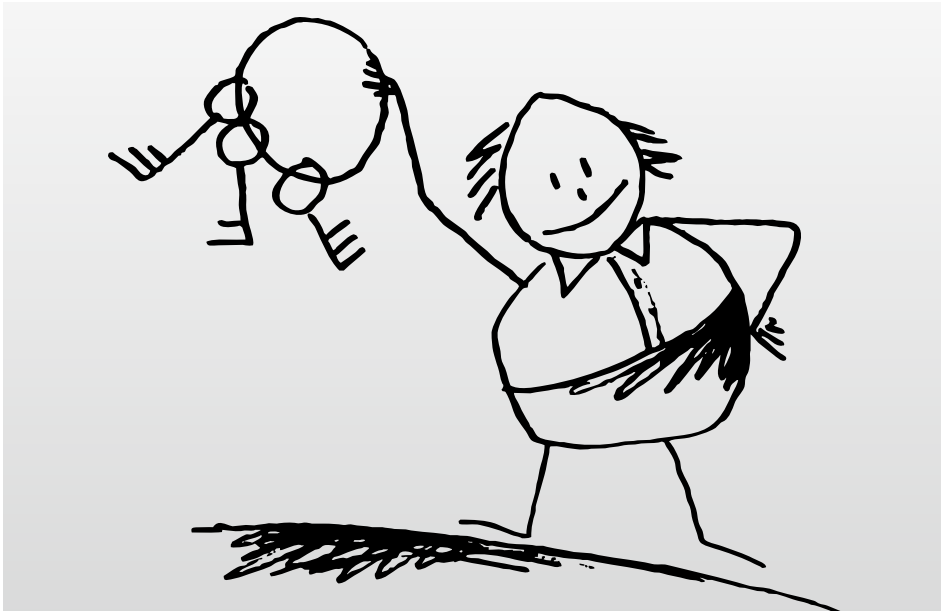


Secure access to eGovernment portals



Benefits:

- » **Secure, data-protection-compliant authentication**
- » **Tried-and-tested operation with over 1.3 million users**
- » **Central service for eGovernment portals and applications**

Whenever citizens communicate with authorities, they expect their data to be secure and protected. With an increasing range of specialised applications as an online-service, authorities need to be able to ensure the confidentiality, authenticity and integrity of these data. Citizens will only react positively to eGovernment offers if online services work simply and user-friendly without any additional technical equipment. **This is precisely where authega comes in: While the user page is kept simple, the solution on the provider's page is a complex and customisable central service component for secure authentication in online portals.** authega's technology has been proving its worth since 2004 in ELSTER, Germany's largest eGovernment project.

Tried-and-tested basic component for central supported data processing services

The authega technology was developed within the framework of ELSTER. As the central security platform it is continually being customised to new requirements for this procedure, such as the integration of the new german ID card for secure registration without media transfer. authega is designed to be a central service and as such can also be used as an authentication infrastructure component for other portals:

- The authentication service is set up once in the computer centre and is then basically available to other portals and applications via web services.
- Computer centres already have specific security structures working around the clock, of which authorities can make use for their own administrative procedures.

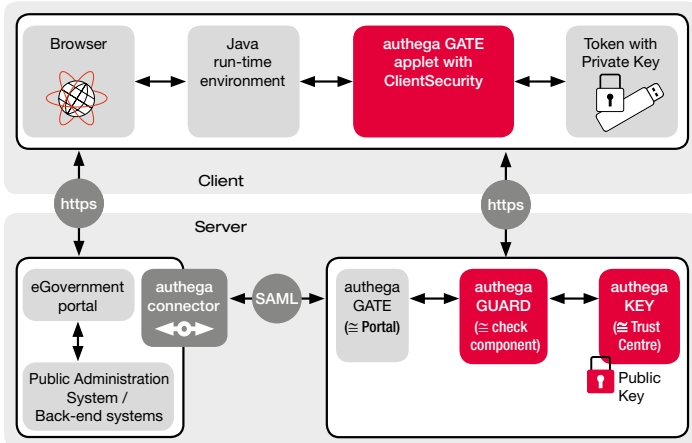
- With authega, eGovernment portals and applications get central supported basic services which can be accessed via web interfaces. Public administration authorities can then integrate these components seamlessly into their procedures without having to run them themselves.

The authega principle: data economy, security and protection

Only personal data details to be required by all means for identification and registration shall be gathered by authega; the identity check and allocation is done via the public administration identity management. authega provides the user's PIN-secured private key which is required for authentication during login, authega splits up tasks as follows: the platform is solely responsible for authenticating the user, while authorisation remains the responsibility of the public administration system.

This way, the greatest degree of data protection and flexibility is safeguarded.

secunet provides the security modules for authega



ClientSecurity for authega GATE

authega GATE is an accessible Java applet which can be executed on all standard operating systems and browsers regardless of platform. The crypto library embedded in the applet makes authentication in web applications possible. It also offers the option of including an electronic signature or user-specific end-to-end encryption. The client security is responsible for generating the keys and authenticating for system registration. This is done by querying the server-side authentication check component, authega GUARD. Additional functions can be added to the authega GATE applet: signature generation and decryption of documents which are stored encrypted on the server, e. g. official letters.

authega GUARD

The server-side authentication check component provides central security services for confirming the identity and electronic signatures of users. It is responsible for managing the registration and login process, the administration of a user-specific account (setup, activation, block) and the authentication when logging into the portal. The authega GUARD is implemented in the same way as GATE in Java and can be accessed flexibly via web services/SOAP. Its function can be upgraded to include signature checking, encryption of documents with the user's public key and logging of all security-relevant processes.

authega KEY

The trust centre component for key management makes it possible to assign keys and certificates on the basis of software keys, USB crypto sticks and smartcards. It runs completely automatically in unmanned operation and, in doing so, saves on administration cost.

authega – highly compatible and scalable

The individual components work on the user side with all standard browsers and operating systems. Automated registration processes enable lots of users to quickly, securely and reliably access the web services. authega supports a large range of security tokens: software keys, USB crypto sticks, smartcards. This way, the security level for access to the portal can be set up according to needs and specifically for applications.



ELSTER

What has become a firmly established "virtual" government service is the electronic tax return ELSTER. The basic idea

and pretence of ELSTER is an efficient and secure electronic transfer of all tax data between citizens, employers, tax advisors and tax inspectors, municipalities and organisations. Commissioned by the Bavarian State Office for Taxes, secunet implemented a security platform for the ELSTEROnline portal, which supports the authentication, encryption and electronic signature for web applications via certificate-based processes. The solution has been proving its worth since 2004; at the start of 2011, more than 1.3 million datasets had been transferred as part of the largest German eGovernment project. The security platform is being further developed and customised by secunet to meet new requirements on a continual basis.

Introducing the partners

authega is a joint product of CIO Stabstelle Bayern and the companies mgm and secunet based on ELSTER technology.

mgm technology partners adds its widespread experience in the technical design, implementation and quality assurance of secure, highly available and scalable portal applications to the services of authega as well as its integration into the respective target environment.

More information on mgm can be found at www.mgm-tp.com.



More information:
www.secunet.com/authega

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen, Germany

Phone: +49-201-5454-0
Fax: +49-201-5454-1000
E-mail: info@secunet.com
www.secunet.com