WEBIDENTITY

THE UNIVERSAL TOKEN FOR INTERNET SECURITY

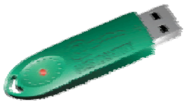
The Reader-less Smartcard

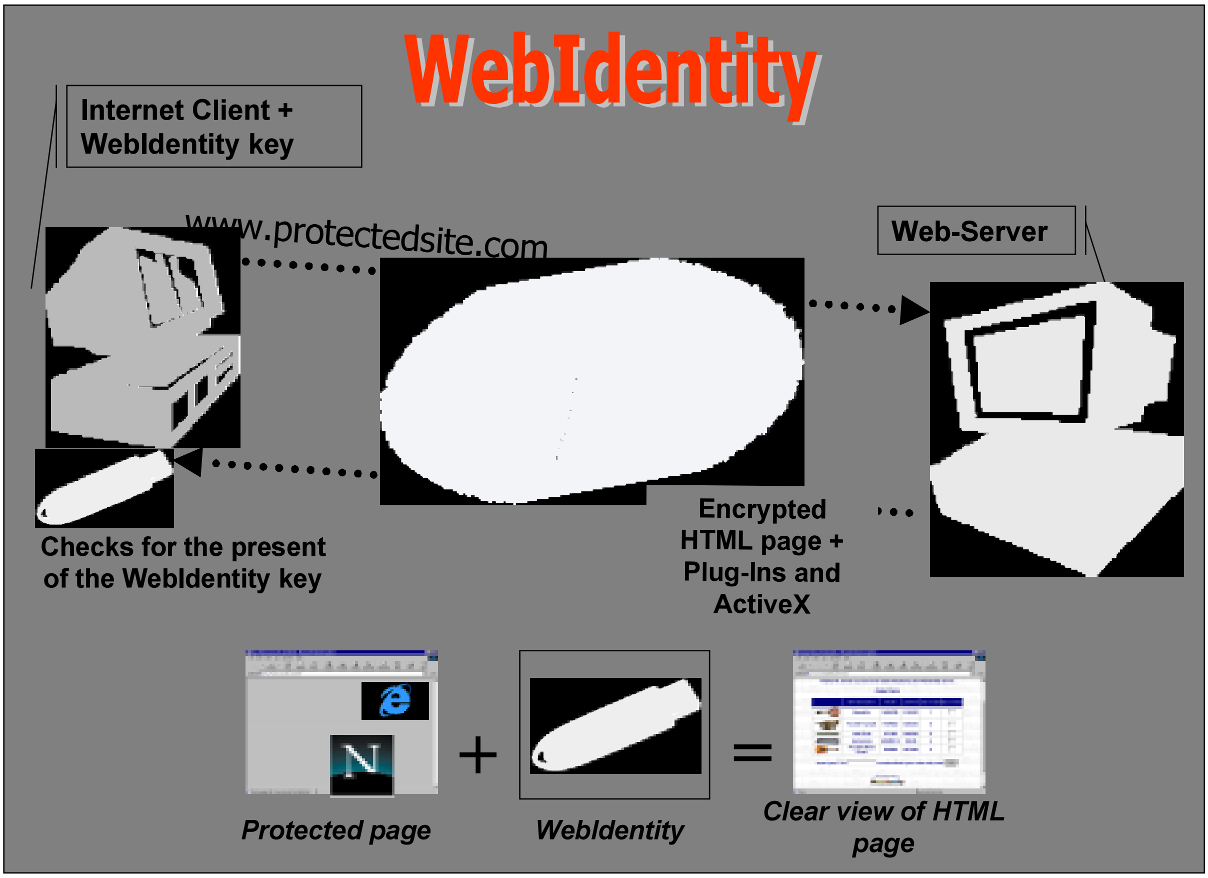
PRODUCT OVERVIEW

Developed by

Eutron

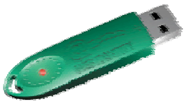
Securing Internet & Software




WebIdentity
Internet Client + WebIdentity key
www.protectedsite.com
Web-Server
Checks for the present of the WebIdentity key
Encrypted HTML page + Plug-Ins and ActiveX
Protected page
+
WebIdentity
=
Clear view of HTML page

WEBIDENTITY

is a hardware device which simply connects to the USB port of a Personal Computer. When it is plugged in it permits secure and unambiguous identification of the user and the transaction of the data, which is encrypted, in all Web-based applications for Internet/Intranet/Extranet.



INTRODUCTION

Internet is the most efficient means of distributing information. It has infinite potential; however, tools are needed which will allow you to carry out new tasks using a simple browser.

WebIdentity, which makes the most of the potential of the Web Server, allows secure access to confidential information on a Web Server connected to Internet.

WebIdentity was developed with the idea of making it possible to unambiguously identify the user of an Internet service and to guarantee access to confidential information held on the site. This must only be allowed following identification and authorization by the Web Server.

Once a user has been identified and authorized, **WebIdentity** technology allows for the secure exchange of information between the Server and the Client. This higher level of security the information is attainable thanks to powerful encryption algorithms which protect the information sent by the Web-Server to the Client and vice versa.

Moreover **WebIdentity** assures further verification of the integrity which is useful for discovering if the encrypted file has been intercepted or changed.

The encryption is based on private key, time-dependent algorithms and are linked to a serial code written at the hardware level within **WebIdentity**.

All of the above features are based on the potential of the **WebIdentity** hardware token, which is similar to but better than a smart card and allows for identification of the user to which it is associated.

WebIdentity is the result of more than ten years of Eutron's experience in the development of security solutions for companies. Eutron is the third vendor worldwide in the design, manufacturing and sales of security systems for the protection of software from illegal duplication: this is an undeniable guarantee for our customers.

A peculiarity of the device is the use of an ASIC chip (Application Specific Integrated Circuit) designed to be secure and at the same time flexible to use. The version with the USB interface has a microprocessor with similar security features which integrate with the hot-plug and plug & play functions available in many operating environments.

The **WebIdentity** token, which is available in different versions (parallel and USB ports and the new PC Wintel and Macintosh standards), allows access to protected areas both from the most recent PCs and from those of previous generations.

I.S.P.s (Internet Service Providers) or I.C.P.s (Internet Content Providers) that have to protect the content of a Web Server (whether it be in the form of HTML pages or a Web-Based database accessible through a Browser) simply have to give the users of their service a properly initialized and programmed **WebIdentity** token. The end user doesn't need anything else.

SETTING THE SCENE

The probable user of **WebIdentity**, the development software at the base of the product, is whoever is interested in protecting the access to information on a Web-Server or, in other words, setting up a VPN (Virtual Private Network).
The know-how requirements for the use of the product by the operational team are very low. One must be familiar with Internet and how it is used, have knowledge of HTML 4.0, JavaScript, Visual-Basic Script, be familiar with the management of Microsoft Internet Information Server.

In any case, the development Kit is supplied with a complete and exhaustive set of manuals as well as a large number of sample applications. All this makes the SDK an easy product to introduce into the company and thus the TCO (Total Cost of Ownership) is extremely low.

THE PROBLEM: TO IDENTIFY A USER ON INTERNET

Today, more than in terms of performance (which is exceptional when compared to other forms of communication) Internet is lacking in the means of unambiguously identifying the user requesting access to protected information.

Identification turns out to be the most critical phase in the process of distributing classified information. This is because, once the user has been identified and authorized, it is possible to proceed with both measured and selective distribution of the information.

In some cases, the unambiguous identification of the user has provoked the abandonment of Internet as a means of moving information which was at risk of being intercepted by unauthorized people.

The widespread adoption of VPNs (Virtual Private Networks) has come up against a problem in the fact that it is impossible to be totally sure of the identity of the user connecting through a remote client on the web.

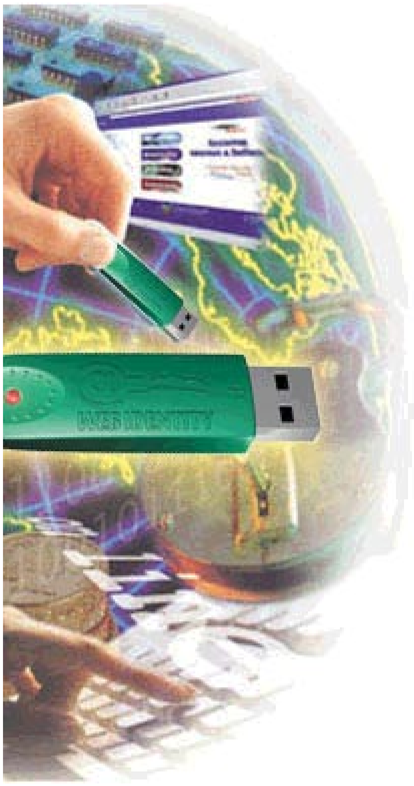
The lack of protection and the resulting risk of sensitive company data falling into the wrong hands endanger the existence of the company: the size of the problem can clearly be appreciated.

What also becomes clear is that if good security mechanisms can be made available, Internet could become the best tool available not only for the free distribution of information but also for sharing of confidential resources without geographic or territorial limits.

This is the reason the analysis model adopted by Eutron foresees an association within the database which is resident on the WebIdentity Web-Server, with a well defined user profile which contains any restrictions or authorizations relative to the user in question.

Independently of Internet, the user identification process can be carried out in different ways:

- I KNOW: I prove my identity since I know it (e.g. login and password)
- I GET: I prove my identity since I have it (e.g. smartcard)
- I AM: I prove my identity since I am it (e.g. biometrics readers)



From the above outline it is clear that to identify a user based on physical features (I AM) or on possession of something (I GET) offers major guarantees of security than identifying him on the basis of I KNOW.

THE SOLUTIONS ON THE MARKET TODAY

Depending on the type of application, there are various methods of identifying the user of a service (independently of Internet).

The same systems, when used for identifying the user of Internet/Intranet, soon came up against their limits and this is principally because of the way they are built.

Starting with the most highly sophisticated systems, there is hardware for biometrics recognition (I AM), which is probably used more often in spy films than in the real world, which has a prohibitive cost, at least for the moment. Probably in this case we are talking about recognition systems which provide near 100% certainty. However the factors which limit their widespread use are clear, at least in the short term.

Going back to solutions which can be applied in the Information Technology and Communications fields, there are solutions on the market which are based on hardware token Smartcards (I GET) which have purpose built readers and writers and serial, PCMCIA or USB interfaces. The basic concept of solutions based on the use of Smartcard readers, like the case of **WebIdentity**, foresees possession (I GET) of a hardware token in which information relative to the identity of the user is written. However this solution was widely used in local area networks but not in Internet. In reality, the limitations of this type of solution are due to the dependence on hardware which is far from being standard: in the real world personal computers are very rarely fitted with a Smartcard reader. The solution adopted in most cases is based on the binomial of login & password. This type of solution certainly has a number of benefits (zero cost, absolutely standard, easy to manage) but also has a number of built in drawbacks which have limited the target market to low level applications (quick and easy to clone, therefore producing the waterfall effect).

Today logins and passwords are widely used in Internet for the protection of restricted areas of a site which probably cannot contain really vital information.

However, many sites have adopted measures which include the use of less usable tools which are more expensive, more complicated but more secure than Internet itself: let’s take the case of a large organization with a distributed sales network which has to update its archives daily (possibly using Lotus Notes). These archives contain information regarding the availability of goods in stock, the latest price lists, marketing and technical support information etc. Internet could be a more cost effective solution (it’s only a local call away) as well as being quicker (for example through the downloading of documents and a database with a web interface. But till now no solutions have emerged which give the same level of security.

WEB IDENTITY

THE UNIVERSAL TOKEN FOR INTERNET SECURITY

THE NEEDS: SECURITY AND STANDARDS

Leaving out the biometrics proposition for reasons of practicality and cost and the login and password solution for the above mentioned reasons, the ultimate solution for the unambiguous recognition of a user is through the use of a hardware token, regardless of the network.

While working in a local environment (a company network, for example) a solution based on Smartcards associated with appropriate readers in an Internet environment, which foresees widely used and, more importantly, distributed applications, can be easily implemented, however the chosen solution must not cause problems to the end user of the service.

In this context, the need is for a system which is both secure, unambiguous and standard.

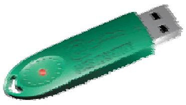
What becomes clear is that both Smartcard based systems and those based on logins and passwords are lacking in the fundamental requirements of practicality and security.

Regarding the safeguarding of information, once the Web-Server has been protected and the user has been unambiguously certified (we have already stated that this will be through the use of a hardware token) it becomes relatively easy to determine secure communications algorithms.

Last but not least, what about the digital signature in the final phase of the stipulation of an agreement. Very soon everyone will be able to buy things, sign agreements or submit declarations via Internet. In this area too, it will be necessary to identify the person connected and assure the non repudiation of his transactions. These are other problems which will have to be solved right away.

Eutron has been making hardware tokens with both parallel and USB interfaces, today's and tomorrow's standards, for other uses in the field of information security for more than 12 years.

The Know-how acquired by Eutron in 12 years of development of information security systems, both at a hardware and a software level (the SmartKey and Smartlock products) has enabled Eutron to come up with a technologically advanced solution which permits the recognition of the user associated with **WebIdentity** and to handle secure transactions between the server and the client (and vice versa), as we will see later in this paper.



Eutron’s answer is WebIdentity: THE SECURE AND FLEXIBLE DEVICE

Eutron’s **WebIdentity** allows you to supply secure access to confidential information residing on a Web server connected to Internet.

Thanks to advanced cryptographic technology, Eutron’s **WebIdentity** can ensure secure, ciphered data exchange over the Web.

A peculiarity of the **WebIdentity** device is the presence of a programmable component within its circuitry. Depending on the version being used, the device connects to a personal computer via the parallel or USB port. This means that Eutron’s **WebIdentity** can be used with any personal computer without having to buy and install extra, expensive hardware (e.g. SmartCard reader).

If on the one hand the guarantee of security and confidentiality of the information during transfer from server to client and vice versa is maintained, on the other the physical interface of the device represents the state of the art in information technology.

The parallel port is an absolutely standard feature of any personal computer, whether it be of the latest or previous generation, and the USB interface has become a unified standard of Wintel, Apple and others in the way of input/output of information.

One peculiarity which is certainly worth noting is the total independence of **WebIdentity** from any other additional hardware devices: this means that we can be certain that the user can use the Internet service seamlessly from his office, home or the airport and from any personal computer connected directly or indirectly to Internet.

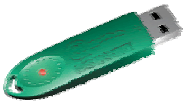
Recognition of the user of the service is always unambiguous and secure in as much as the authentication is based solely on information stored in the token and on the relative password and not on hardware and/or software installed permanently on a personal computer.

The security of the system is the merit of the features of the WebIdentity hardware token: The key has a writeable memory.

The way the device is made means that it is perfectly secure and cannot be cloned: the generation of the PIN, which is the identifier of each individual device, is through a number of parameters relative to:

- the Label defined by whoever is supplying the service;
- the Password defined by whoever is supplying the service;
- the Description of the user;
- a special code at the hardware level of the device defined by Eutron in the manufacturing phase of the key

All this information is stored in the device and is protected and encrypted in such a way as to make it impossible for unauthorized persons or software applications to gain access: only the Web-server knows all the identifying elements of a particular user or device and thus only the Web-Server will be able to recreate the encryption key of the data in the device and the only element capable of “seeing” the content of the key.



AN OVERVIEW OF HOW WebIdentity WORKS

In the previous paragraph we defined the aim of Eutron's **WebIdentity**: to guarantee access to information on a site only to the properly identified and authorized user and to provide for the secure interchange of information over the web.

To manage this, Eutron has developed software components, ActiveX and Plug-Ins, which leverage the storage and encryption potential of the **WebIdentity** device allowing access to a site only to a user in possession of a properly initialized token supplied by the service provider.

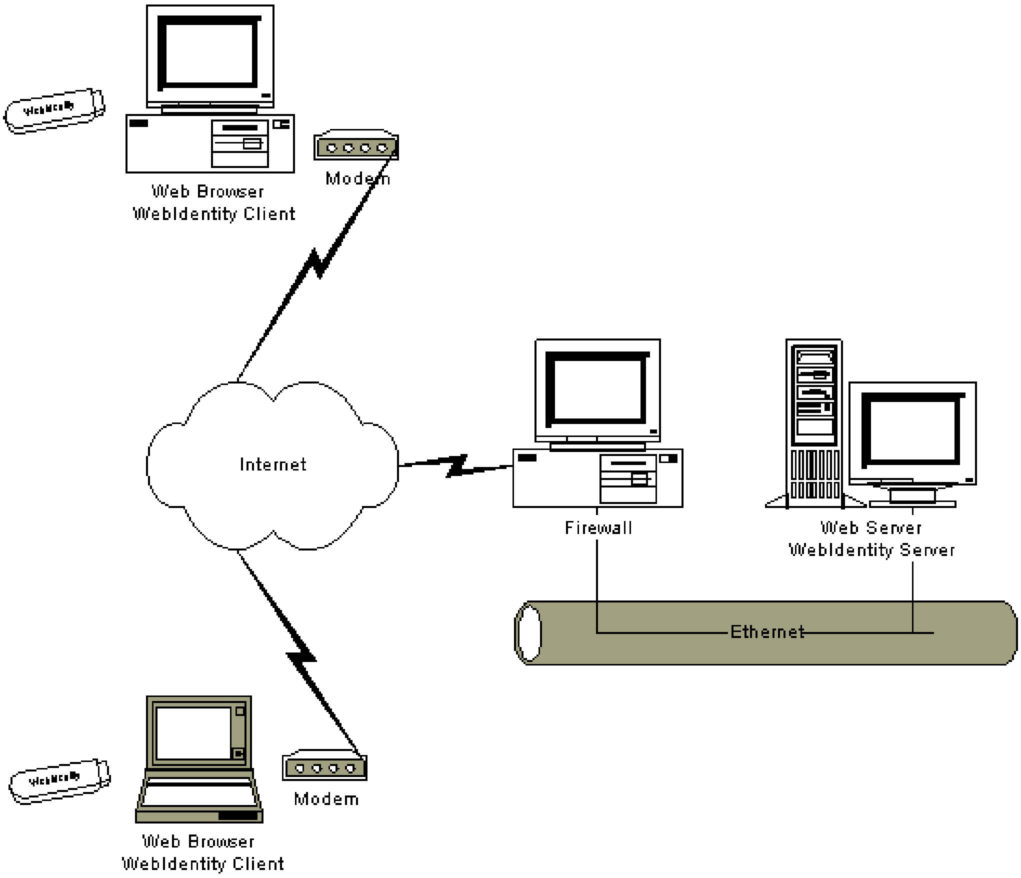
The check of the identity of a user is carried out by means of a process which requires the fulfillment of the following three simple tasks:

1. *Initialization of the **WebIdentity** token* to give to the beneficiary of the service which needs to be protected and the creation of a database which contains the identification certificates (PIN) associated with the different users. The service provider – for example an ISP – that wants to protect his Internet site has to give a previously initialized **WebIdentity** to each of his users. As well as programming the **WebIdentity**, the initialization stage returns a PIN number which will be used by the server to identify the user.

2. *Verification if an intialized **WebIdentity** token is present on the client*; reading, encryption and marking of the PIN number, transmission of the processed PIN number to the server for identification.

Using a JavaScript, a read method is invoked in the ActiveX or Plug-in during the download of a protected page. This operation makes the PIN number contained in the key available for transmission to the server. The PIN number is duly encapsulated in a particular structure whose purpose is to disallow its deciphering or alteration. The use of a time dependent key code sent from the server to the client and the use of data known both to the client and to the server makes it possible to send different computations for different connection sessions. This avoids the reuse of PIN numbers already coded and sent.

Transmission of the coded PIN number uses the POST method or the GET method of the HTTP protocol; this solution makes **WebIdentity** supplied protection transparent to the use of any Firewall and/or proxy allowing you to maintain unaltered existing server security systems aimed at preventing access to information on the Web Server protected by **WebIdentity** by unauthorized, malicious persons; moreover, using this solution allows us to guarantee that it will work with any system capable of using a common Web Browser and Internet navigation.



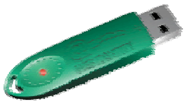
3. *Decoding of the PIN number on the server; identification of the user. Transmission of the information to the client if the user is authorized.* When the processed PIN number has been received, it is decoded by the DecryptPin method of the ActiveX; then a search is made for the decoded PIN in the user database and when it has been found and a validation check has been performed, the requested page is sent to the client. If the code is not authenticated a number of defense measures can be taken, among which that of sending an "access denied" page or of sending a page with a set of meaningless data or re-routing the user to a site with a totally different content and so forth.

As well as positively identifying the user, Eutron's **WebIdentity** technology lets the service provider do another very important thing: send encrypted data over the Internet.
To access information of interest to him, the user need only connect his personal **WebIdentity** token to his personal computer and access the site as if it were not protected at all.

In total transparency, the server is able to securely and unambiguously identify the client and permit only the consultation of information pertinent to that client.

The ciphering systems used are capable of customizing the code key and thus the coding of the data itself based on the user code and on a number which identifies the session.

Such a system prevents pages saved locally or held in cache from being reused to access the server, or the information contained in these pages can be made available, not only to people who normally wouldn't be able to access the site, but also to other clients of the same service but different from the one that initially downloaded them.



CONCLUSION

The rapid evolution and widespread use of Internet and mobile computing have substantially changed the parameters for the handling of security measures in organizations.

The user has to be given the most seamless and economic remote access possible and at the same time care must be taken to make sure that unauthorized access cannot limit or render meaningless the confidentiality of sensitive data of vital importance to an organization.

Thanks to a token of very limited dimensions (**WebIdentity** is no bigger than the house key we use every day) EUTRON is able to provide security and flexibility in the field of user recognition and the transmission of protected program information over LAN, WAN, VPN, e-commerce, Mobile Computing.

WebIdentity is the state-of-the-art solution in the field of computer security technology which can be applied wherever there is a need to check and distribute selective information over Internet. With **WebIdentity**, a level of security of Internet services can be reached which was unattainable until today. The unambiguity of user identification, high protection and encryption levels of the information in transit over the public network, the availablity of standard interfaces on every personal computer all mean that it can be used for an enormity of solutions.

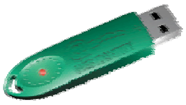
The truly innovative approach of **WebIdentity** *lies in its total hardware independence*: **WebIdentity** does not require any additional hardware (not like Smartcards for example), and also makes use of standard PC interfaces used by past, present and future generations of PCs (**WebIdentity** is available with parallel and USB interfaces).

Eutron's solution is available NOW for all practical user applications:

- Access Control to Web-Server;
- Access Control to intranet or VPN;
- Access Control to Web-based Databases;
- Time or Subscription based Access Control;
- On-line banking, Benefits administration, account management
- Controlled Distribution of software via Internet ;
- Sale of Services over Internet ;
- Integrazione with PKI and electronic signatures;

In any situation, **WebIdentity's** innovative features stand out above the others:

- **Simple integration:** Eutron provides a Software Development Kit (SDK) with the product which permits Partners to integrate **WebIdentity** rapidly into their application software.
- **Security**: **WebIdentity** handles 416 bytes of internal memory which is protected by a double access code and in which the user information is stored. The parameters which are necessary for the definition of the time-dependent encryption key for protecting the transactions are protected within the device.
- **Reliability**: **WebIdentity** is the natural evolution of Eutron's SmartKey, the hardware key for software protection which has been sold worldwide to over a million users in the past ten years.
- **Low cost**: **WebIdentity** is the most cost effective solution available today compared to any other hardware



authentication device on the market (e.g Smartcards)

- ✓ **Easy to use**: the user only has to plug his **WebIdentity** into the USB port of his personal computer (or piggy-backed to other equipment): the Plug&Play features of peripherals with USB interfaces together with the fact that no other hardware or software components are needed make **WebIdentity** truly plug & play.
- ✓ **Compact:** The **WebIdentity** token is very manageable for the user thanks to its size. It is no bigger than an everyday housekey.
- ✓ **Transportable**: the reduced size and the total hardware independence make it the ideal instrument for mobile computing
- ✓ **Appealing**: the size and the appearance of the product make it an ideal gadget with a view to gaining customer or user fidelity.

The technicians and sales staff of Eutron are available to answer any questions about areas where **WebIdentity** can be used. For further information, please visit our Website at www.eutron.com, where you will find numerous practical implementations of **WebIdentity.**