



## In and outside the office: An individual security key regulates data access

At Telefónica confidential company documents are encoded for specific groups and users

### Profile

#### Telefónica Group

Telefónica Group is one of the largest internationally active telecommunications groups. Spanish company Telefónica S.A. is listed on the Madrid Stock Exchange. Telefónica Deutschland GmbH is headquartered in Munich. The company focuses on operating and marketing its own ultra-modern broadband infrastructure. The company is seen as a pioneer of the ADSL2+ Internet access technology and is currently expanding its sizeable network. At this time the Telefónica infrastructure reaches 40 percent of all German households, and after expansion this figure should reach 60 percent by the middle of next year.

For more information, visit  
[www.telefonica.de](http://www.telefonica.de)

#### The Situation

One cable around the world: The entire Telefónica Deutschland GmbH network has a length of 40,000 kilometers – reaching exactly once around the globe. This makes the company one of the largest providers of Internet-based data and telecommunications services in Germany. The 450 employees have always been espe-

cially vigilant with regards to security when calling up and transferring data. However, when Security and Data Protection Manager Romeo Heinert was faced with the challenge of implementing security guidelines across the company, he realized: *"We needed a product that guarantees user-specific access rights to confidential data, and we were also looking for a solution to secure all data traffic both within the company and when working in the field."* After an extensive period of evaluation, SafeGuard LAN Crypt from Utimaco – The Data Security Company was heading the pack.

*"This software was exactly the product we were looking for; it fulfilled all our requirements in one go"*, Heinert explains.

#### The Requirements

Telefónica Deutschland GmbH is part of Telefónica O2 Europe and therefore a 100% subsidiary of the globally operating Spanish telecommunications group Telefónica S.A.

In Germany, Telefónica operates one of the largest alternative infrastructures, orienting itself to Internet Service Providers and Carriers who do not have their own network or comprehensive network coverage. Telefónica's platform uses these to realize differentiated, high broadband offers for end customers, such as Internet access and other services such as telephony or video-on-demand.



Before implementing SafeGuard LAN Crypt, Telefónica used to rely on several Samba servers. Data and information from various departments were stored here, albeit separately. There was no double-checking or specific security checks of documents or folders. The company's new security rules demand a complete solution that meets all legal requirements for the company and its management, cleanly and across the entire company. Sensitive company data should be secured without requiring any real effort by employees. Furthermore, Telefónica was looking for software that could be managed centrally and would save both time and money for its IT department.

#### The Selection

*"Which solution could handle our guidelines and security plans efficiently and in one fell swoop? That was our main priority"*, Heinert remembers the start of the selection process around two years ago. Research on the Internet and in specialist publications provided him with an initial overview of various encryption software.

In the next step, Heinert contacted several providers. *"Utimaco made contact with a sales partner Protea Networks"*, Heinert reports. On-site discussions clarified wishes and requirements for a data encryption solution.



*"In the evaluation phase the various products were compared directly. We chose SafeGuard LAN Crypt because it covers all the areas we require with the quality we require"*, adds Heinert.

Meaning: This new security solution encrypts files on local computers and file servers. Data is also transmitted in encrypted form. *"The software has other distinct advantages, such as central administration, transparent data security for user groups, and encryption of all current media such as CD or USB sticks"*, Heinert explains. He was impressed that SafeGuard LAN Crypt required no additional expansion of the company's IT infrastructure:

*"The competitor products we tested often did not manage this. We were able to seamlessly integrate SafeGuard LAN Crypt into our IT infrastructure: Our employees are not at all restricted in their daily work. "*

#### **The Solution**

Once Protea Networks had summarized Telefónica's plans, work began immediately. A joint solution scenario was worked out. During the subsequent test phase, Protea was on hand to provide technical tips and all-round support. And even after the implementation, Telefónica can depend on Protea's know-how. 200 Telefónica computers have already been equipped

with the new security software; the remaining licenses will be implemented gradually. *"Installing the software is quick and easy thanks to its central administration. In addition there are hardly any personnel costs involved. Of course we are incredibly pleased on that account"*, says Romeo Heinert. *"For a year now, SafeGuard LAN Crypt has been running stably and with no incidents. We are very satisfied customers."* But what happens when an employee switches departments and has never worked with LAN Crypt before? No problem: Their team leader or manager requests the necessary data to be released. After this, the administrator releases and distributes the relevant policies. Once the software is installed, the user receives a brief introduction via telephone or LAN Desk...and away they go.

#### **The Result**

At Telefónica, each employee can only see the files that are released for them. Even system administrators have no access to the contents of confidential documents. The Security Officer defines the individual access rights for working groups or individuals for each new computer, according to the Telefónica security guidelines. That means: Each user receives a personal "keyring" according to their profile. This releases data and allows users to read the relevant data in its original form. Unauthorized data pirates are confronted with an encrypted, unreadable text. Have there been any problems? *"No. If we have the occasional complaint when a user cannot access certain data, that only shows us that the software is doing its job"*, explains Romeo Heinert. Neither system administrators nor the Security Officer have to manually mess with each computer. Recognition, encryption and decoding of encoded data are all fully automatic.

Distributing control powers over the administration of IT and security ensures that only authorized persons have access to specific data. An additional integrated file header concept guarantees that even when someone leaves the company, the company is still able to access important information.



*"SafeGuard LAN Crypt allows us to encrypt data specific to groups or individuals. This also applies to field personnel, mobile devices and data transfer. Backups are also encrypted"*, the security expert summarizes his new security tool: *"We can rely 100% on this software, support and update service. "*