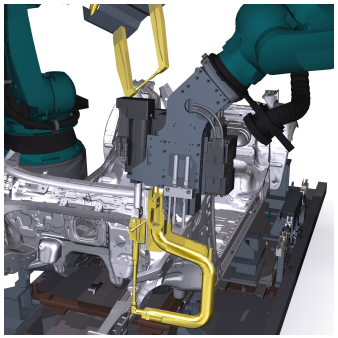
CASE STUDY



Successful Audit Thanks to Two-Factor Authentication

An engineering office for chassis plant construction introduces SecurAccess to safeguard access to highly sensitive CAD data.

The look of tomorrow's automobiles is planned in Fulda. Established in 2010 as a specialized provider of services for the development of modern production solutions in the automobile industry, this company has continued to evolve and has also acquired comprehensive know-how in plant development. The engineering office, which employs a staff of sixty coworkers, is commissioned by automakers to plan, to bid on projects and to provide consulting for chassis plant builders in the process of transforming CAD data into vehicle components for subsequent manufacturing. All coworkers accordingly receive training in the tools, methods and processes of digital engineering. "Plenty of development time passes before data can be transformed into tangible components for automobiles. On behalf of our clients, we accompany and shape the entire process from the design phase for the first plant on paper all the way to production. Finally, the plant must function so well that an automobile can be produced in sixty seconds," explains Daniel Auerbach, managing partner of A&S Engineering and its cofounder along with managing partner Wolfgang Sieckel.

The theme of security plays a major role here because the company is entrusted with prototypes' data from which tomorrow's motor vehicles will be developed. These developmental data are between four and five years ahead of their time and are therefore highly interesting for competitors. So that these business-critical data can be transferred from one server to another at all, the clients who commission the chassis experts have created ultra-secure accesses that can be accessed only with appropriate authorizations. But the transmission line isn't the only element in the system that's rigorously secured to protect these extremely valuable data.

Auditing for Service Providers and Suppliers

Background

A&S Engineering is taking care (among other things) about the look & feel of the cars of the future. From planning to procurement until realization the engineering company, specialized on automotive, supports plant manufacturers for the smoothly development of facilities for car body construction. To safeguard highly sensitive CAD data, the company in Fulda, Germany has introduced the Two-Factor Authentication solution SecurAccess of the vendor SecurEnvoy in mid 2015. Reason for that is a requirement of a purchaser in line with an audit to implement higher security standards that are recommend since the introduction of the German IT security law.

Since 2015, one of the largest clients in the automobile industry has additionally introduced an audit of all service providers to guarantee the security of the data outside the limits of the client's own network. This change also affected A&S Engineering. Alongside an alarm system to protect against burglars, a technology to encrypt hard discs and measures taken to increase the server security, the list of requirements also called for safeguarding the daily authentication process and the remote access. This access was intended to take place via a second factor. "There were two K.O. criteria for the audit: the alarm system and the two-factor authentication," Auerbach recalls. "Our clients must not only guarantee that their motor vehicles are safe, but must also ensure the continued and uncompromised secrecy of the information necessary for developing those vehicles. We naturally contribute our fair share to this and we're well aware that we too could potentially be targeted by cybercriminals." Furthermore, the new IT security law raises concerns in the industry. Increasingly many businesses are looking for ways to protect their sensitive information from unauthorized access.

Authentication with One's Own Smartphone

The company sought a secure and simultaneously practicable solution to satisfy this demand. "As a partner with whom the industry shares know-how and confidential information, it's naturally important for us to not only uphold the required standards, but also to present ourselves as a trustworthy contact. However, we wanted to keep the complexity as minimal as possible. Our coworkers need speedy and secure access to our network and to the data it carries. That's why, in addition to consulting with our in-house IT division and with our contact partners, we also turned to Bucher Netzwerke in Weingarten for up-to-the-minute information about the solutions for two-factor authentication that are currently available on the market," Auerbach says. SecurAccess from SecurEnvoy was an especially interesting solution because it can guarantee secure authentication in interplay with a coworker's smartphone.

Greater Security through Encryption and Divided Transmission

Two-factor authentication works via the "SoftToken" app. Available for iOS and Android, Windows Phone and Blackberry, this app generates a different six-digit pass code every 30 seconds. This pass code is used on a PC or laptop to sign on to the network. When a user signs in, the server checks to ensure that the pass code which the user has entered is valid for this user and for this moment in time. The data per se are stored in encrypted form on the server of the engineering office from Fulda. Highly secure 256-bit AE encryption is used here because it can guarantee that the data remain secure in all directions, even if the network is compromised. Auerbach explains the installation from his point of view: "The setup was very simple. All we had to do was download the appropriate app, then sign in on the SecurAccess secure server and scan a QR code with our mobile phone's camera. Once these steps were accomplished, the setup was successful and a pass code was shown on the smartphone. We could then use this pass code to log in on the company's network with a PC or laptop."

During the setup via QR code, the first part of the user's individualized key (the "seed record") is transferred from the server to the smartphone without the need for a network connection. In the next step, the smartphone generates the second part of the key, which the user then types into the registration page as an eight-character alphanumeric code. The manufacturer relies on this one-time-only process to guarantee that only this device, and no other, can generate valid pass codes. This "Split Seed" technology effectively prevents double registration or the transmission of the key, e.g. via a backup of the telephone's memory.

"As a partner with whom the industry shares know-how and confidential information, it's naturally important for us to not only uphold the required standards, but also to present ourselves as a trustworthy contact. However, we wanted to keep the complexity as minimal as possible. Our coworkers need speedy and secure access to our network and to the data it carries. That's why, in addition to consulting with our in-house IT division and with our contact partners, we also turned to Bucher Netzwerke in Weingarten for up-to-the-minute information about the solutions for two-factor authentication that are currently available on the market."

Daniel Auerbach, managing partner and founder of A&S Engineering.

A Short and Convincing Test Phase Assures a Successful Audit

After the installation of a test license and after a test phase in which both managing partners personally tried out the app on their smartphones, it was clear that we had found the right solution. Now we only needed to check with the auditor to verify that the two-factor authentication complies with the standards defined in the guidelines of the automobile corporation that had commissioned us. The fastest way was to send the specifications directly to the auditor. After a phone call with the management, he granted approval for the implementation of this solution. The managing partners then decided to acquire licenses for two-factor authentication for each staff member. “It doesn’t make sense for us to use this solution only for this one specific client. That’s why we decided to use authentication for all our login processes,” Auerbach says. In the meantime, two-factor authentication is used by every coworker, regardless of the individual’s position or function. The staff members quickly accepted the new solution because it’s very convenient: they can use their own smartphones and they don’t need to carry an additional external device with them. If a colleague runs into problems with the registration, two additional options are available for successful authentication: “Voice-CallBack” is one; transmission of the pass code via email is the other. In individual instances, each of these options can assure speedy access to the network, also without the smartphone app.

Summary

“SecurEnvoy offered the solutions in a bundle of 50 licenses, so we immediately covered our present and future needs. We plan to continue growing and we intend to hire additional staff. These new colleagues will naturally need licenses so that they will be able to sign in on the server. It’s only logical for us to keep a supply of unassigned licenses in-house rather than requesting additional licenses whenever we need new ones,” Auerbach explains. For A&S Engineering, this investment in enhanced security was an investment in the future because the new IT security law impels increasingly many clients to insist on audits. “We’ve proactively equipped ourselves—and that gives us a good feeling,” Auerbach concludes.

SecurEnvoy plc | info@SecurEnvoy.com | www.SecurEnvoy.com

SecurAccess:

Authentication for the modern business

SecurAccess from SecurEnvoy turns any mobile phone that can receive SMS into a ready-made authentication device. This pioneering, zero-footprint solution cuts costs by using hardware that is already in circulation.

Unlike traditional tokens that take months to deploy and replace, SecurAccess can roll out more than 15,000 new remote staff per hour without the pain, cost or environmental impact created by legacy hardware distribution.

The solution fully integrates into Microsoft Active Directory, Novell eDirectory, Sun Directory Server and OpenLDAP. Integration is simple as it requires no additional databases or hardware – not to mention their associated costs.

SecurAccess also integrates with all leading remote access servers and web services; including Microsoft OWA, Citrix, Juniper and Cisco.

There's also no need for extra software; eliminating costly and time-consuming testing and training schemes. SecurEnvoy has been designed to respond to the constant changes in mobile technology to ensure a competitive ROI.

Worried about network coverage or SMS delivery delays?

SecurAccess is fundamentally designed to let you:

- Pre-load one-time passcodes
- Reuse session passcodes that change daily or after multiple days
- Request temporary passcodes through self-help website
- Obtain passcodes via email if necessary

SecurAccess is changing the game for business security. No tokens, no fuss… just rock solid, two-factor security on the move.

Authenticate your way

About SecurEnvoy

SecurEnvoy are the inventors of tokenless authentication and provide two-factor authentication via mobile phones. Passcodes are sent to the user's mobile device in order to access corporate internal networks, cloud based services or private emails.

SecurEnvoy's products:

- SecurAccess
- SecurPassword
- SecurIce
- SecurMail

- are adopted worldwide.

Customers benefit from reduced support time, no database management as existing LDAP servers are used and zero footprint as no token deployment is required; so ROI for organisations is relatively high.

SecurEnvoy distributes through the channel, providing customers the value added benefits of working with local partners. It has built up a technical and sales infrastructure that supports most languages and cultures around the world.

Partners include Juniper, Citrix, Fortinet, Sonic Aventail, Cisco, Checkpoint, Celestix, Microsoft and F5. SecurEnvoy's customers include T-Mobile, Symantec, John Lewis, NHS and Save The Children.

SecurEnvoy was founded by Andrew Kemshall and Stephen Watts in 2003. The UK headquarters are based in Theale, Berkshire; with regional offices in Frankfurt, San Diego and New York.

SecurEnvoy plc | info@SecurEnvoy.com | www.SecurEnvoy.com