



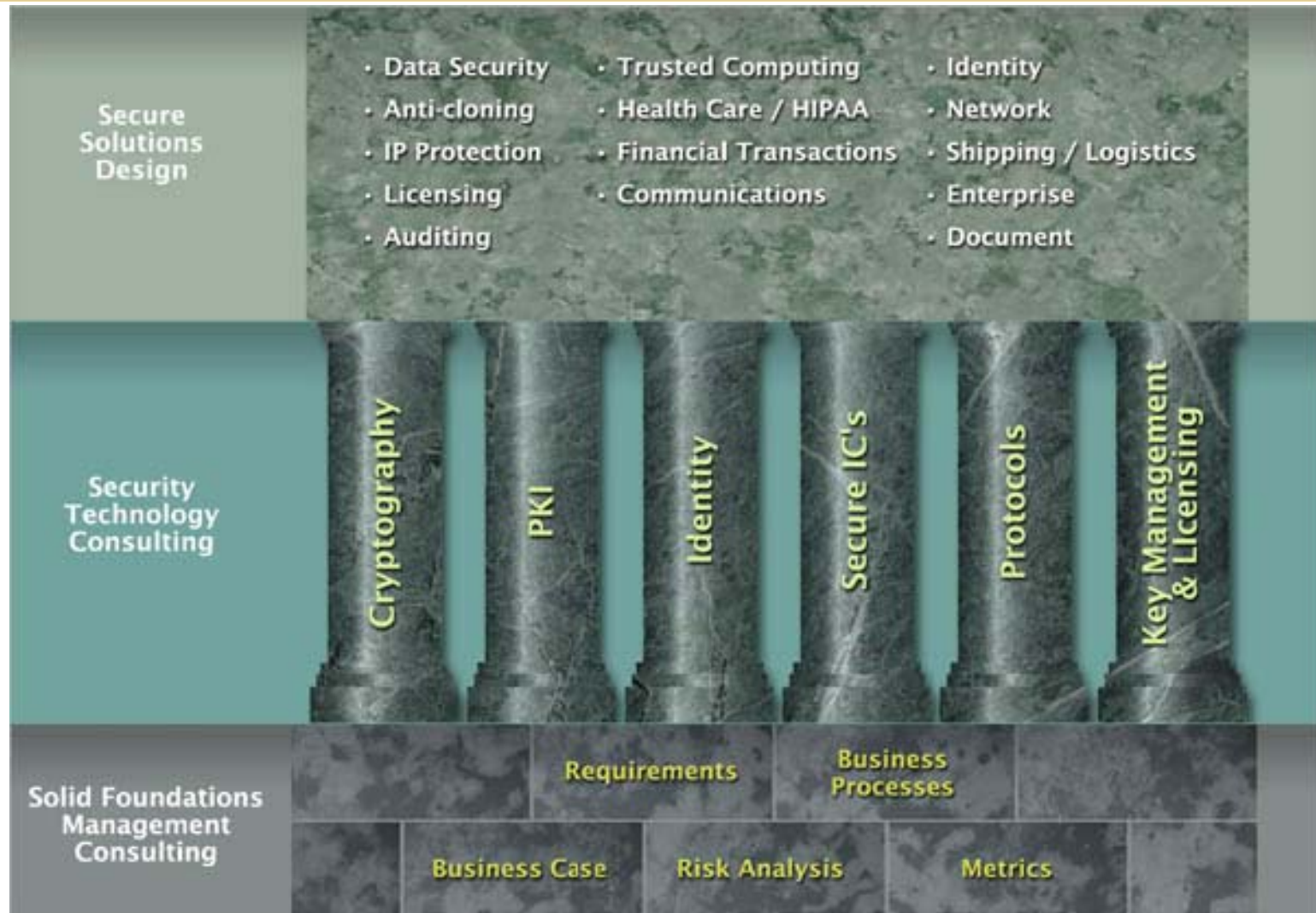
Best In Class Security Design, Management, And Solutions

GraniteKey™

Agenda

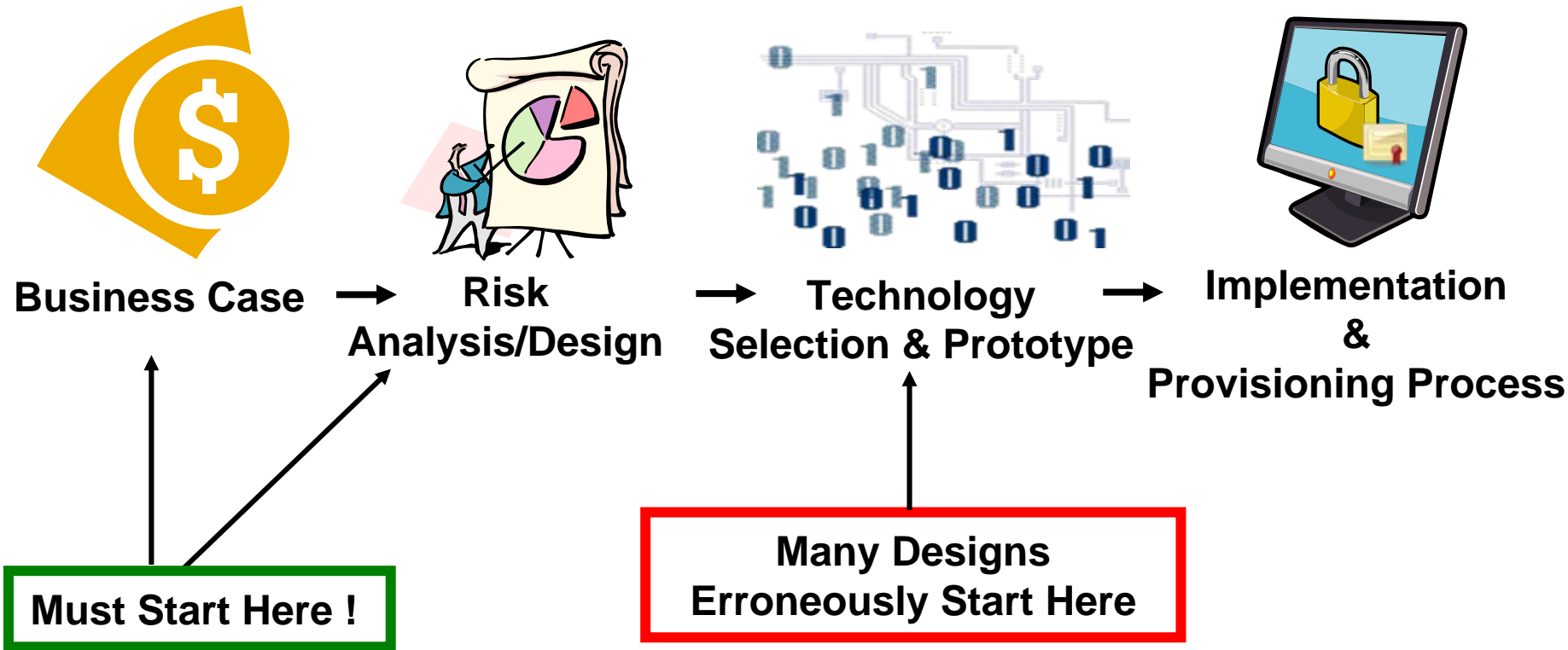
- **GraniteKey Services And Solutions**
 - Development Lifecycle
 - Cost/Benefit Analysis
 - Technology Considerations
 - Engineering/Implementation Services
- **The Security Framework**
 - Threat Modeling/Risk Analysis
 - Security Modules
 - Provisioning
- **Use Case Examples**

GraniteKey™ Services and Solutions



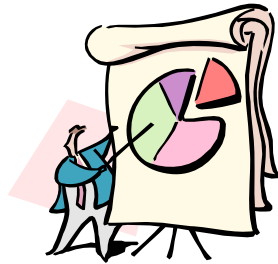
Security Development Lifecycle

GraniteKey Provides The End To End Solution



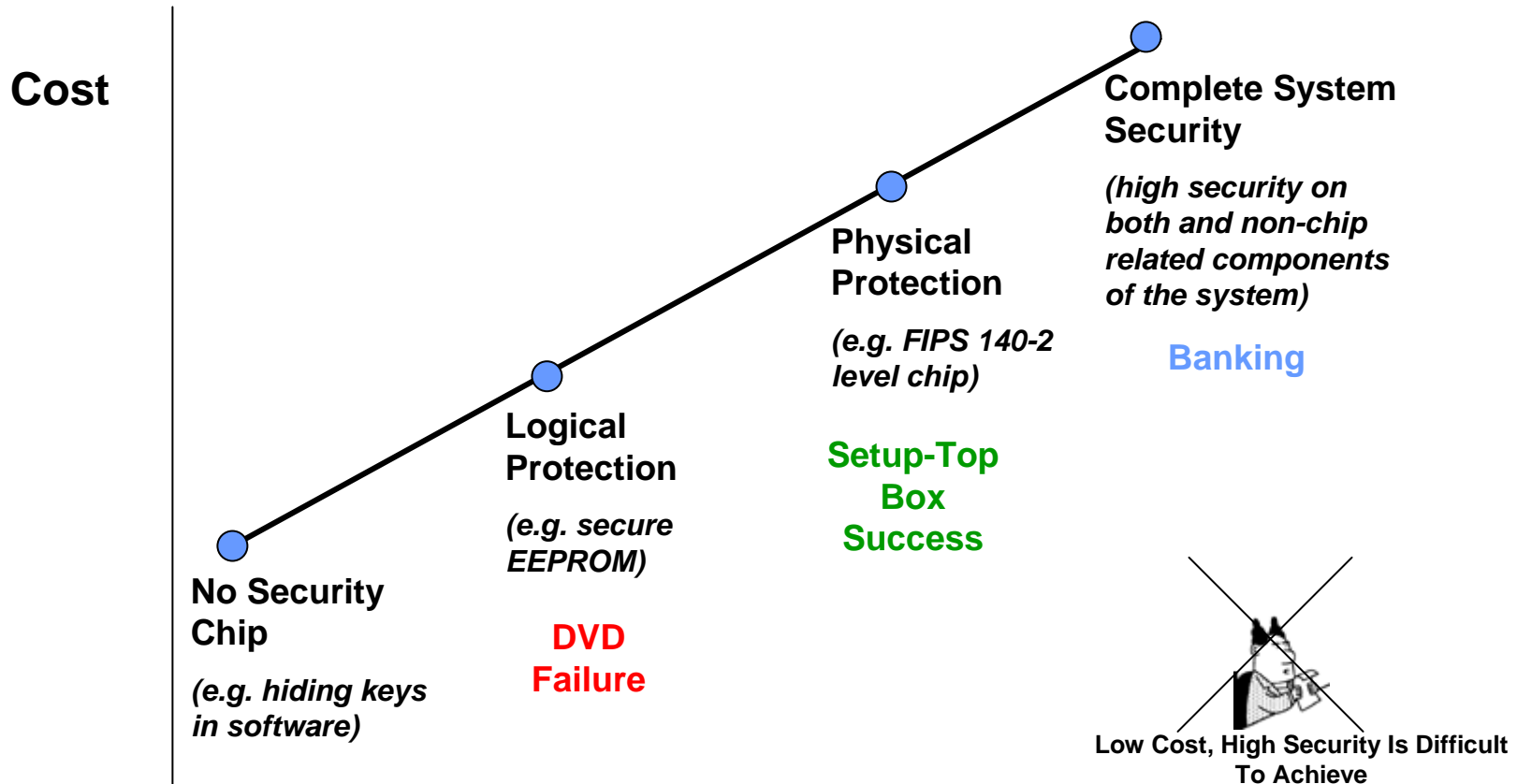
Regardless Of Where You Are In Your Development Lifecycle, GraniteKey Can Help You Succeed !

GraniteKey Security Design And Consulting



- **ROI-Based Approach To Delivering Security Solutions**
- **Holistic Assessment Of The Entire System**
- **Practical Implementation And Application of Secure Technologies**
- **Integration Of Security Lifecycle Management Tools**

Security Levels vs. Cost



Security Level →

- Addresses More Threats
- Lower Probability Of Failure
- Reduced Failure Size/Scope

Security Module Technology Choices

Why FIPS 140-2 ?

- **FIPS 140-2 Level Secure IC Solutions Moves Enforcement To The Hardware**
- **Failure To Authenticate Means Failure To Operate**
- **FIPS140-2 Level Secure IC's Are Extremely Secure Compared To Other Options**

Threats Addressed	Crypto Functionality	Examples	Security Level	Common Applications
Bus / Electrical Attacks	Symmetrical, Limited/Proprietary	Secure EE 1-Wire Solutions	LOW	Anti-cloning, Licensing
Bus / Electrical Attacks Physical Attacks (reads)	Symmetrical, Standard AES, 3DES, SHA1 Asymmetrical (Public Key), RSA, ECC	FIPS 140-2 Level Secure IC	HIGH	Anti-cloning, Licensing Identity, Private Networks (e.g.) Digital Content Protection, Licensing / License control Anti-Cloning, Anti-Fraud

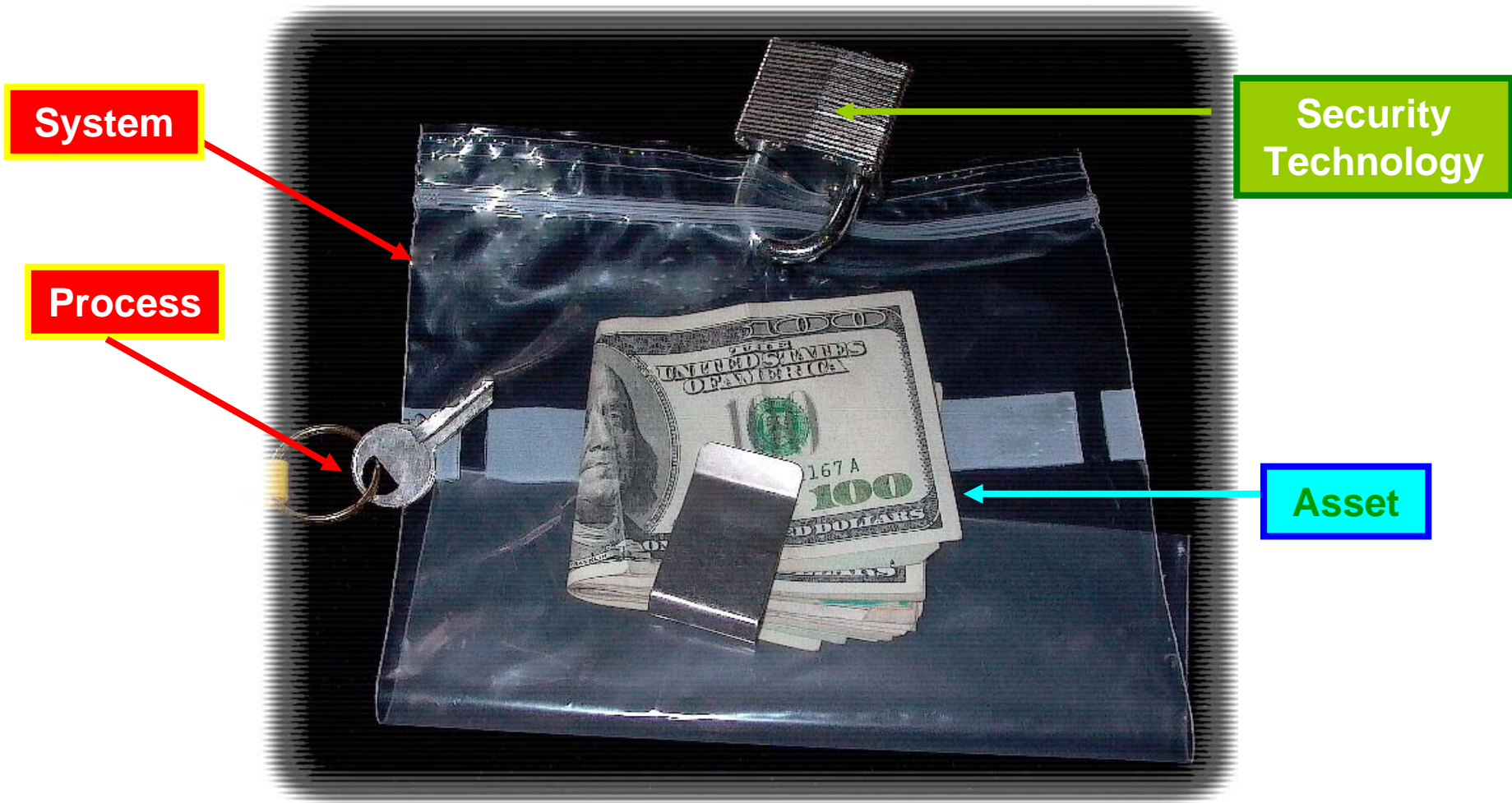
System and Business Process Considerations

Some Examples

- ◆ **E.G. Anti-Cloning Of Appliance Peripheral**
 - Host vs. Peripheral Economics
 - Technical issue: Asymmetrical vs. Symmetrical Encryption
- ◆ **E.G. Appliance vs. Auto Parts**
 - Appliance Is About **Revenue Assurance**
 - Auto Parts Is About **Ownership Of Liability** (Retail Chain vs. Distributor)
 - Either Case Could Be Reversed (Or Include Both)
- ◆ **E.G. Liability**
 - Is The appliance Vendor Liable (e.g. Health Problems Caused By Bad Water Filter)?
- ◆ **E.G. IP Protection**
 - Legal Environment, Scalable Hacks, Proliferation Of Free Versions, Payment Environment

Templates Can Be Utilized For Key Design Issues

The “Challenged” System Design



Despite The Presence Of A Strong “Lock” The System, As Designed, Is Still Quite Vulnerable

Security Objectives

What Are The Drivers?

Lower Security  Higher Security

**Compliance
Marketing Parity**

*Get Into The
Market*

*(e.g. Voting
Machine,
Biometrics)*

**Reduce/Divert
Liability**

*Put
Something
In Place*

**Revenue
Assurance**

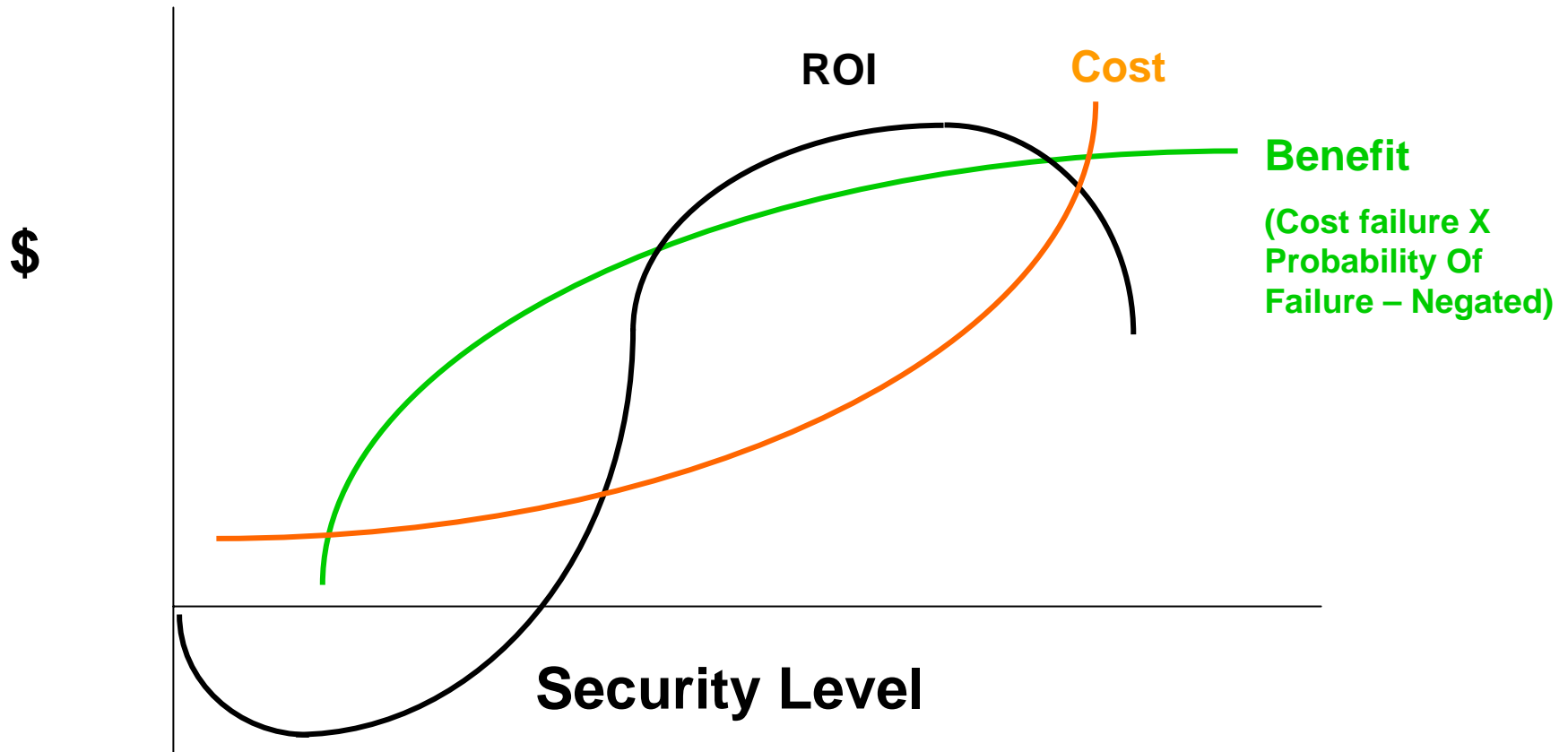
**Save
Costs/Losses**

*ROI Driven
Been Hacked
Enterprise Risk
Management
High Volume*

**Failure Not
An Option**

*Military
Medical*





ROI View Of Security



All Security Implementations Are Ultimately Cost Driven !

What We Do

Products And Services: The Security Framework

-  **GraniteView™:** Tool for Online Collaborative Risk Management and Threat Modeling, Business Decision Making, Business Case and ROI planning
-  **GraniteKey Professional Services:** Assist You With Risk Management, Business Process Design, Auditing/Legal Procedure Mitigation, System Design, Security Design, System and Security Technology Selection and Implementations
-  **GraniteLock™:** For Customers In Need Of Anti-Cloning, IP Protection and Usage Control For Their Products
-  **GraniteForge™:** Secure Provisioning Authority Purpose-Built For Issuing Keys/Certificates For Embedded Systems. Designed To Seamlessly Integrate With GraniteLock™.

Agenda

- **GraniteKey Services And Solutions**

- Development Lifecycle
- Cost/Benefit Analysis
- Technology Considerations
- Engineering/Implementation Services

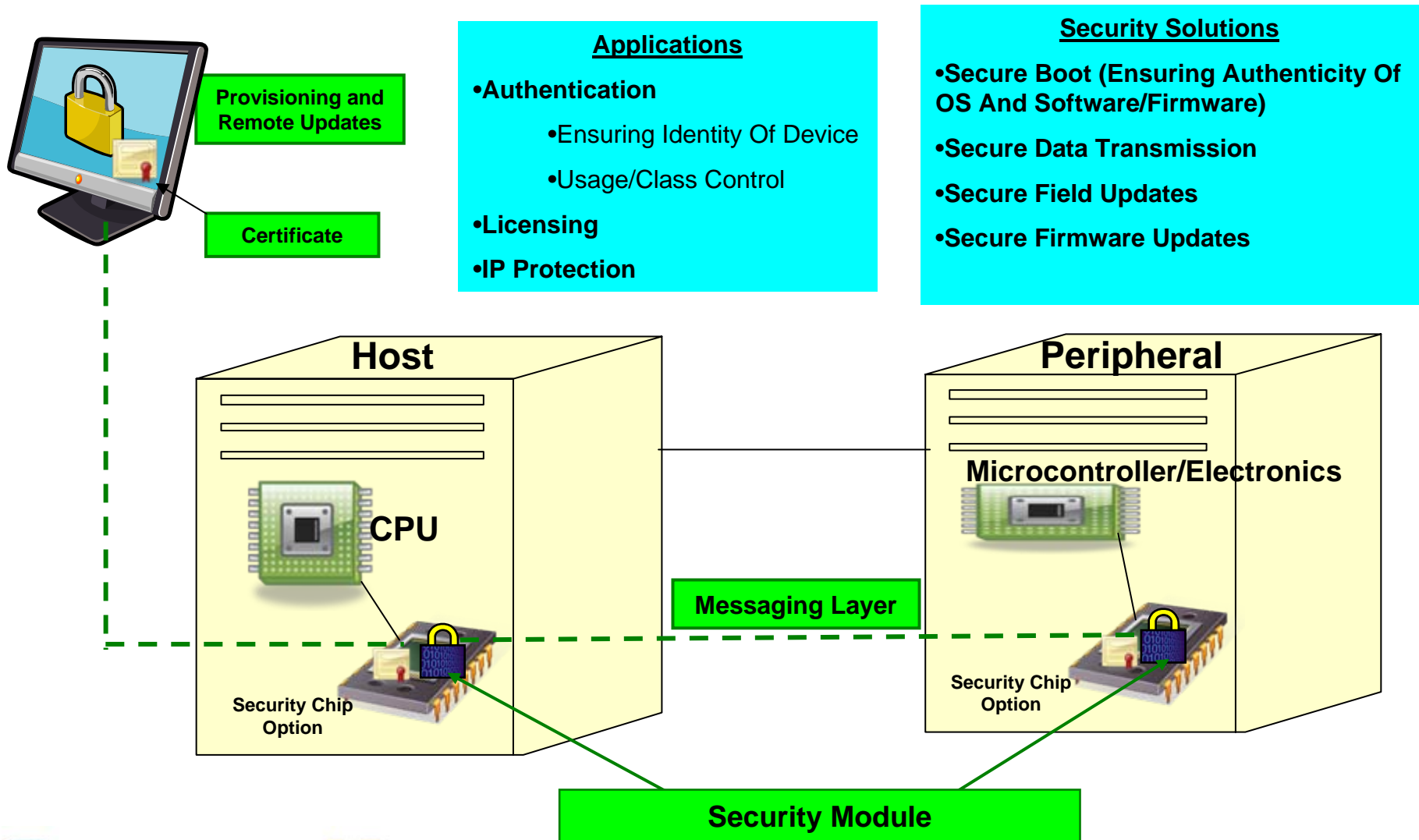


- **The Security Framework**

- Threat Modeling/Risk Analysis
- Security Modules
- Provisioning

- **Use Case Examples**

The Security Framework



GraniteKey Security Solutions

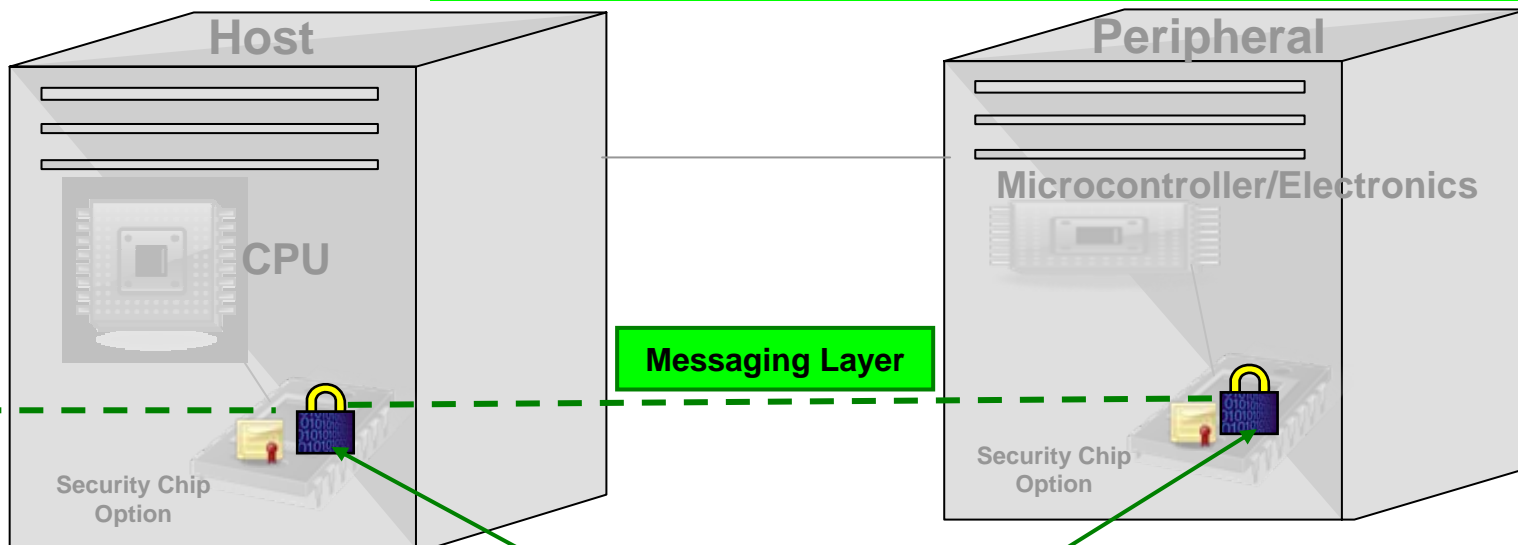
Components



GraniteForge™:
Provisioning and
Remote Updates

Certificate

- **GraniteForge™** Provisioning Authority Delivers Secure Provisioning (Keys/Certificates)
- **GraniteLock™** Security Modules Provide Authentication/Licensing/IP Protection Functionality
- **Integrated Messaging Layer** Allows For Simplified Development



GraniteLock™ Security Module

GraniteView™ Threat Modeling

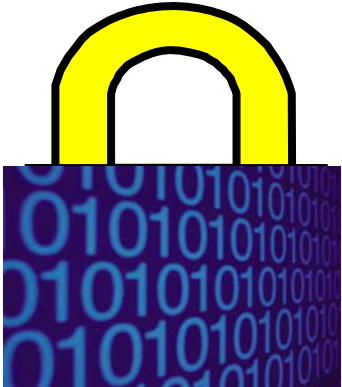
GraniteView™

Threat Modeling

The screenshot shows the GraniteView Threat Modeling interface. On the left, a tree view displays a hierarchy of threats under the heading "Firmware Provisioning". The threats listed include: "Illegitimate Firmware", "Secure Flash By Customer", "Firmware Is Compromised", "Private Key Compromised", "Hardware security chip" (highlighted with a blue selection box), "Locked Down Environment", "Transport Key or Firmware Comprom", "Encrypt and Sign The Firmware", "Locked Down Environment", "Purloined Chips or Assemblies", "Inventory Control", "Use Transport Keys", "ROM Mask or Chipmaker Flash", "Shipment Tampering", "Secure Container", and "Replace Chips". On the right, a logic diagram is visible, showing a "Login" process with a "Logic" block containing "AND" and "OR" operators. A text box with an arrow pointing to the "Hardware security chip" node contains the text: "e.g. The need for Hardware based security: Addition of security chip can impact the entire security solution".

- Collaborative Visual Representations of Threats, countermeasures, and business processes
- Determine Objectives Before Technological Choices
- Scenarios around security / cost tradeoffs
- Build a Security Roadmap

GraniteLock™ Security Modules



- **Application-Specific Firmware Modules Designed To Easily Integrate Secure IC's Into System**
- **Integrated Messaging Layer**
- **Customizable To Suit Customer Needs**
- **Pre-Defined Code Base Specific To Use Case and Application**

GraniteForge™ Provisioning Authority



- **Designed for Highly Secure Machine Security and Identity Solutions (i.e. Compliment To Or In Lieu Of A Traditional Enterprise Security such as CA/PKI)**
- **Strict Control And Auditing Of Provisioning Activity**
- **Not Reliant On Security Of Enterprise Systems, Operators, Database**
- **Integrated with GraniteLock™ Device Firmware**
- **Ideal For Global Operations**
- **Scalable Across A Broad Range Of Price/Performance levels**

Agenda

- **GraniteKey Services And Solutions**

- Development Lifecycle
- Cost/Benefit Analysis
- Technology Considerations
- Engineering/Implementation Services

- **The Security Framework**

- Threat Modeling/Risk Analysis
- Security Modules
- Provisioning

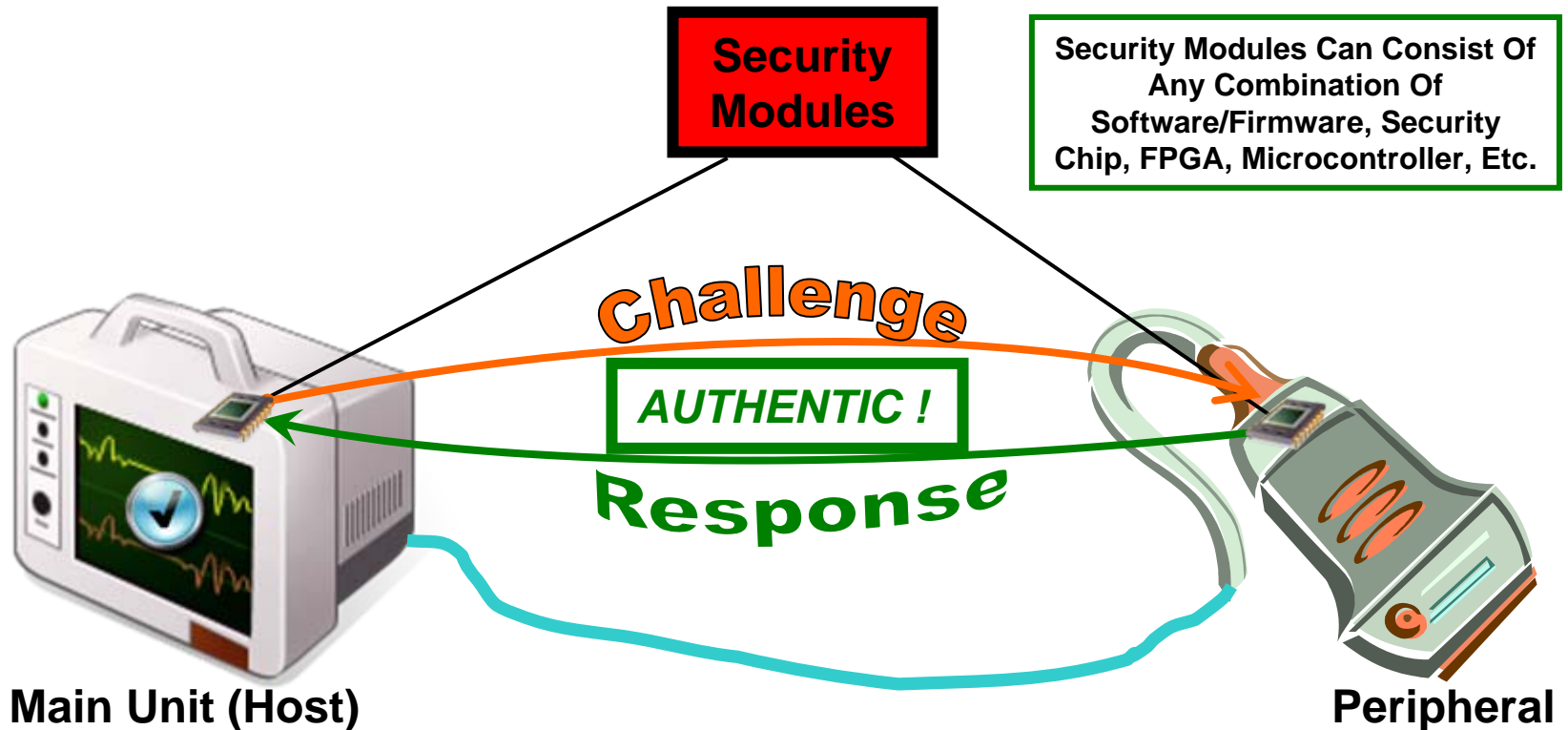
 • **Use Case Examples**

Some Device Authentication Use Cases

- **Anti-Cloning (Anti-Counterfeiting):** Preventing The Duplication Or “Cloning” Of A Device
- **Usage Control:** Preventing Unauthorized Use And/Or Limiting Use Of A Device
- **Tracking And Licensing:** Positively Identifying A Device And Controlling Licensing Of The Device (Feature Sets, Support Options, Etc.)
- **IP Protection:** Preventing The Reverse Engineering Of Intellectual Property And/Or The Subsequent Unauthorized Use Of IP

Use Case: Anti-Cloning

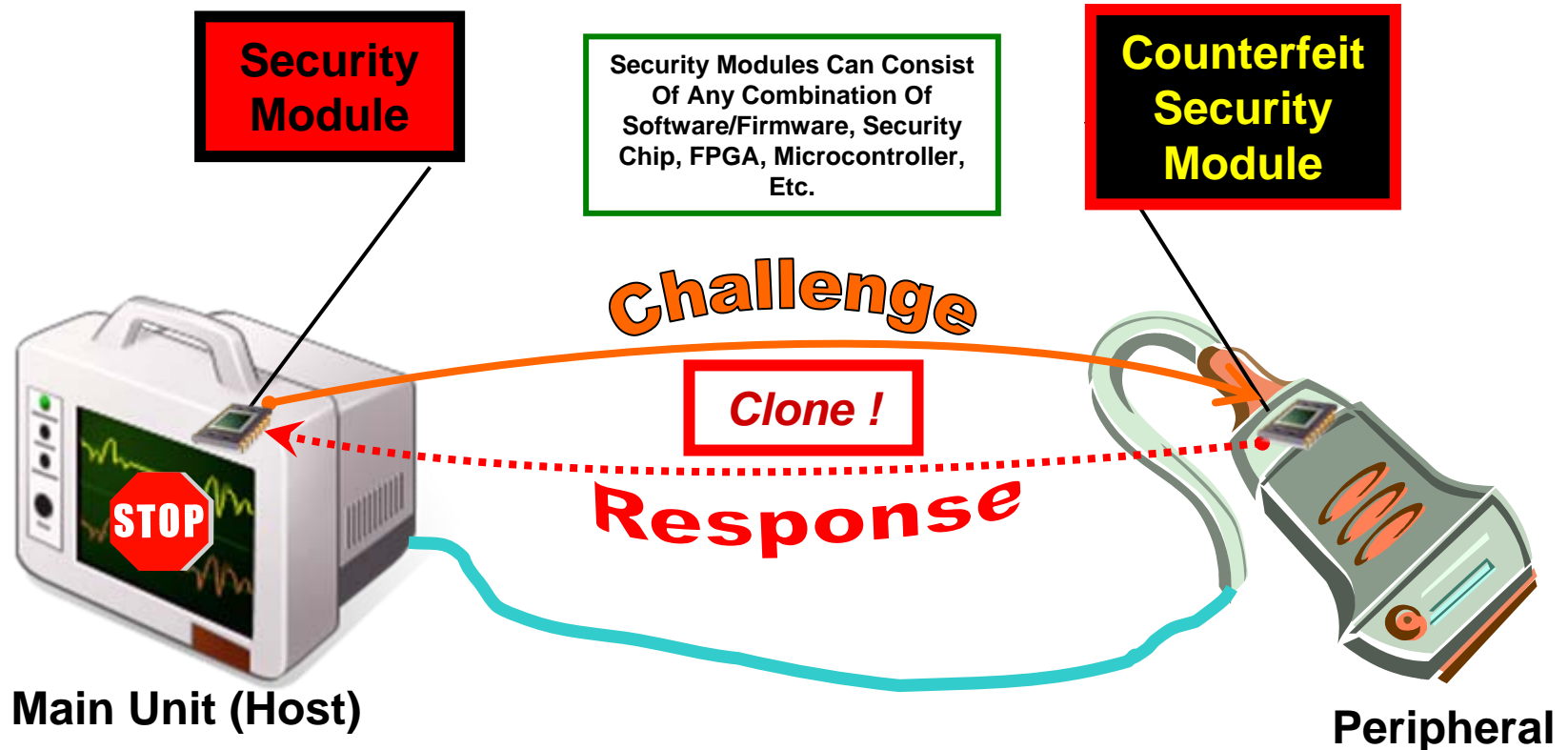
Authentic Peripheral Used



1. Security Modules Are Put Into The Host and Peripheral
2. Once The Peripheral Is Attached And The Unit Is Powered On, The Host Issues An Authentication Challenge To The Peripheral
3. The Peripheral Sends Back An Authentication Response
4. Once The Response Is Authenticated The System Becomes Fully Operational

Use Case: Anti-Cloning

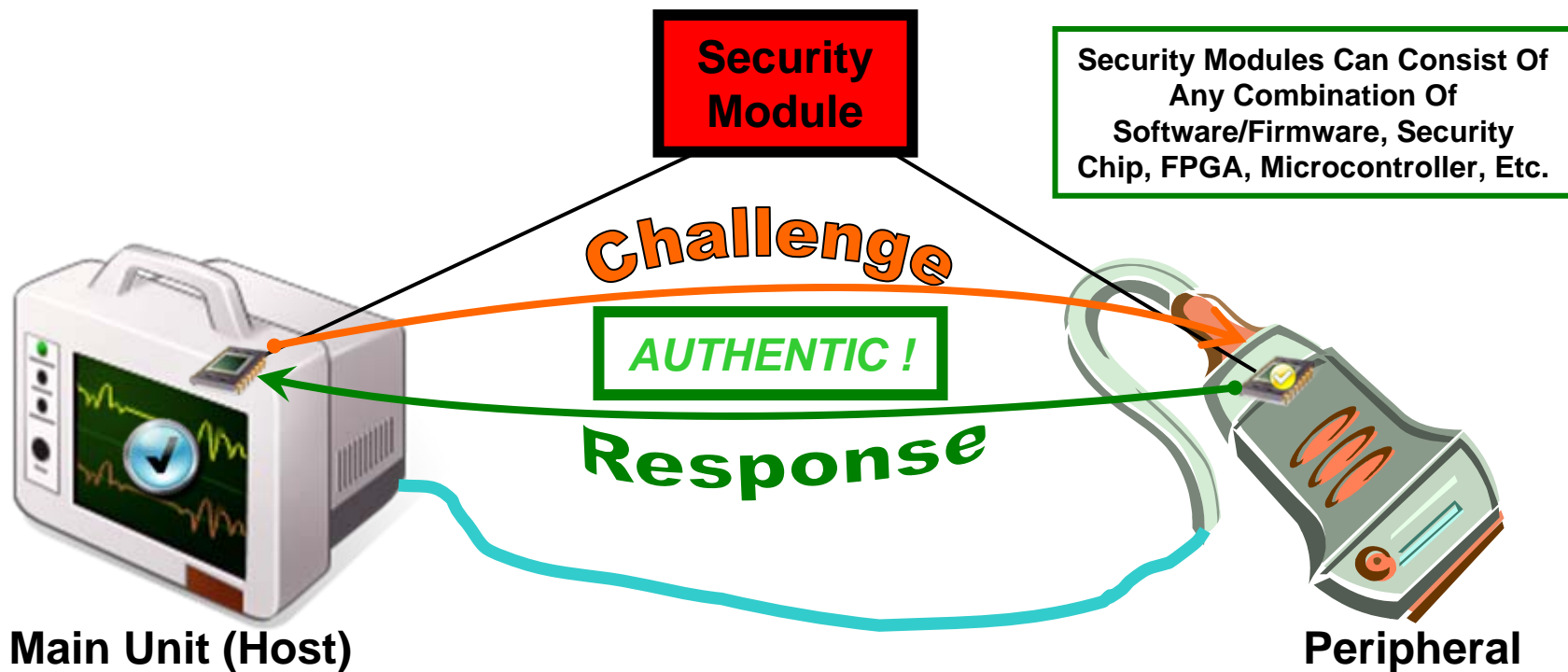
Counterfeit ID Chip Used



1. A Security Module Is Put Into The Host.
2. A Counterfeit Security Module Is Put Into The Peripheral.
3. Once The Peripheral Is Attached And The Unit Is Powered On, The Host Issues An Authentication Challenge To The Peripheral.
4. The Peripheral Sends Back A Non-Authentic Response
5. The System Refuses To Operate Due To Failed Authentication !

Use Case: Usage Control

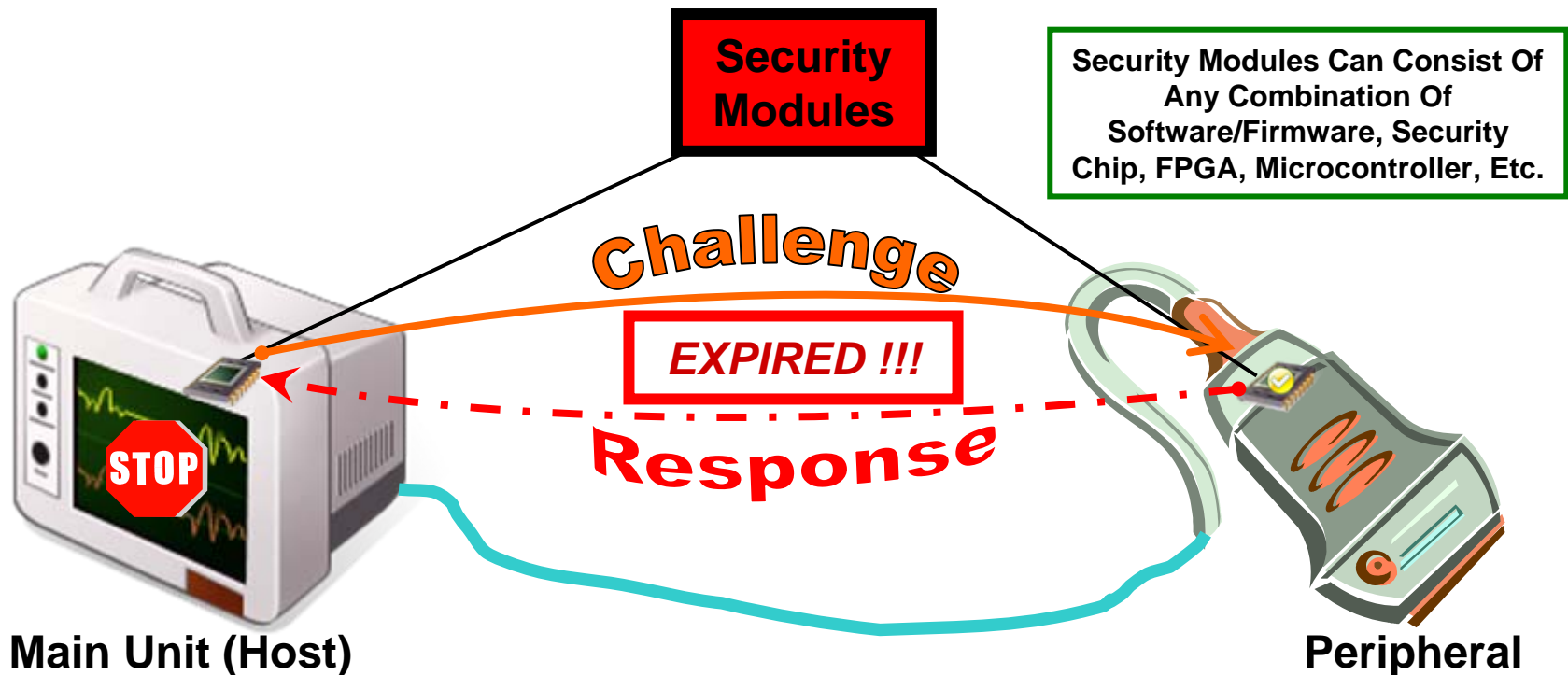
Authentic Peripheral Used – First Use



1. Security Modules Are Put Into The Host and Peripheral
2. Once The Peripheral Is Attached And The Unit Is Powered On, The Host Issues An Authentication Challenge To The Peripheral
3. The Peripheral Sends Back An Authentication Response And Creates A Record Indicating The Device Has Been Used
4. Once The Response Is Authenticated The System Becomes Fully Operational

Use Case: Usage Control

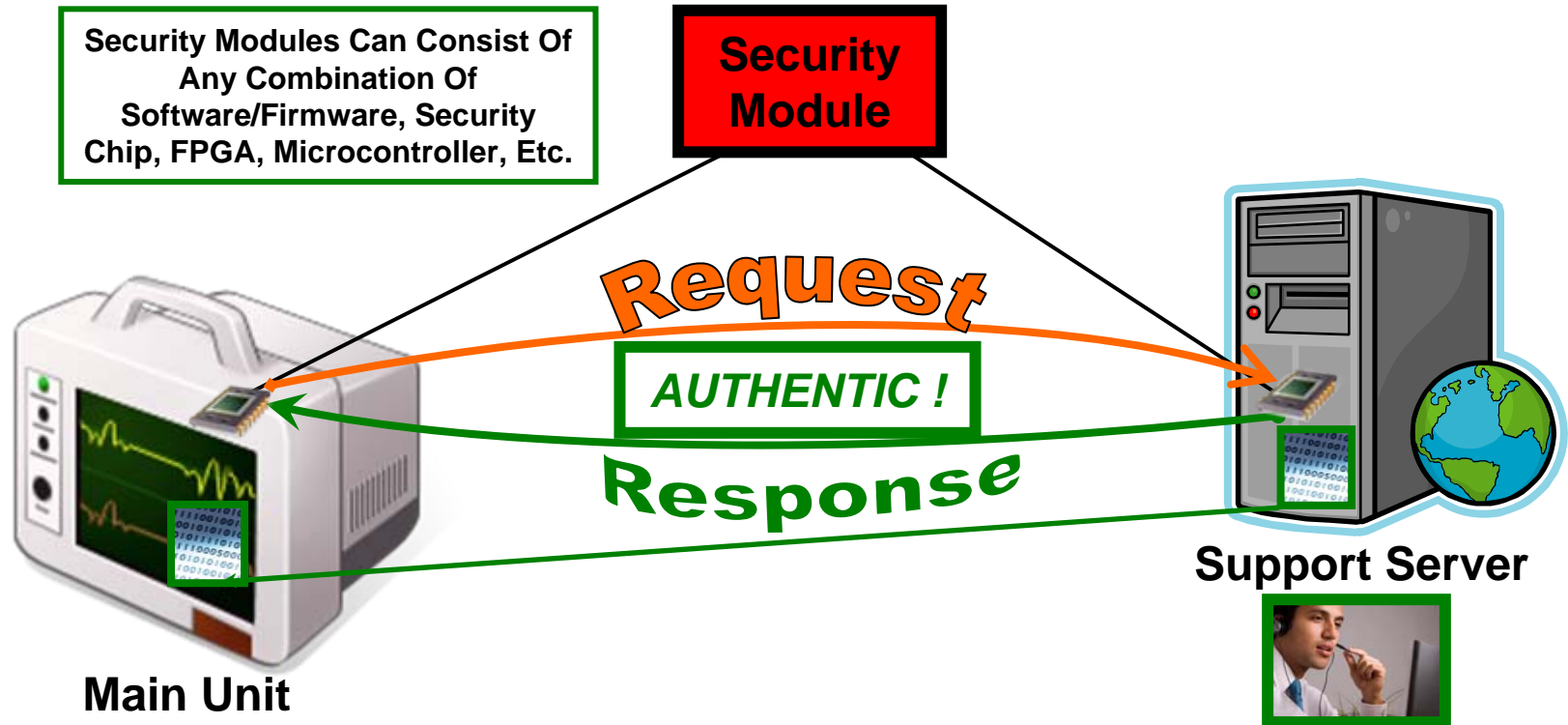
Authentic Peripheral Used - Expired



1. The Host And Peripheral Both Contain Security Modules
2. The Peripheral Security Module Has A Record Of Prior Usage
3. Once The Peripheral Is Attached And The Unit Is Powered On, The Host Issues An Authentication Challenge To The Peripheral
4. The Peripheral Sends Back A Response Indicating That It Has Expired
5. The System Refuses To Operate With An Expired Peripheral Attached

Use Case: Serial Number and Support License Tracking

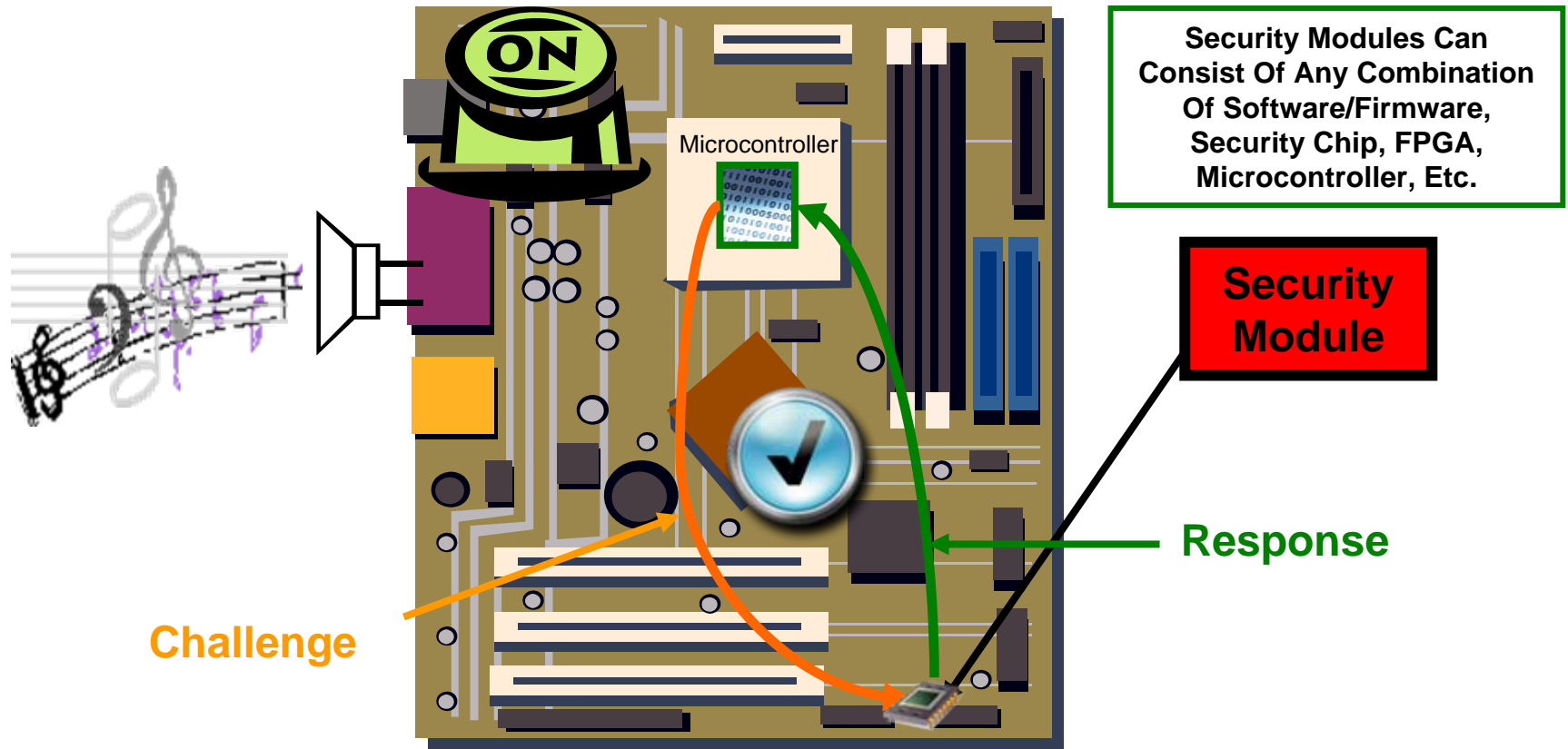
Authentic ID Chip Used



1. Security Modules Are Put Into The Device and Support Server
2. The Device Sends A Request To The Support Server For Service (Updates, Support, Etc.)
3. The Server Authenticates The Device And Sends Back An Authentication Response
4. Once The Response Is Authenticated The Support Server Will Send Firmware Updates and/or Allow Support Services

Use Case: IP Protection

Authentic ID Chip Used



Challenge

Response

1. A Security Module Is Put On The Device Motherboard
2. Code Containing Authentication Instructions Is Loaded Into The Microcontroller
3. On Power Up The Microcontroller Sends An Authentication Request To The Security Module
4. The Security Module Sends Back A Valid Response
5. Once The System Authentication Is Complete The Device Becomes Operational

Current Market Focus

- **Health Care (Medical Devices¹, Pharmaceutical, Records Management)**
- **Global Supply Chain**
- **Consumer Electronics Manufacturers**
- **Networking and Telecom Equipment**
- **Appliance Manufacturers**
- **Government (DOD, Homeland Security, EAC)**
- **Insurance Carriers**
- **Venture Capital Management**

¹\$200B market

Contact Information



268 Bush Street #3350

San Francisco, CA 94104

<http://www.GraniteKey.com>

info@GraniteKey.com

Phone: (925) 413-4365

Phone: (925) 216-1669