The Key to Secure Web Sites

CONTENTS

1. AREAS OF USE

- SECURE WEB SITES
- INTERNET, INTRANET & EXTRANET
- CORPORATE USE

2. IDENTIKEY™ ™ WEB SITES

- STATIC PAGES
- DATABASES AND WEB SERVER PROGRAMS

3. THE SOLUTION

- IDENTIKEY™ ™ SERVERSOFTWARE
- CLIENT-SIDE
- IDENTIKEY™ ™ - THE KEY

4. STRONG AUTHENTICATION

- CHALLENGE/RESPONSE PROTOCOL
- IDENTIFICATION AND ACCESS LOGGING

5. SECURITY ASPECTS

- CHALLENGE/RESPONSE PROTOCOL
- THE DIGITAL KEY
- SECURITY LEVELS FOR THE USER

6. COMPARISONS

- PASSWORDS
- ENCRYPTION
- SMART CARDS

7. PRICING

8. CONTACT

1. AREAS OF USE

SECURE WEB SITES

Identikey™ enables enterprises to control access to websites and protect sensitive data. Progressive companies recognise the potential of the Internet for sharing information, but are unable to use it to its full potential due to security risks. Today's companies need a secure, auditable authentication scheme based on the latest industry standards which can be used over regular Internet connections. Identikey™ is the key to solving this problem.

INTERNET, INTRANET & EXTRANET

The solution is ideally suited to securing any Internet, Extranet and Intranet Site. Identikey™ is a complete authentication system which fully integrates with the latest Web server software to provide a total solution to security issues on the Internet.

CORPORATE USE

Identikey™ is the ultimate solution for the following business areas:

- **Geographically dispersed organisations (eg. Franchise groups)**

- **National and International Offices**

- **External or Travelling Employees**

Geographically dispersed companies can now save on distribution costs for any information material. The sensitive data for all locations can be controlled and managed centrally on the server. Save your partners from maintaining extensive manuals; each location can be set up to only view information pertaining to them. The solution works perfectly for travelling users; they only require Internet access and a web browser.

- **Key-Accounts**

You can now set up customised websites for your most important clients. These sites could include account details, order status and allow your client to order directly online. Identikey™ enables your organisation to deliver superior customer service and strengthen the relationship between you and your clients.

- **E-Commerce, Internet Subscription Services**

With Identikey™, organisations offering high-quality products and services over the Internet can now control and monitor their customer's access to specific sites. Customer access can be granted and denied with a few mouse-clicks only.

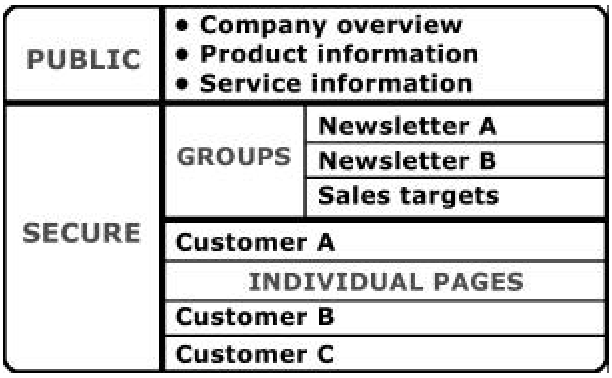
- **Business to Business, Strategic Partners**

Identikey™ is the key to a close business relationship. The solution enables you to share all relevant areas of your Intranet with your business and strategic partners.

2. IDENTIKEY™ WEB SITES

Identikey™ enables corporations to split their web sites into different areas. A web site can now be divided up into a public area which contains information such as a company overview and product or service information and a secure area which can be customised further.

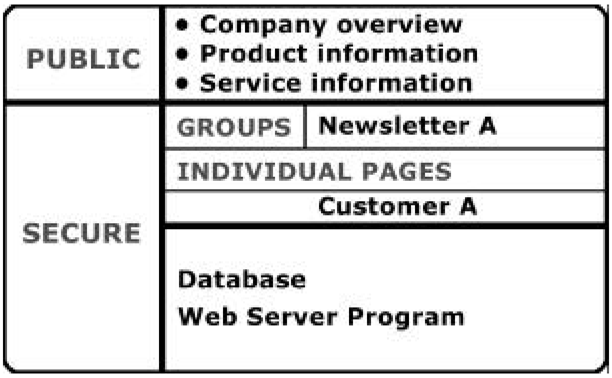
STATIC PAGES


PUBLIC
• Company overview
• Product information
• Service information
SECURE
GROUPS
Newsletter A
Newsletter B
Sales targets
Customer A
INDIVIDUAL PAGES
Customer B
Customer C

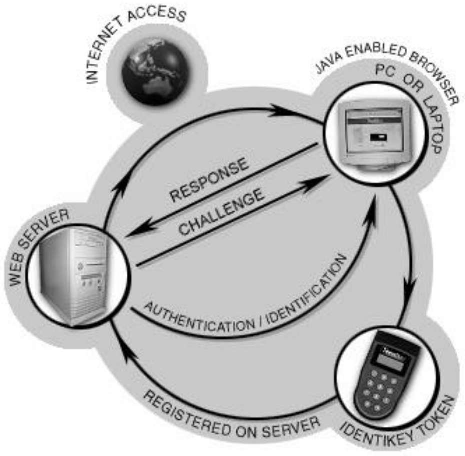
The example on the left shows a corporation that protects static web pages in their secure area. All of their clients are set up to access the confidential newsletters, either version A or B. The external sales staff has access to both newsletters and additionally to a page containing quarterly sales targets. Furthermore the corporation established individual pages for its key-accounts. Customer A, for example, is set up to access newsletter B and the individual Customer A page which features special promotions for this customer.

DATABASES AND WEB SERVER PROGRAMS

The example on the right shows a company that also maintains confidential newsletters and individual information on secure static pages. Additionally, they are operating a web based tracking program which is only accessible for specific employees in several international office locations. Another group of employees has access to a database editing and maintenance page that allows them to update information which is then displayed in the public area of the site.


PUBLIC
• Company overview
• Product information
• Service information
SECURE
GROUPS
Newsletter A
INDIVIDUAL PAGES
Customer A
Database
Web Server Program

3. THE SOLUTION


INTERNET ACCESS
JAVA ENABLED BROWSER
PC OR LAPTOP
RESPONSE
CHALLENGE
WEB SERVER
AUTHENTICATION / IDENTIFICATION
REGISTERED ON SERVER
IDENTIKEY TOKEN

The solution consists of Identikey™ server software and a digital key, the Identikey™ .

IDENTIKEY™ ™ SERVERSOFTWARE
Identikey™ runs on a Windows NT 4.0 or higher server. Four programs complete the server software and offer the option to customise the solution to meet the individual needs of any enterprise.

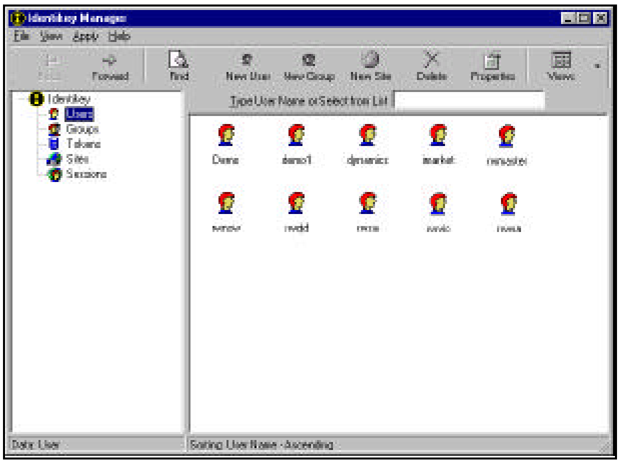
There are four main components to the Identikey™ security system as follows:

1. A Java-applet produces the blinking barcode on the monitor and transmits the challenge produced on the server.
2. An Active-X Server component which allows programmable access to the Identikey™ database so that a totally customised interface is made possible.
3. The ISAPI filter is integrated in the Internet Information Server (IIS) 4.0 and strictly controls and monitors all access to site resources.
4. The Identikey™ Manager which serves as the interface through which the security administrator manages all registered users, groups, tokens and sites.

The user-friendly Identikey™ Manager includes the following functional areas.

Users.
This area allows the administration of all user information, the Identikey™ tokens that the user currently has and which sites the user can access.

As a security measure, the user can be locked or disabled. Furthermore the administrator has the option to make access dependant on the weekday or even on specific hours during any day. Using these combinations, a totally individual portfolio can be set up for each user containing a different mix of secured group sites, individual sites and site resources.


Identikey Manager
File View Apply Help
Forward
Find
New User
New Group
New Site
Delete
Properties
Views
Identikey
Users
Groups
Tokens
Sites
Sessions
Type User Name or Select from List
Demo
demo1
dynamics
market
ransaster
Data: User
Sorting: User Name - Ascending

Groups.
For large sites where user privileges need to be centralised, groups can be established. Groups enable the same privileges as users but may then be applied across a number of users simply by making the user a member of the group. Changes to security may

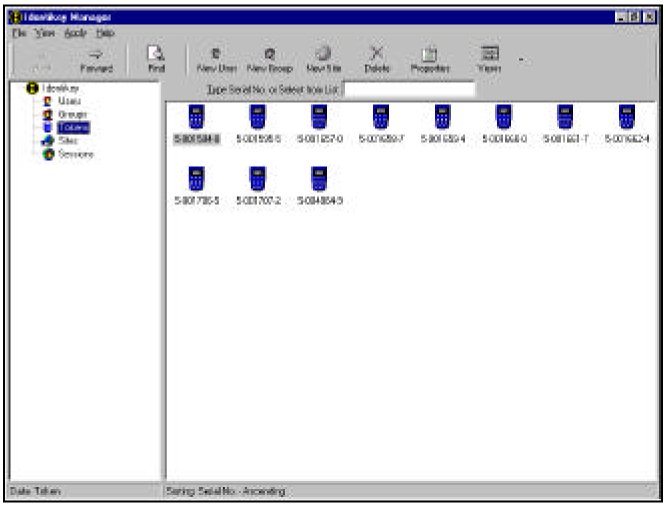
then be applied to the group and will automatically change the privileges for all users within the group.

Sites.
Each Internet site protected by the Identikey™ system must be registered within the Identikey™ Manager. Site details include the name of the site as well as the IP Address and challenge details to be presented for access to the site. Site resources, such as directories and files or documents are also registered. Only registered resources can have security set by users or groups.

Sessions.
This area enables the administrator to view the current users logged on via Identikey™ security. Details include the user name, which token was used as well as the session start time and when it is expected to expire. Sessions may also be logged out via the administrator to ensure that changes to the security database take immediate effect.

Tokens.
The security administrator can load new keys and administer any existing keys within this area. Identikey™ includes a deblock function so that if a user forgets their PIN or a stolen token is recovered, Identikey™ can unlock the token by entering the token's deblock code.

Access to sites is recorded on a token basis and using the managers built-in audit functions allows total tracking of all site accesses.


Identikey Manager
File View Tools Help
Forward
Find
New User
New Group
New Site
Delete
Properties
Views
Type Serial No. or Select from List
Identikey
Users
Groups
Tokens
Sites
Sessions
Date Taken
Sorting: Serial No. - Ascending

CLIENT-SIDE
To view the individually secured portfolios users require Internet access and the registered PIN-protected Identikey™. While travelling this can be done in the office centre of a hotel or even in an Internet Cafe. Unlike many other systems the Identikey™ solution does not require additional software on the client-side. This offers a maximum level of flexibility and mobility for users. Identikey™ supports Laptop users by offering them a LCD-Screen option which has been optimised for the specific requirements.

IDENTIKEY™ - THE KEY
The Identikey™ is a digital key that allows DES (Data Encryption Standard)-based authentication. A PIN needs to be entered to activate the key before each use. After a wrong PIN has been entered several times the key locks itself and can only be re-activated by the Identikey™ Manager. Before the Identikey™ can be used, it needs to be registered with the server software.
The key is battery-operated and has a lifespan of seven to ten years depending on the frequency of use. A "Low Battery" warning is provided and can be customised to the users needs.

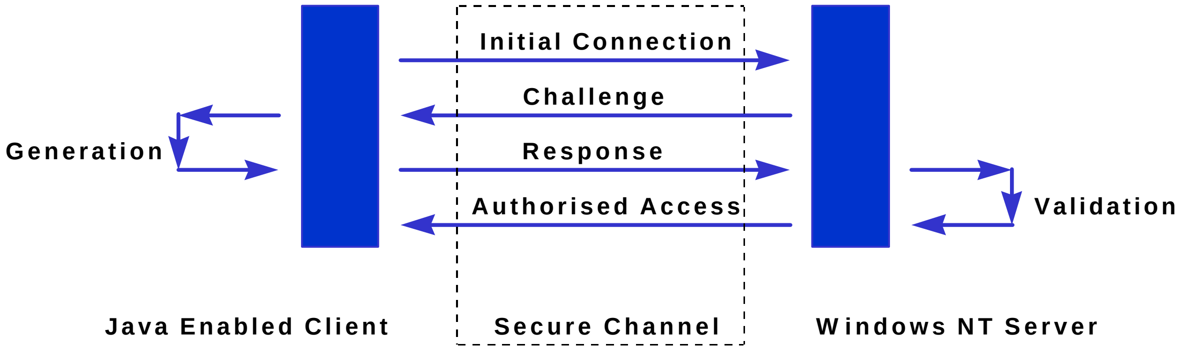
Identikey
INTERNET SECURITY
1
2
3
4
5
6
7
8
9
0

4. STRONG AUTHENTICATION

CHALLENGE / RESPONSE PROTOCOL

The initial connection is made by the user accessing the webpage containing the challenge. By holding the optical interface of the activated key up to the flash on the screen the key can now read the challenge and calculate a key-specific response which will be shown on its display. The response needs to be entered via the keyboard and sent to the server within a minute. If the user fails to enter the code within that time-frame the challenge/response protocol expires and a new challenge is sent from the server.

Entering the right response within the set time-frame enables the user to access secure website areas as authorised in the Identikey™ Manager.



IDENTIFICATION AND ACCESS LOGGING

Each key produces a key-specific response to an identical challenge. This enables the Identikey™ server software to identify the user according to the key being used. Access will then be granted or denied according to the parameters set for the specific user. The access log registers the access time and visited site each time access is granted to a user. This function adds an extra level of security for your enterprise as it allows the security administrator to monitor each visit to the protected sites.

5. SECURITY ASPECTS

CHALLENGE / RESPONSE PROTOCOL

The challenge/response protocol is a dynamic, time-based protocol. It is based on mathematical functions and is not predictable. Each access requires a different challenge and a different response. Additionally, each key produces an individual response to an identical challenge. Even if a user is being watched while entering the response this access code is useless for the next access.

Each challenge is only valid for a short period of time after which a new challenge/response protocol is generated by the server. There is an even shorter time-frame for the user to enter the correct response which virtually makes it impossible to guess a response.

THE DIGITAL KEY

The Identikey™ is protected by several mechanisms. A customisable PIN protects the key from misuse by any unauthorised user. When a wrong PIN is entered, the display on the key presents the user with a “FAIL” message. After a preset number of PIN errors is reached, the key will lock itself. It can only be unlocked by the Identikey™

Manager based on a reversed challenge/response calculation. It is not necessary to ship the key back as the unlocking procedure can be completed over the phone. Furthermore, if a key is lost or misplaced the security administrator has the option to disable or lock the account permanently. The key allows DES (Data Encryption Standard)-based authentication. The Identikey™ Manager takes it one step further and offers triple DES as an added security feature.

SECURITY LEVELS FOR THE USER

The Identikey™ Manager allows the security administrator to allocate different security levels to each user. This can be achieved by allowing or disallowing access to individual sites and resources or by allocating special properties, such as restricted access on certain weekdays or on specified hours during the day. A user can be disabled or permanently blocked with a few mouse-clicks if this is required.

6. COMPARISONS

PASSWORDS

Static, reusable passwords are a security risk to each enterprise and its clients. They can be guessed, "hacked", read from the keyboard or told to a friend. Once compromised, a password can be used by many people many times, exchanged by e-mail or posted on a public site. The material damage for an enterprise can be immense, not to mention restoring the company's image. Passwords are not sufficiently secure to be trusted as the only authentication tool to protect your sensitive data.

ENCRYPTION

Encryption protocols such as SSL will protect data while it is in the communication channel but they can't guarantee that the person at the other end of the encrypted tunnel is authorised to access the data. Encryption does not offer the flexibility Identikey™ offers for each user account. Our recommendation is to use Identikey™ in combination with an encryption protocol, such as SSL, to achieve a maximum level of security.

SMART CARDS

Smart cards require card readers on the client-side. Obvious disadvantages of this system are costs associated with setting up the card readers in various locations and ongoing maintenance of the hardware. Smart cards simply do not offer the same geographic and user-related flexibility as Identikey™.

7. PRICING

Identikey™ pricing is based on a single fee per Server installations and then token licence packs depending on the number of tokens installed on a server. Discounts apply depending on the number of token licences purchased at the same time.
Exact local pricing may be obtained from your authorised Identikey™ reseller.

8. CONTACT

Manufacturer: Identikey Pty Ltd
Ground Floor, 143 Coronation Drive
PO BOX 1606
Milton, QLD, 4064, Australia

Tel: +61 7 3236 5050
Fax: +61 7 3236 5850
E-mail sales@identikey.com