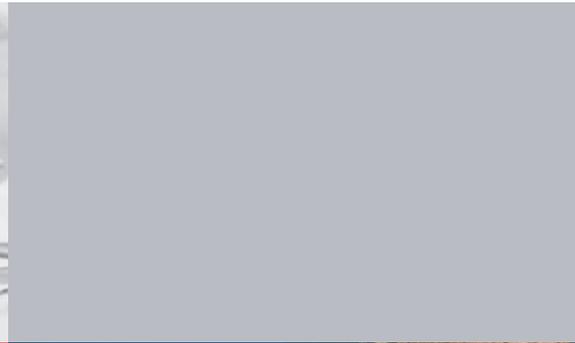
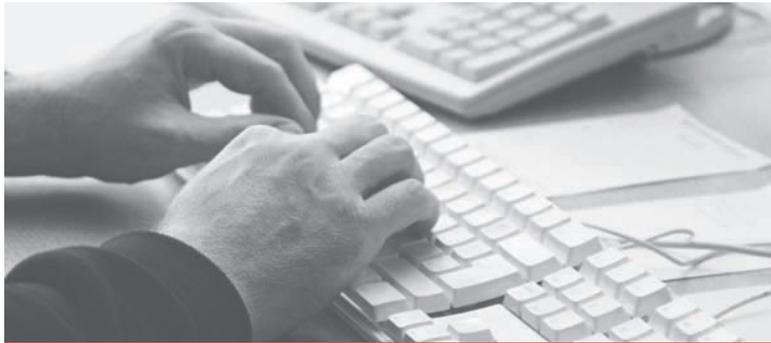


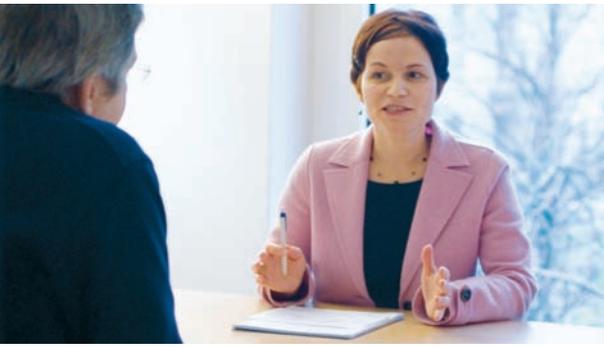
Medusa

Authentication server



Do you want to offer your customers, suppliers, business associates or employees secure access via the Internet to data and applications in your organization? The Medusa authentication server is exactly the right product if you set great store by a solid infrastructure solution that grows in line with your needs.

Medusa features a flexible and open architecture based on Java technologies. Numerous authentication services are already integrated while the number of available plug-ins is increasing continuously. Since Medusa can be configured, it can be integrated in your IT environment extremely quickly. The use of Medusa therefore enables you to attain two conflicting objectives simultaneously, i.e. cost efficiency and accuracy.



Medusa is the ideal authentication server for infrastructure components such as remote access solutions, VPNs and Web applications with one entry server. Medusa offers Single Sign-On, the single authentication for all connected services. Medusa is a cost-effective means of integrating various authentication services to provide a secure, highly flexible and proven all-in-one solution.

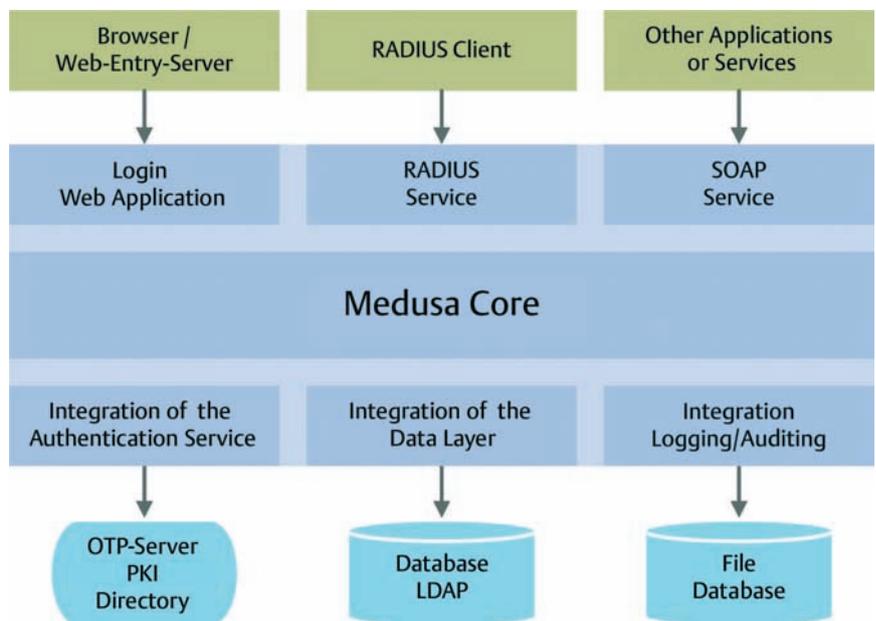
Why Medusa?

- Secure customer-specific authentication applications can be quickly implemented using the Medusa authentication server.
- The plug-in concept allows independent connection and simple integration of any authentication services, persistence layers and other peripheral systems.
- When combined with an entry server and Web applications, Medusa provides Single Sign-On (SSO) based on SAML.
- Medusa automates the administration of authentication means (credentials).
- In spite of many different services, Medusa features one central uniform interface.
- A large number of satisfied customers are already using Medusa. They include, for example, administrations, financial service providers and service companies in the communications industry and health sector.
- Medusa has proven its worth in practice and is secure and stable.
- Medusa was fully developed in Java and can therefore runs on all current platforms.

Overview of services

Medusa combines and consolidates different types of authentication such as passwords, PINs, transaction numbers (TANs), indexed TANs or matrix cards, mobile or SMS TANs, tokens and processes such as Challenge Response and PKI (client certificates). All these authentication methods are made available in one uniform interface.

Architecture



Medusa strictly separates the authentication logic from the surrounding components, thus substantially reducing the level of complexity and ensuring maximum security.



Interfaces

The Medusa components supply the authentication services externally in different ways: as a login Web application, as a RADIUS service and as a SOAP service. The login Web application is an integral part of Medusa for authenticating users. It can be used for logging in, logging out, changing passwords, self-registering users and Single Sign-On based on SAML. The application comes in several languages and is client-accessible. Since it can be configured to a high degree, it can be adapted to a specific look and feel with very little time and effort. Another interface is available in the form of a RADIUS server which enables corresponding clients to access the authentication services. Any other applications can use the SOAP interface to call up the services of the Medusa core, e.g. to change passwords or sign transactions. Besides the already existing interfaces, other interfaces can simply be added.

Core

The integrated authentication services and persistence layers, as well as a logging and auditing component form the basis of the Medusa core. The following components, for example, are already integrated: SecurID Server from RSA, VASCO from Digipass, Internetpassport from AXSionics, a matrix card from Ergon, SMS-based authentication, Active Directory, LDAP, databases and PKI solutions. Thanks to the flexible plug-in concept, other and also proprietary components can be simply integrated and combined to form services containing even more functions.

Security

The security-related functions of Medusa provide a high level of protection against attacks:

- The architecture and implementation of Medusa are designed with emphasis on total security thanks to strict modularization of the individual components.
- Every user input is verified by means of white list filters.
- The entry server filter rules are specially tailored to the login application.
- In the event of an error, the entry server session is terminated and the user is logged out from all applications for security reasons.
- Error pages only contain a unique code, but no information on the cause of the error.
- If login attempts fail, the Web application always behaves in the same way. This means that no conclusions regarding the validity of individual authentication checks (credentials) can be drawn from the behavior of the login application.

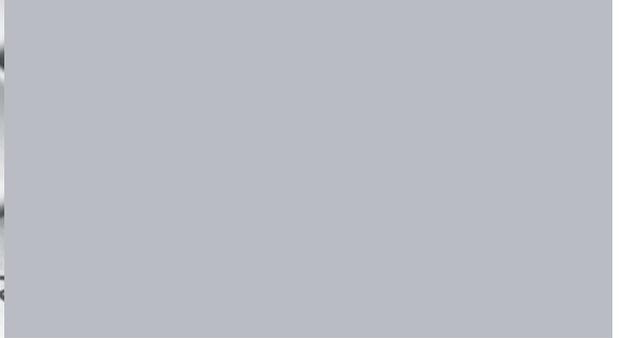
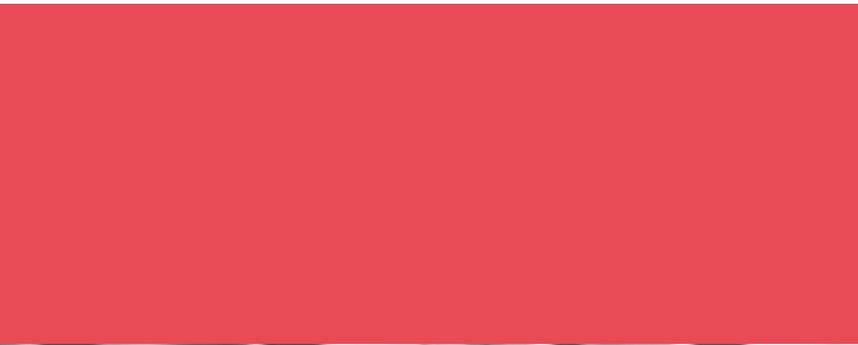
Don't leave the security of your data to chance – use Medusa to protect your data against unauthorized attacks.

“Authentication applications are very exposed. They can be accessed anonymously by all users, including potential hackers. The security of login applications is therefore vital for the security of Web application systems. The Medusa authentication server was designed and developed on the basis of this fact and is subject to the strictest possible quality controls.”

Marc Bütikofer, Crypto & Security Expert at Ergon

Modular and expandable

Modularity and expandability were the basic ideas behind the design of Medusa. The Medusa authentication server can be extended in numerous areas by means of plug-ins and can be adapted to specific requests. A wide range of authentication services, entry servers and Web applications can be integrated along with data exchange via directories or databases.



smart people – smart software

Ergon means a highly productive team made up of well-qualified IT specialists who focus very clearly on customer benefit. The company leads the field when it comes to implementing challenging projects, and it is an established provider of specific solutions in the telecommunications environment. Ergon's applications are based on open systems and Java technology. They feature a modular structure and varied integration possibilities, and they can be extended on a flexible basis. Implementation centers around user needs.

By consistently aligning itself with the market and maintaining close links with science and research, Ergon is quickly able to identify the latest trends and to implement them professionally thanks to its technological creativity. Ergon's software solutions create real competitive edges for our customers, as proven by our long-standing partnerships with discriminating clients and the numerous projects we have completed in the fields of finance and telecommunications, in industry and in the public sector.

The essence of success has remained unchanged for almost 25 years: Ergon focuses on customer benefit.

Copyright Notice

Copyright © 2009 Ergon Informatik AG. All Rights Reserved.

All technical documentation that is made available by Ergon Informatik AG is the copyrighted work of Ergon Informatik AG and is owned by Ergon Informatik AG. Ergon believes all information herein to be correct at the time of creating this document. As such, Ergon Informatik AG makes no warranty as to its accuracy or use.

Microsoft, Outlook and Active Directory are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other products or trademarks mentioned are the property of their respective owners.