



Engedi Technologies, Inc.

Network Security.

Multi-Party Authorization

Version 4.5

Last Update: July 21, 2010

Original Publication date: August 19, 2003

Engedi Technologies, Inc. retains all trade secret, copyright and other proprietary rights to this document. Except for individual use, this document should not be copied without the express written permission of Engedi Technologies, Inc. For contact information see www.engedi.net

Multi-Party Authorization

Protecting networks or control systems from the malicious insider can be accomplished by the use of Multi-Party Authorization (MPA). Multi-Party Authorization requires a second authorized user approve an action before it is allowed to take place in the network or control system. MPA implements a second key in the system, requiring a second authenticated entity approve of certain activity before that action can take place. MPA brings in that “second set of eyes” to ensure an access or action is appropriate before it takes place.

Currently, the most common methods employed by networks or control systems to provide protection from a compromised network insider, if any protection is put in place at all, are auditing for accountability, separation of duties, and job rotation. Engedi’s Multi-Party Authorization technology is a dramatic improvement to those current re-active or limiting practices. Multi-Party Authorization is designed to provide a pro-active capability to protect the network or control system from undesirable acts by a malicious or inexperienced insider before the activity takes place. MPA is a network security solution that can be embedded in or added to other security or control systems. It is patented.

Current protection solutions are generally re-active in nature and provide log records of who did what for later analysis. Most current security practices to protect a network or control system from a compromised insider involve some form of auditing, separation of duties, and job rotation. Those measures are intended to deter the potential malicious insider and to provide a mechanism to address inappropriate or incompetent action after the fact. They are reactive or limiting techniques. **Multi-Party Authorization**, as a pro-active solution, is a dramatic improvement to those current re-active approaches.

MPA is a **pro-active** solution that permits security policy implementation requiring two or more people to know and approve of a critical activity before it takes place. Multi-Party Authorization technology secures the most vulnerable and sensitive activities in network management from attack by a compromised insider acting alone. It stops most malicious or inappropriate activity before it takes place, not after.

MPA enables sensitive and critical network, computer and control systems, and database operations to enjoy greater security against the malicious insider than ever before.

MPA is somewhat analogous to weapons systems that require two individuals to turn two different keys in order to enable the system. One person cannot do it alone. MPA enables use of a second key in the system. An MPA enabled system would require review and approval by a second (or third) authorizer before certain critical tasks, as defined by security policy, could be performed. The MPA solution enables a network administrator to do his or her job efficiently while at the same time

protecting the network against the undesirable acts of a compromised or inexperienced insider, while minimizing inconvenience and delay. The three main elements of Multi-Party Authorization are the Key2 Agent, the Key2 Server and the Key2 Policy Engine. See the Figure 2 below.

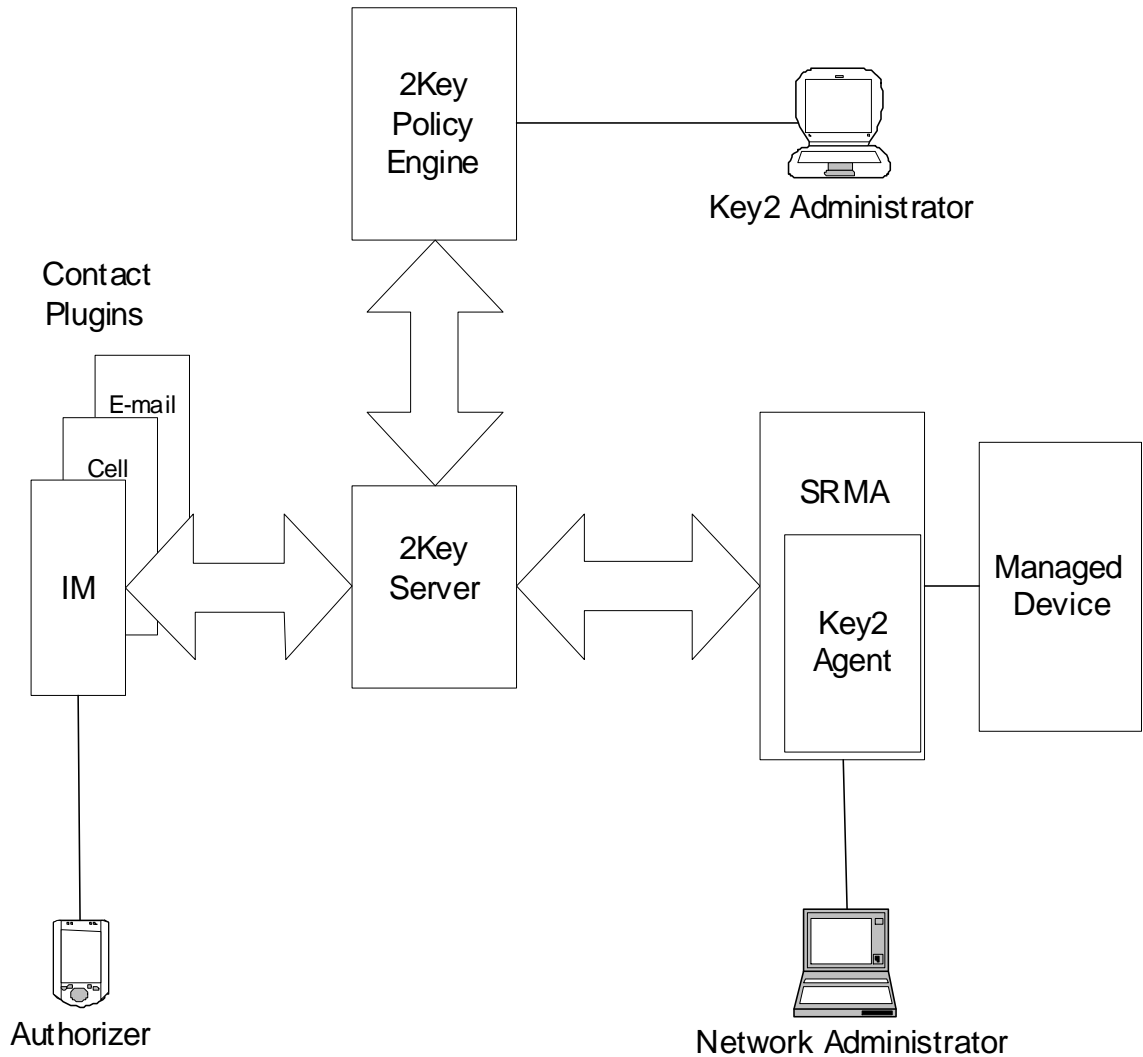


Figure 2

An example of embedding Multi-Party Authorization is the current ability to add and enable MPA on Engedi's Secure Remote Management appliance (SRMa)TM. The SRMa is a network management appliance for remotely managing network devices.

See Figure 2 above showing MPA added to the Secure Remote Management appliance (SRMA), where the Key2 Agent is added to control activity on the network appliance. MPA can likewise be added to other network or control systems to provide pro-active protection from undesirable acts of a malicious or inexperienced insider.

MPA has applications far more numerous than just those in conjunction with a network appliance. Integration of MPA into the kernel of operating systems of computers, control systems, file systems, and database managers would add significant protection against the malicious insider or inexperienced technician. MPA would allow network management to set Multi-Party Authorization requirements for execution of certain commands, for read or write access to certain files, and for read or write access to certain fields of a database.

With the appropriate MPA enabled policy in place one authorized individual would no longer be able to shutdown a critical server, turn a valve or switch on or off at the wrong time, read the entire database of customer credit card numbers, or launch a test procedure in the production network that could take the entire network down. Some of the most destructive attacks that have occurred and some of our most dangerous network vulnerabilities will be mitigated by the use of Multi-Party Authorization.

Multi-Party Authorization Applications

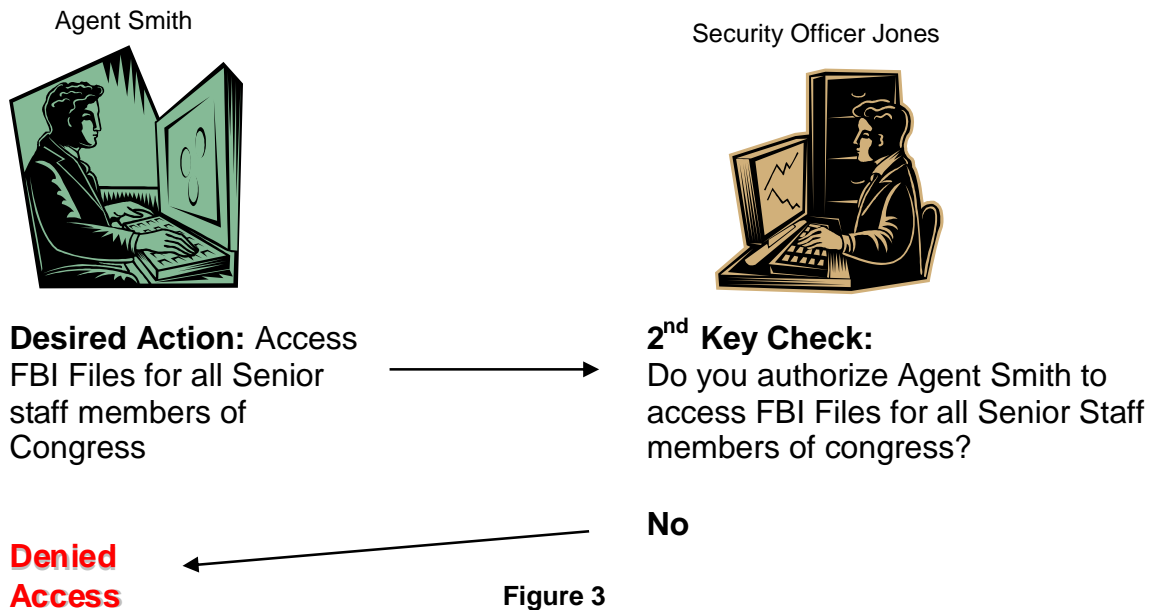
Electric power, water, gas, and oil systems today all depend heavily on systems used for remote monitoring and control known as **Supervisory Control And Data Acquisition (SCADA)** systems. SCADA systems perform critical functions in our nation's infrastructure. Malicious use of these SCADA systems could put the power or water systems out of service, causing enormous loss and inconvenience, and potentially cause system damage. Incorporation of MPA into SCADA devices would be valuable for the protection of our critical state and national infrastructure.

MPA could also be used to address privacy and security requirements such as those associated with electronic medical data and records handling as mandated by the Health Insurance Portability and Accountability (HIPAA) Act of 1996.

Citizen groups have expressed concern about possible privacy issues involved with any future implementation of Total Information Awareness systems designed to collect, scan and collate large amounts of data. Implementing a Multi-Party Authorization enabled policy that requires authorization from different government agencies before accessing select underlying individual data would be possible when using MPA. This could alleviate some of the privacy issues with information awareness projects. See Figure 3 on the following page.

Multi-Party Authorization

Some network or control system actions are too sensitive to allow just one authorized individual to initiate and perform alone. Security Policy can call on MPA to bring in a “second set of eyes” to protect and control access to sensitive data.



Implementing security policy using Multi-Party Authorization to protect against undesirable acts by the malicious insider greatly improves network or control system security. MPA delivers the added level of security while at the same time limiting its burden. The MPA architecture provides a workable distributed system for easy embedding, or addition to access or management systems.

Network and control systems implementing Multi-Party Authorization deliver a highly valuable pro-active security capability to protect systems from the undesirable acts of the inexperienced technician or malicious insider.

Multi-Party Authorization is patented. For more information visit the Engedi web site at www.engedi.net