



Competitive Analysis for Me4Sure

The world of Internet/Intranet security and authentication is continually changing, with new products/solutions introduced daily. This document lists some of the more popular authentication methods and compares those methods to the strong Me4Sure SOLAS authentication solution. The conclusion of this document describes the strength of the SOLAS solution. Attached to this document is a competitive analysis of USB hardware providers, including Me4Sure.

Multifactor Authentication

The strongest forms of authentication involve the combination of authentication factors:

- Something the person knows: Passwords, PIN, etc
- Something the person has: Hardware tokens, private keys, etc
- Something the person is: Biometrics

When designed properly, multi-factor solutions force a potential intruder to compromise several factors before being able to mount a meaningful attack.

Cryptographic smart cards - Are physical tokens that contain a CPU and enough memory to store private keys and perform cryptographic operations like digital signatures with them. They are usually PIN-protected and offer some form of hardware-based tamper-resistance, which is supposed to make them useless without the human-memorized PIN. The obvious weakness is the need for the human to remember and enter the PIN.

Under the right circumstances, they offer a high degree of security. However, they are expensive to issue, require complex installations of special card readers, and are difficult to deploy on a large scale.

Me4Sure's SOLAS solution offers a combination of biometric and cryptographic technology that eliminates many of the limitations faced by smart cards while maintaining the security properties of a multifactor system. By using a technique known as cryptographic camouflage, **SOLAS** issues and responds to random one-time use challenge tokens. The random one-time challenges protect the tokens and solution from brute force attack, a problem that plagues other software-based solutions. Deployment of the SOLAS solution is simple, fast and inexpensive.

Password and Pseudo-Strong Authentication

Although most password systems are single-factor systems, many of today's systems have enhanced security by adding an additional factor, like a software or hardware token, to create a multifactor system. What distinguishes strong password systems from other, weaker one-factor methods is the level of security that they leverage from that one factor.

A popular solution is to require the user to answer security questions or verify a unique picture.

Pseudo-Strong authentication methods, such as Public Key Authentication, Password-protected Client-side SSL/TLS Certificates, and Default Pre-authentication are better than plaintext passwords. However, they have some well-known security weaknesses that make them equally vulnerable.

Public Key Authentication PKI - is a protocol that uses various key exchange methods to encrypt session traffic for remote logins. Although it uses well-known algorithms to perform both session key establishment and session encryption, its security is heavily dependent on the security of the method used to authenticate the user. In many cases, the user authentication method, such as using OTP or PIN, make PKA solutions vulnerable to compromise.

To use Public Key Authentication, generally a user must respond with a public and private key (password/PIN). This enables an attacker who captures the encrypted private key to perform a dictionary attack, recover the private key, and impersonate the user. The vulnerability increases when multiple users share a single computer or store their private key a common fileserver or network accessible computer. The common practice of creating disaster recovery backups, such as in most business environments, also creates vulnerability with PKA methods. A single successful penetration can result in the compromise of a significant percentage of a user community.

Public Key Authentication is similar to [Client-side SSL Certificate Authentication](#), as it shares the same vulnerability to a stolen-credential attack, and it has the same difficulties in coping with *roaming users*, who frequently must log in from different locations. Some implementations of SSL allow the private key to be stored in a hardware device, which improves security in exchange for more deployment obstacles.

Nearly all of SSL authentication requirements require/support "Password Authentication," in which the client sends its password directly to the server. The level of vulnerability of this method is dependent on the method of server authentication employed. An attacker who successfully bypasses server authentication in this case gets the passwords of any users who subsequently attempts to log in, and can do so undetectably.

One commonly used method of server authentication is "ad-hoc" distribution of server public keys. The server sends the client its (non-certified) public host key, and the client uses this to encrypt a session key and send it to the server. The actual protocol is slightly more complicated, but the client has no way of knowing if the key it received was in fact the right one making this method vulnerable to Man In The Middle (MITM) attacks.

Some versions of SSL support PKI-based distribution of host keys, which improves the security of server authentication, but then requires the deployment of a PKI. Sites must then purchase server certificates from third parties like VeriSign, or they must install and administer their own certification platforms like RSA, Vasco, Entrust, and PassGo. Strengthening server authentication does not address the weakness of password authentication.

Password-protected Client-side SSL/TLS Certificates - To initiate a conventional, server-authenticated SSL connection, a Web server provides a certificate from a well-known CA (Certificate Authority), which the Web browser can verify. SSL also provides a mode in which the client can send a certificate to the Web server, which can verify it and use its contents to authenticate the client. The corresponding private key, which resides on the user's PC, is password protected. An attacker who captures this encrypted private key can use a brute-force technique on the password to obtain the private key and impersonate the user, which is the same problem that affects Public Key Authentication. Likewise, it is possible to store these private keys in hardware tokens, which trades off security for convenience.

Default Pre-authentication – In an attempt to address password security weaknesses solutions have added pre-authentication. Pre-authentication requires a user to prove knowledge of their password before the server starts an authentication session. The standard method of preauthentication is an encrypted timestamp: The user password is converted into an encrypted key, which encrypts a binary representation of the current time. If the server is able successfully, decrypt the password within a defined time, authentication proceeds. An attacker who intercepts this message can perform an off-line

The security issues discussed above apply specifically to the authentication methods and not necessarily to a specific product or solution.

THE SOLAS SOLUTION

SOLAS is a biometric, cryptographically protected, portable USB drive. Unlike other security devices, SOLAS features a secure, multifaceted, cryptographic communication process. The multi-layered authentication process ensures accurate, instantaneous verification and authentication of all authorized parties in every Internet-based transaction. SOLAS protects individuals and organizations against impostors, hackers, spies, phishers, pharmers, and other forms of Internet intruders.

SOLAS secures your internet/intranet activities....Simply!

- ❖ Stops unauthorized access, fraud, & identity theft on all transactions
- ❖ Eliminates all keystrokes, Usernames, Passwords, or PINs
- ❖ Does not use or require the end user to load any software
- ❖ World-class encryption, true multi-factor authentication
- ❖ Biometric single sign-on authentication
- ❖ Meets regulatory requirements
- ❖ Never transmits or exports fingerprint data
- ❖ Users can customize the devices to meet branding requirements
- ❖ Is Plug-and-Play

In addition to protecting Internet/Intranet transactions, SOLAS can function like a standard USB storage device when configured with additional memory. Unlike other USB storage devices, SOLAS protects access to the stored data with biometric technology. Only the enrolled user can access the stored data. Even if the user loses the SOLAS device or someone steals it, the stored data is inaccessible and remains protected.

Encryption and Protection of Customer/User Identity

The SOLAS solution provides the maximum in user protection by digitizing and encrypting the enrolled data/fingerprint(s) and by storing this information only in the SOLAS device. SOLAS does not use external programs, software, or hardware in the storage and encryption process.

The SOLAS device and authentication process never exposes, transmits, transfers or exports the encrypted fingerprint data. The encrypted fingerprint data only verifies the user to that particular device.

Multi-level Authentication Process

SOLAS uses a multi-level verification and authentication process to ensure that each user has connected to an authorized entity before any transaction can begin. The Authentication Service Provider (ASP) issues random challenges that prevent any replay of prior transactions. This ensures that each response corresponds with the current random challenge and not with one previously generated. The biometric authentication process activates SOLAS, and the corresponding transaction verifies the enrolled user's identity and authorizes the required authentication or payment/transaction.

Using SOLAS for Secure Internet Transactions

To use SOLAS for a secured transaction, the user simply inserts SOLAS into a USB port on any Internet-enabled PC. The user then places an enrolled finger on the biometric sensor panel.



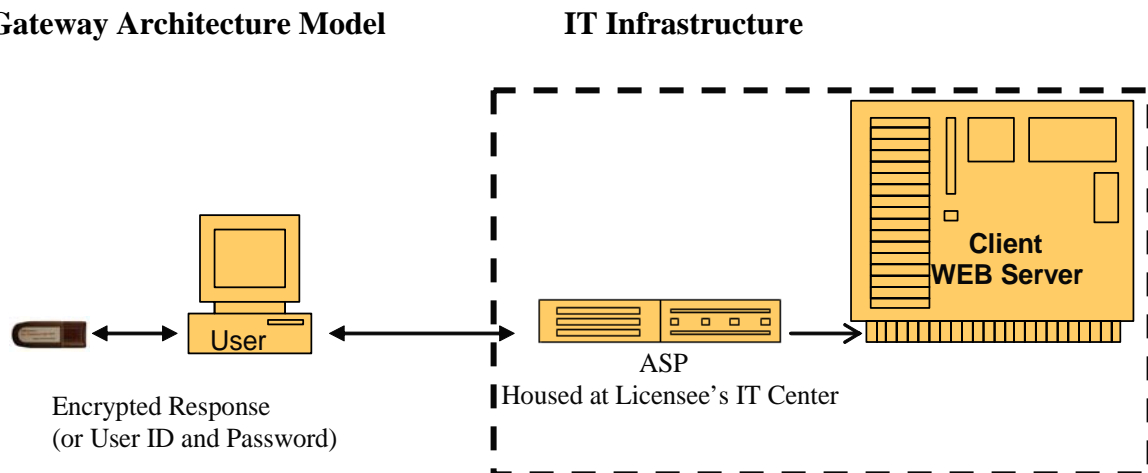
Once SOLAS validates the user's fingerprint, SOLAS activates the cryptographic authentication process with the ASP's database. Then, the ASP, via a secured link to any compliant financial, commercial or government Web presence, issues a random, encrypted challenge to the SOLAS device. The SOLAS device then replies with a time-sensitive, encrypted response to the ASP. The entire process takes less than two seconds.

It is this secure, encrypted 'dialogue' that provides SOLAS with a large competitive advantage over any other security authentication and transaction solution.

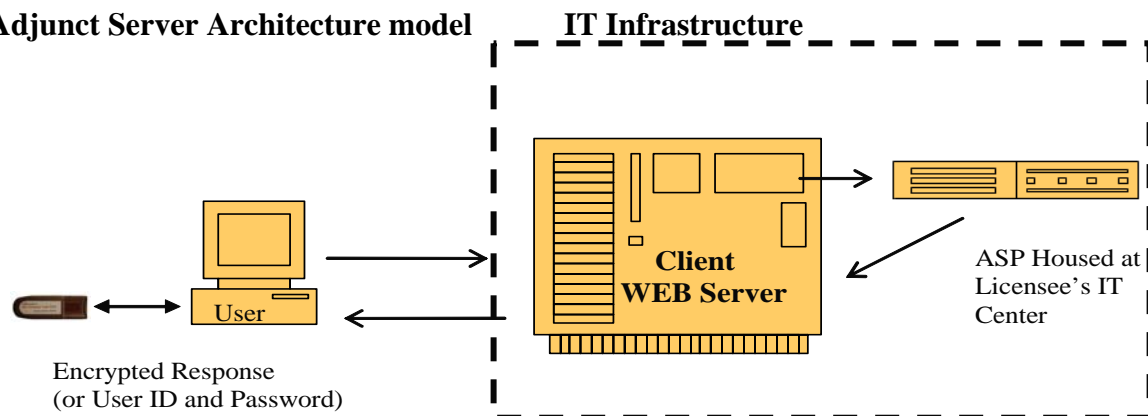
Deployment of the SOLAS Solution

Deployment of the SOLAS Solution requires little if any configuration changes to the client's IT infrastructure. This enables rollouts to occur in a matter of days, unlike other authentication platforms that usually take weeks or months. Me4Sure Professional Services Group can install either a Gateway Architecture or an Adjunct Server Architecture Model to fully conform to and comply with each organization's IT standards.

Gateway Architecture Model



Adjunct Server Architecture model



Competitive Analysis of USB Hardware Solution Providers

COMPANY	URL	DEVICE TYPE	WEAKNESSES	STRENGTHS
ActivelDentity	ActivelDentity.com	Smart Cards/USB	Stores User Credentials on Device User must enter PIN or identification # No biometric protection Static Identifier	FIPS Certifications Multiple offerings
RSA Security	RSA.com	Smart Cards/USB	Utilizes rolling Password User enters one-time password Device is not sync'd live to server Complex deployment & Maintenance	Large Market Presence Multiple Offerings Middleware
Vacso	Vasco.com	USB	User enters onetime password No biometric protection	Market Presence Multiple Offerings Middleware
Entrust	Entrust.com	USB	User enters unique PIN # No biometric protection	Market Presence Multiple Offerings
PassGo	Passgo.com	USB	Utilizes rolling Password User enters one-time password Device is not sync'd live to server	Market Presence Multiple Offerings
Me4Sure	Me4Sure.com	USB	Market Introduction Stage	Biometrically Protected Utilizes cryptographic technology User does not enter any data Encrypted challenge/response platform Easy deployment and maintenance Easy user enrollment Plug and Play – No Software for the user to load Provides authentication to multiple platforms with a single integration