indevis
security in a connected world

Your benefits

- Highly secure multifactor authentication (hardware tokens, SMS tokens, software tokens)
- Connection over VPN and AES encryption
- High level of availability by redundant outsourcing to professional datacenters
- Optional virtual system with its own administration user interface
- Comprehensive service by indevis: setup and design, token rollout, replacement service, service desk
- Scalable costs, investment shift from CapEx to OpEx

cloud services
MADE IN GERMANY

DO YOU WANT
TO KNOW MORE?

Your personal contact person will be happy to advise you and discover together with you what concept bestfits your needs.

+49 (89) 45 24 24-100
sales@indevis.de
www.indevis.de

INDEVIS AUTHENTICATION

STRONG AUTHENTICATION FOR EVERY SIZE OF ORGANIZATION

Static passwords (comprising user name and password) only provide inadequate security for protection of networks against unwanted access. Passwords are often very easy to guess or they make their way into unauthorized hands. Discovering static passwords by spying also presents no great difficulty using state-of-the-art technology. Dedicated tools automatically try millions of word combination in short spaces of time. When passwords are transmitted over the Internet, potential attackers can often intercept them without much effort.

THE DECISIVE FACTOR FOR GREATER SECURITY

A two-factor authentication with an additional (hardware) token is the optimal solution for secure network access. The login to the enterprise systems does not involve the use of a static password, but rather a combination of a PIN (the first factor) and a continuously changing code, which is displayed on a separate device or sent by SMS (the second factor). A straightforward yet very secure network login can be achieved with this kind of strong, user-friendly authentication: for administration, management, sales, customers, external service providers, etc.

TECHNOLOGY PROVEN OVER MANY YEARS

indevis Authentication offers companies and organizations of all sizes a user authentication system with dynamic passwords based on RSA SecurID. Since 1999 indevis has been operating an RSA authentication server in a specially secured data center of a large bank. In the meantime, there is high availability of the infrastructure owing to a redundant second data center. Many thousand tokens of the *indevis Authentication* solution have been rolled out since that time, protecting corporate resources of inestimable value right up to this day.

SCALABLE SOLUTION – MAXIMUM BENEFIT

indevis Authentication is a perfectly scalable rental model that is available for a minimum cost per month. For a monthly fee, your company leases as many tokens as your organization requires. You can lease single tokens for each new staff member. In this way, the total cost of ownership (TCO) can be significantly reduced and your company immediately uses fully functional RSA SecurID authentication without any large initial investment.

indevis Authentication services

- indevis operates and manages the RSA authentication server
- indevis administers the RSA SecurID user administration
- indevis takes charge of token rollout in your company
- indevis replaces old and lost tokens

INDEVIS AUTHENTICATION FUNCTIONALITY

When logging on to a network resource and authenticating with RSA SecurID, users must enter their user name, self-assigned PIN and the corresponding token code. Different authentication tokens and also SMS token codes can be used.

The input data is transferred through the RSA Agent, which encrypts the authentication request and forwards it to the RSA Authentication Manager server operated by indevis for verification of the user's authenticity. The RSA Authentication Manager computes the currently valid access code based on the time and the initial value, and returns the authentication result to the RSA Agent. The authentication is successful if the data is matching. The RSA Agent then grants (or refuses) the user access to the network resources.

CONNECTION OVER VPN AND AES ENCRYPTION

indevis Authentication is the most cost-effective option for most companies to replace static passwords by dynamic ones. The customer's LAN is connected over a VPN to the indevis authentication server. The authentication is implemented with AES encryption over the Internet. No corporate data is sent to the indevis RSA Authentication Manager during the process. Only the token code, PIN, user name and RSA Agent name are transmitted.

SOFTWARE TOKENS: SIMPLIFIED AUTHENTICATION AND DISTRIBUTION BY QR CODE

By using software tokens, the workflow for distributing and managing two-factor authentication can be optimized for global mobile workers. The token seed - the secret key that generates the password - can be sent to the user as a QR code by post. This facilitates the distribution of tokens especially for companies that operate globally. When shipping the QR code as a letter, no import or customs regulations must be followed, so that the token arrives quickly. The distribution path itself is also safer than sending via unencrypted e-mail because it makes hacker attacks impossible.

For users, the software token offers the advantages that it is user-friendly, always accessible on the smartphone and easy to put into operation. The QR code automatically leads to the RSA app as soon as the user takes a picture of it with his smartphone. To activate the token, employees receive a password separately with a second letter by mail. The operation via the app is simple, since only the personal Pin must be entered and the passcode is calculated automatically from the Pin and the token code.

Would you like to get to know *indevis Authentication*? We can provide you with a test configuration free of charge for you to open your systems to authorized users on the Internet without any risk.

About indevis GmbH

Since 1999 indevis GmbH, ISO 27001 certified, has been providing IT security, datacenter and network solutions, accompanied by professional consulting, management and support services. In doing so, indevis fully meets the demands and requirements set out by the economic sector and public authorities and higher education institutions.

As one of Germany's leading managed security service providers, indevis is the partner for IT security and network technology for companies of all sizes and in any sector – after all, IT security is not a given, but rather has to be strategically planned.

indevis offices are located in two cities in Germany: Munich and Hamburg. Additional staff members work at a number of other locations distributed throughout Germany.

TÜV SÜD ISO 27001

indevis
security in a connected world

indevis GmbH

Irschenhauser Straße 10
81379 München

Tel. +49 (89) 45 24 24-100
Fax: +49 (89) 45 24 24-199

sales@indevis.de
www.indevis.de