

PRODUCT



Encryption



Authentication



Digital Signatures



fideAS[®] web

fideAS[®] web in a nutshell

- Electronic signature and encryption for Internet applications

fideAS[®] web offers:

- low Total Cost of Ownership
- easy integration
- platform independence
- two-way authentication
- use of standards (HTML, XML, HTTP)

Typical applications:

- Online Banking
- Signing electronic forms
- Secure online portals
- secure web-based business processes

Sign online, just as you are used to do with your manual signature

Town halls, business companies, most public authorities – everybody is “online”. This means more and more processes will be done via Internet. But how is this possible, if under existing circumstances you have to sign a paper personally? The answer is fideAS[®] web.

Electronic forms – make your life simple.

fideAS[®] web is a user friendly solution for electronic signature and encryption of forms distributed via the Internet. You can now sign all forms electronically via Internet that you previously had to sign personally for legal purposes. Contracts, orders, order acknowledgements, forms for public authorities or even bank business can now be done online.

Obviously, private users save time and money using fideAS[®] web, but institutions offering this service have an even higher potential of saving money and efforts. All incoming information can directly be processed and integrated in existing workflows. Security and stability of processes will be improved, administration of processes can be centralized, storage of paperwork is not necessary any longer – all this yields significantly increased efficiency.

Electronic signature – fast, simple, secure



fideAS[®] web works according to the German signature law. Every user has a signature key, which can be stored on a smartcard or on a USB Token. Alternatively, the user can have a software key, which of course means a reduced level of security.

An example shows how it works:

A user wants to order something via Internet. He opens an order form, fills in all relevant data and clicks “send”. Another dialog opens, asking him to type his personal PIN which identifies him. Afterwards, the complete form or just the relevant data will be signed, maybe encrypted and sent. This is of the same legal quality as a handwritten signature. Within the vendor’s network, the order can be processed automatically.

An electronic signature can only be done with the combination of private key (e.g. on a smartcard – ownership) and the personal PIN (knowledge). This combination offers the highest security possible. An electronic signature does not only prove that the sender is authentic – receiving the form and opening it forces an automatic verification whether the form data were manipulated or not. Manipulation would instantly be displayed and / or reported.



fideAS[®] – amazingly simple.



Be sure. Be **ap₃ec**.
applied security

PRODUCT



Encryption



Authentication



Digital Signatures

Technical data:

Certificates

X.509

Supported Client Operating Systems

Windows 2000
Windows XP
Red Hat Linux
Suse Linux
and most other Linux systems

Supported Server Operating Systems

Windows 2000
Windows XP
Windows 2003 Server
Red Hat Linux
Suse Linux
Solaris 8
HP/UX 11
and many further Unix systems

Key Media

PKCS#11 Interface
PKCS#12 Software Key

Signature/Asymmetric Encryption

RSA

Symmetric Encryption

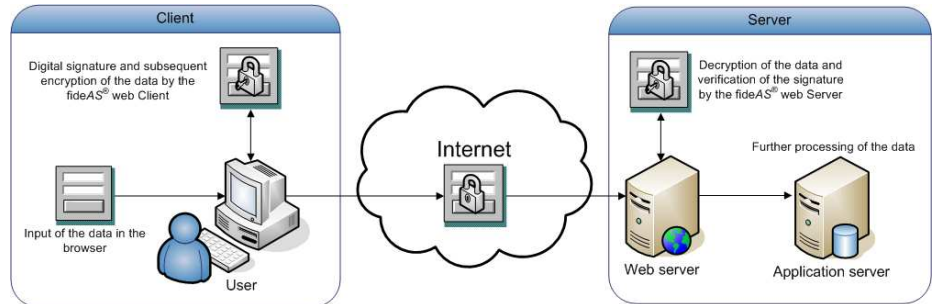
Triple-DES
AES

Hash Procedure

SHA-1
MD5

Internet Technology:

CGI-enabled web server
(e.g. Apache, IIS)
HTML
XML
HTTP
SSL



Functionality of fideAS® web

Signature according to existing law

In Germany and Europe the law says the private key has to be stored on a smartcard. The key itself has to be produced by an accredited trust center, in Germany e.g. T-TeleSec (T-Com) or Signtrust (Deutsche Post). fideAS® web works with any smartcard, as long as it provides a standard PKCS#11 interface. In Germany, you can use the electronic signature almost everywhere, where you had to sign personally in the past.

Strong encryption – keep the spies out

Often signature and correctness of content are not the only things you need in electronic business. Often you want to keep your data confidential, although you need to send it over an Internet application. By default, anything you send over the Internet is as open as a postcard.

fideAS® web is offering strongest encryption. We only use widely spread and best known standard algorithms - standards which have resisted all hack attacks. The receiver needs the correct key and personal PIN to decrypt your message.

Infrastructure behind it

fideAS® web server will be installed on a server of the institution. All forms will be in HTML format. Every user will receive a smartcard and smartcard reader (alternatively USB token or software key) allowing him to communicate with the fideAS® web server.

Talk to us.

apsec offers a wide variety of services dealing with all relevant questions of data security

Applied Security GmbH
Industriestraße 16
63811 Stockstadt – GERMANY

tel. +49 (0) 60 27 / 40 67-0
fax: +49 (0) 60 27 / 40 67-99
web: <http://www.apsec.de>
email: info@apsec.de

Consulting

Design of security policies, threat analysis, internal network security.

Network security

Internet/Intranet/Extranet security, access control for databases, firewalls, VPN, virus protection, remote access.

Software security

Cryptographic functions in applications, PKI, secure email, digital signatures, encryption.

fideAS® – amazingly simple.



Be sure. Be **apsec**.
applied security