



# Major Telecoms Provider Secures Mission-Critical Data with FoxT ApplicationControl

*The telecoms provider featured in this success story is the largest mobile telecoms provider in its domestic market, with several million customers. The company is distributed geographically, with twelve sites in its home country, including headquarters and a major datacenter.*

## CASE STUDY

FoxT solutions are deployed to manage and protect highly confidential, mission-critical environments. The FoxT customer highlighted in this case study has requested to remain anonymous, but has assisted us in compiling this information and ensuring that it is true and accurate.

*“While the original goal of the company was to protect its SAP™ applications with certificate-based security, it is now finding an added value in the fact that the FoxT solution can be extended to other key applications.”*

### The Requirement: Certificate-Based Access to SAP

Like all mobile telecoms providers, this European-based company has mission-critical applications processing a tremendously high volume of transactions: the many calls made and text messages sent by its subscribers. The company needed to secure their transaction information (3.5 million transactions every hour) because it is used as a basis for billing customers, and contains sensitive data about subscribers and the calls they make. The company therefore initiated a project to protect its SAP R/3™ applications.

The company's primary requirement was to find a PKI-based solution for securing its applications. It believed that certificate-based security was the way forward, and wanted to build a scalable, integrated corporate security platform. When examining the different options on offer from a variety of vendors, among them some of the largest in the Identity and Access Management sector, the company was impressed by FoxT ApplicationControl, a PKI-based solution for securing and managing application access.

FoxT has an out-of-the-box solution developed specifically for SAP R/3™. In consultation with its supplier, a leading integrator, the company felt that the FoxT solution would require less consulting work and support for implementation than offerings from other vendors.

The company therefore decided to initiate a proof of concept of FoxT ApplicationControl, which began in mid-2002. During the proof of concept, the integrator and FoxT worked closely with the customer to ensure an optimized implementation of the solution, turning the customer's feedback into positive enhancements in the software.

At the end of the proof of concept, pleased with the support they had received from FoxT and the solution itself, the company decided to invest in FoxT ApplicationControl, and roll out the solution to secure its SAP applications.

The solution provides certificate-based logon to applications, role-mapping for federated identities and single sign-on, encrypted communication with application servers, and centralized logging of application traffic.

### Integrated Infrastructure

Today, FoxT ApplicationControl forms one of the company's three security pillars. Operating under an umbrella provisioning system – Tivoli from IBM – the company deploys AMOS from IBM to secure operating systems, SiteMinder from Netegrity for web security, and FoxT ApplicationControl for application security.



## About FoxT

FoxT protects corporate assets with an enterprise access management solution that centrally enforces granular access entitlements, in real-time, across operating systems and business applications on any networked device. The ability to proactively administer, authenticate, authorize, and audit access across diverse platforms, down to the file and device level, enables organizations to greatly reduce compliance and audit costs, streamline IT security administration, and protect corporate value by mitigating the risk of insider fraud. Headquartered in Mountain View, California, FoxT serves Global 1000 customers in 32 countries. For more information - [www.foxt.com](http://www.foxt.com) or email [sales@foxt.com](mailto:sales@foxt.com).

The customer required that all usernames and passwords should be handled in one location: an external LDAP repository. FoxT Manager, the security server used in the FoxT ApplicationControl solution, authenticates indirectly to this LDAP repository via SiteMinder. In this way, the FoxT solution is perfectly integrated into the company's existing infrastructure.

Among the customized features developed by FoxT to ensure the solution would meet all the customer's requirements were plug-ins for authentication modules, which enabled customized authentication mechanisms to be integrated with the system.

### Reduced Helpdesk Traffic

The FoxT solution also enabled tailored error messages for authentication, which are displayed to users at their workstations. The purpose of these straightforward error messages is to give end users more information on how to resolve errors, reducing helpdesk traffic and making it easier to localize the solution for the company's international operations.

The solution enables certificate-based authentication for all users accessing the company's SAP applications. User workstations are secured with FoxT Desktop, which handles the user certificates issued by the FoxT Manager security server. At the moment, certificates issued using the Certificate Authority in FoxT Manager are used for user authentication to applications, but the company plans to implement a third party Certificate Authority, which will then be used to issue all certificates. The FoxT ApplicationControl solution is fully compatible with third-party Certificate Authorities.

### Improved Data Sharing

FoxT ApplicationControl has also enabled the company to share parts of its SAP R/3™ applications with its parent concern. The company has rolled out 6,500 installations, some of them for users at the parent concern, which is in a separate geographical location. This enables users to securely access the SAP R/3™ application server at the subsidiary. In this way, a security solution is actually helping the company to safely open up parts of its infrastructure to affiliated organizations.

This setup also provides a uniform set of logs for all application traffic, whether it be from the parent company or the subsidiary, which is a valuable resource for auditing purposes.

### Range of Applications

The customer is now up and running with FoxT ApplicationControl for SAP R/3™, and has discovered the added value of this solution: Namely, that the FoxT technology can be easily leveraged to secure a whole range of applications. The ability to leverage the technology lowers the solution's total cost of ownership and facilitates building a consistent application security platform that can grow with the company moving forward.

With the support and help of FoxT and its integrator partner, the customer is now busy developing new FoxT Agents using the FoxT Agent SDK, a powerful toolkit for programming new application-specific agents. The customer is looking to extend the values provided by FoxT ApplicationControl to secure Oracle databases running on a variety of operating systems, its billing system (NBS), and a statistics package (SAS).

While the original goal of the company was to protect its SAP applications with certificate-based security, it is now finding an added value in the fact that the FoxT ApplicationControl solution can be extended to other key applications, and is using tools such as access routes and user classes to achieve more efficient and effective management of application security.