

November 2011

M4S Pilot Program Overview



PILOT Overview:

M4S provides comprehensive Identity Assurance and Access Management protection from the information security risks brought about by worker mobility, cloud computing, and the growing use of personal devices for business.

M4S combines into one package the strength of protection, breadth of capabilities and ease of use needed to work with confidence in a highly mobile and increasingly risky business world.

The M4S PILOT program lets companies directly experience the product's capabilities and value with a minimum of effort and without disruption to the customer's IT infrastructure or work processes.

The PILOT period spans 30 days from M4S installation.

All M4S product components and capabilities needed are furnished as part of the PILOT.

- Ten (10) portable, biometric (fingerprint-enabled) USB devices (Personal Smart Keys™)
- Me4Sure software for the Me4Sure Authentication Gateway Server, Me4Sure GINA/CP, Me4Sure Client, and Me4Sure administration consoles.
- M4S installation and testing
- Knowledge transfer to Client personnel assigned to the PILOT
- Remote and onsite support during the PILOT

Customer agrees to provide the following for the PILOT:

- Server platform as specified to host the Authentication Gateway (AG) software
- Housing of the AG server(s) within Client's data center
- Internet connectivity to the AG server(s)
- Personnel and PC and/or Laptops participating in the PILOT
- Definition of the test environment, applications and use cases comprising the PILOT prior to its commencement.
- Workspace for Me4Sure personnel within Client facility for the duration of the PILOT, if Me4Sure deems onsite support necessary.
- Feedback at agreed intervals throughout the PILOT regarding the performance and suitability of M4S in meeting the customer's requirements.

Important PILOT Technical Notes:

A Personal Smart Key (PSK) is required for each participant. In addition, two seed PSKs are needed to configure the initial deployment.

The technical contact should have a firm knowledge of:

- General server setup and administration
- Internet Information Services (IIS) w/ASP.NET
- Web server certificates for SSL communication
- AD Lightweight Directory Services (LDS)/Active Directory Application Mode (ADAM)
- Domain Name System (DNS)
- TCP/IP addressing and ports
- General workstation setup (Windows 7 and/or Windows XP)

Will a commercially obtained certificate or a self-signed certificate be used?

- The preferred method is to use a commercial certificate;
- Using a self-signed certificate will require all devices that will host the PSK (workstations, laptops, etc.) to have in its certificate data store a certificate from the Certificate Authority that issued the self-signed certificate.

Will the PILOT use a production domain or a test domain?

- Using the customer's production domain is preferred.
- Using a test domain requires either issuing special computers to run the PILOT, or requiring everyone participating in the PILOT to un-join their computers from the production domain and join them to the test domain for the PILOT duration.
- It is also necessary to know if the hardware server hosting the Authentication Gateway (AG) is a domain member server or a Domain Controller.

Servers and operating environment

- M4S supports Windows 2008 R2 (preferred) and Windows 2003. All servers need to have installed current revisions levels for service packs and patches.
- Any server hardware that is capable of running Windows Server OS, IIS, ASP and ADAM will satisfy the PILOT needs. Typically, a server class computer w/ 2GB RAM, dual-core CPU's and approximately 20 GB of disk space will suffice. M4S supports both 32 bit and 64 bit systems.
- M4S supports cloud and virtual machine installation. In either case the technical contact needs to have privileges, permissions and capability to configure ports, create service accounts and computer accounts, etc. that are needed for implementation/configuration and testing.
- A "collapsed" server is preferred for the PILOT where the Authentication Gateway software and AD LDS/ADAM are on the same server hardware.