



# Vision, Products & Solutions

**CONFIDENTIAL AND PROPRIETARY**

**This document includes confidential and proprietary information of Made4Biz Inc..  
Contents may not be disclosed to a third party without the express permission of  
Made4Biz, Inc. Features and pricing are subject to change.**

- **Vision**

**IDentiWall** is positioned as:

- Authentication platform which mainly, but not exclusively, revolves around the user's mobile phone.
- Secured web transactions platform.
- Secured eBanking platform.

As a platform **IDentiWall** is designed to support multiple authentication methods as well as various transaction security technologies. In this way it can secure not only the authentication phase at the beginning of the session, but rather all the session up to its secured conclusion.

**Made4Biz** is committed to constantly enrich **IDentiWall** with new methods and technologies in existence today and those that will become available in the future, as well as to incorporate protection against new threats as they emerge. That ensures that IDentiWall customers are guaranteed a state of the art platform that incorporates maximum security, flexibility and ease of use.

## • Technologies

### ○ Authentication methods

- *Two Factor* – user's regular password and **IDentiWall**'s One-Time-Password (OTP)
- *One Time Password (OTP)*
  - *Event driven* password issuing
  - *Time driven* password issuing
  - *Pre-issued* password
  - *Seed driven* (RFC #: 2289) password issuing
- *EAP* support
- *LDAP* support
- *MD5* support
- *Voice ID* voice biometrics based authentication
- *Radius* support.
- *Token device* – support for physical token devices
- *Location - based authentication* – integration with **Made4Biz's Dynamic! Security**. These location- based authentication methods will be applied both for the user's location as well as for the location of the laptop.

### ○ Secured transactions

- *Block My Account* response over cellular network.
- *Encrypted OTP* which gets decrypted exclusively by Pin Code based Mobile Agent.
- *Transaction Verification* over IP and cellular networks.
- *Split Transaction* over two networks.
- *Session recording server*
- *Behavioral engine*

○ **SMS transmission**

- *SMPP protocol* supported by selective high end SMS Brokers.
- *Web Service (SOAP)* Published by various SMS Brokers.
- *API* provided by various SMS Brokers.

○ **Billing methods**

- *Pre-paid User License* – discounted SMS. The organization pays for SMS credit.
- *Pay-As-You-Go* – free User License but undiscounted SMS.
- *Reverse Billing* – the end user pays for SMS credit.
- *SMS paying through Billing server* – the customer or the user buys SMS credit from Made4Biz's Billing server.
- *SMS paying through external SMS broker* – the customer buys SMS credit from his SMS broker
- *SMS paying through Skype* – the customer or the user buys SMS credit from Skype.

○ **HTTP gateway**

This technology sits between the user and Web site and monitors the HTTP content that flows between these two. Typically the gateway reads the URLs that pass through and when it detects one that was pre-defined it looks into the HTML body as well. This technology helps in interpreting the HTML content and it can zoom into the content of a specific field and check it against the organizational policy.

For example: the HTTP gateway can go into a money transfer HTML form, check the content of the 'sum to be transferred' and the 'target account' fields, consult the organizational behavioral engine as to the compliance of the transaction and thereafter act upon its recommendations.

- **Radius server**

**IDentiWall** utilizes its own full blown Radius server.

- **SMPP client and server**

**IDentiWall** is an SMPP client and the SMS routing server, which is described below, is both SMPP client and server.

- **Security**

Support for SSL encryption as well as two-way SSL.

- **Secured registration**

This is a technology that helps users perform secured registration in **IDentiWall**.

- **LDAP client**

Authentication against LDAP servers such as MS-Active Directory.

- **SOAP client**

- **Mobile pre-installed agent**

A pre-installed **IDentiWall** agent on the user's mobile handset and performs various security tasks such as:

- Open up only after the user supplies a Pin Code.
- Decrypt those SMSs which were sent by **IDentiWall**
- Encrypt messages sent from the user's handset to **IDentiWall**
- Additional functions that are confidential at present...

○ **WAP pushed agent**

This WAP page that is actually an **IDentiWall** Mobile Agent gets pushed to the user's mobile handset together with the content that IDentiWall wishes to send to the user. This agent performs tasks such as:

- Open up only after the user supplies a Pin Code.
- Decrypt those SMSs which were sent by **IDentiWall**
- Encrypt messages sent from the user's handset to **IDentiWall**
- More functions that couldn't be discussed yet ...

○ **SMS Routing gateway**

**IDentiWall** or other products send their SMSs to the gateway and it redistributes them to the various SMS brokers depending on their coverage and associated cost structure. Communication to the server from the SMS originators can be accomplished via SMPP (in such case the gateway acts as SMPP server), SOAP or its published API. At the other end, the gateway communicates with SMS brokers via SMPP (SMPP client), SOAP, and published APIs of the SMS brokers. The gateway is designed to support over a billion SMSs per month.

The gateway works in conjunction with the Billing server that is described below. For this communication it supports a proprietary protocol that is in use only between the gateway and the Billing server.

○ **Behavioral engine**

This is an engine that records and follows up the user's behavior during their session. The engine is designed to record full patterns of behavior accumulated over time and determine whenever the user is going out of a known pattern. IDentiWall is designed to use such behavioral engine whether its his own or when it interfaces with an external one that is already in use by the customer.

○ **Recording server**

This server has the capability of recording and playing back HTTP user's sessions. When working in conjunction with the Behavioral engine, the Recording server can get instructions to start recording even in the midst of an ongoing session.

A recorded session gets saved for various periods of time depending on the organizational policy and in conjunction with the Behavioral engine's instructions.

○ **Billing server**

This is a web server that its main task is to:

- Manage the customer's profile
- Manage the user's profile
- Facilitate the SMS credit purchase both for customers and users
- Notify the customers and the users that their credits reached the minimum balance that they defined.
- Supports PayPal and other payment options
- Multiple pricelists

○ **Syndication server**

The Syndication server is designed to facilitate cooperation between parties who wish to do so. For example:

- Insurance companies who wish to deploy **IDentiWall** for the insurance brokers. In this situation the relationship is a many-to-many relationship (insurance company has many brokers and each of the brokers is connected to many companies).
- Emergency notification of terror event. This could be used in real time by universities to notify their students of a security event that gets unfolded.

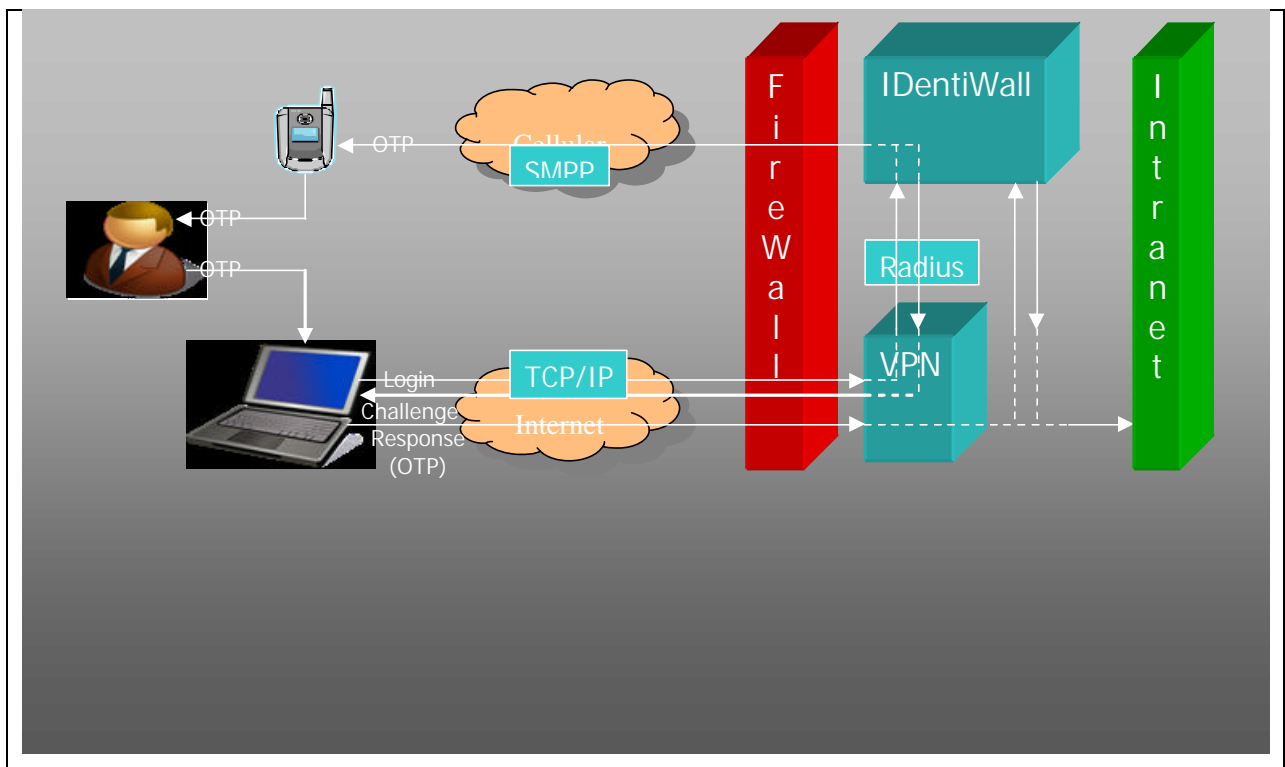
- **Products**

- **IDentiWall VPN**

- **Target market**

Any VPN or SSL-VPN users who wish to implement Multi-Factor authentication.

- **Product schema**



- **Typical workflow**

- The user starts the login process to the VPN by submitting their User-ID and Password (credentials)
- The VPN refers the credentials to **IDentiWall's** Radius server.
- **IDentiWall** checks in Active Directory or in its own database if the particular user is managed by **IDentiWall** and verifies the user's

password either by LDAP authentication or by checking the password against its own database. If the organization already utilizes a third party radius server, **IDentiWall** can authenticate the user through it.

- If the user is managed by **IDentiWall**, it sends a One-Time-Password (OTP) to the user's handset (both mobile or Dect handsets are supported)?
- **IDentiWall** instructs the VPN to send the user a challenge screen onto which they have to copy the OTP they got on their handset.
- If the user is protected by **IDentiWall's** pre-installed Mobile agent or WAP pushed agent, the agent asks for a Pin Code in order to decrypt the encrypted OTP.
- The user copies the OTP to the challenge screen and submits it to the VPN
- The VPN refers the OTP it got from the user to **IDentiWall's** Radius server that, in turn, compares it against the original OTP it has sent to the user.

Please note that **IDentiWall** maintains a one-to-one relationship between the user's VPN session and the OTP that was sent for that session. Legitimate OTPs which were supposed to be used in other sessions are not accepted. Only the original OTP of the particular session is accepted.

- If the OTP comparison is successful, **IDentiWall** authorizes the VPN to open the door for the user.
  
- **Included technologies**
  - Authentication methods
  - SMS sending
  - Radius server
  - Security
  - LDAP client

- **Optional technologies**
  - Billing methods
  - HTTP gateway
  - SMPP client
  - Secured registration
  - Mobile pre-installed agent
  - WAP pushed agent
  - SMS routing gateway
  - Billing server
  - Syndication server
  
- **Implementation issues**
  - 10 minutes installation
  - One hour set up
    - Active Directory credentials
    - Active Directory IDW group establishment for all the users who are to be covered by **IDentiWall**.
  - Testing
  - Training local staff
  
- **Billing issues**
  - Who serves as the SMS broker?
  - Opening an account with the SMS broker
  - Who pays for the SMSs, the customer or its users?
  - If the users pay (such as in a university typical situation), each user needs to activate their account by purchasing SMS credits in the Billing server.
  - Set up the user's profile of preferences

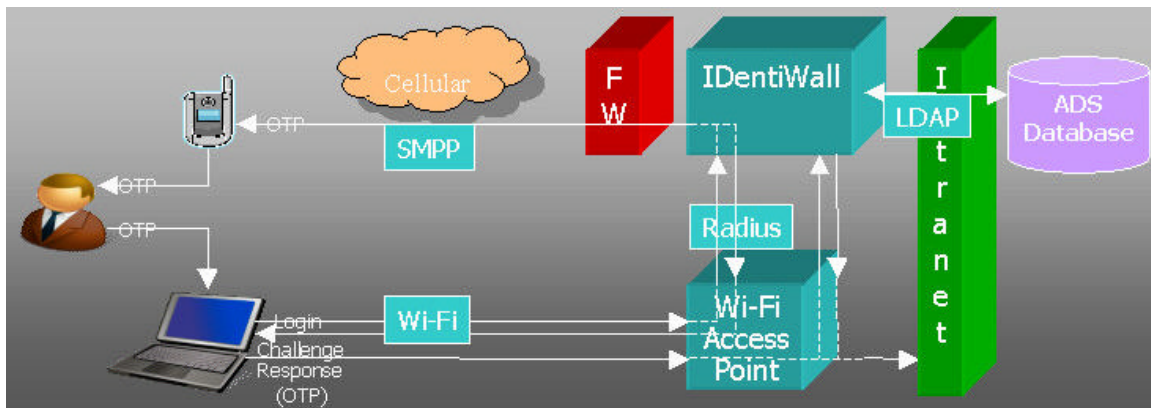
- **Licensing issues**
  - Number of users with pre-paid license fees to be covered by **IDentiWall**. These users will pay discounted prices for their SMS consumption.
  - Does the customer wish to implement Pay-as-You-Go users? For these users the customer has to purchase undiscounted SMS credit.

○ **IDentiWall Wi-Fi**

▪ **Target market**

Any Wi-Fi users who wish to implement Multi-Factor authentication.

▪ **Product schema**



▪ **Typical workflow**

- The user starts the login process to the Wi-Fi access point by submitting their User-ID and Password (credentials)
- The Wi-Fi refers the credentials to **IDentiWall**'s Radius server.
- **IDentiWall** checks in the Active Directory or in its own database if the particular user is managed by **IDentiWall**, and verifies the user's password either by LDAP authentication or by checking the password against its own database. If the organization already utilizes a third party radius server, **IDentiWall** can authenticate the user through it
- If the user is managed by **IDentiWall**, it sends a One-Time-Password (OTP) to the user's handset (both mobile or Dect handsets are supported)
- **IDentiWall** instructs the Wi-Fi to send the user a challenge screen onto which they have to copy the OTP they got on their handset.

- If the user is protected by **IDentiWall's** pre-installed Mobile agent or WAP pushed agent, the agent asks for a Pin Code in order to decrypt the encrypted OTP.
- The user copies the OTP to the challenge screen and submits it to the Wi-Fi
- The VPN refers the OTP it got from the user to **IDentiWall's** Radius server that, in turn, compares it against the original OTP it has sent to the user.

Please note that **IDentiWall** maintains a one-to-one relationship between the user's Wi-Fi session and the OTP that was sent for that session. Legitimate OTPs which were supposed to be used in other sessions are not accepted. Only the original OTP of the particular session is accepted.

- If the OTP comparison is successful, **IDentiWall** authorizes the Wi-Fi to open the door for the user.
- 
- **Included technologies**
    - Authentication methods
    - SMS sending
    - Radius server
    - Security
    - LDAP client

- **Optional technologies**
  - Billing methods
  - HTTP gateway
  - SMPP client
  - Secured registration
  - Mobile pre-installed agent
  - WAP pushed agent
  - SMS routing gateway
  - Billing server
  - Syndication server
  
- **Implementation issues**
  - Who serves as the SMS broker?
  - Opening an account with the SMS broker
  - Who pays for the SMSs, the customer or its users?
  - If the users pay (such as in a university typical situation), each user needs to activate their account by purchasing SMS credits in the Billing server.
  - Set up the user's profile of preferences
  - Training local staff
  
- **Billing issues**
  - Who serves as the SMS broker?
  - Opening an account with the SMS broker
  - Who pays for the SMSs, the customer or its users?
  - If the users pay (such as in a university typical situation), each user needs to activate their account by purchasing SMS credits in the Billing server.
  - Set up the user's profile of preferences

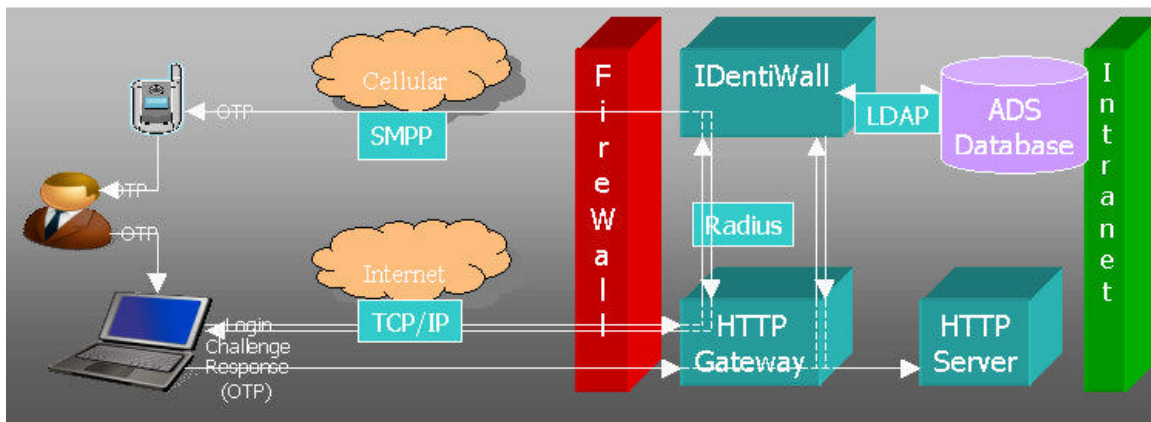
- **Licensing issues**
  - Number of users with pre-paid license fees to be covered by **IDentiWall**. These users will pay discounted prices for their SMS consumption.
  - Does the customer wish to implement Pay-as-You-Go users? For these users the customer has to purchase undiscounted SMS credit.
  - Does the customer want their users to pay for their service? Such users will have to open and/or activate their account by purchasing SMS credits from in the Billing server.

○ **IDentiWall Web**

▪ **Target market**

Any Web users who wish to implement Multi-Factor authentication and transaction assurance.

▪ **Product schema**



▪ **Typical workflow**

- The user starts the login process to the Web server by submitting their User-ID and Password (credentials)
- The IDentiWall session manager sits in front of the web site and gets the request before the Web server.
- The session manager refers the request to the IDentiWall's Radius server for further processing.
- The Radius server checks if that customer is managed by IDentiWall and if it is, it sends OTP via SMS to the customer's mobile phone.
- The session manager sends the customer a screen in which the customer is requested to key in the OTP they got.
- Upon receiving the OTP back from the customer, the session manager refers it to the Radius server for comparison.

- If the comparison is successful, the customer's login request gets referred to the Web server.
  - The session manager monitors all the URLs that go through between the customer and web server and when it detects one that was pre-defined as one that gets special treatment, it reads the HTML body and executes the organizational policy.
  - An example of an eBanking policy might be: Whenever the customer transfers money, execute transaction verification. This type of transaction verification extracts the sum of money that is being transferred as well as the target account to which the money is supposed to be transferred and send these details (via SMS) to the customer's phone. The summary is accompanied by 'OK' and 'Not OK' numeric codes. The customer has to choose the appropriate code and copy it to the form that IDentiWall has sent for this purpose.
  - If the customer has submitted the 'OK' code, it means that the transaction was not tampered with through browser malware and it should be processed as requested.
- 
- **Included technologies**
    - Authentication methods
    - Secured Transactions
    - SMS sending
    - Billing Methods
    - HTTP gateway
    - Radius server
    - Security
  
  - **Optional technologies**
    - SMPP Client & server
    - Secured registration
    - LDAP client

- SOAP client
- Mobile pre-installed agent
- WAP pushed agent
- SMS routing gateway
- Billing server
- Syndication server
  
- **Implementation issues**
  - Installation
  - Set up
  - Testing
  - Training local staff
  
- **Billing issues**
  - Who serves as the SMS broker?
  - Opening an account with the SMS broker
  - Who pays for the SMSs, the customer or its users?
  - If the users pay (such as in a typical university situation), each user needs to activate their account by purchasing SMS credits in the Billing server.
  - Set up the user's profile of preferences

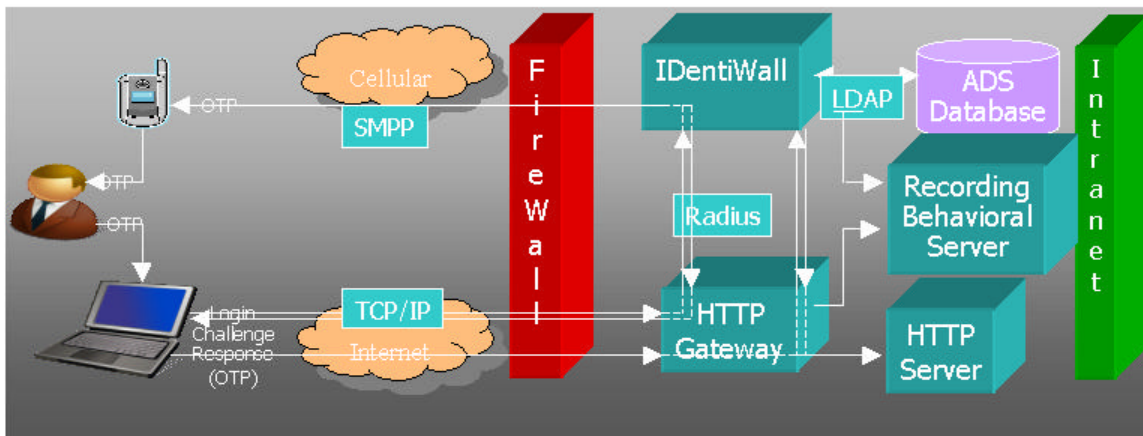
- **Licensing issues**
  - Number of users with pre-paid license fees to be covered by **IDentiWall**. These users will pay discounted prices for their SMS consumption.
  - Does the customer wish to implement Pay-as-You-Go users? For such users the customer has to purchase undiscounted SMS credit.
  - Does the customer want that the users to pay for their service? Such users will have to open and/or activate their account by purchasing SMS credits from in the Billing server.

○ **IDentiWall eBanking**

▪ **Target market**

Any eBanking providers who wish to implement Multi-Factor authentication and secured ebanking methods.

▪ **Product schema**



▪ **Typical workflow**

- Same as in the case of IDentiWall web but with the addition of:
  - Behavioral engine that follows the customer's normal behavior and instructs IDentiWall to execute special measures if the behavior is suspect.
  - More elaborate Transaction Verification
  - Split Transaction over two networks in which the customer is asked to key in details of the transaction both in the HTML form over the IP network as well as over the cellular network.

▪ **Included technologies**

- Authentication methods
- Secured banking

- SMS sending
- Billing methods
- HTTP gateway
- Radius server
- Security
  
- **Optional technologies Implementation issues**
  - SMPP client
  - Secured registration
  - LDAP client
  - Mobile pre-installed agent
  - WAP push agent
  - SMS sending gateway
  - Billing server
  - Syndication server
  
- **Billing issues**
  - Who serves as the SMS broker?
  - Opening an account with the SMS broker
  - Who pays for the SMSs, the customer or its users?
  - If the users pay (such as in a typical university situation), each user needs to activate their account by purchasing SMS credits in the Billing server.
  - Set up the user's profile of preferences

- **Licensing issues**
  - Number of users with pre-paid license fees to be covered by **IDentiWall**. For these users the customer will be charged discounted prices for their SMS consumption.
  - Does the customer wish to implement Pay-as-You-Go users? For such users the customer has to purchase undiscounted SMS credit.
  - Does the customer want their users to pay for their service? Such users will have to open and/or activate their account by purchasing SMS credits from in the Billing server.

## • **Vertical Solutions**

### ○ **IDentiWall for Universities**

Universities often wish to implement **IDentiWall** in a unique way whereby they register their students in the **IDentiWall** database and each student has to activate their account by purchasing SMS credit from **Mad4Biz's** Billing server.

Only the students with positive SMS credit balance get served by **IDentiWall**.

Each student can maintain their own profile in which they can register for various SMS notification services such as:

- Test results
- Changes in scheduled classes
- Due dates reminder
- Special events
- Library waiting list notifications
- Notification of low SMS credit
- More...

Each notification SMS that will be sent to the student will be subtracted from their SMS credit balance.

○ **IDentiWall for Insurance companies and brokers**

The typical case for the insurance business is that every insurance company has multiple insurance brokers and at the same time the insurance broker can work with multiple insurance companies. This presents a number of challenges that need to be met by an adequate solution.

It is quite obvious that token usage will not help security but rather harm it.

Imagine a security broker's office that employs 10 people and represents 10 insurance companies. If each insurance company will issue a token device for each employee of the insurance broker they will have  $10 \times 10 = 100$  devices spread all over the office. Since the broker's employees wish to distinguish between the token and their allocation to the specific employee, they are sure to stick little stickers on each token and specify on them who the token belongs to (user-ID), what is the specific password and/or pin code for that token, which insurance company login does that token facilitate.

Furthermore, sad experience of human frailties assures us that not all those tokens will be securely stored at all times and worse than that, not all the lost or stolen tokens will be reported in a timely manner. And we haven't even begun to discuss the distribution and maintenance nightmare the insurance companies are going to face if they choose the token device path.

**IDentiWall** for insurance companies and brokers offers a far superior solution.

Each employee's mobile handset will replace all 10 token devices in our example.

This guarantees that:

- There are no stickers
- There are no unreported lost or stolen devices
- There is no mess at the broker's office and no employee's aggravation.

However, even this elegant solution leaves us with the little problem of number of SMSs that the broker's employees are going to get every morning when they log onto the various insurance companies' networks. No employee would like to get 10 SMSs at the same time just because their single sign-on product logged them in to all insurance companies.

The solution is a special developed technology called the ‘Syndication server’. The Syndication server is run outside the insurance company’s network, by **Made4Biz**, and provides the following functionality:

- Keeps track of any OTP that was sent to the broker’s employee
- Facilitates a policy engine for the insurance companies

And here is how it works:

- The employee logs onto the first insurance company which can be any of the companies.
- The company’s **IDentiWall** realizes that it is dealing with a broker employee and diverts the request to the Syndication server which includes an embedded **IDentiWall**.
- The Syndication server sends the employee OTP via SMS and registers that in its own database with a time stamp.
- Each insurance company can manage its own security policy in the policy engine. For example: company A might decide that the OTP that was sent to the broker’s employee can be also used as an OTP to enter its own network provided that the OTP is not older than 10 minutes. Company B might decide that the OTP can be up to an hour old and company C might decide that they want a new OTP to be sent to the employee in any case.
- Since in a syndication situation the syndication server’s **IDentiWall** sends the OTP, such diverse policies can coexist in a natural way.
- The Syndication server can offer many more services than just authentication service. For example it can act as a central repository of employees who were banned from accessing an insurance company, and use that information according to the specific insurance company’s policy, deciding whether to allow access for such employee to its own network or not.
- Since the Syndication server is an open platform, its services can be extended to cover additional Syndication needs of insurance companies.

○ **IDentiWall for Banks**

Banks have special requirements which are accommodated via IDentiWall:

- Secured remote access for employees.
- VPN port management (See the following **Firewall/VPN port management**).
- Secured eBanking (Transaction Verification, Split Transaction, Secured mobile agent...).
- Interface to an existing behavioral engine or
- IDentiWall Behavioral engine.
- IDentiWall Recording server.

IDentiWall for banks is a suite of solutions designed to accommodate these needs.

For each bank we configure the suitable solution depending on their requests.

○ **IDentiWall Pay-as-you-go**

For those organizations that wish to postpone purchasing **IDentiWall** until after they test it, or maybe do not wish to purchase it at all, we offer a Pay-As-You-Go model. In this model the software gets downloaded with a free usage license but with one restriction – this **IDentiWall** version can only send SMSs via our SMS gateway, which in turn will work only for customers who have a credit surplus in it. In other words, for the product to work the customer need to purchase first SMS credit via our Billing server. Obviously the SMS cost is undiscounted for the users of the Pay-As-You-Go model.

○ **Firewall/VPN port management**

If your organization is torn between the two alternatives of:

- Not allowing its employees to enter the network from the outside just because it doesn't allow opening the firewall/VPN port for external access (typically opened in 'any' mode).
- Allowing external access but losing sleep over the unnecessary open door that remains open even when no one is actually using it.

**Made4Biz** designed a sophisticated solution that:

- Keeps all the VPN ports closed until a valid employee wishes to enter from the outside;
- Authenticates the employee via **IDentiWall** before it opens up the VPN port;
- After the employee is satisfactorily authenticated and his or her current IP was revealed, it opens up one port for that IP to enter;
- The port administration is done via **Made4Biz's Dynamic! Security** with no need to compile the VPN rules.
- Once the employee's session is over, the port gets closed again automatically.

• **Competitive analysis**

	<b>IDentiWall</b>	<b>Token device</b>
<b><u>Manageability</u></b>		
User management	Done in active directory Via MMC	Proprietary GUI
SMS credit management	Yes	No
Order management	Not a problem	Done by the organization
Stock management	Not a problem	Done by the organization
Repair management	Not a problem	Done by the organization
Loss management	Not a problem	Done by the organization
Theft management	Not a problem	Done by the organization
Expiration management	Not a problem	Done by the organization
<b><u>Implementation</u></b>		
Change existing systems	No changes	Changes required
Installation	Up to 10 minutes	Cumbersome
<b><u>Functionality</u></b>		
All-In-One	The user's mobile phone is used to access multiple networks, organizations, web sites and banks which are not related to each other	Each organization, bank and Web site issues its own device. The user walks around with a keychain of devices
Alert of illegal use	The arrival of an OTP alerts that the user's identity was compromised	The token device has no communication; cannot alert.
Proactive user	Upon arrival of an unplanned OTP, the user can send in reply a 'block my account' command	The token device has no communication; cannot alert
<b><u>Flexibility</u></b>		
Licensing flexibility	IDentiWall supports hybrid pre-paid and pay-as-you-go license.	Pre-paid only license
<b><u>Usability</u></b>		
All-in-One	The user's mobile phone is used to access multiple unrelated networks, organizations, Web sites and banks.	Each organization, bank and Web site issues its own device. The user walks around with a keychain of devices
Always with	The mobile phone is always with the user, providing the better security	Token devices tend to be away when needed
Always serviced	The cellular companies' service 24x7	Totally dependent on self organizational service
<b><u>Vulnerability</u></b>		
Man in the browser	Full protection via transaction verification	No protection
Lose/theft immediate notification incentive	The user is sensitive to calls theft hence immediate reporting incentive	No real incentive for immediate reporting
<b><u>TCO</u></b>		
Five years TCO for 1000 users (including SMS, break and other costs)	<b>\$168K</b>	<b>\$460K</b>