentiality/Cryptography

- Confidentiality is the use of encryption to protect information from unauthorized disclosure. Plain text is turned into cipher text via an algorithm, then decrypted back into plain text using the same method.
- Cryptography is the method of converting data from a human readable form to a modified form, and then back to its original readable form, to make unauthorized access difficult.



## Cryptography Uses:

- Ensure data privacy, by encrypting data
- Ensures data integrity, by recognizing if data has been manipulated in an unauthorized way
- Ensures data uniqueness by checking that data is "original", and not a "copy" of the "original". The sender attaches a unique identifier to the "original" data. This unique identifier is then checked by the receiver of the data.



# Data Integrity

- *Has my data arrived intact?*

This mechanism ensures that data was not lost, corrupted or manipulated in an unauthorized way when it was sent to the recipient

***This is the function that verifies the characteristics of a document and a transaction. Characteristics of both are inspected and confirmed for content and correct authorization. Data Integrity is achieved with digital signature cryptography that assigns a unique identity to data like a fingerprint. Any attempt to change this identity signals the change and flags any tampering.***

# Authentication

- *Is the data or device expected and does it come from an approved source?*

Proves user or system identities

This inspects, then confirms, the proper identity of people involved in a transaction of data or value. In authentication systems, authenticity is measured by assessing the mechanisms' strength and how many factors are used to confirm the identity. In a PKI system, a Digital Signature verifies data at its origin by producing an identity that can be mutually verified by all parties involved in the transaction. A cryptographic hash algorithm produces a Digital Signature.

# Non-Repudiation

- Can I confirm the sender and the receiver of a message did in fact send and receive the message.

**Incorporating a Digital Signature allows a third party to verify a transaction took place, eliminating the possibility of that transaction being repudiated, or invalidated. Both parties digitally sign the message with their private keys, providing a path to verify that both parties took part in the transaction. This is much like notarizing a contract. The notary verifies the identity of the parties, then two parties sign a document, which is then certified by the notary.**



# Authorization & Delegation

- Authorization is the processes of allowing access to specific data within a system
- Delegation is the utilization of a third party to manage and certify each of the users of your system. (Certificate Authorities)



# Auditing and Logging

- *Can I Keep This Data Private?*
- Ensures only senders and receivers access the data. This is typically done by employing one or more encryption techniques to secure your data



# Management

Is the oversight and design of the elements and mechanisms discussed. System and card management also requires the management of issuance, replacement and retirement as well as policies that govern a systems deployment.



# Hacking Motivations

## Reasons...

- Competitively backed
- Anger
- Geo/political causes
- Money, money, money
- Glory-underground recognition
- Technical challenge –Your system is a target
- Random...
- Automated scans
- Worms using “trace-route” or “pings”



# Typical Hacking Tools

- Port Discovery (NMap)
- Footprint Tools (Network Solutions, Netcraft)
- Password Discovery (LC4, John the Ripper)
- Vulnerability Assessment Scan (Saint, Satan, Nessus)
- Obtaining Access (Using Discovered Vulnerabilities)
- Maintaining Access (Rootkits)
- Concealing Access (Log cleaners)

*All available on the internet*



# General Strategies for Deployment

## *1<sup>st</sup> steps*

- Understand the current vulnerabilities
- Plug existing holes
- Make Obvious Physical & Policy improvements

## *2<sup>nd</sup> Phase*

- Build in hardware speed bumps
- Design and implement a *Hardened System* with next generation security mechanisms (i.e. NSA Suite B algorithms)
- Third Party Certification, i.e. Infoguard
- Implement Management Security Policies



# Understand the Current Vulnerabilities

## *Research Possible Exploits*

- **Hackers Use Vulnerability Scanners**
- **Discover software configuration errors**
  - No user password, incorrect system permissions, passwords passed in the clear, mail relay, etc.
- **Find outdated software components**
  - Operating system components (FTP, Telnet, SSH, HTTPS, PHP, Windows components, etc.)
- **Identify general security issues**
  - Use of encryption, proper passwords, etc.



# Understand the Current Vulnerabilities

*Vulnerability scanners and private third parties can:*

- Warn when a known exploit is found
- Rank each exploit for severity
- Provide repair suggestions or instructions



# Plug Existing Holes

## *Port Scan --- Ports talk too much*

- Every computer has 65,535 TCP and 65,535 UDP ports
- Also PC cards, smart cards, keyboards and USB possibilities
- All modem services must communicate through open ports
- Port scanners are fast and thorough
  - They work against servers “protected” by the best firewalls
  - Can find software weaknesses
- Weak Port -> Software insertion-> BUGS = Exploits



# Make Obvious Physical & Policy Improvements

*Prevent Compromises through Technologies & Policies*

- **Technologies**
  - Firewalls
  - Vulnerability Assessment
  - Intrusion Detection & Prevention
  - Data Encryption, etc.
- **Policies**
  - Physical Access
  - Passwords
  - Logging/Tracking of systems and components
  - 3<sup>rd</sup> party Security Validation, etc.



# Transparency

- “Glass Box” Development
- No Security Through Obscurity
- Security Processes Documented and Verifiable
- Use of Industry approved algorithms
- Top tier 3<sup>rd</sup> Party Validation
- Easy to Follow Processes
- Secure key storage policies



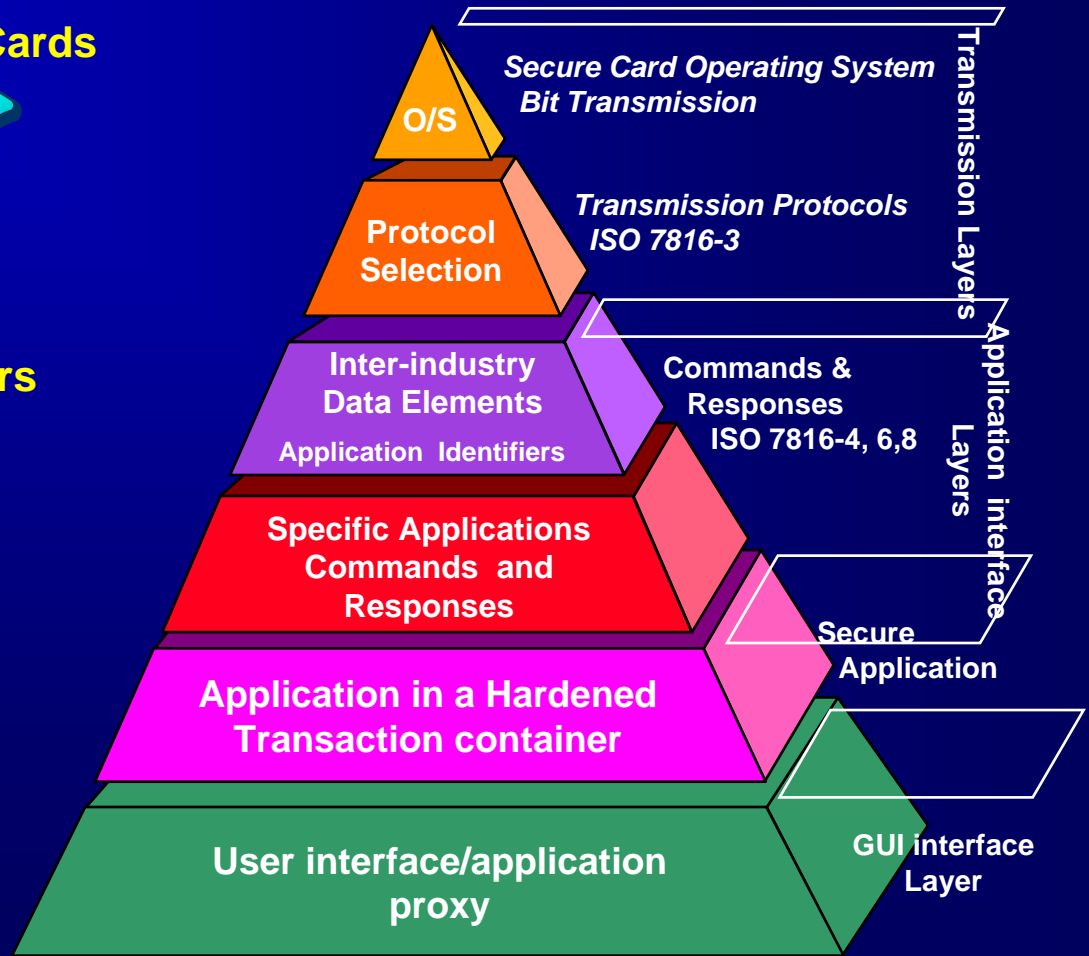
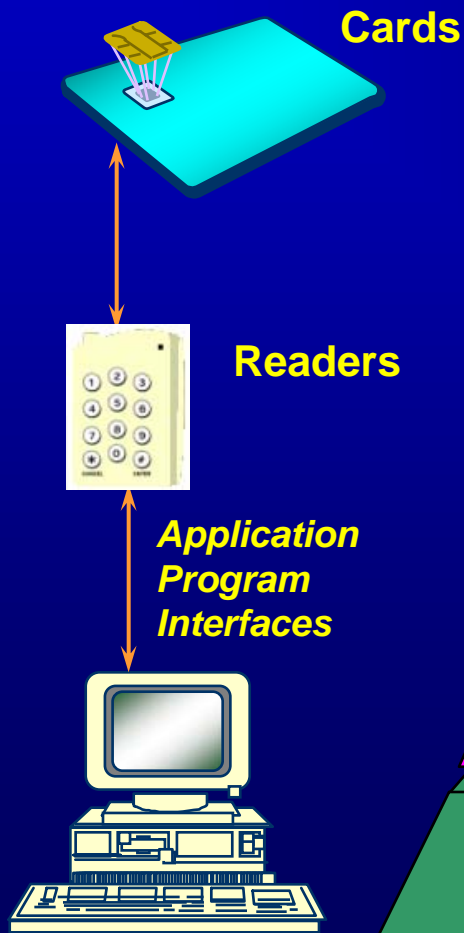
# Hardware Barriers / Speed Bumps

*Castle/Onion layered architecture approach*

- Custom locks to servers
- Custom holographic tamper evident seals - kept under tight control
- Specialty I/O connectors i.e. cell phones
  - Or rewired pinouts on standard connectors
- Invert data streams
- Buried and scrambled busses on PCBs
- Remark component P/N to subvert all IC logic on PCBs



# System Hierarchies



# Design of a Hardened System

- Establish a chain of trust for applications and transactions
- Security Application vs. Graphical User Interfaces
- The Security Interface Remains Constant
  - Can be Open Source
- Graphical User Interface
  - Changes Often
  - May not be fully Open Source



# Design of a Hardened System

- Abstract the security application as a separate component into a separate embedded board
- Utilize trusted tamper proof silicon and keep your application and SAM's resident within the embedded environment
  - Not Susceptible to Security Holes in GUI, i.e. Microsoft Windows
  - Open Source Potential
  - Can easily Support multiple Operating Systems, i.e. Linux, Microsoft, BSD, etc.
  - Provides an Upgrade Path for new security and GUI Features as they become available

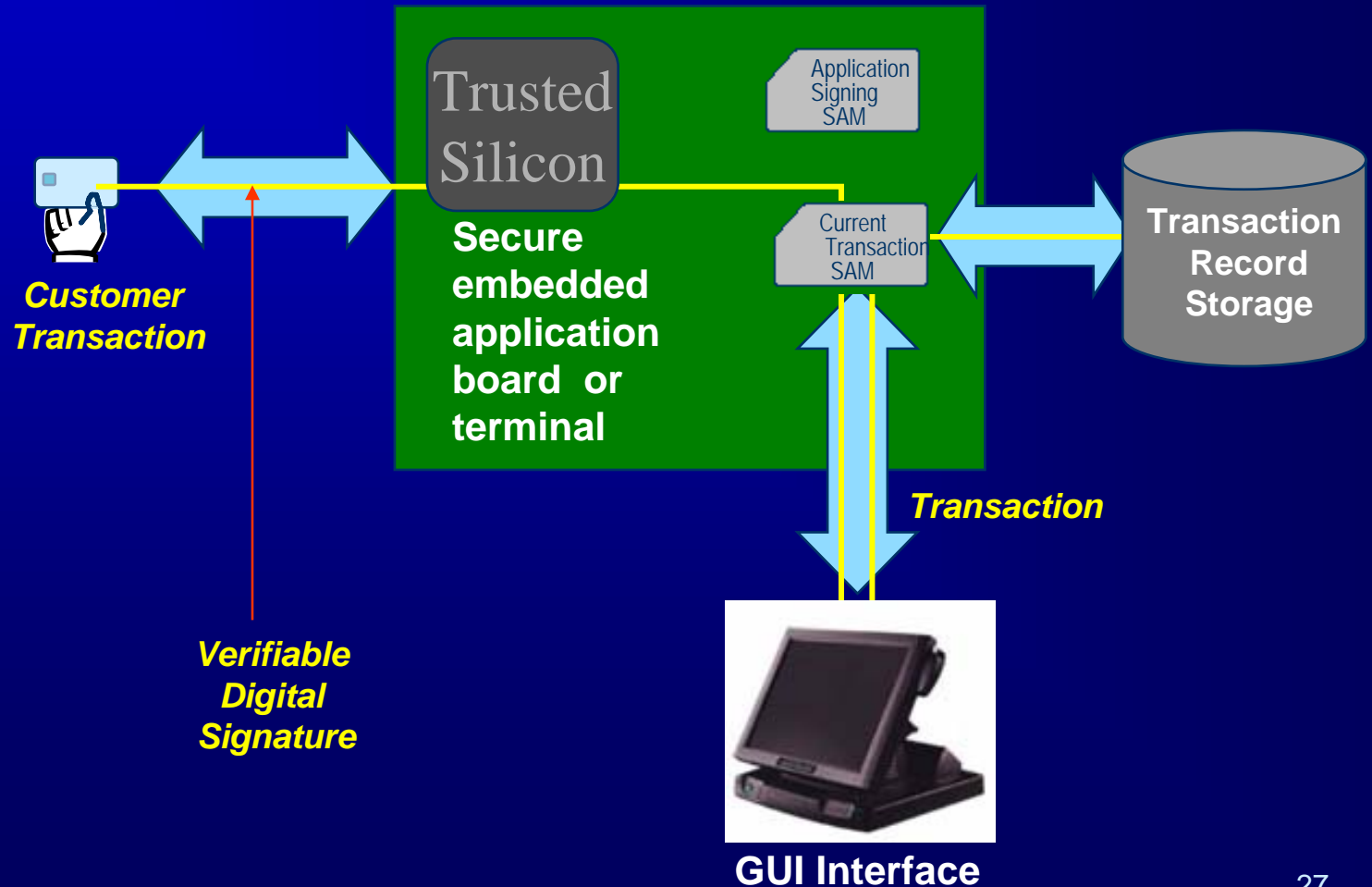


# Design of a Hardened System

- Build in tamper detection
- Incorporated hardware speed bumps
- Employ security mechanisms in concert
  - Confidentiality/Cryptography
  - Data Integrity
  - Authentication
  - Non-Repudiation
  - Authorization and Delegation
  - Auditing and Logging



# Suggestions for Design of a Hardened System

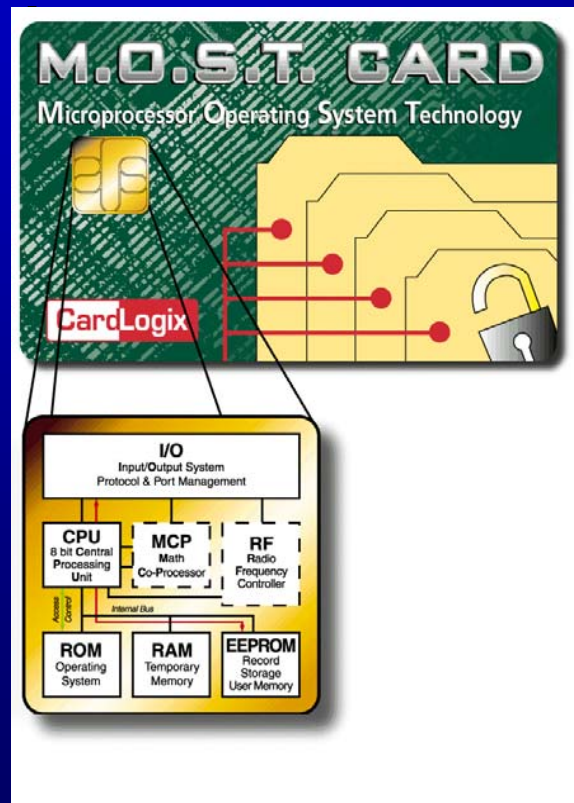


# What do We Add for Security

- Cards that can Encrypt, and Digitally Sign Transactions
- Cards that are almost impossible to replicate physically – high entry barrier
- A chain of trust regarding supply and data loading
- Controlled Silicon



# M.O.S.T. Cards

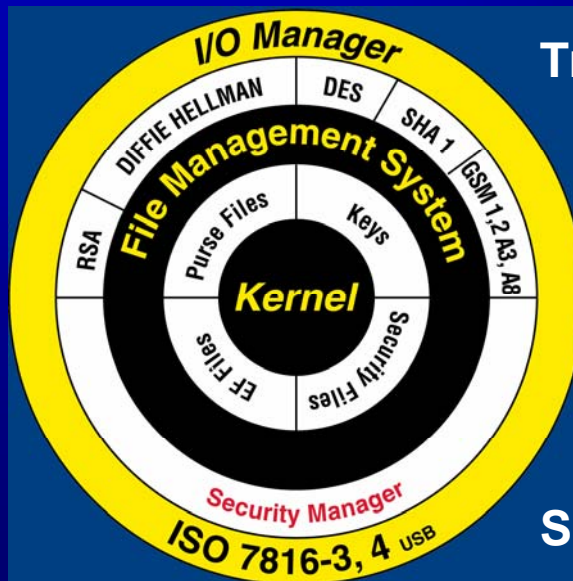


## Features:

- User Memory from .5k to 64k bytes
- Tamper Resistant Design
  - (DPA-DTA)
- IC Independent Operating System
- Contactless Extensions
  - (Mi-Fare-HID)
- Variety of Security Features

# CardLogix M.O.S.T. Architecture

## Microprocessor Operating System Technology



- Truly Multifunctional-Multiapplication
- High Performance Design
- Platform Independent
- Reconfigurable
- Robust File Management
- Tamper Resistant Design
- Supports, ISO, PC/SC, OpenCard



# CREDENTSYS Cards



- Full FIPS 201 and 140-2 Level 2 certified
- 2 Types to choose from:, Java Card and Multos
- Full support for NSA Suite B algorithms
  - DES, 3DES, SHA-256, AES and 2048 RSA
  - Full PKCS 11 support
  - Full CAPI support
  - Long file name support
  - 64K, & 144K user EEPROM
  - Admin and user modes
  - On card key generation
- System Level Middleware

# Security Printing & Card Bodies

- High Quality Composite PVC card Bodies (10 year life)
- Full Compliance with ISO 10583
- Optional Colored Interlayer
- Optically Variable Devices
- Guilloche and Microprinting
- Hologram and HoloMag-Stripes
- Laser Engraving



## Card Services

- Variable data imaging
- Embossing & Tipping
- Encoding: magnetic stripe and chips
- Affixing: labels, scratch-off panels
- Tamper evident packaging
- Certificate enrollment
- Tracking

### *Products in development*

- Mailing, distribution & intelligent insertion



# Integrated Card Production



# Partner With CardLogix

- Our primary objectives are Service, Quality and Technology development
- Complete Platforms and Solution
- Lowest Cost Barriers to Entry
- Momentum
- Our Commitment to You

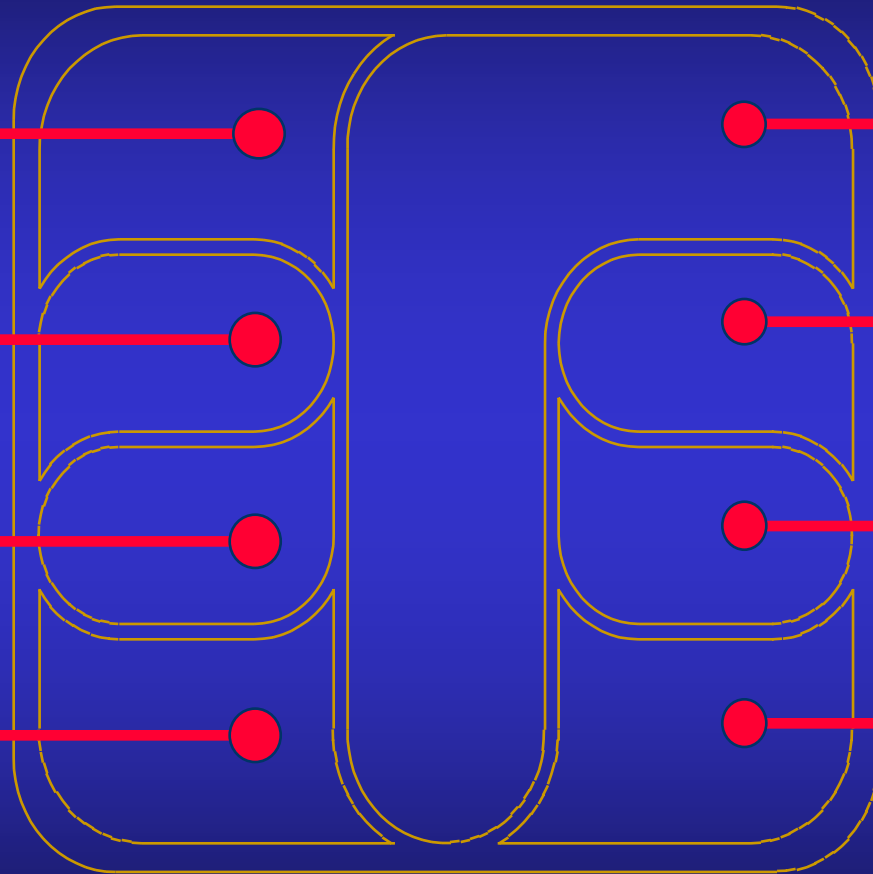


# CardLogix Is the Right Choice for Smart Cards

- Customer Centered Organization
- Deliberate Focus On Stable Software, Clear Documentation and Quality Card Manufacturing
- Response To Opportunities With Innovative Products
- Customer Response Is Fast And Flexible
- U.S. Based Manufacturing



**MAKE CONTACT WITH**



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



*Thank You*