

Credible Security

Handheld and Communication Security

Authentication

Two-factor authentication is employed when the handheld application sends and receives data from the central server. The first factor consists of a combination of the hardware device ID and username, and the second factor is a strong password supplied when the user is logging in. The password is hashed (using MD5) to allow quick local logins, but is never stored directly on the device.

Encryption

The Credible communication layer for both PalmOS and Microsoft Mobile use the Advanced Encryption Standard (AES), an encryption standard from the National Institute of Standards and Technology's (NIST). A 128-bit rotating key is used to encrypt data on both the device and in transit. Created as a replacement for Data Encryption Standard (DES) and specified in FIPS Publication 197, AES is approved for securing sensitive government information effective May 26, 2002. Assuming that one could build a machine that could recover a DES key in a second (i.e., try 255 keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key. For more information on AES, see <http://csrc.nist.gov/CryptoToolkit/aes/>.

Non-repudiation

Transactions are signed two different ways to provide a clear audit trail. First, an electronic signature is imprinted with the AES encryption key, which is created in part with information unique to the user and the user's device. Second, actual signatures are captured with each transaction after details are completed. The digitized signatures are transferred wirelessly and available online immediately to view and for generating printed records. All transactions are date and time-stamped on the handheld. The wireless gateway logs all communications, including the originating IP for both information requests and updates.

MD5 Algorithm

The MD5 algorithm is a way to verify data integrity. The MD5 algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA. MD5 was developed by Professor Ronald L. Rivest of MIT.

Source: *The MD5 Message Digest Algorithm* by Ronald L. Rivest. Internet RFC 1321 (April 1992).

For more information on MD5, go to <http://theory.lcs.mit.edu/~rivest/Rivest-MD5.txt>.

| Data Center Security |

Physical Security

Our managed servers reside at ServerVault in Dulles, Virginia—the **only commercial data center to EXCEED Department of Defense standards for Sensitive Compartmented Information Facility (SCIF) protection.** Physical protections include multiple dark fiber paths through armored conduit, dozens of cameras, access restriction and armed guards. ServerVault secures business applications for some of the world's leaders in healthcare, financial services, manufacturing, government, e-business, and technology. For a virtual tour or more information, go to <http://www.servervault.com>.

SERVERVAULT



MORE THAN SECURE...
SERVERVAULT SECURE

Data Vaults

At the core of ServerVault's SCIF-compliant facilities are industry-leading Lampertz® data vaults that are impervious to all environmental threats. All networking, power equipment, and customer servers are housed in these segregated vaults and are untouchable by fire, moisture, smoke, water, and electromagnetic pulses (EMP). Vault doors are secured with biometric thumbprint readers and continuously monitored by security cameras. Access is absolutely restricted to technical staff. Customers and visitors are not permitted access to any Lampertz data vault.



ServerVault Lampertz Vault

Redundant Power and Cooling

Power abnormalities and high temperatures can kill the most sophisticated technology. That's why ServerVault designed a state-of-the-art environment with built-in redundancy for all power and cooling systems. ServerVault's double, triple, and in some cases quadruple levels of redundancy allow it to guarantee the highest uptime in the industry, because there is no single point of failure. In an event of a utility system power failure, our own generated power assumes the full load within nine seconds. Since our systems were certified in early 2001, ServerVault has maintained 100 percent power uptime.

Site Perimeter and Building Security

ServerVault's site perimeter is secured with an eight-foot iron fence and an entrance gate that is guarded 24/7/365. Pan-tilt-zoom surveillance cameras monitor the site and building. Approved visitors are admitted only during normal business hours and must be escorted by an employee into

the visitor conference area. Only ServerVault employees and investigated third-party contractors are allowed beyond the visitor conference area. Advanced biometric authentication is required for all employees to enter the employee area of the building.

| Internet Security |

Network Security

Our client's central databases are not directly accessible by any means other than a secure VPN channel, using a ServerVault-issued RSA SecureID PIN pad with Radius authentication. Inbound web traffic protected by advanced network intrusion systems, and all web application screens are accessed with strong encryption (over a 128bit SSL channel).

Multi-Tier Firewall Technology

ServerVault's multi-tier firewall delivers security strong enough to prevent unauthorized access and secure systems from any malicious activity. Leading the industry, ServerVault has developed an advanced, redundant, multi-tier firewall architecture that works dynamically to set appropriate firewall policy rules. This adaptive technology is a great advance over traditional firewall rules that are set statically to protect only against known attacks.

Vulnerability Analysis and Penetration Testing

At ServerVault, all servers are given constant vulnerability scans to protect against both external and internal threats throughout the network and application layers. Constant threat assessment and scanning for network vulnerabilities provides the strongest defense available against external attack or compromise.

PKI Dual-Factor Authentication Systems

All external network access to IT resources in the application environment is provided through 3DES encrypted VPN tunnels built upon dedicated hardware and software iCSA certified VPN solutions. ServerVault maintains, monitors, and manages strict policy control for all VPN connections. ServerVault has deployed a powerful, dual-factor authentication system to verify the identity of every person before allowing them to gain access to your application IT infrastructure. This PKI-based authentication system requires users to identify themselves via two distinct factors: something they have (the PKI authenticator) and something they know (a password or PIN). Only when a person provides both factors is access granted to the application environment. In addition, ServerVault uses proven hashing algorithms to encrypt all traffic entering and exiting the network for maximum protection.

Back Up and Recovery Services

All client databases are stored on dedicated servers with RAID 5 disk configuration, to protect your data from corruption that can result from hardware failures. Off-machine and off-site backups are performed nightly and weekly respectively.