

# Secure Ultra-Mobile Computing for First Responders

Secure, Manageable and Flexible - Anytime, Anywhere Computing Platform

## *Characteristics of an Emergency*

- Emergencies are very fluid and require quick deployment and mobility during and after event.
- Officials and experts will likely not know how long the emergency could last.
- Local resources will likely be unavailable for long periods of time – power, communications resources, etc.
- Local authority will likely be stretched beyond capacity – remotely managed, credential-based access to information is critical.
- Communities may be affected in waves that last for months and even years.
- State and federal laws may be modified, suspended or enacted in response to an emergency.
- Healthcare resources will likely be stretched beyond capacity.
- Social and economic disruption is likely.

RocITSafe™ - Bare-Metal-Boot Virtual System on a Stick is designed from the ground up to provide one of the most secure virtual USB computing platforms ever constructed – the ultimate in secure mobile computing. RocITSafe leverages virtually any PC-based laptop or desktop computer system as the host platform. Then it seamlessly incorporates device management within the RocITSafe guest operating system, supports industry standard software packages and proprietary packages that run within the RocITSafe guest operating system(s) (Windows XP; Windows 7) providing users the flexibility to customize their individual RocITSafe platform according to specific needs or desires without compromising security and data protection within the RocITSafe computing system. RocITSafe supports everyone from the casual user to the sophisticated Super-user.

## *Problem Statement*

You can't read the headlines on the Internet or turn on the T.V. without seeing one disaster or another. It seems the magnitude, type and frequency of disasters is increasing, almost exponentially. From Katrina to the Gulf Oil Spill to Earthquakes in South America and Asia, first responders are being called upon to go into the heart of disasters and help victims, restore social order and rebuild critical infrastructure even when they themselves are under-resourced and vulnerable.

Even then – maybe especially during those times – it is vitally important that First Responders have secure access to critically important information. Often, the ad hoc communications networks that get set up in the middle of the chaos are the ONLY form of connection to the outside world during these disasters. Every type of information is moving across those networks from personal medical information to personal financial and even corporate “Family Jewels.” Cyber-thieves know this and use these events to score big hits – getting in and out often before anyone is aware they have struck. And information moving to and from the center of the mess is as important to protect as any other high-value information on the Internet.

Disaster preparedness and recovery planning is designed to reduce the disruption of essential services when an emergency situation occurs. In formulating your plans, the goal is to develop and implement strategies that ensure the continued operation of facilities before, during, and after an incident. Hence, the main steps are **preparation, response, and recovery**.

## Solution Brief: First Responder Solution

Emergency communications planning is a key component of any disaster plan. Disaster plans should be flexible enough to be adapted to particular emergency situations. This flexibility is key to the overall success and outcome of any First Responder activities during a major disaster.

### *RocITSafe™ - complete data protection on Ultra-mobile platforms*



RocITSafe is available today on multiple sizes of FIPS and non-FIPS certified thumb drives as well as FIPS and non-FIPS certified USB spinning hard drives in sizes to over 500GB. RocITSafe creates a highly secure and ultra-mobile container in which the user environment resides including a user-specified OS, user-specific application software, device management tools and Anti-Virus software as well as user-generated data.

By adding CAC/PIV/Smartcard fully integrated login support within RocITSafe, the system has multi-factor authentication, which virtually guarantees your system cannot be compromised through unauthorized access and because of the unique design characteristics of the RocITSafe stack, outside unauthorized access points into the system are eliminated.

### *Real Threats - Real Solution*

Crime and technology are getting ever closer. 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.

In one unguarded instant, you might be facing lost revenues, lost reputation, and even regulatory exposure. 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.

Organizations today operate on a slender thread, striking a balance between security as protection, and security as a trust builder. And this thread can snap at a moment's notice. Organizations need to be visible in not merely preventing problems but also inspiring trust.

Nowadays, it's accepted wisdom that modern organizations must address issues of corporate social responsibility - their effect on the environment, their engagement with the community, as well as their financial performance. But, we believe security will become another yardstick of corporate social responsibility. How companies are seen to manage these issues will become central to corporate reputation. In other words, security will become the new reputation bellwether.

These duties and expectations don't go away during an emergency or disaster. Quite the contrary, society expects corporations and government to step up to a higher degree and protect individuals and corporations. And yet, it is at these times when everything is running counter to solid protection that cyber-thieves are at their most active and looking for the crack to penetrate.

No data protection strategy is complete unless it takes into account all levels of the security hierarchy - a holistic approach taken from the beginning is the only way to guarantee the design of any solution targeted at secure data protection at all times.

RocITSafe combines technologies to provide a standardized method to secure information on Ultra-mobile devices - technology that allows the information to protect itself. RocITSafe technology is highly portable and standards based so can comply with local, state, federal and international data protection standards as they are adopted around the country and around the globe.

**Pre-loaded & User Configurable Software**

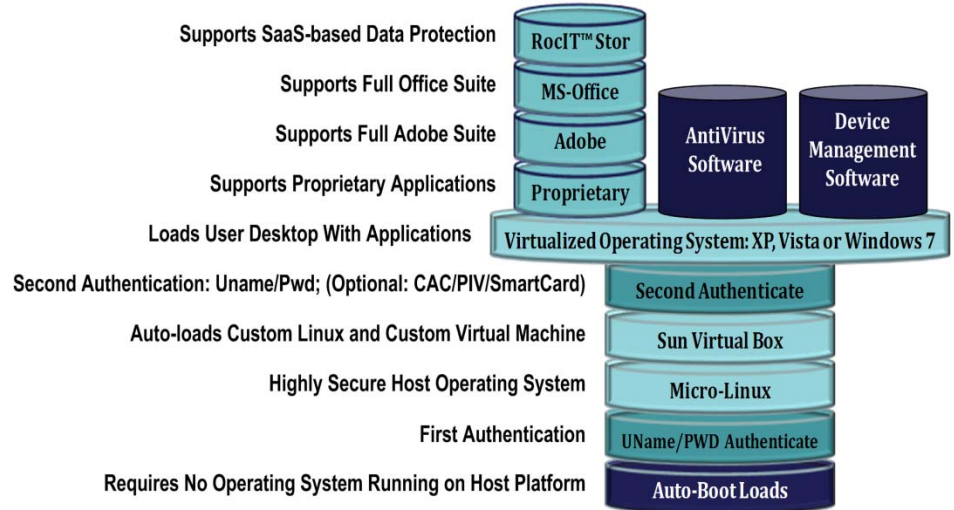
The software stack is designed to provide a high degree of flexibility in configuring the systems according to specific user requirements.

**Secure Mobile Solution**

*ViSoS™ Runtime Environment (VRE)  
The VRE is comprised of the Secure Kernel, Boot-loader, First Authentication, Secure Micro-Linux, Virtual Box, and Second Authentication components of the Secure ViSoS™ Stack. This configuration is completely locked down and does not change.*

*The Virtual OS layer and above are completely user-configurable.*

*The combination of the VRE and the user-configurable layers creates one of the most secure virtual USB computing platforms ever constructed – the ultimate in secure mobile computing.*



- **Auto-Boot Load:** Proprietary software that auto-sets the hardware into a secure configuration and auto-boots the virtualized software stack.
- **UName/PWD or Biometric Authenticate:** Proprietary software to authenticate user name, password or fingerprints – match-on device. Users can enroll multiple fingers at initial start-up.
- **Micro-Linux:** Custom Linux distribution including open office suite and Firefox Internet browser.
- **Sun V-Box:** Virtual middleware layer to provide the foundation for a virtualized OS.
- **Second Authenticate:** Proprietary software integration that supports user name, password and/or all major CAC/PIV cards. With this authentication, RocITSafe complies with Multi-factor Authentication requirements from Government DoD.
- **Virtual Operating System:** Users can have multiple virtual machines running within the virtualized middleware to create multiple users and/or personalities including custom user environments with applications and user settings that reside inside a virtual space, then lock them to specific user credentials and securely store your entire virtual desktop environment so that it is protected.
- **Proprietary:** RocITSafe solution supports custom and/or proprietary user applications which normally run within the Windows XP or Windows 7 operating environment.
- **MS Office:** RocITSafe supports the entire MS-Office Suite
- **Adobe Suite:** RocITSafe supports the entire Adobe Tool Suite
- **RocITStor™:** Proprietary software application which provides data protection, high data availability, business continuity and disaster recovery using a proprietary FIPS certified user credential to cryptographically sign, encrypt and manage user data in the Federated Data Cloud.
- **Device Management:** With its single agent and single-console architecture, the software provides security and compliance management that is intelligent, automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.
- **Anti-Virus Suite:** Provides complete anti-virus tools within the guest operating system.

### ***First Responder Solution***

Quick to configure and deploy in a local emergency or a major catastrophic event, RocIT*Safe* combines technologies that provide a standardized method to secure and share information on Ultra-mobile devices – technology that allows the information to protect itself. RocIT*Safe* technology is highly portable and standards based so can comply with local, state, federal and international data protection standards as they are adopted around the country and around the globe.

The software stack is designed to provide a high degree of flexibility in configuring the systems according to specific user requirements. Specialized applications can be easily incorporated into the user environment and available as a resource within the RocIT*Safe* secure container. Specific policies governing Disaster Recovery and Business Continuity within the organization can be included, managed and enforced within the RocIT*Safe* solution.

RocIT*Safe* supports standard methods for connecting to the network including landlines, basic WiFi, WiMax, Mobile Intelligent MiFi hubs, VPN access and others to support mobile computing while maintaining smaller functional coherent workgroups which allow the users to lock down an open Internet connection, create a highly mobile and secure endpoint to safely connect to critical resources and use a uniform tool set that is easily maintained by centralized or distributed IT organizations.

First Responders that need to be highly mobile and authorize into the operating environment can connect to the secure RocIT*Safe* solution using their ID Cards and a portable CAC/PIV or Smart Card Reader.

### ***About RocITSafe Family: Securing, Enabling, Mobilizing***

The RocIT*Safe* bare-metal-boot (BMB) solutions are best suited to companies that want to virtualize the entire user's desktop, while RocIT*Safe* 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 RocIT*Safe* family of products are designed and developed from the core with the highest level of security in mind. Every RocIT*Safe* solution contains a fully integrated and highly secure operating environment that dramatically enhances the ability to protect the user against Cyber-theft.

#### **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**

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)