

Secure Handling of Plug&Play Hardware in Enterprise Environments

- **New Software Module protects from risks by uncontrolled use of Plug&Play Hardware**

Oberursel, 12th December 2003 - The new Plug&Play module of SafeGuard Advanced Security gives back the control of Plug&Play Hardware in companies to IT administrators. Without this module, every user can easily connect new hardware to a computer and export sensitive data or import any kind of software. By the central control of Plug&Play devices, unauthorized data export by quickly removable modern memory media such as USB memory sticks, is efficiently prevented. Moreover, malware and non-licensed software no longer can be smuggled into the system.

In the past, drivers had to be installed manually to use printers or other hardware. By the modern Plug&Play technology, it is sufficient to connect the respective device to the computer to address it immediately. But what seems desirable under the aspect of a fast and simple use of computer -periphery, is a considerable problem for security-conscious companies and their IT administrators, that cannot be solved with the available functions of the operating system. Because just as easy as a printer or a mouse can be connected to a computer by a user, a bulk memory (e.g. in form of a USB memory stick or a USB hard-disk) can be connected to a computer and be used as well.

This way, a user is easily able to smuggle malware (viruses, Trojans, etc.), games and non-licensed software into the computer system of an organization which is normally well-secured, or misuse a Plug&Play hard-disk e.g. for the export of a complete customer database of a company.

By the new Plug&Play module of SafeGuard Advanced Security, the devices to be used by the respective users or user groups are defined in a central location. The implementation of the system is made easier by the fact that authorized devices can be registered both in a central location and by remote access to the user's workstation.

The central administration by means of the Microsoft Management Console (MMC) is completely integrated into the Windows Active Directory. By the integration into Windows standard- mechanisms, neither an additional training of the administrators or users nor an additional server is required. By a brief instruction manual, each administrator shortly is able to close this security gap efficiently.

The new Plug&Play software module will be available as of the middle of December 2003 separately or as component of SafeGuard Advanced Security. Additional information concerning the Plug&Play module and SafeGuard Advanced Security can be found under: www.utimaco.com/sgas.

A free demo download of SafeGuard PDA as well as additional information are available under: www.utimaco.de/sg-pda

Utimaco Safeware AG is one of the leading technology manufacturers of professional solutions for IT security. The security technologies and solutions developed by Utimaco Safeware protect electronic values of companies and authorities from unauthorized access and guarantee that business processes and administration procedures are binding and confidential.

The business unit Personal Device Security provides technologies and solutions to guarantee mobile security in the fields of strong authentication, including biometric procedures, encryption and integrity control. The products and solutions secure data in Terminal Server and Citrix environments, on PCs, Laptops and PDAs.