



## Financial data protected despite radio access

by Nicola Schmidt, freelance journalist from Munich.

MUNICH (COMPUTERWOCHE) - These days, the field staff from the IT service provider Datev is accessing their data via WLAN. In order to satisfy its high security demands, the company - located in Nuremberg - commissioned the development of specialised, safe client software.

Purchasers of the Datev services offered centrally and on site are tax consultants, lawyers, accountants and auditors as well as their clients. Order data provided by them may on no account fall into the wrong hands. The result would otherwise be legal consequences not excluding imprisonment, as Datev is subject to a professional confidentiality law specified in the Tax Advisory Act.

Centrally stored customer data is accessed by field staff, consultants and telecommuters as well as Datev information centres distributed across Germany - approximately 800 external employees in total. Until recently they were only able to access the company network via ISDN lines. Because they were often connected to head office for hours, they caused high online costs.

Datev found a solution to this problem in the Digital Subscriber Line (DSL): the DSL signal is additionally fed to the copper cable of the ISDN line. With a flat rate or volume billing, dial-in costs far less than internet access via ISDN. Higher bandwidths than the maximum 128 kilobits of an ISDN connection can also be used - depending on tariff, between 384 and 3072 kilobits per second for data download. A DSL splitter ensures that telephone and DSL signal are clearly separated, even if someone phones while surfing the Net.

### Interesting perspectives for the future

The use of the DSL technology requires either a special modem or a wireless LAN router with an integrated DSL modem, which can send a wireless signal to the computer. Datev decided on the second option: DSL via WLAN. Apart from the cost-efficient flat rates from internet providers, the company gained a further advantage - clearly reduced costs in the case of one of the 26 information centres changing its location. In this case, only the access points would have to be reinstalled; laying of cables, switches and hubs becomes obsolete.

Furthermore, radio technology opens interesting perspectives for the future: employees will soon be provided with PDA and UMTS devices for access to the network.



Datev will only permit multi-authorized users into their inner sanctum.  
Photos: Datev

But first it was necessary to solve a problem: actually, a radio connection is less safe than copper or glass fibre cabling. But safety is a basic prerequisite for the Nuremberg service provider: "We have to connect the field staff to the company's inner sanctum, the internal data network", explains Heinrich Golüke, Communications Technology Manager at Datev.

The WLAN protocol Wired Equivalent Privacy (WEP) responsible for safety was cracked long ago. Therefore the internal security policy actually excluded a radio network. But Golüke wanted to utilise the cost and performance advantages of the new technology and therefore searched for a back door.

## Smartcard had to be integrated

Therefore the required solution had to provide the same security as cable-bound access, whereby it had to fulfil a Datev-specific requirement: As a certified Trust-Centre, the service provider may issue legally binding, digital signatures. As a result they introduced a company smartcard as employee identification. This card also stores the authentication and encryption data for the WLAN and the Virtual Private Network (VPN). The Client software therefore had to integrate the internal smartcard for all three applications.

Thus the scenario for the registration procedure was as follows: The employees do not send their data openly via the radio connection, but rather adhere to three security steps. On the one hand the data are encrypted and, if necessary, secured with a digital signature stored on the smartcard. The card on the other hand also provides the access data with which the user logs into the WLAN. As a third step it develops - also with the help of the smartcard - the VPN tunnel, via which the encrypted data are sent.

With this specification in mind, Golüke and his team took a look at the solutions provided by various providers. They finally decided on their long-term partner Network Communications Products (NCP), also located in Nuremberg. "The direct contact provides advantages in project work", says Golüke. Datev had also worked with NCP in the past regarding the encryption and authentication of the ISDN dial-up. The "NCP Secure Client" therefore already supported the Datev smartcard. Client and Provider came to a mutual decision to further develop the existing client software for the new requirements.



As a service provider for tax advisors and auditors, Datev is subject to severe safety requirements.

## No bit sneaks past the server

A further crux of the matter was the categorical demand that all Datev laptops were only to go online via the Datev server. "Irrespective of the telecommunication header record existing on the computer - no bit may sneak past the Datev server", says Golüke. The user must



therefore be prevented from changing the data transfer configuration in order to log into his private internet provider, for example.

The new version of the "Secure Client" ensures this: The system recognises if the user tries to bypass the internally fixed dial-up modi with a new WLAN card or an external modem and blocks the connection. Last, but not least the client software has a new integrated "fire wall" protecting all network adapters existing in the system.

## **Supplemented Security Policy**

The first concepts for the solution were completed at the end of 2002, and software development was completed during spring of the following year. An intense testing phase now followed with penetration analyses, which in turn required a few improvements to the software. Six months later they were ready: the Datev Board supplemented its security policy in such a way, that the highly secure WLAN Internet connection could be introduced to the information centres and the telecommuters.

In order to remain flexible and sustainable, the NCP software had to be adapted in such a way as to accept other security servers at Head Office - from Cisco, for example. NCP adopted the development of this new requirement. However, Datev participated in the development costs of the client update, as they were the first client with such high security demands.

NCP spent approximately five personnel months for the development of the new Secure Client. Datev invested a total of 20 to 30 personnel months on planning, conception, implementation and roll-out, as these tasks were completed by their own IT team. "The knowledge for safety-relevant solutions must be internalised, we only pass on development orders and safety expertises externally," said Golüke.

## **Safety first**

At the beginning of this year the first information centre in Kassel was equipped with the new WLAN technology. Since June, 40 pilot users in the field staff have been working with DSL internet connections. Golüke wants to complete the project with a general release in October of this year. He has a plausible explanation for the long interim period between development and area-wide introduction: "For us, absolute security is more important than a short-term release".

So far, experience gained from the pilot phase has been good throughout. The WLAN connection in the information centre is in no way inferior to fixed cable connection, the DSL connection of the field staff provides the desired performance surge in comparison to ISDN dial-up. Datev also expects online costs for field staff with a large traffic volume to be halved, which would result in savings of up to six digit amounts.



## In the pipeline: UMTS

As a further step, Datev is planning a mobile access via UMTS networks and a PDA/MDA connection. A UMTS pilot project was already conducted last year in cooperation with Lucent and T-Mobile. In the interim, Datev is testing how the released UMTS networks of the larger providers could be utilised.

The basic conditions of the internal security policy also apply in this area - a further challenge taken on by NCP. Here the important aspect is the interaction between the NCP solution and the Terminal Server technology, as the actual data will not be stored on the end device.

### Project characteristics:

**Project type:** introduction of a safe WLAN for remote access to data and resources in the office communication network.

**Sector:** service provider

**Time frame:** approx. 3 months

**Current status:** productive

**Costs:** 20 to 30 personnel months on Datev's side

**Products:** continuous development of the "NCP Secure Client".

**Service Provider:** own IT Team, partially NCP, for the UMTS pilot Lucent.

**Scope:** connection to office communication network for 800 external employees.

**Result:** halved online costs for sales force.

**Challenge:** high-security area with penal consequences.

**Next step:** extension to UMTS and PDA connection.