SafeGuard® Easy 4.0

The electronic fortress goes on-line

Technical Whitepaper

Utimaco Safeware AG

Table of Contents

SafeGuard® Easy 4.0 1

1 Preliminary Notes 4

1.1 Abstract 4

1.2 Document Information 4

2 Executive Summary 5

3 What's new in SGE 4.0? 6

3.1 Extended security functions: 6
3.1.1 Optional 2-factor authentication in the PBA (Aladdin eToken support) 6
3.1.2 TCPA/TPM support (IBM ESS chip) 6
3.1.3 Secure Hibernation (Suspend to Disk) support 6
3.1.4 Extended password rules 6
3.1.5 Event logging in the PBA and operating system 6

3.2 Improved administration: 7
3.2.1 Optional central administration database 7
3.2.2 Scripting interface 7
3.2.3 Secure Wake on LAN support 7
3.2.4 Challenge/Response Wizard for PDA 7
3.2.5 Windows Installer-based installation 8

3.3 Other new functions: 8
3.3.1 Integrated boot manager (TwinBoot) 8
3.3.2 Removable media encryption now also covers USB memory sticks 8
3.3.3 More flexible user management during pre-boot authentication 8
3.3.4 Demo version 8
3.3.5 Optional extendibility 8

4 New Central Administration Overview 10

4.1 Introduction 10

4.2 The SafeGuard Easy Server Machine 11

4.3 The SafeGuard Easy Administration Console 12
4.3.1 The Handling of Groups and Queues 13

4.4 The SafeGuard Easy Client Machines 13
4.4.1 Special Case: Offline Clients 14
4.4.2 Changing Clients from Offline to Online and vice versa 14
4.4.3 Migration of SafeGuard Easy Clients 15

4.5 Authentication and Encryption in Administration 15
4.5.1 Mutual Machine Authentication and Data Encryption 15
4.5.2 Key Handling 16

4.6 Remote Kernel Backup 16

4.7 Remote Administration 16

5 Two-factor Authentication / Token Support 18

5.1 Overview 18

5.2 User Authentication during Boot 18
5.3 User Authentication for OS Level tools 18
5.4 Token Issuing modes 18
5.5 Recovering from lost Tokens 19
6 PBA Enhancements 20
6.1 Secure Wake on LAN 20
6.2 Logging 21
6.3 Challenge/Response Dialog 21
6.4 Legal Notice 21
6.5 Enhanced Password Rules 21
7 SafeGuard Easy TCG (TCPA) Support 23
7.1 Introduction 23
7.2 Functions in Detail 23
7.3 Security gains by this approach compared to a normal SGE 4.0 24
8 Other new features 25
8.1 Automation API (Scripting Interface) 25
8.2 Demo Version 25
8.3 Removable Media Encryption Configuration Application 25
9 Summary 26
10 Appendix A 27
10.1 Technical Details 27
10.2 Additional Literature 28
10.3 Abbreviations 28
11 Further Information 30

1 Preliminary Notes

1.1 Abstract

SafeGuard® Easy (SGE) is a software security product that encrypts hard disks, external media, and floppy disks fully transparent to the user, it also includes strong user authentication at pre-boot time.

It is certified according to common criteria and has withstood all cracking attempts, because of its well-tested and robust key management, which has been over repeatedly examined and analyzed by its customers and professional certification offices.

Despite security functions being integrated into operating systems and machine hardware, SafeGuard Easy still delivers an indispensable security benefit as far as confidentiality and integrity of data are concerned.

SafeGuard Easy version 4.0 is the current evolution of SafeGuard Easy versions. Its new features are both reactions to customer requirements and architectural design decisions of Utimaco Safeware AG.

This document describes not only the new features of SafeGuard Easy 4.0, but also the detailed concepts and thoughts behind them. It addresses technical persons, who are especially interested in details of SGE 4.0. It is assumed, that the reader is generally familiar with the principles of boot protection, disk encryption and the product SafeGuard Easy up to version 3.20. For further or more general information on the subject, please take a look at the documents referred to in Appendix A, section 10.2.

1.2 Document Information

Version: 1.20.04 draft, last modification: 14.05.2004.

Author: SafeGuard Easy Team - Utimaco Safeware AG.

2 Executive Summary

In 2003 Utimaco Safeware AG celebrated the tenth anniversary of its most widely sold product (around 2 Million licenses): SafeGuard Easy.

It started in the year 1993 with SafeGuard Easy for DOS and its sister product Crypton for DOS. Over the years versions for newly released operating systems were added. Meanwhile there have been versions for MS DOS, MS Windows 3.x, MS Windows 95/98, MS Windows NT4, MS Windows 2000, MS Windows XP, and even IBM OS/2 up to Warp 4.

The basic approach and philosophy of SafeGuard Easy remained unaltered since 1993: To deliver invincible boot protection and data confidentiality using an approach that seamlessly integrates into the operating system and does not hinder the end users in their daily work.

Hundreds of different hardware platforms, BIOS systems, hardware configurations have been supported for many years. Utimaco is dedicated to provide the products to address the security needs mobile users in enterprise companies.

Despite the unchanged basic functionality the product has been constantly developed and evolved to fit perfectly into the changing enterprise infrastructure.

Interfaces to deployment and administration systems like Tivoli have been implemented in earlier versions, as well as tools for help desk integration, central administration and the ability to use service providers for rollout and support.

State of the art encryption algorithms are used by SafeGuard Easy and the best performance for initial encryption is provided. Transparent use and, uniquely in the market, ‘install & forget technology’ achieves perfect ‘power off protection’ with unbeatable TCO.

In this respect SafeGuard Easy version 4.0 continues perfectly the philosophy of its predecessors.

The commitment to integrate SafeGuard Easy into enterprise infrastructures is core in the concept for SafeGuard Easy 4.0. SafeGuard Easy 4.0 can be best described by mentioning its main design goals, which were:

(1) SafeGuard Easy 4.0 helps to reduce TCO further, without sacrificing any security and without introducing relevant organizational overheads (e.g. via the new Secure Wake on LAN function, the automation API or the remote management console).

(2) SafeGuard Easy 4.0 is easier to manage centrally in small and large environments.

(3) SafeGuard Easy 4.0 takes advantage of up to date security hardware, such as cryptographic USB token for user authentication and Trusted Platform Module (TPM chips).

(4) SafeGuard Easy 4.0 sets up secure communication between the central database and the SafeGuard Easy client machines without having to setup an elaborate PKI system.

(5) Further enhanced logging and auditing features give customers the chance to react on actions taken by a friendly user or a hostile attacker more efficiently.

(6) SafeGuard Easy 4.0 adapts to more types of client environments (TwinBoot functionality, Hibernation) and encrypts more classes of removable storage media (e.g. USB memory stick).

On the following pages the new features and concepts behind them are explained in further detail and put in the context of real-life environments.

3 What's new in SGE 4.0?

3.1 Extended security functions:

3.1.1 Optional 2-factor authentication in the PBA (Aladdin eToken support)

SafeGuard Easy can now be configured in such a way that only users with an appropriate Aladdin eToken can access the PC. Naturally, besides being used in pre-boot authentication (PBA), the token can also be used at operating-system level for other, certificate-based applications, via the PKCS#11 or CSP standard. In addition, the Aladdin token can now also be used by the SGE administrator to logon to the administration programs.

Users, who have forgotten their token, may get help from a central helpdesk, who can grant the user a defined period of time, within which he is allowed to do a token less logon, until he got a replacement token. The challenge/response helpdesk procedure is secure and ideal for mobile workers, as it doesn't require an on-line connection between client PC and helpdesk.

3.1.2 TCPA/TPM support (IBM ESS chip)

SafeGuard Easy is the first hard disk encryption product to use the security chips, specified by the Trusted Computing Group (TCG), that are nowadays integrated in modern laptops. Among other things, SafeGuard Easy uses these chips to secure the link between the client and administration server, and also to generate random numbers. Naturally, SafeGuard Easy's Secure Auto Logon (SAL or SSO) function can also be used for IBM's User Verification Manager, providing optimum integration in the ESS chip infrastructure.

3.1.3 Secure Hibernation (Suspend to Disk) support

It is especially users of mobile devices who most frequently avoid booting, instead simply "pausing" and later "restoring" their current work, since these options are provided by modern operating systems. In contrast to most other hard disk encryption products available, SafeGuard Easy now supports use of hibernation mode, even encrypting the generated image data in order to store it securely on the hard disk. Consequently, security is provided at all times, power consumption is reduced and users save time, compared to the normal boot procedure.

3.1.4 Extended password rules

Even in earlier versions, SafeGuard Easy offered a multitude of options for implementing special password rules in the PBA. The current version contains some additional options such as a configurable list of forbidden passwords, extended rules for special characters, password ≠ UID etc., providing even better functionality for implementing pre-defined corporate rules.

3.1.5 Event logging in the PBA and operating system

SafeGuard Easy now also logs events involving security, such as failed logon attempts, in the pre-boot phase, and later passes on these log entries to the Windows Event Log for evaluation. Alternatively (via an additional component) logs can be transferred to a central server, and evaluated there. Consequently attacks can be recognised more quickly and statuses can be diagnosed more easily.

3.2 Improved administration:

3.2.1 Optional central administration database

Past customers who have implemented central software distribution tools already know and value the ease with which SafeGuard Easy can be integrated in these applications for installing and distributing configuration files.

In addition to these proven options, SafeGuard Easy now includes a dedicated, central administration software package. This administers all installed SafeGuard Easy clients in a corporate network and also ensures the secure central distribution of configuration data to groups of clients, displays their current status, and acts as a central archive for kernel backups. The product itself can be installed using standard Windows Installer (MSI) mechanisms, independent of this central administration console. Options such as auto-registration, or the importing of offline clients, ensure that it can be integrated in all kinds of environments, regardless of size.

With the "Remote Administration" module, which is also available, it is possible to configure a specific individual client over the network.

3.2.2 Scripting interface

SafeGuard Easy now offers an Automation API for different administrative tasks such as generating new user accounts. Administrators can use this API in their own scripts (such as VBScript) to automate repetitive tasks, not only speeding them up, but also avoiding operating errors.

3.2.3 Secure Wake on LAN support

SafeGuard Easy's pre-boot authentication offers best-possible protection against attacks by hackers, since the key to the hard disk is not saved on it when PBA is active. However, there is also a need for maximum security when distributing software via Wake on LAN when active disk encryption is in operation, so SafeGuard Easy now provides new functions for that purpose.

With them the administrator can restrict the clients to a certain number of reboots without user interaction before pre-boot authentication is automatically activated again. If Wake on LAN mode is active, a user can logon in the normal way by pressing a hotkey and typing a password. If this hotkey is not activated in the pre-boot phase, the computer boots itself and the automatic software update can be carried out over the network. In this auto-boot state the computer is secured against local user login.

By this means, SafeGuard Easy provides an ideal compromise between security during booting and convenience for the administrator, unmatched by any other product.

3.2.4 Challenge/Response Wizard for PDA

SafeGuard Easy users who have forgotten their passwords or token quickly become productive again with the help of a central helpdesk. From now on, helpdesk staff can also carry out their work on a completely mobile basis, using a PDA (Pocket PC), so they are no longer dependent on having access to a PC.

3.2.5 Windows Installer-based installation

As the installation procedure is completely compliant with the current Windows Installer (MSI) standard it can be distributed and installed easily and efficiently in Windows networks.

3.3 Other new functions:

3.3.1 Integrated boot manager (TwinBoot)

Companies involved with the insurance sector are among those most commonly requiring a laptop's hard disk to be split into a private, unprotected partition, managed by the user, and an encrypted partition that is managed by the user's company. SafeGuard Easy now provides an integrated boot manager for this purpose, with which configurations of this kind, or similar ones, can be implemented easily and securely from one central point. In this way the company data remains protected and the user has absolute freedom on their private partition, even when it comes to choosing the operating system. In addition, if SafeGuard Easy is in use, there is no need to spend extra money on purchasing a separate boot manager application.

3.3.2 Removable media encryption now also covers USB memory sticks

SafeGuard Easy encrypts not only the entire contents of hard disks, but also the contents of removable media such as diskettes, or ZIP or JAZ disks. This allows the implementation of secure data medium exchange within the company, while simultaneously protecting the contents of mobile data media against unauthorised access. It also provides an effective way to prevent the unauthorised importing of data such as unlicensed software or viruses via removable media, since users without the appropriate authorisation cannot use plain text media.

The range of removable media supported by SafeGuard Easy has now been extended to include the current generation of Plug and Play memory cards (USB memory sticks), so they can also be used for secure data exchange.

In addition, it is now possible to temporarily switch encryption for an individual floppy drive or removable media disk drive on or off, separately from the others.

3.3.3 More flexible user management during pre-boot authentication

Many of the options available for user management in the PBA have been improved in different ways. For example, when a user is logging on, SafeGuard Easy can also display an additional message, specified by the administrator, concerning legal interests, ownership of the device, or similar.

3.3.4 Demo version

From version 4.0, SafeGuard Easy is also available as a fully-functioning demo version, to make it easier to evaluate. The only restriction is that the system password, which is pre-assigned, cannot be changed, and displayed in the PBA.

3.3.5 Optional extendibility

SafeGuard Easy is not a stand-alone solution. Benefiting from the wide range of Utimaco's product portfolio, the customer can extend SafeGuard Easy in many directions to meet their requirements. For example:

- A web-based helpdesk interface with connected Hardware Security Module (HSM) for key management, or biometric voice recognition via a VoiceTrust server, offer additional helpdesk options, of special interest in large-scale corporate environments.
- Transparent file and folder encryption guarantees that data for working groups remains confidential on the network or terminal server.
- The implementation of extended security guidelines, for example for access to PnP devices, exchangeable data media (CD/DVD) or certain file types, protects against unauthorised data export and import, and prevents computer viruses from being smuggled in.
- Single Sign On (SSO) increases user-friendliness and reduces helpdesk costs. It can be implemented on almost every password-based application, locally, on the web or on the Terminal Server.
- Small mobile devices such as Pocket PCs can also be protected just as efficiently using SafeGuard PDA, SafeGuard Easy's stable mate.

4 New Central Administration Overview

4.1 Introduction

SafeGuard Easy has always provided the possibility to be handled by third party central administration systems by means of configuration files created by the admin and shipped to the client via his software management tool.

As an optional alternative, SafeGuard Easy 4.0 now offers the functionality to centrally manage SGE client machines based on a dedicated central administration console, database and integrated transaction methods.

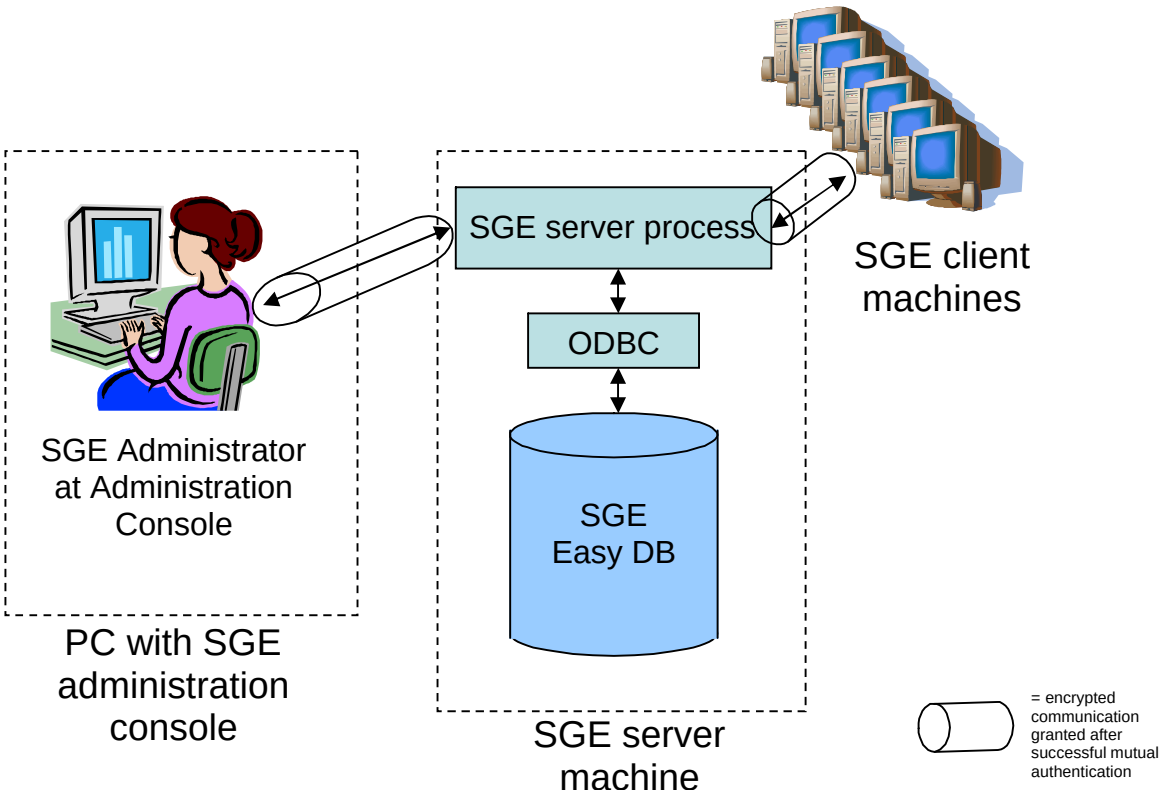
Utimaco Safeware AG took the decision to implement central administration functionality for 2 key reasons:

1. SGE client machines should be easily and centrally controllable, also for customers that do not yet a special third party software management tool like Microsoft SMS or NetInstall.
2. It should be as simple as possible to retrieve the actual settings and status information on any given SGE client machine.
   This is necessary in order to define a configuration change for a specific machine, to track progress and to monitor events centrally.

These goals are achieved by introducing a central data storage holding SGE configuration settings of SGE client machines and an administration GUI to control the database contents.

A typical installation consists therefore of three different major components:

- SafeGuard Easy client machine(s).
- The SafeGuard Easy server machine.
  This machine enables the SGE server process to schedule configuration changes / manage configuration data and the SGE database that contains configuration data for all attached SGE client machines.
- The SafeGuard Easy administration console to control the server.



The central SafeGuard Easy database holds all configuration settings of the SafeGuard Easy client machines. The SafeGuard Easy administrator uses the SGE administration console to control the DB contents. The SafeGuard Easy clients read configuration changes out of the SGE DB and report configuration changes back to the SGE server machine as soon as they are committed on the respective SGE client.
The communication with the SGE server machine is generally made through the SGE server process using an ODBC interface to give customers complete flexibility in the type of DB used.

All SGE related information transferred to and from the SGE server machine is encrypted.
→ Each SGE client machine has to authenticate itself based on asymmetric encryption towards the SGE server machine. During the process of mutual machine authentication a symmetric session key is generated and exchanged. All subsequent communication is then encrypted. The same is true for the communication between the SGE administration console and the SGE server machine.

4.2 The SafeGuard Easy Server Machine

A very important component of SGE 4.0's central administration concept is the SGE server machine, on which the SGE server process and the SGE database reside. It's main purpose is, to collect and maintain all SGE client related configuration data and distribute configuration files to clients as specified by the administrator.

By design, the SGE server process and the SGE database can be located on different machines, but we will not discuss this topic here.

The SGE database holds the following information on a per-client basis:

- Current settings (all, excluding passwords[1])
- Current queue of configuration files to be executed
- Queue Type (offline, online, online w/push)
- RSA Public key
- Machine Unique ID (GUID created during registration)
- Machine's network name
- BOOLEAN array of machine group memberships

Except for the case when queues are operated in "push" mode, the server is basically passive and waits for clients or the administration console to call it up.

The queues retain information about configuration files already executed, pending execution, and files waiting to be executed in the future. The queue can hold a limited number of elements; this number can be configured during initial server setup. This limit is simply a precaution with regards to required storage space. Because of this limited number of elements it can only retain a limited amount of historical data. If all entries are used, the oldest entries are overwritten if new requests are put in the queue. The historical data basically is the status of the respective configuration file (successfully executed, failed, pending, waiting) plus the time/date of the last status change.

The queue entry states in detail:

- **Successfully executed**: The file was executed on the client and the server has received a notification of successful completion.
- **Failed to execute**: The file was executed but the client aborted execution due to an error and notified the server. This puts the queue on hold until this entry is either removed or rescheduled.
- **Pending**: File was sent to the client but no notification of success or failure has been received yet.
- **Scheduled**: This file is waiting to be sent to the client. This will happen when the client contacts the server or if the queue goes to active (push) mode.

4.3 The SafeGuard Easy Administration Console

The administration console is simply a front-end program that establishes a special administrative connection with the server. It can be run on any computer on the network. Only one administrative connection is allowed at any one time to ensure database consistency. If the connection is in use, the server denies further administrative connections and notifies the administrator that the administrative connection is already in use. No elaborate setup is necessary for running this component; basically the application must be installed on the machine and the server's network name must be defined.

A 'normal' SafeGuard Easy installation is required for running the console.

[1] Storing client user passwords in the central server is not necessary for practical life and would unnecessarily introduce additional security issues.

The console is used to

- query machine or queue states,
- control queue operations,
- and to call on the existing Configuration File Wizard to create the configuration files to be deployed.

The console submits a configuration file to the server, along with instructions on what to do with it. The administration console can be set up whenever convenient. It is not required for initial deployment.

4.3.1 The Handling of Groups and Queues

The console basically manages machines or collections thereof. Since there will usually be collections of machines sharing the same settings and usage scenarios, it is possible to organize them into groups. These groups of machines do not implement any hierarchy, so a group cannot contain other groups. But: Every machine can be member of several groups at once. There is no limit to how many groups a machine can belong to.

This mechanism allows for efficient application of a change configuration file to a large number of machines sharing specific properties.

Normally, the changes are executed when the client contacts the server the next time. It could probably take days until the desired changes have been effected on all machines selected. If a more timely execution is required, the server can be forced into active ("push") mode on a per-machine basis. In this mode, the server tries to contact the machine(s) in question directly and will continue to do so until the queue associated with this machine is either empty or the execution of one of the scheduled configuration files fails. In both of these cases, the queue will go back to standard (passive) mode and remain so until forced active by the administrator again.

4.4 The SafeGuard Easy Client Machines

The clients are basically set up as in earlier versions of SGE. The one big difference is that the client can be supplied with the UNC NETBIOS name (e.g. "\\SERVER1") or IP address of a server to contact. If such a server name is known, the client will contact the server and register itself after installation.

At this time the RSA key pair and GUID are generated (if the machine contains an active TPM e.g. the IBM ESS chip it is used for this operation). The client then reports its configuration, GUID, public key, and network name to the server. In addition, the configuration file used for the install (if there is one) is sent to the server and filed as the initial configuration for this client. This file can be used as the base configuration file in the wizard to make creating future change files easier. In the course of this same exchange, the client receives the server's public key.

From this time on, the client can be centrally managed. In case of local changes (e.g. performed by an SGE administrator interactively on an SGE client machine) the client will again report its current configuration to the server to keep the database up to date.

When a SafeGuard Easy client gets uninstalled it must report that fact to the server. The SGE server will then delete the machine's record from the operative part of the database.

If the SGE client is not supplied with a SGE server name it will behave as earlier versions did. Deployment and maintenance schemes developed for earlier versions will continue to work with only minor changes – the central server is not a mandatory part of a SafeGuard Easy 4.0 installation!

4.4.1 Special Case: Offline Clients

Offline clients are computers that are known in advance to be disconnected from the network most of the time (or never connected at all) but still subject to central administration. Clearly a network-based central administration cannot cope with such a situation. In order to handle this, the client is supplied with a special reserved "server name" which activates an alternative mechanism for communication.

For such a machine, installation is performed as usual, including key and GUID generation. But instead of registering with the server directly, the client puts the data it needs to send to the server in a special "result" file. The result file can contain registration data (at initial installation time only), the configuration report, and configuration file execution results (success or failure). This result file can then be transmitted to the administrator using any transport mechanism that seems convenient.

The administration console program is able to import these result files. If the result file contains a registration record the console creates this machine in the database and marks it as being "offline". This offline flag mostly controls queue management for this machine: At strategic points during the administrative session (e.g. whenever the administrator wants to close the console) a check is performed to see if there are any waiting files in queues marked "offline". If such queues exist, the console will offer to write a "request" file for each client affected. The administrator can then have the file written or defer it to a later time - a request file can well contain more than one change configuration file. This is to allow the administrator to optimize the cumbersome manual data exchange process while ensuring the change files are still executed in proper sequence.

When a request file is successfully written, the change files included are marked "pending" in the server queue to prevent them from being included in later request files.

The user of the client machine will have to import the request file manually, the client will (due to the reserved server name) create a result file, and the user must send the result file back to the administrator, who then again imports it to the database. This import refreshes the current configuration record for this client and also changes the status of the relevant change files in the client's queue.

While an offline client does not try to contact any server, the local agent is still listening for possible connect requests from a server. This is necessary for the transition between online and offline states as described in the next paragraphs.

It is important here to understand that no clients become offline clients automatically – only the administrator can define if a client is an offline client or not (default). A client that for some reasons (e.g. network failures, vacations, business trips) cannot reach its server is not an offline client, and cannot automatically become one. The client will simply remember the connection failure and try again at the next boot until it succeeds (or is explicitly told to become an offline client).

Likewise, the server does not automatically make a client an offline client just because it is told to contact the client and fails to connect. The server will just retry periodically until it succeeds or is told to stop.

4.4.2 Changing Clients from Offline to Online and vice versa

An offline client can be migrated to online status by modifying the client's queue operation mode. If the server doesn't already have a network name for the client from its result files, this name must be supplied. There must be no pending request or result files at this point. The server can then actively try to contact the client in question, passing a "set new server name"

command in the process. This command sets a new server name on the client. Upon successful completion of this request, the server can change the queue mode from offline to online.

Going offline is handled in much the same way. Again, a "set new server name" command is sent to the client, specifying the already-known specially reserved "server name". Upon successful completion, the queue goes from online to offline. Again, there must be no pending operations when the queue mode is switched.

To allow for situations where network-based communications become unavailable unexpectedly, the administrator can specifically force the console to export a request file for a client, even if this client is not a designated as an offline client. In much the same way, a result file can be imported for such a client, if available. This ensures that e.g. the transition to offline client can be handled gracefully even if a computer designated for central management suddenly becomes unreachable via the 'normal' network.

4.4.3 Migration of SafeGuard Easy Clients

Migrating existing client installations to the new release is done just as it was in previous versions. During migration the client must be supplied with a server name and the SGE network agent component, if registration with a central server is desired. At the next possible time this migrated client will auto-register with the server.

Note that the SGE network agent must be installed in order to set up a connection between the workstation and the central administration server. This component is not needed, if SGE is managed in the 3.x style via config files and a software distribution tool.

4.5 Authentication and Encryption in Administration

One of the design goals of SafeGuard Easy 4.0 was to reduce TCO without sacrificing any security and without introducing big organizational overheads. This section explains how this was achieved in terms of authenticating machines and encrypting data during transfer.

Prior to version 4.0, SafeGuard Easy did not concern itself with securing any network connection, because the product was strictly stand-alone and configuration data was transferred only in encrypted configuration files. With version 4.0 this changes slightly. Now configuration data is transferred between the SGE administration console and the SGE server machine and SGE client machines can retrieve configuration data online from a central database or configuration data is reported back to the central database.

This raises the issue of how to correctly authenticate a SGE client machine requiring central service and how to protect (=encrypt) data on transfer.

SafeGuard Easy 4.0 solves these security critical tasks by introducing the concepts of ‘mutual machine authentication’ and ‘data encryption’.

4.5.1 Mutual Machine Authentication and Data Encryption

Encrypted communication only makes sense after you have successfully authenticated with your communication partner. Why should you go through the hassle of encrypting data, if you aren’t even sure, who you are talking to or if the person you’re talking to is really who he/she claims to be? Hence, SafeGuard Easy 4.0 first tries to authenticate the other communication partner before it exchanges any security relevant information.

In the technical implementation both aspects (authentication & encryption) can be cleverly combined. Authentication is made by making use of the RSA key pairs of both involved parties.

After the successful mutual machine authentication a randomly generated symmetric encryption key is exchanged, which is then used for encrypting configuration data in transfer.

4.5.2 Key Handling

Mutual machine authentication and data encryption are achieved using a hybrid encryption approach with asymmetric and symmetric encryption.

Key Creation and Distribution:

For mutual machine authentication RSA is used with 1024 bit keys.

For bulk data encryption RC4 is used with a 128 bit key. The life-cycle of this key can be defined. However, for every new connection a newly generated random key is used anyway. As a typical session between a SGE client machine and the SGE server transfers only 1KB – 3KB of data. A new random key is used for each session. In addition, the transferred configuration file is encrypted by itself as is has been all the time in previous SGE versions.

SGE 4.0 uses RSA key pairs and not X.509 certificates to implement mutual machine authentication. This decision was made, as SafeGuard Easy 4.0 should be installable, configurable, and last but not least usable without forcing the customer to setup and maintain an elaborate PKI system first. This approach earns the benefits of PKI based systems without overloading a company with the requirement to provide a full blown PKI infrastructure.

Therefore any SGE 4.0 client machine creates its RSA key pair during the installation of the SGE 4.0 client software. When then the SGE client machine contacts the SGE server machine for the very first time to auto-register it exchanges RSA public keys with the SGE server machine. The server gets the RSA key of the client and the client receives the RSA public key of the SGE server machine.

Both machines store the public key of the other involved party and from this time on, they can mutually authenticate each other.

Optionally this RSA keypair generation and usage can be handled by a Trust Platform Module (TPM) like the IBM ESS chip for example. This adds hardware security for the key store but is slower than a pure software solution.

4.6 Remote Kernel Backup

The local SafeGuard Easy Backup Agent can be configured to regularly back up the kernel to the server. The time related settings are similar to those used by the Emergency Wizard of today's SafeGuard Easy versions. In consequence, a machine can be configured to run either the Emergency wizard, or the (silent) backup agent, or neither.

If the local agent is configured to regularly back up the SGE kernel to the server, then there's always an up-to-date kernel backup file to help the SGE client machine recover from Master Boot Record (MBR) or SGE kernel corruption.

4.7 Remote Administration

Independent from the central administration server, SafeGuard Easy 4.0 offers the remote administration console. This is basically the normal administration program shipped with earlier versions but with the additional capability to connect to remote machines in addition to the local system. The administrator can establish a secure one-to-one connection to a remote machine and modify settings directly.

While the central administration server is useful to deploy configuration to large groups of SGE workstations, the remote administration function is especially useful for smaller networks or special tasks.

The remote administration program can be used both as a standalone tool and an integral part of the administration console. As a standalone tool (i.e. run without any runtime parameters), the program enumerates any machines it finds on the network dynamically. Optionally, the remote administration program accepts the network name of a machine as a runtime parameter. If called in this way, the program connects to the designated target machine directly without trying to look for other machines on the network.

If any encryption/decryption process is running on the targeted machine, the progress is shown within the administration program.

Customers with smaller networks, where it is the default that machines are online, might even want to use remote administration as the only central part. The IT security administrator could simply connect to the respective SGE client machine to modify its security settings.

5 Two-factor Authentication / Token Support

5.1 Overview

Besides the traditional method of authenticating a user via the credentials UID and password, and allowing automated logon (SAL) to a smartcard at operating system level, as introduced in SGE 3.20, version 4.0 also allows the user to use a hardware token (Aladdin eToken Pro) for authentication at PBA time.

Using the token at operating system level for OS logon and desktop lock upon token removal requires the combination of SGE with the corresponding base module of SafeGuard Advanced Security, which offers the proper smartcard management and GINA integration.

SafeGuard Easy has been certified to be Aladdin eToken enabled, which guarantees interoperability of SGE with other eToken enabled applications.

5.2 User Authentication during Boot

SafeGuard Easy can be configured to offer either normal password based logon, optional token logon or token mandatory mode. Most commonly used will likely be the optional token logon, where the admin can define for each user account separately whether a token is required or not.

The token mandatory installation mode will require token logon without exceptions, in this case there is also no recovery option for lost tokens. To gain access again, one has to have a properly issued replacement token. So this option is likely to be used in special high-security environments only.

Token logon happen directly at pre-boot authentication level. The user inserts his token into the USB port and enters the token PIN. This will unlock the protected storage area of the token and SGE can read the necessary credentials to log the user on to the harddisk and continue booting.

5.3 User Authentication for OS Level tools

Of course, SafeGuard Easy does not only support PBA based user authentication with token, but also all SafeGuard Easy administrative tools may now be used with a Token to authenticate to them.

5.4 Token Issuing modes

SafeGuard Easy offers a choice of different options to enroll the necessary token credentials. The administrator can define which suits best the company demands and environment.

Case 1: "Token issuing" = USER

If token support is activated, the user is prompted at next PBA logon (after specifying the SGE UID), to insert a token and present the token PIN. If the token does not contain a proper UID/password for this SGE client, the user is asked to enter these credentials. Once they are correct, they are stored on the token for future use and the user is logged-on to SGE (i.e. the system boots up).

At next logon, the user will be prompted for the token and the token PIN. If the token is empty or does not contain the correct credentials, the user is asked to present the correct UID/password which are, once they are correct, subsequently stored on the token and the user is authenticated (the system boots). This implies that SGE will create a proper data field for the SGE data on the token if it does not exist yet.

This is the most simple and straightforward roll out mode for token logon, since just empty tokens with default PIN need to be sent to users without the overhead of a central personalization process. Of course SafeGuard Easy will also force the user to change the token default PIN to a personal value along with the issuing of the SGE credentials.

Case 2: "Token issuing" = HELPDESK

If token support is activated, the user is prompted at next logon (after specifying the UID), to insert a token and present the token PIN. If the token does not contain a proper UID/password for this SGE client, the user is asked to call the helpdesk. The helpdesk shall be able to set via challenge/response a flag that allows the local user to set a new SGE UID/password to his token (see case 1).

Setting this flag means more work for the helpdesk and more effort for the user, but prevents, that more than one token is issued for this machine without central notice.

Case 3: "Token issuing" = CENTRAL

If token support is activated, the user is prompted to insert a token and present the token PIN. If the token does not contain a proper UID/password for this SGE client, the token is rejected and a different token is required for logon.

Setting this flag means, that the tokens have to be issued by a central administrator. Centrally preparing the tokens has the advantage, that the end-user does not need to know the SGE account stored on his token, they just know their personal token PIN. This allows implementing special scenarios e.g. where a pool of users shares a pool of notebooks and just log-on with a "role account".

5.5 Recovering from lost Tokens

If a user forgets his token PIN or looses his token (and the PBA Installation mode is not "Token mandatory"), he has the chance to perform a challenge/response process with his associated helpdesk. The helpdesk can then grant him the possibility to define a new SGE password and allow a limited number of token less logons. This number relieves the user from having to perform a challenge/response process every time until he gets a replacement token as this may take a while if the user is e.g. currently on a business trip when he lost the token.

6 PBA Enhancements

Apart from the new features ‘central and remote administration’ the other major improvements to SGE at 4.0 are those within SafeGuard Easy’s PBA environment.

6.1 Secure Wake on LAN

Up to now SafeGuard Easy with activated PBA and Wake on LAN (termed WOL hereafter) could not coexist peacefully.

To be able to explain this in an easy way a short definition of Wake on LAN is given:

> *Wake on LAN is a technology that allows a network professional to remotely power on a computer or to wake it up from sleep mode. By remotely triggering the computer to wake up and perform scheduled maintenance tasks, the technician does not have to physically visit each computer on the network.*

It is pretty obvious, why this feature cannot coexist peacefully with SGE. The machine could still be remotely powered on or woken up, but the real job could not be performed, because the SGE client machine would simply remain in the PBA screen and wait for valid SGE credentials to be keyed in. Since the operating system would not boot in this case, a network connection could never be established which would be needed to perform the scheduled maintenance tasks. The only way around so far has been, either to not to use WOL or to not use PBA authentication.

Nevertheless, SGE 4.0 provides a solution for such situations in the best possible way:

The SGE 4.0 feature ‘secure WOL’ is based on the assumption that in big enterprises, product maintenance tasks which are performed overnight (via WOL) need decent preparation by the IT department anyway. This means that they do not happen ‘out of the blue’, but are probably scheduled for a certain point in time.

Immediately before this point in time is reached, SafeGuard Easy 4.0 can be given an administrator-defined number of reboots without PBA screen. This machine could then be woken up by WOL and would in fact boot up to the Winlogon.

Utimaco recommends granting one boot without PBA more than is technically necessary. This is to allow the system to cope with unforeseeable problems that might cause the machine to reboot once more than planned. Every WOL boot will reduce a SGE internal WOL counter by one and reactivate the PBA if ‘zero’ is reached.

Important: The goal here is to ensure that after a few reboots the system goes to secure operation mode again. To prevent unauthorized users from tampering with the system when it auto-boots in WOL mode, the GINA component will block further interactive access to the system. Maintenance logins over the network will be possible.

Because the system should remain accessible to authorized users, it is possible to perform the standard emergency login which is also available when the PBA is turned off. When in WOL mode, the kernel will clearly state the fact that it is in WOL mode. Thus SGE users will know about this and they will be aware that the system is in a special maintenance mode.

Alternatively one could think of a "PBA timeout" method, where the PBA appears at boot time and ask the user for a password, but continues to boot after a while if no user enters anything. Although this looks as a nice combination of the benefits of PBA and Wake on LAN, it is not. This approach suggests a false impression of security. In order to be able to boot unattended after a timeout, the key information has to be store somewhere and so the security in this approach would be identical to a deactivated PBA. This is the reason why Utimaco has chosen

not to implement such a timeout solution but created the previously described secure approach instead.

6.2 Logging

SafeGuard Easy now contains a reserved space for a log file in its PBA security kernel. This log receives all security relevant events, such as logins, failed login attempts, password changes, virus alerts, etc.

The logged events arel be forwarded to the Windows event log (or optionally to other locations in combination with SGAS Base module) after the next successful SGE logon and machine boot, thus allowing the administrator to even monitor events that at pre-boot on the clients.

6.3 Challenge/Response Dialog

The Challenge/Response input in PBA is improved to include basic editing capabilities. So if the response code is rejected, users can review and, if necessary, change their input without having to re-enter the entire response.

SafeGuard Easy also offers additional challenge/response options such as:

- a Pocket PC version of the helpdesk application (response code wizard) so that helpdesk personnel becomes more mobile and is not required to use a PC
- an add-on helpdesk Web interface with cryptographic, tamper protected hardware server that creates response codes on request of the helpdesk personnel.
- an add-on biometric voice recognition server from VOICE.TRUST, that can perform the challenge response process with a user fully automated 24 hours a day.

6.4 Legal Notice

This is a text box shown before login that is centrally defined by the administrator. The text typically is a legal notice to the user or finder of the PC where to return this machine to and that is not allowed to tamper with it.

The box must be confirmed by the user before the system continues operation.

6.5 Enhanced Password Rules

SafeGuard Easy 4.0 contain further enhanced password rules that are in addition to the comprehensive rules supported in previous SGE versions.

New rules include:

- Minimum number of characters, digits, special characters etc. that must be contained in a password can be defined independent from each other.
- Password must not be identical to user ID
- List of undesirable passwords
- Minimum user ID length for templates
- Minimum password age
- Allow / disallow password change

Existing password rules (already in SGE 3.20):

- Validity period
- Minimum length
- Password history (user may not use last *n* passwords again)
- User must change password at next logon

7 SafeGuard Easy TCG (TCPA) Support

7.1 Introduction

The Trusted Computing Group (TCG), which is a group of international manufacturers, has set itself the aim of improving the security and trustworthiness of modern computer platforms and operating systems. The core is the Trusted Platform Module (TPM), a cryptographic hardware chip that is integrated in the motherboard, and is used to generate and save keys securely and to generate random numbers.

Similarly to smartcards, the TPM also requires suitable software to make full use of its capabilities. With its base functions the TPM can manage keys securely, and make them available for use by users and applications, via standard means such as Cryptographic Service Providers (CSPs), but does not encrypt operating system or user data itself.

Computers equipped with a TPM also require the efficient basic protection of a transparent hard disk encryption tool such as SafeGuard® Easy to protect the saved data against loss or theft of the device.

Encryption solutions for individual users (SafeGuard® PrivateDisk) or working groups in a network (SafeGuard® LAN Crypt) are also typical applications for the X.509 certificates used in this new hardware technology (TPM).

In addition, with the use of the TPM, entirely new security concepts, such as machine binding, can be created.

Today, IBM already equips many of its laptops and desktop PCs with a TCG-compliant security chip. IBM calls the system ESS (Embedded Security Subsystem) and the associated client software "Client Security Software" (CSS). IBM is for a long time the leading supplier of laptops and desktops with TPM.

Utimaco Safeware is member of the Trusted Computing Group since 1999 and now the first professional supplier to upgrade IBM's base solution by adding ESS-enabled hard disk encryption and additional security products. These show how users can gain the best-possible benefits from "security in hardware" while retaining complete control over their infrastructure. So you get a comprehensive and consistent security system.

7.2 Functions in Detail

The SafeGuard® product range supplies proven and certified security on almost all Windows-based computer platforms, with or without TPM.

A modular system can be extended from the basic protection provided by the transparent encryption of an entire hard disk, through virtual disk drives for individual users to local or network-based file and folder encryption for workgroups.

Working together with User Verification Manager
After pre-boot authentication by SafeGuard® Easy, users are also automatically logged on to the TPM, if required (SSO). Here SafeGuard® Easy works together with IBM's User Verification Manager (UVM). Thus, the user is not delayed in their work by having to enter additional passwords.

Machine binding
As a possible extension to SafeGuard® Easy, the "machine binding" functionality of SafeGuard® Advanced Security can be used to bind an encrypted hard disk to a particular TPM, which means that if the hard disk were stolen, it would be unreadable in another computer.

Key generation/authentication
SafeGuard® Easy 4.0's central on-line administration function uses TPM-generated RSA keys for authentication between the client and server. In this way a unique binding is set up between the configuration and a machine. The chip is also used to generate random numbers (key values).

Certificate-based access control
Other products in the SafeGuard range such as SafeGuard® PrivateDisk or SafeGuard® LAN Crypt 3.x make use of the functionality provided by the TPM/ESS chip by using ESS user certificates for logon to encrypted areas

Modular security solution
The different SafeGuard® modules can be combined to meet each customer's requirements. They offer efficient data security functions which can be managed centrally, and require scarcely any user training.

They use modern security hardware such as smartcards or ESS, but do not require it as a prerequisite, to provide a uniform security solution, even in heterogeneous environments.

SafeGuard® products and TPM (ESS) technology achieve data security at the highest level.

7.3 Security gains by this approach compared to a normal SGE 4.0

- The RSA secret key is not only protected by operating systems means, but cryptographically by the TPM chip. → A RSA secret key, which is protected in this way, can be regarded as absolutely trustworthy.
- As the RSA key pair is bound to the machines hardware – to the ESS integrated security chip and therefore to the motherboard -, mutual machine authentication reaches a new level:
  Without TCPA/ESS mutual machine authentication can only guarantee that a certain hard disk that holds the RSA key files gets access or not. With TCPA/ESS it is now possible to really grant access or not to an entire machine – not only its hard disk.
- TPM generated keys for harddisk encryption are based on a true hardware-noise random generation and therefore reach the highest degree of "randomness" that is achievable.

8 Other new features

8.1 Automation API (Scripting Interface)

The purpose of this is, to provide a programming interface for SGE to customers and project teams that

- is easy to use
- remains stable across versions
- is robust against improper use
- protects the security system

in order to implement customer-specific adaptations and repetitive administrative tasks without requiring modifications to the core product.

This interface allows access to a subset of the SGE security system only. Supported functions are (amongst others):

- Get version: returns, whether SGE is installed and its major and minor version
- Get current SGE user
- Get Drive state: Returns type, encryption state, volume label of a given drive. Additionally, the media state is reported, i.e. if a medium is inserted or not.
- Set Wake on LAN boot count: Sets the counter that controls how often the system will boot in WOL mode. Setting the counter to zero disables Wake-On-LAN boot and reverts to normal configured login behavior.
- etc.

8.2 Demo Version

The demo version of SafeGuard Easy 4.0 may be used by an interested individual so that he/she can get a feeling about the capabilities of SafeGuard Easy.

However, the demo is limited in functionality, so that it does not provide real security. The limitation is implemented by a fixed and non-changeable password for the SGE user SYSTEM. Additionally this password gets displayed in the PBA screen.

Therefore the product can be tested completely, but still provides no security at all as anyone can logon to the machine.

8.3 Removable Media Encryption Configuration Application

The only icon currently on the System Tray is from SGECRYPT, which is a little tool used to toggle floppy or device encryption statuses. The drive icons in the Windows Explorer reflect now the current state of the drive (encrypted or plain). In addition, there is now a context menu item or a property page to switch encryption for these drives individually. This replaces the current global removable media encryption switch in SGECRYPT.

Please note that with SGE 4.0 it is possible to switch the encryption state in both drive specific and media type specific fashion. Changes to the encryption state using this menu and/or the property page are temporary and are not available for hard disk partitions.

9 Summary

The main focus of SafeGuard Easy 4.0 is to (further) reduce TCO without sacrificing any security and continue to meet the needs of large organizations to carefully manage their overheads.

As far as central administration is concerned SafeGuard Easy 4.0 is an evolution of the configuration file concept of earlier SafeGuard Easy versions.

Additional significant enhancements like the two factor token authentication, TPM support, the secure Wake-on-LAN support or the enhanced auditing and scripting functionalities ensure up-to-date security for modern environments.

SafeGuard Easy adds a lot of features that make life easier, more predictable and even more secure. Customers can choose, whether they want to use the new concept or stick to their existing and tested deployment scenarios.

SafeGuard Easy is the ideal basic protection system for all computers. The SafeGuard product family extends this basic protection by providing modules for other application areas and can therefore provide a tailor-made security platform that grows along with your needs.

10 Appendix A

10.1 Technical Details

[System requirements]	
Hardware	PC with Intel Pentium or compatible processor
Operating system	Microsoft Windows XP / 2000 Microsoft Windows 2003 Server Standard Edition
Network	All Windows-supported networks
[Interaction / technical data]	
Third-party suppliers	SafeGuard® Easy is compatible with all typical software distribution systems (MSI packets). Optional fully-automatic, biometric challenge / response helpdesk via VOICE.TRUST Server.
Additional Utimaco Safeware products	**SafeGuard® Advanced Security** modules as add-ons to support other smartcards, central auditing, Multi- Desktop, SSO, PnP management, Application Specific Access Rights etc. **SafeGuard® LAN Crypt** for File/Folder encryption. **SafeGuard® Easy Web Console** for Challenge / Response Helpdesk, with CryptoServer 2000 Hardware Security Module.
Encryption	AES (256 and 128 bit), Rijndael (256 bit), IDEA (128 bit), DES (56 bit), Blowfish-8/16 (256 bit), Stealth-40 (40 bit), XOR (64 bit).
Smartcards	Aladdin eToken Pro for user authentication at pre-boot level. eToken via PKCS#11/CSP interface can also be used for other applications. Other types of smartcard can be integrated via PKCS#11 at operating system level.[2]
TPM modules	Integration of security chips that meet Trusted Computing Group (TCG) specifications for: Machine binding[2] of disks, authentication between clients and administration servers, as well as for hardware based key generation. Currently tested for IBM ESS.
Certification	• Common Criteria EAL1 (EAL3 exp. in Q2/2004) • FIPS 140-2 (in evaluation) • Aladdin eToken enabled
Special features	• pre-boot authentication before the operating system starts • allows a combination of (up to 8) bootable operating system partitions that are either encrypted or not encrypted • encryption of removable media (diskette, ZIP, JAZ, USB memory stick) • supports hibernation (Suspend to Disk)

[2] Also requires a SafeGuard® Advanced Security module.

10.2 Additional Literature

Whitepaper – SafeGuard® Easy - The electronic Fortress

Whitepaper – SafeGuard® Easy – Cost and administration advantages

Whitepaper – SafeGuard® Easy – Challenge/response advantages

Whitepaper – SafeGuard® Easy - Automated 24/7 Emergency Help Desk

Whitepaper – Evaluating computer risks for mobile users

Whitepaper Intel – Secure Mobile eClient – IBM Websphere + SGE/SG PDA

10.3 Abbreviations

CAPI	(**C**ryptographic **API**): Microsoft Crypto API, e.g. used by CSPs
CSP	(**C**ryptographic **S**ervice **P**rovider): Software module in the sense of a driver that allows applications based on the Microsoft CryptoAPI to access cryptographic devices such as smartcards.
ESS	(**E**mbedded **S**ecurity **S**ubsystem): IBM's TCPA specifications compliant hardware based security subsystem
GINA	(**G**raphical **I**dentification a**n**d **A**uthentication): Interface defined by Microsoft which controls the desktop and login to Windows NT/2000/XP.
GUI	(**G**raphical **U**ser **I**nterface)
MBR	(**M**aster **B**oot **R**ecord): The first sector on a hard disk holding the MBR loader code and the partition table. SafeGuard® Easy modifies the MBR and uses it to get started as the first application during machine boot.
PBA	(**P**re-**B**oot **A**uthentication): Method used by SafeGuard® Easy to authenticate a user after power-on of the computer, before any operating system is booted (which in fact resides already on some, by SGE encrypted partition). This provides maximum security and prevents attacks to the file system from outside e.g. via bootable CD-ROMs etc.
PDC	(**P**rimary **D**omain **C**ontroller): in Windows NT domains.
PIN	(**P**ersonal **I**dentification **N**umber): Sort of password that identifies the user. This term is usually used in connection with smart cards, whereas the term "password" is used for the same thing, if it is provided to some software application (e.g. Operating Systems).
PKCS#11	(**P**ublic **K**ey **C**ryptography **S**tandard): Platform independent cryptographic token interface standard worked out by RSA Laboratories, used by applications like Netscape to access cryptographic devices like smartcards.
PKI	(**P**ublic **K**ey **I**nfrastructure): Applications and infrastructure for the issuing and administration of X.509 certificates.
TCG	(**T**rusted **C**omputing **G**roup) - see TCPA.

TCPA	(**T**rusted **C**omputing **P**latform **A**lliance) – see http://www.trustedcomputing.org.
TPM	(**T**rusted **P**latform **M**odule): defined by TCPA - secure HW module usually integrated on a machine's motherboard.
SGE	(**S**afe**G**uard® **E**asy): Transparent, sector based hard disk encryption product from Utimaco.
SAL	(**S**afeGuard **A**uto **L**ogon): A functionality of SafeGuard Easy that performs an automatic logon of the logged-in SafeGuard Easy user into Windows.
TCO	(**T**otal **C**ost of **O**wnership): TCO is a type of calculation designed to help consumers and enterprise managers assess both direct and indirect costs and benefits related to the purchase of any IT component.
VPN	(**V**irtual **P**rivate **N**etwork): Method to encrypt network traffic on low-level IP packet layer, ensuring confidentiality of transferred data over public networks (i.e. the Internet) to those participants who share the proper key material.
WOL	(**W**ake **o**n **L**AN): Wake on LAN is a technology that allows a network professional to remotely power on a computer or to wake it up from *sleep mode*. By remotely triggering the computer to wake up and perform scheduled maintenance tasks, the technician does not have to physically visit each computer on the network.

11 Further Information

If you would like to find out more about mobile security products, please contact your nearest Utimaco Safeware distributor or visit our website:

http://www.utimaco.com

Utimaco Safeware AG

P.O. Box 20 26

D-61440 Oberursel