



## Me4Sure's Secure On-Line Authentication Solution (SOLAS)

### *Executive Summary for SOLAS Technology*

Me4Sure's SOLAS presents a secure, automated, plug-and-play solution for user authentication and access control (with non-repudiation) for applications typically presented via the WEB (https). In its typical deployment context for such applications, it requires NO changes to Enterprise software application code. While SOLAS and its unique features can and have been extended for use in additional authentication and non-repudiation access control scenarios (Citrix, Standard Desktop application authentication, etc.), the plug-and-play, out-of-the-box focal point is WEB based Enterprise applications.

Me4Sure's SOLAS uses biometric identification (fingerprint) and strong encryption (AES 256 bit standards based methods and elements) to authenticate and non-repudiate users. The business Enterprise is assured that; "Yes, the person electronically asking for access to applications IS INDEED [user by name] AND no other person masquerading as [user by name]. Compromised (intentional or unintentional, friendly or unfriendly) username and password credentials become a thing of the past. Users no longer have to remember passwords (and the Enterprise no longer has to spend time and money supporting password management) for applications protected by SOLAS. SOLAS assures; "Yes it was [user by name] that was individually responsible for posting that transaction, downloading that document, etc."

The visible elements of SOLAS are the actual SOLAS user device and the SOLAS Authentication Gateway (AG) software installed on server(s) inside Enterprise data-center facilities.

The SOLAS user device is a single, composite USB flash memory disk drive with fingerprint reader, controlled by Me4Sure software embedded on the device. The physical appearance of the device is often coined as a "thumb-drive." Each employee (or other type of authorized user) needing access to SOLAS protected applications is issued a SOLAS device. The scenario is also applicable for applications vended by a business (such as financial institutions) to its customers.

SOLAS "stands-in-front-of" Enterprise servers and the applications they present

to users. The SOLAS server-side element, the AG, is installed INSIDE the Enterprise domain (inside the Enterprise data center) and is typically inside the boundary of the Enterprise Internet Firewall (often referred to as "in-the-DMZ"). It is equally effective and often convenient for it to be inside the corporate Intranet boundary (on the corporate LAN). All network communication connections are secured via standards based SSL encryption protocols (HTTPS). SOLAS AG deployment scenarios include installation of redundant physical servers or installation of the AG server software in virtualized server environments. The AG installation and configuration timeline is typically expressed in hours or days, not weeks or months.

The SOLAS device works with Microsoft Windows XP and above (Vista, 2003, 2008) and works with Microsoft Internet Explorer or a variety of other browsers (FireFox, Opera, Safari, etc.). If the browser(s) in use for the Enterprise support 256-bit SSL, SOLAS automatically uses 256-bit SSL; otherwise 128-bit SSL is the minimum. NO software is installed on the user's assigned PC(s) - all SOLAS client-side software is located on and runs from the SOLAS device itself. The actual authentication and non-repudiation features are ALWAYS protected via AES 256-bit standards based encryption. Unique to SOLAS, actual credentials are never passed via the network connection ("over the wire") between the SOLAS device and the SOLAS AG. Also, the user's fingerprints enrolled to their assigned SOLAS device are never exposed to the user's computer and never exchanged over the network.

The plug-and-play nature of SOLAS makes it extremely simple to use and operationally manage. SOLAS is highly adaptable to individual Enterprise security policy frameworks.