

# Secure Mobile Computing for Financial Services Providers' Mobile Customers

Secure, Manageable and Flexible - Anytime, Anywhere Computing Platform

## Secure Mobile Solution

- FinanceSafe™ system is highly secure
- Complete data protection solution
- Configurable and flexible operating environment
- Easily integrate into existing IT infrastructure
- Supports FIPS certified devices
- Minimal host hardware required
- Restricts access to local host resources (i.e. Hard Drive, Printers, etc.)
- No hard drive required on host platform
- Requires use of at least one free USB port
- Multi-factor authentication support
- Supports CAC, PIV and Smart Cards
- Multi-OS support
- Standard web browser support
- Broadband support
- Standard applications software support
- Supports full e-mail client (i.e. Outlook)
- Supports proprietary user software
- Approved for Government & DoD use

FinanceSafe™ - 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. FinanceSafe leverages virtually any PC-based laptop or desktop computer system as the host platform. Then it seamlessly incorporates device management within the FinanceSafe guest operating system, supports industry standard software packages and proprietary packages that run within the FinanceSafe guest operating system(s) (Windows XP; Windows 7) providing users the flexibility to customize their individual FinanceSafe platform according to specific needs or desires without compromising security and data protection within the FinanceSafe computing system. FinanceSafe supports everyone from the casual user to the sophisticated Super-user.

## Problem Statement

In the 21<sup>st</sup> Century, we have a global climate, highly mobile and more technologically savvy than at any other time in history. Individuals and corporations take for granted, the ability to instantly communicate anywhere, anytime, anyplace with anyone – 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 – a severely under protected network and mobile environment where people are lulled into the misplaced belief that their information is safe and secure.

Even today, with all of the public information about how unsafe the Internet has become, individuals and corporations 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.

## FinanceSafe™ - financial data protection on Ultra-mobile platforms

FinanceSafe 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. FinanceSafe 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.

## Solution Brief: Mobile Customer Support

By adding CAC/PIV/Smartcard fully integrated login support within FinanceSafe, 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 FinanceSafe stack, outside unauthorized access points into the system are eliminated.

### ***Real Threats – Real Solution***

Surely, for any organization there is nothing more important than trust. Breach that trust and you may face legal, governmental, financial, and reputational consequences. For financial services, this means that people might love technology, but are getting the picture that things can go wrong. 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.

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 security data protection.

FinanceSafe combines technologies to provide a standardized method to secure information on Ultra-mobile devices – technology that allows the information to protect itself. FinanceSafe 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.

### ***FinanceSafe Solution***

FinanceSafe combines technologies to provide a standardized method to secure information on Ultra-mobile devices – technology that allows the information to protect itself. FinanceSafe 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. Specific policies governing Disaster Recovery and Business Continuity within the organization can be included, managed and enforced within the FinanceSafe solution.

FinanceSafe 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 IT organizations.

Mobile workers can connect to the secure FinanceSafe solution using their ID Cards and a portable CAC/PIV or Smart Card Reader.



### Pre-loaded & User Configurable Software

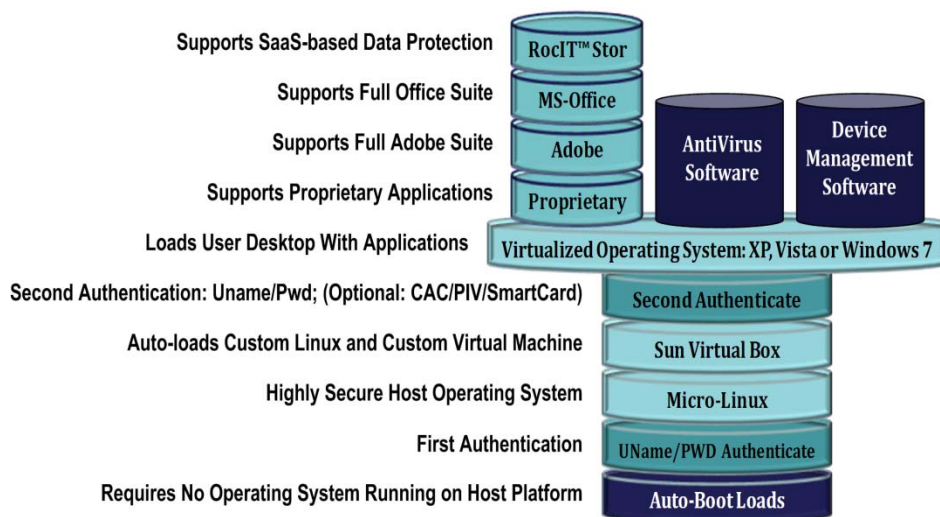
The software stack is designed to provide a high degree of flexibility in configuring the systems according to specific user requirements.

**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, FinanceSafe 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:** FinanceSafe solution supports custom and/or proprietary user applications which normally run within the Windows XP or Windows 7 operating environment.
- **MS Office:** FinanceSafe supports the entire MS-Office Suite
- **Adobe Suite:** FinanceSafe 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.

### FinanceSafe Dual Bootable/Pluggable Solution

FinanceSafe Bootable solution is a Bare-Metal-Boot solution designed from the ground up to provide one of the most secure browser Internet environments available today. The solution consists of a secure micro-kernel and locked down Linux-based runtime environment (RTE) with a secure browser that automatically launches when booted.

## Solution Brief: Mobile Customer Support

Once booted, the solution is configurable to automatically start a secure browser that runs within a jailed environment that does not have any access to the runtime environment, host filesystem, or host computer hard drive. This locked down browser will only provide access to the Financing sites that the Finance administrator configures to ensure that the user cannot inadvertently browse to another site that may contain malware. The runtime environment is manageable by the service administrative staff and specific white and black lists, and network protocols can be managed.

Each device is uniquely assigned to a specific user and the user's X-509 Certificate is securely stored in a secure location on the device. When the user browses to the Finance sites, they will leverage their specific certificate to securely authenticate to the Finance servers. This provides a truly secure network communication channel, and provides absolute identification of the end user to the Finance's systems and servers. FinanceSafe Pluggable Solution

FinanceSafe Pluggable solution prevents malware from infecting a browser by providing customers with a trusted browser stored on a USB smart card token with portable memory. When users log on to the Financing portal, they load a clean untainted browser from the USB token and use it to access their account. The typical financial institution supports a variety of access scenarios—local and remote employees, vendors, contractors, and customers—located at points around the world, through wired and wireless connections.

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

The 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.

#### **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)