

A large, stylized letter 'A' in blue with a black outline. The 'A' is positioned to the left of the main title, with its right side overlapping the 'ABSOLUTE ID' text.

# **ABSOLUTE ID**

**When You Absolutely  
Need to Know!**

A dark blue circular badge with a white border, containing the word 'WHITEPAPER' in white capital letters.

**WHITEPAPER**

**Government Product Family**  
*Secure Solutions to Top Threats in Data Protection*

***Introduction***

In the 21<sup>st</sup> Century, we have a global climate, highly mobile and more technologically savvy users than at any other time in history. Individuals and institutions take for granted, the ability to instantly communicate anytime, anyplace with anyone over a worldwide heterogeneous technological environment into which more data is transmitted in a single hour than the sum total of the entire Library of Congress and then some. The Internet is a severely under protected network and storage environment where people are lulled into the misplaced belief that their information is safe and secure.

With the rising incidence of threats to sensitive data, and increasing requirements to protect that data, organizations must focus squarely on their security infrastructure. Protecting sensitive and critical data, no matter where it resides, and ensuring that only the appropriate persons have access to that data, must be a core requirement of every company’s security strategy.

Ad-ware, spy-ware, mal-ware, etc., are now all more correctly named crime-ware, giving them a more appropriate descriptor. Crime-ware is any computer program or set of programs designed expressly to facilitate illegal activity online. There are many types of attacks including the more pervasive attacks listed below and described in more detail in Appendix of Risks:

- *Phishing*
- *Password Database Theft*
- *Password Stealing and Identity Theft*
- *Man-in-the-Middle (MitM) Attacks*
- *Man-in-the-Browser (MitB) Attacks*
- *Identity Theft*
- *StuxNet Worm Derivations*

Even today, with all of the public information about how unsafe the Internet has become, individuals and financial institutions alike routinely put their highly cherished “Financial Family Jewels” of information out for the cyber-thief to steal. Whether it’s the cost to build the necessary protective environments or the poor deployment of security technology, the result is the same – everyday cyber-thieves add another notch in their data theft belts.

***The “REAL” Threat***

Crime and technology are getting ever closer. Today’s reports on security risks mostly cover amateur frontal attacks that exploit poor system administration or the latest hole that is not yet patched and are relatively inexpensive to mount.



Builders of viruses take a little less direct approach by planting malicious code, but even this can be done nowadays by amateurs with limited means and unserious motives.

Serious hackers are less interested in hacking for fun and more interested in attacking for profit. Organized crime from diverse geographies is devoting extraordinary amounts of energy and resources to online fraud and theft. Technology has created a new super-empowered criminal.

Information warfare professionals are distinguished from the amateurs by objectives, resources, access, and time. A professional is well funded and has adequate resources to research and test the attack in a closed environment – to make its execution flawless and therefore less likely to attract attention. The resulting attacks do not get press coverage because they are not mounted against low value assets; however, in one unguarded instant, you might be facing lost revenues, lost reputation, and even regulatory exposure.

### ***RocITSafe™ Government Product Family***

Equipping mobile workers with laptops is expensive and risky. Machines must be secured and patched regularly and if lost, they present a tremendous security risk.

With the increasing availability of high-capacity USB memory sticks, an alternative to traditional mobile business computing is emerging. By creating a virtual desktop on a USB thumb drive, companies can provide employees with the means to communicate safely with corporate systems and work securely from any PC, including a home machine or a device in an Internet café.

If the virtual environment is correctly configured, the user should be protected from any viruses or keyloggers that may be lurking on the host machine. And when they close the session and remove the USB stick, users should leave no footprint or clue that they had ever used the machine.

Provided the user can find a PC to use, the advantages are clear. The USB stick is cheaper, lighter to carry and can be centrally managed. If it is encrypted, it has zero value to a thief or to someone who finds it in the street. It can also be a useful business continuity measure if employees are suddenly prevented from using their office systems. The rapid distribution of USB devices would allow employees to work from home while maintaining policy control.

When companies deploy the device to individuals or groups of workers, they register themselves as users on their networked corporate system where *RocITConsole™* ties their Active Directory details to the unique identifier on their USB stick. It then deploys the virtual desktop software, and thereafter the users are free to take the stick with them and use it from any host machine.

*RocITSafe* bare-metal-boot (BMB) solutions are best suited to companies that want to virtualize the entire user's desktop, while *RocITSafe* Pluggable (PG) is better suited to deploying certain applications that the users need all the time, such as a VPN connection or certain desktop applications. PG collaborates with the operating system on the PC, while BMB runs with its own standalone highly secure operating system.

Under central administrative control, both versions can restrict what executables can run within the virtual desktop, and thus prevent data leakage via malware on the host PC.

Absolute Identification's *RocITSafe* family of products are designed and developed from the core with the highest level of security in mind. Every *RocITSafe* solution contains a fully integrated and highly secure operating environment that dramatically enhances the ability to protect the user against Cyber-theft.

### ***GovSafe™: Local & State Government Solution***

*GovSafe* focuses on the needs of Local & State Government to support mobile and remote office workers with a safe and secure platform. *GovSafe* provides a highly secure computing platform that supports teleworkers, emergency mobile location and Pandemic Social Distancing support.

Administrators are able to define the “Gold Image” of the teleworker’s platform and then monitor the efficiencies and behaviors of the teleworker throughout the business day. Remote device management provides administrators with the ability to shut down devices of teleworkers who are abusing the system.

***FedSafe™: Federal Government Solution***

FedSafe focuses on the needs of Federal Government to support mobile and remote office workers with a safe and secure platform. FedSafe provides a highly secure computing platform that supports teleworkers, emergency mobile location and Pandemic Social Distancing support. Administrators are able to define the “Gold Image” of the teleworker’s platform and then monitor the efficiencies and behaviors of the teleworker throughout the business day. Remote device management provides administrators with the ability to shut down devices of teleworkers who are abusing the system.

The Senate on Wednesday, September 29, 2010, unanimously approved compromise legislation to expand telecommuting opportunities government-wide.

- The bill, [H.R. 1722](#), requires federal agencies within 180 days to determine employees' eligibility to [telework](#), establish policies under which those personnel are allowed to work remotely and develop written agreements with authorized employees. The legislation also requires agencies to integrate telework into their continuity of operations plans and to train managers, supervisors and employees on the new policies.
- The Senate initially passed its version of the 2010 Telework Enhancement Act in May, while the House passed a similar measure in July. The compromise legislation was necessary to clear up minor differences between the two bills.
- The Federal Managers Association expressed support for the legislation and encouraged House lawmakers to follow the Senate's lead.
- "Telework has the potential to revolutionize federal agency operations and is a vital resource in meeting the challenges of retaining experienced professionals and enticing talented employees," said FMA President Patricia Niehaus.

Since being confirmed as director of OPM in April 2009, John Berry has spoken extensively about the need for telework. Here are some highlights:

- Telework capabilities are a key aspect in ensuring viable continuity of operations programs, as well as the continuance in an uninterrupted fashion of important government services and functions. OPM has set a strategic goal to increase the number of eligible federal employees who telework by 50 percent from fiscal 2009 to fiscal 2011.
- We know telework is valuable for the recruitment and retention of employees. We are aware that it mitigates environmental damage from commuter traffic and, lastly, we understand it can help employees balance work and other life responsibilities. However, unless we look at telework as a good business decision, incorporating it as an integral part of doing business in the federal government, we will continue to ignore the one effective and important tool that could make the difference between shutting down federal government services and continuing to operate with minimal interruption in emergency situations. Telework enables business to continue services and operations without jeopardizing the safety of its employees. This is something the president cares about. The response [from the Cabinet secretaries] was, "This makes perfect sense, and we're going to get to work on it." People get it.

- Strong, consistent [telework] policies are critical to program success. Of course, we are particularly interested in agency expectations with regard to telework during emergency closures. Most policies require teleworkers to fulfill their duties during closures, but also allow for consideration and latitude with regard to child or elder care issues or other personal responsibilities that may occur due to specific circumstances of the closure. We plan to give individual feedback to agencies . . . and will provide guidance on how to better incorporate telework as part of their emergency planning.
- We are aware that we have many obstacles to overcome in achieving this goal. The results from the 2008 government-wide annual call for telework data showed that 49 percent of agencies reported that management resistance remains a major barrier to telework. In addition, 32 percent reported that information technology security and IT funding are each significant barriers to the use of telework.
- I believe we can move telework forward to the point where we never again need to close the federal government for snow emergencies. By creating a mobile workforce, employees will always be able to work regardless of their location. With proper equipment and appropriate emergency planning, we need only to declare a "mobile workday," and the federal government can seamlessly conduct business as usual.

***MilSafe™: DoD, Homeland & Federal Enforcement Agency Solution***

MilSafe focuses on the needs of Military and Federal Law Enforcement to support in-theater, mobile ops, Officers and Soldiers and mobile & remote office workers with a highly secure platform. MilSafe's VRE is DoD hardened, tested and verified to provide the highest level of data protection as well as oversight of user activities on the devices. Remote management guarantees that devices can be shut down remotely should a device fall into the wrong hands.

***MedSafe VA™: Healthcare Workers Solution***

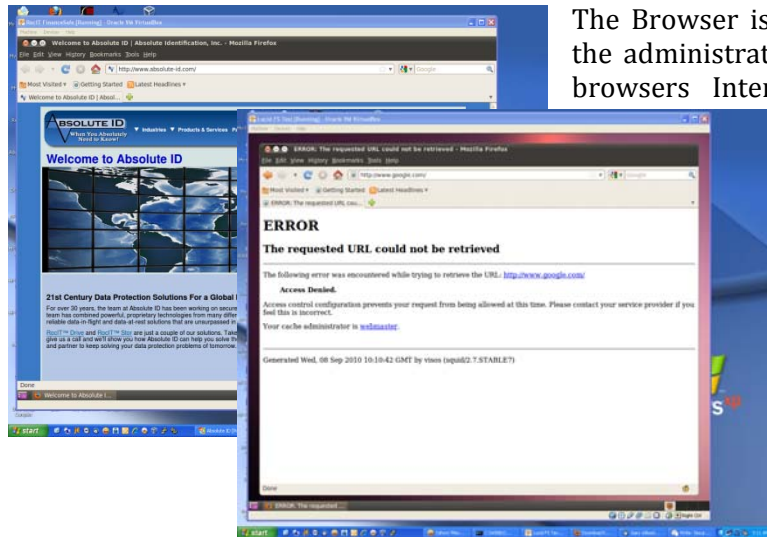
MedSafe VA supports the needs of VA healthcare providers by providing mobile and remote office workers with a safe and secure platform. Disaster recovery/business continuity planning has reared its head within the health care industry, and is a prime component of HIPAA. This portion of the rule was created, developed and implemented to protect health care information records that are transmitted electronically. Under terms of HIPAA, all health care organizations must consider the following areas:

- A data backup plan (required). The health care organization establishes and implements procedures to create and maintain retrievable copies of electronically protected health information.
- A disaster recovery plan (required). The organization establishes and implements, as needed, procedures to restore any loss of data.
- An emergency mode operation plan (required). The organization establishes and implements, as needed, procedures that facilitate the continuation of business processes, as well as protects and secures electronically protected health information while operating in emergency mode.

MedSafe supports Disaster Recovery, Business Continuity and medical records data protection in a unified Ultra-mobile computing platform. Hospital Administrators can set up "Gold Images" on MedSafe and can then monitor all activities on and off the devices 24 hours a day providing the ultimate in data security.

### ***Dual Bootable/Pluggable:***

This solution contains the RocIT*Safe* highly secure VRE and Browser which auto-mounts when plugged into either a PC or Intel-based Mac computer that is running its standard operating system.



The Browser is managed inside the secure VRE and the administrator can set a “Whitelist” to define the browsers Internet access permissions. If a user attempts to access any Website other than those “Whitelisted”, an “error” message pops up and the user is prevented from accessing the Website.

### ***Bare-Metal-Boot:***

This solution is a completely integrated and secure Computing Platform which takes control of the host hardware and supports all software that runs on any Windows-based system including

the following short list: MS-Office Suite, Adobe Office Suite, SaaS-based products and Proprietary Applications.

## ***RocIT*Safe*™ Secure User Applications***

### ***RocIT*Crypt*™: Credential-based Data Protection Service***

RocIT*Crypt* is a centrally managed security service that provides the enterprise with the ability to provision and manage a variety of different credentials for their organization and end users. Through the use of sophisticated key management technologies, it provides the ability to define and set up individual security keys (credentials) that can be granted to different users and groups within the organization. These credentials can then be used to encrypt different data within the organization; including simple data blocks, database records, full files or folders, or individual documents. Once encrypted the data becomes “opaque” and packaged into a secure data object that can be securely passed around the network, or within enterprise applications.

Each opaque data object has an associated metadata record that defines the credential algorithm (keys) that was utilized to encrypt the object. Only users that have the necessary credentials may gain access (either read-only or read/write) to the object to be able to decrypt and utilize the object. Absolute ID provides utilities that can be integrated into enterprise applications and infrastructure, such that encryption and decryption occurs on the “edge” utilizing end user credentials that are securely stored within user tokens or secure credentials storage locations.

Each integrated end-user application, enterprise service, or web site leverages these credentials to ensure that unsecure data is no longer available “in the clear” at rest, on the wire, or within the specified application itself. Information such as user’s on-line e-identity and credit card information (two key targets for cyber-thieves), on-line banking statements, stock portfolio information, etc.

The RocIT*Crypt* service is a highly fault tolerant, scalable, and redundant service that virtually eliminates the need for key bunkering, and dramatically minimizes the cost of “server encryption

farms”, since it decentralizes the highly processor intensive operations of encryption and decryption to the edge within the end-user’s secure RocIT*Safe* platform and environment.

### ***RocITStor™: Secure Storage Service***

RocIT*Stor* is the newest generation of SaaS (Software as a Service), or enterprise data protection solution that provides users with the power of RocIT*Crypt* to crypto-protect their data while also offering a secure way to collaborate with workflow partners and/or communities of common interest. RocIT*Stor* is a small footprint data protection application targeted to any individual who needs to lock down data on a laptop or desktop computer. RocIT*Stor* is loaded directly onto a user’s desktop and provides a secure mapped drive as an additional resource from within the windows explorer.

RocIT*Stor* is available as either a SaaS solution or as an enterprise solution for corporate customers desiring the ability to control their own servers, or leverage existing storage infrastructure including NAS (Network-Attached-Storage) and SAN (Storage-Area-Network) solutions.

### ***ConferenceSafe™: Secure Conferencing Solution***

Conference*Safe* is a credential-based conferencing product suite designed to provide a complete secure and mobile conferencing environment for real-time collaboration. This solution leverages RocIT*Crypt* user credentials to provide secure channel communication by encrypting and decrypting voice and data packets at each end of the communication link utilizing a shared community credential.

### ***RocITSafe™ Product Overview***

The RocIT*Safe* family of highly secure mobile platforms includes a DoD grade FIPS certified hardware encrypted, password protected USB Platform and applications that ensure a secure environment against a variety of attacks including those listed above. The product is delivered as a customizable set of applications and services.

Every solution contains multiple physical partitions and a secure area that is used for storage of device configuration and policies, and secure storage of X-509 certificates and other end-user credentials. It is fully manageable from a centralized enterprise server that can be provided to customers to manage their solution deployments, and can be provisioned, updated, and maintained consistently across the entire organization.

RocIT*Safe* solutions are able to boot directly to the thumb drive (Bare Metal Boot), or run as a secure virtual environment when plugged into an existing running Windows operating system (Dual Bootable/Pluggable Boot). The solution is fully customizable for an enterprise and provides a mechanism to define, deploy, maintain, and update the configuration of both the Bare Metal Boot and Pluggable versions.

RocIT*Safe* solutions are built on an extremely secure Linux-based runtime environment that has been hardened and locked down from end-user access, disabling cyber-attacks from occurring by enabling the control of the environment in which the solution runs. Competitive solutions employ a “defend from attacks” strategy whereby multiple types of control and security measures are taken to defend from the variety of different attacks. However, since their solutions run within an *unsecured, hostile* uncontrolled environment, this strategy is a continuous battle, where each new security measure is bypassed by malicious attackers, and new security measures in the solution must be continuously upgraded and revised. RocIT*Safe* is built with a highly secure runtime environment at its core that virtually eliminates attacks that could infect the system.

RocIT*Safe* solutions support hosting of a secure and managed virtual Windows desktop when running within the Bare Metal Boot mode. This feature (ViSoS™ – Virtual System on a Stick) enables enterprises to deploy a standard Windows desktop configuration and applications to customers that require a full Windows environment. This provides users with what effectively is their entire computer in a pocket-sized device that can be plugged into virtually any desktop or laptop computer; enabling the ability to boot, and run within a secure, consistent, manageable, and robust operating environment.

Finally, RocIT*Safe* solutions offer the flexibility to create multiple encrypted partitions that can be used to store end-user data files or enterprise shared data such as marketing materials, procedures or guidelines, or user information. These “shared partitions” are available from both the Bare Metal Boot mode, and the Bootable/Pluggable mode after successful authentication to the platform.

### ***Dual Bootable/Pluggable Mode***

As an optional boot method, RocIT*Safe* solutions can run in “Dual Bootable/Pluggable Mode.”

When the RocIT*Safe* drive is inserted into a host computer running a Windows operating system, the Public Read-Only Partition is auto-mounted by Windows and starts an autorun executable that launches the RocIT *Control Center*. The RocIT *Control Center* then auto-installs a secure Virtual Machine Manager (VMM) application. The VMM enables the host computer to run a secure virtual runtime environment, allowing the user to access and run their applications from within a secure environment created between the host computer and the RocIT*Safe* solution.

When running in Bootable/Pluggable mode, the VRE Linux-based journaling filesystem is loaded and installed within a virtual hard drive utilized by the RocIT*Safe* virtual machine running within the host Windows operating system. In this mode, the first time that the solution is run on a new computer system, a Virtual Machine Manager (VMM) application will be installed into the Windows host operating system, which will provide the ability to load and run the VRE securely within the existing Windows environment. Running the VRE as a virtual machine within the host provides the following benefits over simply attempting to secure and run a browser off of the secure drive itself.

- It provides a DoD hardened Linux-based runtime environment that is isolated from the host’s Windows operating system, providing the highest degree of security, and eliminating any possibility of Windows based malware from being able to access or modify the browser’s memory or peripherals.
- It secures and encapsulates the solution’s hard drive, such that it is inaccessible by the host operating system, thereby eliminating the ability for malicious applications or viruses to infect the runtime environment.
- Since the VRE is secure, locked down, and centrally managed & controlled by the enterprise administrator, network and other system settings can be controlled within the virtualized environment, thereby blocking any potential MitM or MitB attacks prior to communicating with the Internet.
- Running with a VM ensures and isolates the memory space from the host system, such that viruses or malware running on the host system cannot inspect the process and infer or get access to critical corporate or personal information stored in memory.

### ***Bare Metal Boot Mode***

The most secure operating mode for any of the RocIT*Safe* solutions is “Bare-Metal-Boot Mode” where the host computer’s hard drive is physically turned off and unavailable to RocIT*Safe*.

When RocIT*Safe* is operating in Bare Metal Boot Mode, the ViSoS Runtime Environment (VRE) is directly loaded onto a journaling filesystem on a sub-partition of the Secure Encrypted Partition.

This filesystem and the VRE contained within it are inaccessible to the host computer system's Windows operating system and are completely secure and isolated. In this mode, the solution runs on a host computer system and turns off the host hard drive, if it exists, or runs on a host system that does not have an internal hard drive. The internal hard drive is actually "unavailable" to the end user, providing the highest level of security, and minimizing any potential data leakage, or viral infection from the host system.

For the Bare Metal Boot solution, this partition contains the RocIT *Bootloader*, which provides a custom bootloader that enables the drive to be booted on most computer systems when plugged into the USB port. Upon booting of the device, the RocIT Authenticator is launched authenticating the user to the secure partition of the drive.

*Note: The host computer system BIOS must be configured to support "boot from USB drive."*

### ***RocITSafe™ Architectural Overview***

RocITSafe is designed hierarchically where each layer of the solution provides additional levels of security and user control.

The architecture has three major elements in the hierarchy starting from the core and moving up the secure stack - VRE™ » ViSoS™ » RocITSafe Solution.

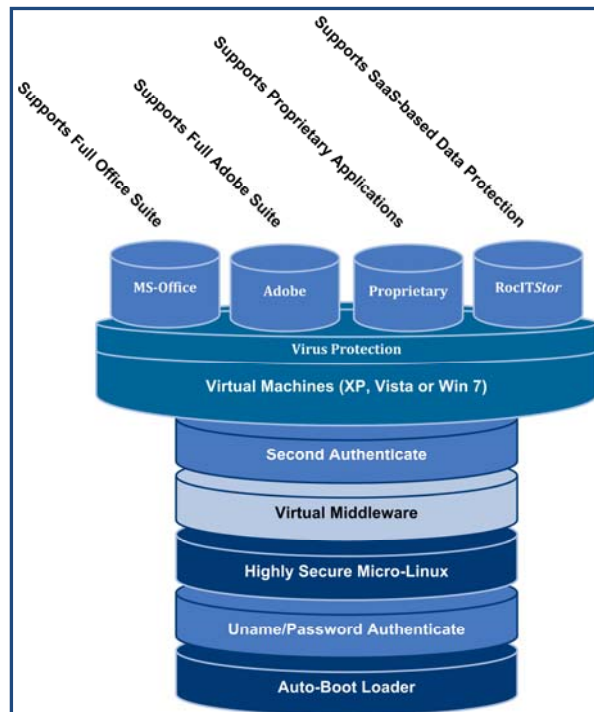
At the core of every RocITSafe solution lays the VRE™. The VRE includes: 1) Auto Boot Loader; 2) Secure Kernel; 3) Micro-Linux.

Just above the VRE is the ViSoS layer which includes: 1) Virtual Machine Manager; 2) Guest Operating System.

Finally, at the user layer, RocITSafe includes: 1) Proprietary & Standard User Application Software; and 2) Proprietary & Standard User-specific Hardware.

RocITSafe drives are configured with a Secure Drive area and two physical partitions that create a layered security approach to data protection, including:

- *Secure Drive Area*
- *Public Read-Only Boot Partition*
- *Secure Encrypted Partition*



The entire RocITSafe Software stack is; 2GB in size for the Pluggable version and 8GB in size for the Bootable/Pluggable version, requiring a 4 GB and 16GB device respectively.

### ***RocITSafe™ Hardware Platforms***

The RocITSafe software is hardware independent and supports several best-of-breed USB hardware platforms, including:

- *Kanguru Defender Elite (Preferred Choice)*
- *MXI Security*

- *Lexar*

All brands of RocIT*Safe* drives support both a secure bootable USB flash drive that is partitioned with a public accessible, or CD-ROM boot partition, and a secure AES256 encrypted partition that is unlocked upon authentication to the drive with a password, or through biometric authentication. The entire software solution stack stored on the drive is called ViSoS – Virtual System on a Stick.

The boot partition contains a bootloader that enables the drive to be booted on a standard X86 host computer, drive authentication application (ViSoS *Authenticator*) which prompts the user for the drive password and provides the ability to change the drive password, and a secure AES256 encrypted private partition that contains a full Linux-based runtime environment & applications called ViSoS Runtime Environment (VRE).

The VRE is “locked down” and “hardened” to DoD standards and is only inaccessible to an Administrative user. The VRE can be customized, configured, and centrally controlled and updated via an enterprise Update Service by the enterprise administration staff to meet any custom enterprise requirements.

Optionally, the VRE can be configured to host a Virtual Machine Manager (VMM) that is preconfigured with a Microsoft XP or Windows 7 virtual machine that will provide full access to end user applications.

There are 2 primary alternatives available for the solution:

- Secure Browser running within a Secure Virtual XP or Win7 virtual machine.
- Secure Browser running within the VRE without a Virtual Machine. This option would effectively provide ONLY a browser on a bootable drive.

End-user certificates can be stored within a Secure Certificate Store on the drive itself or within the secure VRE filesystem stored on the encrypted secure partition. The certificates could then be used for PKI-related needs such as multi-tier authentication and website authentication and access control.

### ***Kanguru Defender Elite***

The RocIT Drive Encrypted USB Platform is a hardware encrypted, password protected FIPS 140-2 validated drive. The drives are password protected and fully manageable from a central management server that supports many management capabilities including the ability to disable drives in the field if lost or stolen.

Defender Elite is a FIPS 140-2 certified USB Flash Drive. The drive has an onboard cryptographic processor which handles all data encryption/decryption. The chip also handles the authentication component of the password login process (on-chip matching). Defender Elite holds the following hardware security certifications:

- *FIPS 140-2 Certificate # 1270 (Device)*
- *FIPS 197 Certificate # 1066 (AES with 256-bit key in CBC mode)*
- *SHA-1, SHA-256 Certificate # 1099*
- *RSA Certificate # 506*
- *ANSI X9.31 DRNG w/ AES 256-bit Certificate # 603*

The AES key (which is generated onboard through a FIPS approved random number generator) is used to encrypt / decrypt data on the secure partition and is obfuscated and stored in a hardened secure location on the device. This location is inaccessible to the users of the device. The device is filled with a tamperproof hardened epoxy which completely covers all chipset components and pin

connections. Brute force attack countermeasures are built into the firmware of the device which will trigger an AES key deletion to prevent unauthorized access to the data set.

### ***Remote Disable for Virtual Environment***

Defender Elite provides an administrator with the ability to remotely disable a lost/stolen device. In the RocIT*Safe* configuration, there is a service initiated upon boot-up of the virtual Linux environment (which runs in the background – completely transparent to the user). This service calls out to the central server (hosted by the enterprise) over a TLS encrypted tunnel to alert the server that the particular device has just authenticated. The server checks against any pending actions for the specific device and provides the corresponding command back to the service running on the device. If the device has no pending action (ideal), then the user's virtual environment opens and allows access to the device. If there is a pending action such as a disable command, access to the virtual environment is terminated and a flag is set to disable access unless an administrator allows access again.

### ***Kanguru Defender Elite Management Features***

The Kanguru Defender Elite provides the following additional management features and capabilities:

#### **Device Configuration**

- Enable & Disable Devices
- Master Password Configuration
- User Password Configuration
- Define Password Security Policies
- Reset Devices to Default Configuration
- Customize Auto Unmount Settings
- Save / Load Settings for Quick Provisioning
- Store Contact Info on Devices
- IP Domain Control (Whitelist / Blacklist)
- Set Offline Access Settings
- Network / Remote Mgmt Configuration
- Dormant Device Mode

#### **Remote Actions**

- Wipe Device Data
- Disable Device
- Wipe Device Data & Disable Device
- Change User Password
- Change Security Policies

- Update Device Version
- Send Message to Device
- Set or Update IP and Domain Permissions (Whitelist/Blacklist)

#### **Control**

- Export Audit Logs to XLS
- Graphical Reports
- Advanced Users and Roles
- Device Groups
- Advanced Auditing, Filtering and Logging
- Active Directory Support

#### **Device Control**

- Computer, User and Device Management
- System Wide Policies
- Computer Policies
- Policy Templates
- Email Alerts
- Advanced Filtering

## *Appendix of Risks*

### ***Phishing***

Although passwords can also be obtained through less sophisticated means such as eavesdropping, guessing, dumpster diving, and shoulder-surfing, phishing is a common form of cybercrime typically carried out through e-mail or instant messaging, providing links or instructions that direct the recipient to a fraudulent Web site masquerading as a legitimate one. The unsuspecting user enters personal information (such as user names, passwords, Social Security Numbers, and credit card/account numbers), which is then collected by the hacker. Of particular attraction to phishing scams are online banking, payment services, and social networking sites.

According to the Gartner survey referenced previously, phishing attacks continue to exact financial damage on consumers and financial institutions, with a trend toward higher-volume and lower-value attacks. The survey found that more than five million U.S. consumers lost money to phishing attacks in the 12 months between September 2007 and 2008, a 39.8% increase over the number of victims a year earlier.

### ***Password Database Theft***

Stolen user credentials are a valuable commodity and often times, cybercrime rings operate solely to obtain this information and sell it to the highest bidder or use it themselves to access user accounts. Hackers steal user data and passwords from one web site operator to hack other sites. Since many people use the same user ID and password combination for multiple sites, the attacker can hack additional accounts that the user has.

The Sinowal Trojan is a well-known attack developed by a cybercrime group several years ago that is responsible for the theft of login credentials of approximately 300,000 online bank accounts and almost as many credit card accounts. In late 2009, Microsoft Hotmail<sup>7</sup>, Google Gmail, Yahoo, and AOL were victims of phishing attacks that exposed thousands of e-mail account user IDs and passwords.

### ***Password Stealing and Identity Theft***

These types of attacks rely on the ability of the attacker to fool users into giving up their personal information and credentials. Since users are typically vulnerable to these types of attacks, any method that relies on a credential that can be disclosed is vulnerable to social engineering attacks. Note, however, that this does not include a physical transfer because users can be rather easily fooled over the phone or via e-mail and the Internet to disclose personal information, but just like the keys to their house or their ATM card, people are less likely to hand someone they don't know their physical smart card or token device.

In contrast, hardware-based secure storage and smart cards are non-transferable and, resist cloning therefore, are less vulnerable to social engineering. The status of software-based secure storage and software-based smart cards is very dependent on the implementation. Many popular implementations enable a user to copy and paste the credential, making it transferable and, therefore, vulnerable. However, it is possible to prevent the user from doing this (without expert hacking skills), in which case, the solution does provide some degree of protection.

### ***Man-in-the-Middle (MitM) Attacks***

In this type of threat, the attacker can actively inject messages of its own into the traffic between the user's machine and the authenticating server. One approach for MitM attacks involves pharming, which involves using malicious network infrastructures, such as malicious wireless access points or compromised DNS servers, to redirect users from the legitimate site they are trying to access to a malicious fraudulent Website that accesses the user credentials and acts on behalf of the user to perform malicious activities.

This type of attack is only successful when the hacker can impersonate each endpoint to the satisfaction of the other. The use of SSL authentication using a mutually trusted certification authority provides strong protection against MitM threats. When the certificate validation relies on the user, the user may fail to correctly validate server certificates and will click through the warning messages. Therefore, when using a certificate-based authentication solution, the onus is usually on the bank itself to ascertain whether the user's

certificate is valid and will not allow a session to be created when the certificate does not match the one in its system.

Although SSL with server authentication makes man-in-the-middle attacks harder to carry out, they are still possible by using phishing or other methods. We do remark that one-time passwords have the advantage that stealing the credential provides the attacker with a single access only (in contrast to stealing a regular password or a credential in secure storage, which provides the attacker with long-term, repeated access). Damage is limited but the vulnerability still exists.

The most effective implementation to defend against these attacks is through the use of smart cards/tokens that utilize the device along with a user ID and password for secure two-factor authentication.

### ***Man-in-the-Browser (MitB) Attacks***

MitB is a Trojan horse program, a variant of a MitM attack that infects the user internet browser and inserts itself between the user and the Web browser, modifying and intercepting data sent by the user before it reaches the browser's security mechanism. A MitB attack has the ability to modify Web pages and transaction content in a method that is undetectable by the user and host application. It operates in a stealth manner with no detectable signs to the user or the host application. Silent-banker is a well-known example of a MitB attack targeted at bank transactions. It uses a Trojan program to intercept and modify the transaction, and then redirect it into the attacker's account.

A MitB attack is carried out by infecting a user browser with a browser add-on, or plug-in that performs malicious actions. In principle, as soon as a user's machine is infected with malware, the attacker can do anything the user can, and can act on their behalf. If a user logs into their bank account while infected, the attacker can make any bank transfer that the user can. By the virtue of being invoked by the browser during Web surfing, that code can take over the session and perform malicious actions without the user's knowledge.

An effective defense against MitB attacks is through transaction verification utilizing either out-of-band (OOB) technology, in which a user's identity is verified through a separate channel, such as a telephone. Using a separate channel reduces the risk that both the internet and the additional channel have been compromised. In large financial environments, for example, when a user initiates a transaction, such as a funds transfer, the details of the transaction can be captured and sent back to the user via an automated phone call or SMS message for verification before the transaction is processed. User input is performed either through Interactive Voice Response (IVR) or the keypad. Both of these approaches assume that the user has mobile phone connectivity during the transaction.

Another approach involves the use of a secure portable Web browser that is launched from a bank-issued USB token after the user inserts the device and enters their password. After successful login, the user is taken directly to the issuing bank's Web site. Utilizing a clean, non-infected browser helps ensure that there is no malware in the browser.

Fraud detection also helps limit the damage an MITB attack can wreak. Although fraud monitoring works after the fact, once a threat has been detected, it can provide useful information to the financial organization as to the types of threats being perpetrated against their infrastructure. User behavior analysis and trend reporting that most fraud detection programs provide can help FSPs determine the risk associated with certain types of transactions. However, fraud detection alone provides little comfort without a formidable defense strategy. When working together with strong user authentication, threats can be captured and contained, while authorized users are allowed secure access to their accounts.

### ***Identity Theft***

Identity theft refers to all types of crime in which someone illicitly obtains and uses another person's personal data through deception or fraud, typically for monetary gain. With enough personal information about an individual, a criminal can assume that individual's identity to carry out a wide range of crimes. Identity theft occurs through a wide range of methods—from very low-tech means, such as check forgery and mail theft to more high-tech schemes, such as computer spyware and social network data mining.

***StuxNet Worm Derivations***

Targets Scada Systems: Thumbdrive-based: Exploits Zero-Day vulnerability in MS Windows Systems: specially crafted link file and just by viewing the link file vulnerability icon you launch the worm. Digitally signed from RealTech or J-Micron in Taiwan.

***About ABID***

Absolute Identification, Inc. is an innovative provider of data protection products and services that protect critical data throughout its entire lifecycle. Every Absolute ID solution employs technologies which create sophisticated, highly secure data that cannot be broken, dramatically enhancing data availability, confidentiality, and integrity and prevents unauthorized access or theft of digital data while providing a new total cost of ownership (TCO) for key management. Absolute Identification, Inc., is headquartered in Scotts Valley, CA.

***Contacts***

For further information about the company, visit [www.absolute-id.com](http://www.absolute-id.com) or contact Absolute Identification, Inc. at one of the locations listed below:

.....

**Headquarters**

5353 Scotts Valley Dr.  
Suite D  
Scotts Valley, CA 95066  
Phone: (831)459-8199  
Toll Free: (888)459-8199  
Fax: (831)480-5886  
[Info@absolute-id.com](mailto:Info@absolute-id.com)

**ABID International**

114 France St.  
DDO, Quebec  
Canada, H9A 1K1  
Phone: (831)278-0957  
Fax: (831)515-5256  
[Canada@absolute-id.com](mailto:Canada@absolute-id.com)

**ABID Federal Group**

22 East 35th Place  
Steger, IL 60475  
Phone: (708)755-1583  
Phone: (831)278-0952  
Fax: (831)515-5215  
[Federal@absolute-id.com](mailto:Federal@absolute-id.com)