SECURING ON-LINE PAYMENT USING DYNAMIC SIGNATURE VERIFICATION

Valentin Andrei, Sorin Mircea Rusu, Ștefan Diaconescu, Adrian Dinescu
Research & Development, SOFTWIN, Bucharest, Romania
vandrei@softwin.ro, srusu@softwin.ro, sdiaconescu@softwin.ro, adinescu@softwin.ro

Keywords: E-Payment, Information Security, Biometry, Dynamic Signature, E-Commerce, Web-Services

Abstract: Since the "explosion" of the number of on-line transactions, many IT researchers have concentrated their efforts to offer solutions to the security demanded by operations involving financial data. This paper proposes a novel system which employs biometry to secure electronic transactions by using the dynamic signature as the single individual characteristic to be verified before the processing is made. By attaching the signature to a payment instrument, a new security layer will be implemented being able to reject a percentage of identity theft attempts close to 100%. All verification requests will be processed at a dedicated processing node, signalling the response through secured customized interfaces.

1 INTRODUCTION

Since the Internet became more and more widespread, it served as a support for replacing the traditional goods trading with commerce conducted electronically. As a result the amount of money travelling across the Internet increased with orders of magnitude. Nowadays one can buy almost everything he needs only by using a card attached to his bank account, just by sitting in front of his Internet connected computer. For example, *Amazon* managed to generate in a single day in 2004, a number of 32 transactions per second, selling 2.8 billion units (Paul Demery, 2004). In 2006 *eBay* reported at a presentation that it-s users trade more than 1590$ every second (R. Shoup, D. Pritchett, 2006). This data only reflects the huge growth of electronic commerce.

Unfortunately, this spectacular growth was proportional to the increase of on-line fraud. Many of the attack attempts are based on identity theft. For example, a popular method of stealing a person's identity, called "phishing", involves convincing the user to input his credentials (ex: username, password and credit card information) into a fake interface, very similar with the one he uses every day. From that point, the attacker uses the stolen data in illegal purposes. In 2009, on-line fraud generated losses of around 559.7 millions of U.S. dollars, 25% of this amount stemming from identity theft and credit card fraud. (IC3, December 2009). These statistics were computed from reported frauds but the damage could be greater. The data makes sense when we consider that the great majority of on-line shops only use basic authentication methods, and also that the payment service providers require data that can be easily replicated, like credit card number or security code, in order to finalize a transaction.

Of course, some measures and methods to eliminate the threats were conceived and implemented. Most of them rely on something that a user knows or has, or a combination of both elements. The password or the PIN number attached to a card is something that the user knows. These are some main elements used to secure a transaction but the amounts lost through electronic fraud prove that they are insufficient. Passwords and PIN also have disadvantages like that they can be forgotten, stolen, or even generated through brute force attacks. That is why lately, security tokens were introduced. A security token is a device that the user owns, generating a code that used together with a username and a password, grants access to a private virtual location from where transactions can be made securely. This measure indeed reduces the risk of fraud, but the token can also be stolen and used without restriction.

One science branch that comes to help against identity theft and on-line fraud is biometry. It employs the usage of individual characteristics in order to secure a critical information, location or

action. Biometry divides these characteristics into to physical and behavioural. Physical features are represented by something that a person uniquely has like the fingerprint, the iris, the face, the hand's topology, etc. Behavioural biometry studies characteristics that describe you as a person, "who you are", like the dynamic signature, the voice, etc. We mentioned the characteristics that offered encouraging results across the years.

This work proposes a system that adds a new security layer to existing on-line payment methods, by using the dynamic signature. While features like voice, fingerprint or face offer the possibility of being recorded for further illegal use, the dynamic signature of an individual cannot be stolen, mainly due to its specific behavioural component expressing the owner's will on realizing an action. It also has a high degree of social acceptance.

The first section of this article will present the changes made on a clasic on-line payment scenario when using a biometric authentication method. The next sections will detail the system's software architecture and implementation. The description of the security measures will also be treated in a distinct chapter. Finally, some performance indicators will be given in order to offer an overview of the system's serving capabilities.

2 USAGE SCENARIOS

When implementing the proposed security layer, three major transaction types involving credit cards were considered:

- E-Commerce transactions – Represented by payments made by someone who buys a product from a virtual store, using his credit card;
- E-Banking operations – Operations realized when the user accesses his e-banking account to process payments, bank transfers, etc., or when he goes the bank's front office;
- Regular credit card payment – Represented by regular POS payments, in a store that accepts credit cards.

Several types of fraud need to be prevented for these types of transactions. The first two are vulnerable to on-line attacks aiming to obtain the essential data needed to complete a payment. E-Commerce transactions can be successfully processed only when providing the credit card data, so if someone owns a printed copy of the card, he can complete payments. E-Banking operations are somehow protected by security tokens and passwords. However, all types of transactions are vulnerable to theft, because if the credit card or security token is stolen, they can be used for fraud.

In order to prevent fraud, the card must be attached to something impossible to be stolen, like a behavioural individual characteristic. The dynamic signature can successfully be used for protection. Considering this, the following scenarios will be subject to change:

- Registering a credit card at the bank-s office;
- Realizing an electronic payment via an on-line virtual store;
- Logging in to an e-banking account;
- Completing a regular credit card payment.

To be completed, each transaction scenario must include the acquisition of the user's dynamic signature. We developed an electronic device (Adrian Dinescu, 2008), capturing a set of acceleration signals, representing the hand's kinetics during the signing process, which also captures the relative movements signal used to reconstruct an approximation of the signature's image as it appears on the signing paper, by using an optical navigation system, presented in Figure 1.

Figure 1: Signature acquisition device

When a bank customer wishes to open a current account, having an attached credit card, and also selects as an additional security measure the verification of the dynamic signature, he will complete the following steps, at the front office:

- He will identify himself using requested documents (ID Card, Passport) and he will have his data introduced inside the bank's application database;
- The bank's application will open an interface provided by the proposed biometric system;
- The user will input a number of five specimen signatures, using the acquisition device (we selected this value because it represents a

threshold that once overpassed does not generate a significant performance increase regarding correct detection ratios, but can significantly slow the authentication process);
- A complexity and consistence measure will be computed for the captured specimens, and if it passes an established threshold, the specimens will be accepted. If not, some additional signatures (maximum five) will be required in order to complete the registration, and to have a consistent and complex set of specimens;
- The user will receive an acquisition device if he does not own one already.

Having the account opened, the user can use his credit card in an on-line transaction, being confident that fraud attempts regarding identity theft will be rejected by using the biometric pen capturing his signature's individuality. A typical scenario that involves buying a product from an on-line shop will be modified as follows:

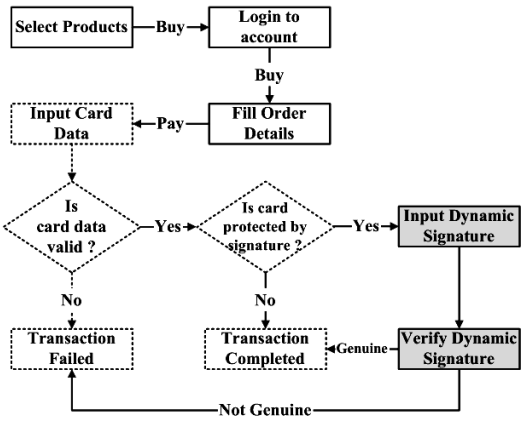

Figure 2: e-Commerce basic scenario protected by dynamic signature

The actions represented with dotted lines are completed by a *Payment Service Provider* (PSP), contracted by the on-line store, which connects to the bank that issued the credit card. The actions figured with gray blocks are done by the proposed system, realizing the signature verification. In order for the scenario to be completed, the new security layer must communicate properly with the PSP.

Logging in to an e-banking account, is very similar to the classical method, except that the dynamic signature can be required as an additional security measure, besides the code generated by the security token, username and password. The acquisition device and the handwritten signature can also be used as the sole security measure, replacing the digital password. If the user has multiple security methods available on his account, he will be able to select the ones being active at the login process, using the credit card's issuer e-banking application.

Completing a regular credit card payment in a shop will be slightly changed by adding the biometric signature as measure of security. When the seller inserts the card, the POS will notice that the handwritten signature is required and will ask the client to input a valid signature, using the biometric pen and a customized hardware interface.

The presented usage scenarios (which address an important percentage of the total transactions involving credit cards) are completed by a set of use cases related to administrating the new authentication process, and to manage it's functioning together with the classical security measures. However, using the card at an ATM is not protected by the proposed system, because it would be rather uncomfortable to use dynamic signature, outdoor at such a machine. For that, the fingerprint can be successfully used. (Ibidapo, 2010).

The following section will describe the architecture of the proposed system that completes the presented usage scenarios.

3 SOFTWARE ARCHITECTURE

We presented in the previous section four regular usage scenarios modified when the dynamic signature verification was added as a new security layer. For them to be completed, the proposed system needs to be linked with three different entities involved into the flow of money amounts:

- The bank's software applications;
- The PSP set of applications;
- The virtual store's website.

This is why the software architecture will be composed out of parts that work independently with the entities mentioned above. Figure 3 represents the general architecture of the described system.

To explain the main implementation details, we must introduce some abbreviations. From this point, the system will be mentioned as "SISEB", which is an approximate abbreviation for *System for Securing E-Banking Operations*. The main component of SISEB will be mentioned as "EBPSP" derived from *E-Banking Protection Service Provider*. We must enforce the idea that the term "e-Banking", from the project's full name, does not only refer to transactions accessible from the software applications provided by the bank institution, but to all transaction types described in Section 2.

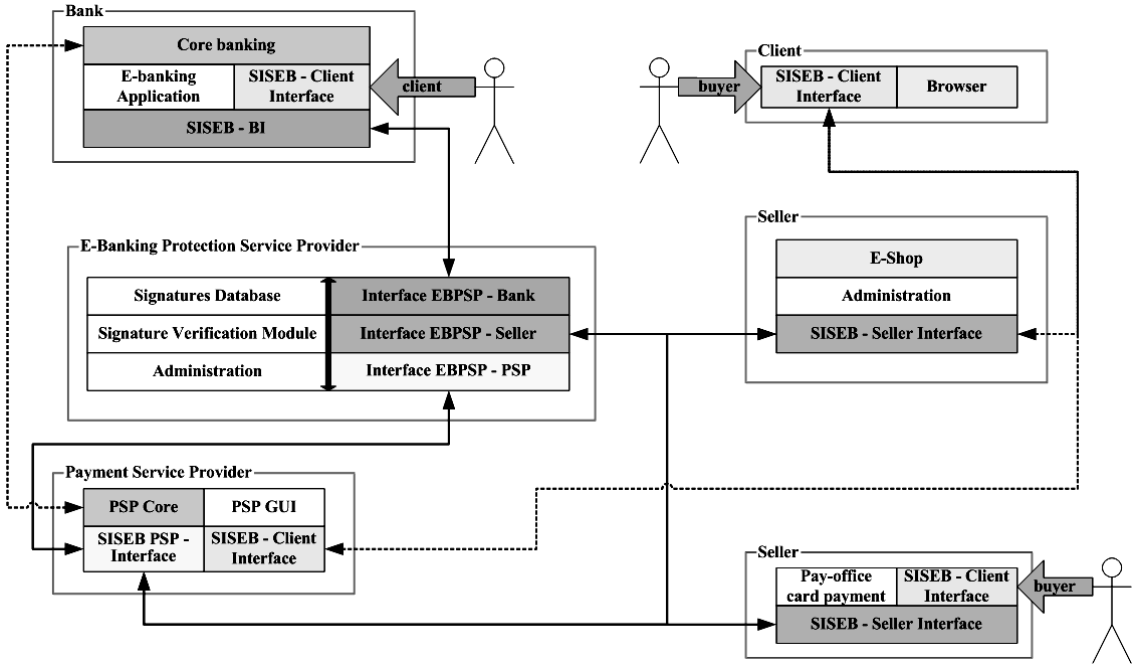

Figure 3: System-s software architecture

We can see clearly that each main entity, mentioned in the section's beginning, represents a different architectural module. The *bank* entity will have as central component its *core banking* applications. These are responsible for managing all the bank's client accounts and operations. Also the bank will provide the customers with a set of programs (*e-banking applications*) they can use to realize financial operations, in front of an Internet connected PC, unassisted by a front desk officer.

The core banking closely communicates with the *Payment Service Provider*, the other entity having to communicate with SISEB. The PSP will verify the given credit card credentials by sending a request to the bank that issued it, and will command the transaction initiated by the client if the data is valid, and the account having the card attached, has a sufficient amount of money. The PSP will be accessed from an independent graphical user interface.

The *Seller* entity represents an on-line store or just a regular one, accepting credit card payments. Its applications can be hosted on a server and exposed to the Internet, or they can be represented by simple POS embedded software that connects to PSP exchanging information.

The figure also shows a set of communicating interfaces, attached to the bank's applications, to the PSP and also to private virtual stores. These interfaces are built for the system to interoperate with all the described components and can also serve as support for ensuring proper security of the communication, because they offer the possibility of configuring encryption mechanisms, and of setting-up firewalls.

However, SISEB is composed only out of two main parts: a signature verification core, figured as the EBPSP, and the set of interfaces attached to every independent entity.

3.1 Signature verification

The signature verification module is the "brain" of the entire SISEB system. It represents a succession of operations individualized as blocks in figure 4. First, the signature needs to be captured using the acquisition device presented in Section 2. The raw sample, consisting of a set of unprocessed signals (accelerations and relative movements) is passed to a *feature extraction* module. This block extracts the key information characterising an input signature. This information is represented by a set of *invariants*, or *features* (Dinescu, Diaconescu, 2008). When the user registers into SISEB system, an associated database entry is built from the five specimen signatures, consisting of five sets of invariants' sequences computed out of each signature. At the verification phase the invariants will be extracted from the sample signature

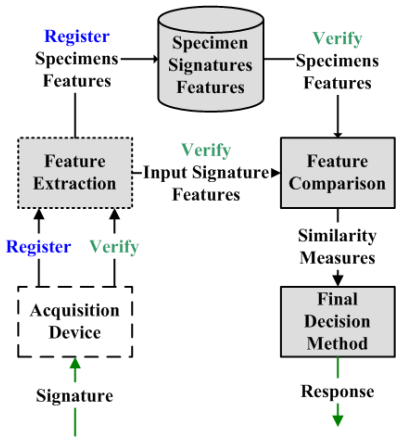

Figure 4: Signature verification chain

The feature comparison block has to compute a similarity measure between the input signature invariants' sequences and the ones saved for each specimen signature. A relevant similarity measure could be for example, a Levenshtein distance.

The final decision is taken by combining the similarity measures. There are several methods that can take this kind of decision, varying from employing artificial neural networks (Marcu, 2009), Hidden Markov Models (Dolfing, 2002) to computing statistical thresholds for each registered client.

Inside SISEB, the signature verification is the core of the EBPSP component. The administration module is responsible for setting-up parameters for the signature analysis blocks (decision method, thresholds, etc). The same module is also in charge with managing the specimen signatures inside the database, and also with the registered user's data.

Because the number of requests directed to SISEB can be high, the option of replicating the entire signature verification core into multiple processing units is a solution needed to be considered. Also, the same replication can be made for the most computational intensive operation inside the verification chain, which in our case is the feature comparison block.

3.2 Interfaces

A set of different interfaces ensure the system's interoperability with the 3 different entities (bank, PSP, virtual store).

The EBPSP *Bank* interface represents the link to the signature verification core for the bank's software applications. All the authentication requests generated by transactions initiated from e-banking accounts or at the bank's front office will be received and answered through this interface. The SISEB BI (*Bank Interface*) will be used by the system to communicate with the bank's programs.

EBPSP PSP (*Payment Service Provider*) interface will be the gateway towards the verification core for all the requests generated by the PSP. These will occur at each credit card operation initiated by virtual stores or regular payments (*sellers*). That is why this interface will gather the highest number of verification requests, so it will need proper configuration. The EBPSP PSP interface will communicate with the *seller* through SISEB *Seller* interfaces.

Another interface drawn in figure 3 is SISEB *Client*. It is not similar to the ones described above, being only a graphical user interface, needed to capture the signature using the connected acquisition device. The interface will be shown in every usage scenario which involves securing a transaction through dynamic signature:

- At the bank's front office, displayed by the bank's software;
- Displayed by the PSP graphical user interface, when realizing an on-line payment;
- Displayed on a station connected to a regular POS when using a credit card protected via handwritten signature.

An additional usage scenario, detached from the e-payment topic, can occur if a *seller* or any other web application contracts SISEB for securing the access to their user accounts. In this case, the applications will display also the SISEB *Client* interface, for signature acquisition, and will communicate directly with EBPSP *Seller* interface, via SISEB *Seller* interface.

The following chapter will give details on the software implementation of the system's described components.

4 IMPLEMENTATION

The SISEB system is a complex software application that needs to cross barriers imposed by the multitude of operating systems and technologies used by entities that operate e-payments. In order to achieve that, a standardized technology that ensures a high degree of interoperability relative to multiple different implementation technologies must be used. The work will now detail the efforts made towards a final implementation.

The developing efforts were concentrated towards 3 areas:

- The signature verification core;
- Implementation of SISEB *Client* interface;
- Implementation of interface pairs.

4.1 Signature verification core

The signature verification core, representing the *E-Banking Protection Service Provider* from the architectural specifications, will be the component hosted on the SISEB owner's servers. It will be the final destination of all the authentication requests. We used the *C/C++* languages to implement the algorithms realizing the signature analysis and verification, as dynamic link libraries. An interface fully compliant with the BioAPI standard was developed, providing access to algorithms (ISO, 2006). Figure 5 illustrates this succession of modules.

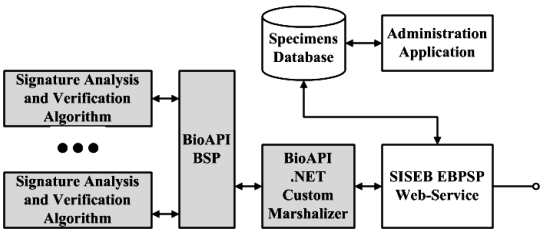

Figure 5: EBPSP Implementation

In order to offer an interface to signature verification modules, that ensures interoperability with different software technologies, we used web services. We have chosen to implement the SISEB EBPSP web-service by using *Windows Communication Foundation*, selecting C# as the developing language. We used first the *.NET 3.0* provided classes. A problem that occurred due to combining DLLs that contained C++ classes to applications implemented in .NET was the lack of marshalling. This is why we have built a custom module realizing the marshalling of the parameters exchanged when calling BioAPI BSP interface. We have chosen *MS SQL Server* as the database management system.

Special attention was paid to ensuring a low latency in the context of numerous authentication requests. The feature comparison module, from figure 4 was identified as being the most time consuming block and we tested some methods of mapping its tasks into several processing units. We ran some tests using a powerful server with 16 processors, and we also found an alternative for this solution, consisting in the usage of nVidia CUDA graphic cards. We found out that a single nVidia GeForce GTX 275 card that incorporates a number of 240 independent cores, can reach the performance of the tested server, when placed into the PCI Express socket of a medium class desktop PC (Valentin Andrei, 2010). However, a hybrid solution will be implemented, consisting in replicating the EBPSP in multiple stations (servers or PCs with nVidia CUDA video cards), managed by a load balancer.

The most important functions provided by the EBPSP are listed bellow. They are completed by a number of database administration and report generating functions.

- *EnrollUser* – Registers an user into SISEB system, testing if his signatures are complex and consequent enough;
- *UpdateUser* – Changes a user's database entry (specimen invariants' sequences, data);
- *VerifySample* – Represents the function that realizes the authentication of a given input signature.

4.2 SISEB Client Interface

The SISEB *Client* interface has to operate exactly the same, for each application that displays it. A high percentage of electronic payments are made via Internet, initiated by on-line stores accessed from web browsers. The multitude of existing browsers makes the task quite difficult.

We first implemented the interface for Internet Explorer. We have used an ActiveX control, which has the capability of accessing the USB port of the working station, in order to connect to the acquisition device. The ActiveX can be opened in two modes:

- Register Mode;
- Authentication Mode.

When displayed in the first situation, the control captures a number of five specimen signatures without sending each one separately to the server. After the process ends, it can compute the complexity and consequence measure of the specimens, and can successfully accept the signatures or it can request more signatures until the thresholds are passed. The ActiveX can also be configured to realize the feature extraction, in order to take over a percentage of servers' load.

When the control is displayed in *authentication mode* it will capture a single signature, commanding its sending to the server, for verification.

Unfortunately the ActiveX controls are not supported on other browsers like Mozilla or Chrome. However, if we use a plugin, we can successfully use the ActiveX with these browsers (Aharon, 2010). If the plugin solution is not accepted, the user interface can be implemented like a Java Applet for Mozilla or by using Google Native Framework for Google Chrome.

4.3 SISEB Interfaces

The interfaces that provide the means of communicating with the entities that operate payments using credit cards are also implemented as *WCF* web-services, providing functions specific to each entity. So we have the following web services:

- EBPSP Service – Gateway to signature verification core;
- EBPSP Bank Interface;
- SISEB Bank Interface;
- EBPSP PSP Interface;
- SISEB PSP Interface;
- EBPSP Seller Interface;
- SISEB Seller Interface.

Each of the interfaces illustrated above, can be installed on separate stations, raising the possibility of installing multiple security applications or firewalls. We can install them also on a single server, but we must consider solutions of managing the traffic amount generated by all the authentication requests incoming through the interfaces. Each interface will have a configuration file (*Web.config*) which leaves numerous options of configuring the communication parameters.

Section 5 will describe security measures that were implemented in order to ensure proper protection for each e-payment transaction.

5 SECURITY

In order to ensure the security of the entire system, the following communication areas were selected as the most important for protection increase:

- SISEB Client;
- EBPSP – SISEB interfaces;
- PSP – Bank.

The last communication channel has to be secured according to collaboration between the bank and the PSP. The most common security standards are 3D-SET, 3D-Secure and UCAF/SPA. 3D-Secure (VISA, 2006) is commonly used in e-payment transactions. It is based on SSL (*Secure Socket Layer*) technology and it assumes splitting the responsibility (and the associated risks) for a transaction between the bank, the seller and the client. One great advantage is that the client is not asked to store security certificates on his working station and he does not have to complete an enrolment, leaving this task to the card issuer institution. A risk that may occur when using this model is that the seller can redirect the user to a fake PSP, with the goal of stealing the credit card data. However, if the card is protected by dynamic signature, the risk will be eliminated.

In order to ensure the security of the communication between SISEB interfaces, the EBPSP will issue a digitally signed certificate being be the only one trusted by the SISEB interfaces. The HTTPS protocol will be used for message exchange, based on SSL/TLS cryptographic protocols. The usage of these measures can be easily activated from the web services configuration files.

To secure the usage of SISEB Client, two measures need to be taken. First, the graphical user interface (for example the ActiveX control), displayed by applications has to be digitally signed and recorded as trusted by the web browsers. Also, a hardware friendly encryption mechanism, like AES for example, will be used in order to prevent some applications that scan input ports to steal the signature from the biometric pen.

We also implemented a security measure that reduces the number of "man in the middle" attacks. The measure is based on the fact that the similarity measures obtained when verifying a signature are unique just like the input signature. By storing these values, we can be sure that one genuine signature that has been stolen due to security leaks, cannot be used again to authenticate a transaction. Even if the attacker tries to slightly modify the stolen signature, the new obtained similarity measures will be highly modified towards considering the sent signature as a forgery, due to the complex transformations made on raw signatures, by the feature extraction block.

6 PERFORMANCE RESULTS

The project's feasibility depends on two main factors: the signature verification accuracy and the authentication response time.

During the project's development, several signature analysis and authentication methods were developed. The parameters configuration directs the system permissiveness. During testing SISEB managed to reject 99.9% of the forgery attempts while authenticating more 80% of than genuine signatures at the first request. These tests were made using skilled graphic forgeries, on datasets of around 20000 signatures (with a ratio between originals and forgeries close to 3.0), generated by 500 subjects.

For an attack attempt to succeed, the attacker needs first to closely observe its target during the signing process (which is highly unlikely), and then he can try to forge the signature (by imitating his hand movement and also reconstructing an approximate image), with less than 0.1% chances of success.

We also tested the response time obtained when using SISEB on a single powerful server, varying the number of enabled processors. The results are synthesized in Table 1.

Table 1: Average response time for authentication requests

Server active processors	Requests per day	Mean delay
8CPU@2400 MHz, 4GB DDR2	288000	0.996s
12CPU@2400 MHz, 4GB DDR2	576000	1.403s
16CPU@2400 MHz, 4GB DDR2	576000	1.251s

The table demonstrates that a single server, running SISEB is capable of serving a number of over 500000 requests per day with an average response time of 1.2 seconds. The system is scalable, so using more processing power will determine a proportional performance increase. A similar increase will be generated also by using newer hardware, for example DDR3 memories or higher frequency processor cores.

7 CONCLUSIONS

This paper presented a complete system, based on dynamic signature, for securing electronic transactions that use credit cards. SISEB has the capacity to successfully secure operations generated from Internet e-banking accounts or at the bank-s front office, transactions generated when buying products from on-line virtual stores, paying with credit cards, or even when performing regular card payments using POS devices. The system aims to be implemented as a new security level, by attaching the owner's dynamic signature to the credit card. When using the proposed system, risks regarding theft of identity or card data are successfully eliminated. The correct authentication and rejection ratios (80% and respectively 99.9%) obtained on large datasets and also the response time for numerous requests comes to demonstrate the project's feasibility.

REFERENCES

Paul Demery, December 2004, www.internetretailer.com http://www.internetretailer.com/2004/12/27/amazon-sells-a-record-2-8-million-items-in-a-single-day

Randy Shoup, Dan Pritchett, November 2006, in *SD Forum 2006*, The eBay Architecture. String a balance between site stability, feature velocity, performance and cost

IC3, December 2009, Bureau of Justice Assistance – U.S. Bureau of Justice, In *2009 Internet Crime Report*

Adrian Dinescu, Stefan Diaconescu Moise Gabriel Alexandru, Secrieru Marian, December 2008, System and Methods of Acquisition, Analysis and Authentication of the Handwritten Signature, in *European Patent Office EP1846868*

Ibidapo, O. Akinyemi, Zaccheous O., Olufemi M. December 2010, Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System, in *International Journal of Electrical & Computer Sciences IJECS-IJENS Volume 10*

Marcu, E., 2009. Method of combining the degrees of similarity in handwritten signature authentication, using neural networks. In *AI-2009, The Twenty-ninth SGAI International Conference Cambridge, UK.* Springer

J. G. A. Dolfing, E. H. L. Aarts, J. J. G. M van Oosterhout, 2002. On-line signature verification with Hidden Markov Models. In *Pattern Recognition, 1998. Proceedings. Fourteenth International Conference on*, pp.1309-1312 vol.2, 16-20 Aug 1998

International Standardisation Organisation, 2006. Biometric application programming interface – Part 1 BioAPI specification. In *ISO/IEC 19784-1:2006*

Valentin Andrei, Sorin Rusu, Ştefan Diaconescu, 2010. Solutions for speeding-up on-line dynamic signature authentication. *In Proceedings of 12th International Conference on Enterprise Information Systems, Madeira, Portugal, June 2010*.

Leeor Aharon, 2010. A NPAPI based plugin that enables the use of ActiveX controls. In *Google Project Hosting. http://code.google.com/p/ff-activex-host/*

VISA, 2006. Verified by VISA System Overview. In https://partnernetwork.visa.com/vpn/global/retrieve_document.do?documentRetrievalId=119