



Microsoft Deutschland protects data on mobile devices with SafeGuard® PDA

Profile

Microsoft Deutschland GmbH

Microsoft is the world's leading supplier of software, services and Internet technologies for use in companies and at home. Microsoft Deutschland GmbH, founded in 1983, is the largest European subsidiary of the US based Microsoft Corporation, today employing about 1.800 staff.

Industrial sector

Information technology

Region

Germany

Field of application

700 mobile end devices based on Windows Mobile 2003 for sales, consultation and management, of which 330 are MDAs (Mobile Data Assistants) with additional telephone functionality.

Utimaco solutions

SafeGuard® PDA Enterprise Edition

Implementation

Utimaco Safeware, Germany

Features

Perfect protection for the data on Pocket PCs against being accessed by unauthorised people through

- secure authentication components
- secure encryption components

Optimum protection against unauthorised accesses for corporate data and applications on Pocket PCs and on external memory media.

Central administration and simple software distribution over the network: no need for the user to be involved in configuration.

Convenient authentication options. If required, the PIN, symbol, password or biometric handwriting recognition can be specified centrally.

Extremely user-friendly, can be used immediately and without training, no interruption to work processes.

The challenge:

"Who would have thought a few years ago that so many Pocket PCs would be in use in today's normal working environment?", says Sascha Hanke, who is responsible for data protection at Microsoft Deutschland GmbH. "The new mobile technologies make dramatic demands on security concepts, since a lot of highly-sensitive enterprise data is saved these devices. However, if you plan sensibly, and implement your security concept efficiently, you can use them without any worries."

The situation at Microsoft Germany

Microsoft Deutschland provides its mobile staff with everything they need to work productively, whether they are in sales, consultation or management-. For this reason, their standard equipment includes not only notebooks but also Pocket PCs and MDAs with telephone functionality. While they are on the move, the users use Windows Mobile software, and a wireless link, to synchronise centrally-stored data with their mobile end devices. Nowadays, they do not just transfer their PIM (Personal Information Management) data from their Inbox, Calendar or Contacts red: these devices are now much more powerful. Using Windows technologies, the current CRM data can also be synchronised automatically with Microsoft Outlook and the mobile end device, so- that Microsoft staff always have all the updated information they need to work quickly and efficiently.

At Microsoft Deutschland GmbH the threat to Pocket PCs is seen as



extremely high – with the greatest risks being from the loss or theft of devices or memory cards.

"Nowadays it's almost never just a problem of pure calendar or contacts information", says Hanke. "A whole lot more can be hidden in e-mail attachments."

Project background

Microsoft's IT department and data protection department produced a mobile security concept in which they defined is necessary to protect mobile devices

- secure authentication
- encryption for all data
- central administration and configuration
- none need for the user to install or de-install the security software
- non-location-specific helpdesk support

Practical aspects and user acceptance were also important: it was important for the end devices to remain easy to use, and the security software should not restrict staff in their work.

The solution:

A project team was put together which included staff from the IT and data protection departments, and from a service provider who specialises in mobile communications technology for Microsoft Deutschland. This team tested and evaluated the features of the products that were market leaders. They quickly made a choice.

The choice

SafeGuard® PDA fulfilled all the requirements defined in the security concept. However, its flexibility was an even more convincing factor. For example, the effectiveness of its configurable user login helped reduce helpdesk costs: *"We decided to go for authentication via signature because we promised ourselves that we would keep support costs to the absolute minimum. And this has paid off: no users call the helpdesk because they have*

forgotten their signature", says Hanke. During biometric handwriting recognition, the software not only recognises the user's writing style, but also the way they write (the "dynamics"). An attacker can only copy this combination of features with extreme difficulty.

"Everything is going really well, and staff are accepting authentication without any difficulties. This, combined with data encryption, means that our security concept has been implemented perfectly", according to Hanke who belongs to the project team.

For Microsoft it was important for particular telephone numbers –such as the helpdesk or the security services– were always available in an emergency, even when PDAs and mobile telephones were in use. SafeGuard® PDA even meets this requirement: it allows users to call centrally-defined emergency numbers even if they are not authenticated.

And it also provides a central helpdesk solution: SafeGuard® PDA includes a secure challenge/response emergency procedure. If the user presses an emergency icon on their end device they are given a challenge code that they can transmit to their helpdesk. The staff on the helpdesk uses this challenge code to generate a response code. When the user inputs this code the system releases them again and they can define a new password – there is no need for the PDA to be online for them to do so, and the user can start working again after a very short interruption.

The result:

Planning, tests and product evaluation began in January, and 330 new mobile end devices had already been supplied with

SafeGuard® PDA in May.

"Everything went to plan, and we only needed a few days for the actual configuration. Even when it came to implementing specific modifications, Utimaco showed itself to be very flexible and able to handle our needs", continued Sascha Hanke.

Microsoft's in-house data protection guidelines state that particular information that needs to be kept secret is not to be saved on a Pocket PC without additional protection. The successful implementation of SafeGuard® PDA has had an influence on these guidelines: All mobile devices protected with SafeGuard® PDA fulfil the guideline.

Would you like more information? You will find details of the solution at www.utimaco.com/SG-PDA.