PERIODICA POLYTECHNICA SER. SOC. MAN. SCI. VOL. 11, NO. 1, PP. 13–26 (2003)

CUSTOMER AUTHENTICATION, AS A MATTER OF RISK IN FINANCIAL SERVICES

Kristóf SZABÓ

Department of Information and Knowledge Management
Budapest University of Technology and Economics
H–1521 Budapest, Hungary
Phone: (36 1) 463-1832, Fax: (36 1) 463-1225
e-mail: kristofszabo@freemail.hu

Received : January 9, 2003

Abstract

According to some experts' opinion, in such a technocrat society as ours, in the last decade of the 20th century the speed of the technical developments can be equal to the changes in the first 90 years of the same century. Besides the chances and opportunities, which came into existence with the spreading of the Internet, the exact recognition of the real *dangers* caused by the development and the changing of the customer relationships is of an enormous significance. The 'information highway' incredibly reduces the time needed for spreading the news, and at the same time shortens the lifecycle of the information. The most obvious sources of danger of the information revolution are remarkably increased:[1]

- without the introduction of appropriate restrictions and measures, the faceless contact between people and computers on the data-network can easily become a hotbed of anonymous crime,
- the mistakes arising during the increased information-flow can cause chain-reactions, that can forecast a so-called information-catastrophe,
- in a world that becomes more and more automatic, people are less and less prepared for managing unexpected actions,
- the mixing of the real and the virtual information, i. e. the merging of the borders of the real and an imagined world can become a serious danger for the users.

One of the new challenges that were born with the information technology is making the already operating IT structures more safe. A possible standardization and central management of the safety elements become unavoidable tasks for many organizations. As a consequence of these above mentioned arises the necessity of a knowledge-based access management. The twofold character of the task is on the one hand to find a solution to the restriction of the availability of information and functions, on the other hand to settle the universal managing of the identification variables supported by the modern law.[2] These challenges are more increased in the banking sector, since on the level of social expectancy the word 'bank' is identified with the word 'trust'.

Keywords: authentication, customer identification, multi-channel, financial, PKI, electronic signature, scoring, administration, access, risk, knowledge, media, customer relationship, limit.

[1] This thesis is to deal only with the first two sources of danger mentioned.

[2] Most of the conditions are given to change the traditional paper-based documents with reliable, digital signatures supported electronic documents: the standardized PKI technology (Public Key Infrastructure), the Hungarian Electronic Signature Act (which meets the EU-directives), and the first authentication-services (CA) were established.

1. Multi-Channel Sales

The wide-range availability becomes a part of the service in the banking sector until the end of the 20th century. Nowadays, nearly everyone uses a bankcard, knows the service of Call Centers. More and more customers have at the workplaces or in their homes internet-based bank services. This multiple service satisfies the customers' needs: to be able to reach the bank any time, anywhere and anyhow [DEDMAN, 2001]. With the help of the so-called e-business the banks are able to give personalized information to their customer 24/7, and it enables them to give financial instructions to their banking institutes. This seems to be a very simple task, but it is actually not. In the banking sector, the appearance of the multi-channel based sales activity leads to an obligatory change of the way of customer care. Nowadays customers use the financial services through a wide spectrum of the media. With the spreading number of the electronic based sales channel, the number of supported services increases. The development is particularly significant on the subject of financial services. Among the currently applied communication methods there are channels based on telephone, cell phone, fax, Internet and RAS[3].

While using the particular sales systems (media), depending on the technological circumstances, the customers identify themselves in a different way. That is why, the registration of customer-identification and authority-management information becomes an essential part of the customer service of banks.[4] The coordinated management of these pieces of information becomes a good example of the application of knowledge-management.

Development of the Knowledge-Based IT Systems

The question of knowledge-management, which arises already in case of authority managing, requires a special attention to several functions of the financial institutes' information technology. The appearance of the information technology in the bank sector was realized by the spreading of the high performance, robust equipment, which ensured the continuous support. In the middle of the '60s the wide-range use of computer technology made it possible to establish centralized data-processing management. The IT supported processing of customer data opened up new prospects for the organizations. Since the end of the '70s the rapid develop-

[3] RAS = Remote Access System

[4] With the use of electronic channels the personal contact between the bank and the customer disappeared. As a conclusion of this with the help of the e-channels the methods for identification of the users must be ensured on a new way. There are several different methods for customer authentication. The different methods are connected to different channels, so the customer needs to have more tools, passwords, or PIN code, if he/she wants to use more services. This means high administration and IT costs for the organization. Furthermore the introduction of a new way of authentication (for example a chip-card) into all of the existing channel-systems requires high development costs.

ment of the banking business required newer and newer IT systems. Slowly the business generated such requirements that the systems on the technical level of that age could not meet. The lack of processing capacities made the earlier centralized data-management distributed. The falling of the systems into pieces raised a barrier to the further development.

By the ’90s the technological development becomes able to meet the users’ requirements again. For today it is possible to create standardized (or completely integrated) systems, which are ready to ensure the data processing on a higher level. In the life of the banks it means the centralization of knowledge centers which register customer information . Among the central accounting units (core systems) and the access channels a new concept was born: the so-called middleware layer. Middleware is a kind of module in a three-layer IT architecture, through which every customer data runs at least once. With the introduction of this technology next to our existing legacy systems a centralized datamart of customer information can be created. On this middleware level the possibility is given to transfer the information flooding through the organization to a knowledge-based one. The managing of the access right, the workflow, and the pricing were earlier all system-specific tasks of different product core systems. With fitting these knowledge cores together and organizing them into an information technology layer (so called ‘containers’) the organization is able to make steps towards a real knowledge-based service.

2. The Separation of Protection and Identification; the Risk-Management

On the subject of customer identification the protection of the system and the customer identification must be differentiated. Though the two expressions are often mixed up or merged by the users, there are significant differences between them [EGERSZEGI, 2001]. The question of identification can be thought to be a part of the protection of the system, so that the service could not be available for the unauthorized or illegal users. It is to know, that only a trifling part of the abuses are settled through breaking up the identification systems. A typical case is when a user of bad purposes obtains the internal information and the abuse is carried out with the help of this information. According to some researches the rate of these abuses can be even more than 80%. This is why the question of protection is much more complex than that of the identification.

Why the problem of identification is still worth dealing with is the managing of an ordinary customer-relationship. Users who are supposed to be generally benevolent handle their authority incorrectly and it can cause very disadvantageous situations to the organization. It is true, that the risk still is a part of every business for every financial institute. But on the subject of profitability the level and quality of risk-management can cause efficiency differences between the organizations.

Three factors must be considered when building up the access risk-management of an organization:

- the *frequency of use* of the particular service or product,

- the *characteristics* of the media/technology used for the service,
- the *legal background* supporting the media and the method of customer relationships.

These three factors are far not about technology. The reducing of risk must not mean making the customer identification systems more strict, since after a while the level of safety would go at the expense of usefulness. There are some more efficient means to live with, and banks do so. Such means are, for example the user limits on transactions or use of customer's habit analysis.[5] Outstanding of the financial institutes but a very helpful step for their risk management is a realization of the full legal support of the *electronic signature*[6] technology [9]. In connection with the above mentioned it is worth to tell that the legal guarantees given for the electronic signature can only be helpful in the part of the multi-channel sales, since the use of the PKI technology in some cases (i.e. Call Centers) would be very complicated [4].

3. The Question of Customer Identification

Most of the customers handle the products of financial institutes as a service. Therefore they want to use and enjoy the services, and not necessarily to understand them. In order to be able to give the customers a service of a higher and higher quality it would be reasonable from the first moment of the relationship on to know that which customer's service requires to be more prepared. The question of customer identification applied in the modern financial institutes' services is of more significance than the traditional access control, because it can strongly influence the quality of the customer care, too (see CRM[7] technologies). The model of customer identification has to answer two different groups of questions [1]:

1. The use of the product
    - Whether the product use of the customer on a specific channel with an acceptable level of risk manageable is passing (for example: is it possible to give instructions to money transfer of HUF 10 million on the phone)?

[5] Nowadays this method is used mainly for the protection of card-transactions, where the behavior of the user is continuously examined, and in case of unusual transactions automatic restrictions are made (for example when cash withdrawal is made in more countries in a short period of time). This kind of artificial intelligence based protection is the safest of all.

[6] The electronic signature is generally a solution built up on the PKI method, where a coded information is generated by a key (first key) from the message and attached to it at the sender-party. This information can be decoded only by a second key, specific for the first one. So its solution proves the sender's person, and the integrity of the message.

[7] CRM = Customer Relationship Management. In general it means the database supported customer service methodologies.

- Whether the information service of the customer through a particular channel is safe or not (for example: is it safe enough to send account information to the customer by e-mail)?

2. Customer service
   - How should the organization behave towards the customer (CRM)?

In the traditional services the customer identification is based on the identity card, or other written (signature) or verbal (password) identification methods determined by the customer. These 'branch-based' methods became completely useless as the electronic commerce appeared. As a solution, at first appeared the so-called PIN[8] codes used mainly at bankcard products during the progress of development. As a following stage, some other 'easy' methods formed to improve safety (see: signature file, time password code). But these distance identification methods carry in themselves the opportunity for the anonymous crime. A solution to this safety problem is the method of the electronic signature, but only in that case when the issuer and the register of the signature is a third party charged by the partners.

At the design of modern customer authentication logic our aim is to gather a branch of methods expanded to all kinds of sales systems:

- the bank and the user should mutually and definitely identify each other,
- the bank should be able to set up flexible rules concerning the users' authorities (according to its own business logic),
- the authorization system should have 'opened' architecture, so that different identification variables of new services could be plugged in.

The Legal Circumstances

On international levels, so also in Hungary there are three factors influencing strongly the development of electronic commerce:

1. the level/standard of IT developments,
2. the development on the legal circumstances,
3. the cultural/social habits.

While mainly the technical development, but also the social preparedness are determined by the economic performance of the countries, ensuring the legal circumstances is not a question of material aspects. Due to the codification works done, in the last few years this legal regulation system seems to become settled in Hungary. After being approved the legal regulation by the Hungarian Parliament (Act of Electronic Signature/2001, Act of the Information Society/2001) slowly begins also the necessary reorganization of subordinate regulations in most of the

[8]PIN = Personal Identification Number

industry sectors.[9] *The legal regulation needed is built around two main groups of questions:*

1. Electronic Data-Exchange

The legal regulation of the electronic signature, which is supposed to be the basic one of the modern commerce, plays a particularly important role in the acceptance of the electronic documents in court. In order to get the digitally generated assignment as evidence in court, the followings must be ensured:

- the definite identity of the sender-party,
- the guarantee of the integrity of the information,
- the exclusion of the unauthorized users, confidentiality,
- the possibility of reproduction (of the document),
- the exact settling of the time of sending.

The international legal practice wishes and makes efforts to assure these criteria with the prescription of data-coding technology used by electronic signature. This is the so-called Hash-code method, which is spreading built in asymmetric key-code-couples.

2. Related Databases

Another fundamental aspect of electronic commerce is the connection between databases. For today not only enterprises, but also state owned data registration and processing centers are ready to manage country- or world-wide data communication systems. This is very useful for those market players, who want to make the best use of cross-sales or build a part of their job (see credit analysis) upon data obtained from official sources. At the same time the connection of different data-storing systems brings the protection of privacy into question, since with the help of the adequate software anybody can get a full picture about the situation of a private person or a company he is interested in.

4. Types of Identification Methods

The identification methods can be sorted according to the way we hold/store the information of authorization:

[9] The Hungarian Bank Association has a working team for defining the exact content of electronic signature format for the banking sector.

- *Something, that the user knows.* The identification called elsewhere 'one-factored' is based on the 'something to know' principle, that is the user has to define a password, PIN code, or an agreed pair of question and answer. In this case more possibilities are at disposal with different safety. The given password can be static, often changing, or dynamic; the so-called password file can be opened or coded.
- *Something, that the user has.* It is based upon the concept that the user possesses a physical object for the identification. It can be a key, a magnetic strip card, a smart card or a token. The use of these tools is often combined with the principle of 'something to know' detailed in the previous paragraph, so e.g. the password should be given, too. This is called two-factored identification, or 'strong identification'.
- *Something that only the user has.* This is the safest type of identification. The identification is based on the biometric features of the user. It can be, for example the geometry of the user's palm, a fingerprint, the 'retina-map' in the eye, the human voice, etc.

As we can see, the ideal solution in general becomes a very relative concept. Namely the aim of the solution to be used can only be the satisfaction of the risk level of the protected information. A higher safety level than needed would lead to far complicated processes. These overprotected systems contain expensive, not cost-effective, and complicated solutions, which usually cause a dissatisfaction of the users.

The applied media determine the possibility of the identification theories. For this reason it is obvious, that in case of multi-channel sales the customers identify themselves necessarily in very different ways. Creating the centralized identification system enables the managing of *different authentication methods* at the same time (PIN code, token, PKI). This way several of the methods can be attached to the user at the same time. Furthermore *the level of authentication* can be attached to every authentication method (see in *Table 1*). This value is influenced by the *characteristic features of the method used* for identification (for example static or dynamic code), and the technical characteristics of the applied media (e.g. the risk level of tapping the phones). With this method a chance is given that the use of the product or service could be attached to the risk level of the medium.

5. Customer–Channel–Product Relation

The problem of customer identification in the financial services is the simplest to illustrate as a 3D matrix:

- The first dimension contains the groups of the *already served users*. A speciality of the account-keeping services is, that not only the owner of the account, but a person charged by the owner can have the disposal on it. So the identification process must cover not only the customer base of the banks, but those charged with the disposal, as well.

Table 1. Example: score system for identification types

Types of identification	**Medium**	**Points**
Password	Telephone	1
	HTTPS[10]	2
PIN	Telephone/IVR[11]	2
	ATM (DES coded)	3
Dynamically changing PIN/one-time-password	Telephone/IVR	4
	ATM (DES coded)	5
'Signature' file	Unprotected communication	7
	Protected communication	8
Electronic signature		10
		...

Source: own

- The second dimension contains *the available sales channels*. Their number and types continuously change. Naturally, different identification methods are used to connect to different media.
- The third dimension contains the defined *limits on product-usage*. The type of identification applied, and the (value) limits fixed by the account-holder determine the possibility of the service access.

If the three dimensions are filled with the information about the identification methods, the channel information, and the customers and product-usage limits, then any of the actions initiated by the users can be matched with a particular spatial point in the matrix. As each and every point in the matrix indicates a score level, this method could be an easy way to generate exact score information for all product-usage.

6. The Black-Box Conception (Central Identification Module)

For the centralized identification of customers, an IT solution can be created, which identifies the users and manages their authority at the same time. The system should cooperate with all of the already existing core systems, or with those now being under development. A front-end application of the central identification and authority-managing systems is used to register customers and set the available service levels. The other connecting area of the system is created for the sales support software applications. With the help of this API kind of interface, a connecting

[10] HTTPS: Secure HTTP, i.e. data protecting method supported hyper text transfer protocol

[11] IVR = Interactive Voice Response. A service system based on the double frequency-code telephony protocol (touch-tone). Typically the Call Center solutions support this control method.

customer service system can check any time whether the applied authentication method is ready to support the required service.

The function described is attained through the following steps:

1. The comparing of the incoming identification request with the registered customer's database (customer identification),
2. Preparing the scoring[12] value
   - generating the scoring level out of the customer–channel–product 3D matrix,
   - searching for the risk value of the service required by the user,
3. matching the score level to the risk value and generating the answer.

Three kinds of answers can be generated by the system: authorization of the service, prohibition of it, or initiation of the request for further identification[13].

The task of the central module can be divided into two parts. The first one is the function of identification (A, B); the second one is the permission of the function belonging to the authority of the identified user (C). Take one after the other. The identification step has two tasks:

A. The Identification

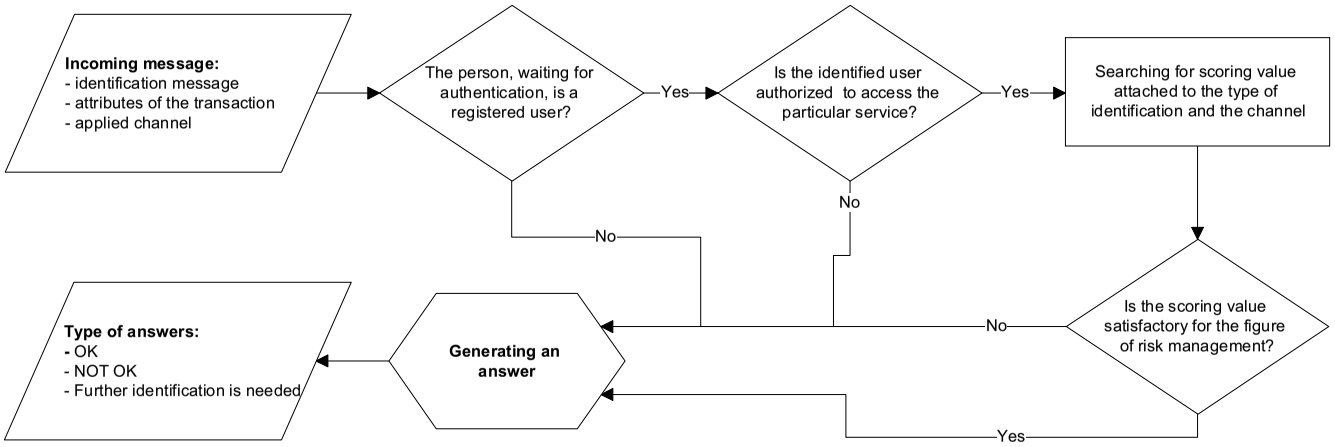
The first of the three functional steps is carried out by specialized identification submodules, depending on the incoming identification methods. The modular designed system is able to manage the authentication method used by the organization: PIN codes, static or dynamic passwords, PKI, biometric or external single sign on[14] authentication. By using the so-called plug-in technology, the system becomes more and more flexible, since this way the introduction of new identification methods requires no changes in the central unit. A centralized access system must ensure the following services:

- identification of users based on different kinds of authentication methods,
- possibility of external connection to other identification systems (for example CA services) [3],
- registration process of new users/maintenance of user profiles.

[12] Scoring = an expression used for supporting decision procedures in financial businesses

[13] Actually this third function is already used by several organizations. For example, when for special services, further identification is asked by the service provider (for example personal data).

[14] Single sign on = enables to access more systems with one authorization process.



Source: own

Fig. 1. The identification and authorization process

Since earlier the function of identification was a special duty of each channel, the centralization of identification methods creates an especially free space of usage for the customers. Translated this fact into the quality of the customer service, it means a real advantage referring to the users. The service organization does not have to deal with the spreading of identification tools; it is enough for them to register what kinds of services are available with the authentication methods used by the customers. So when the customer chooses a personal method for identification, he/she can consider the kinds of services desired to access. Entirely this means for the financial service providers, that their customers use customer-channels more easily and with a great pleasure.

Today the most frequently used methods for identification are the following: signature (handwriting), a pair of username and password (static and dynamic), PIN code, signature file, PKI (floppy, chip-card, TAN-based).[15]

B. Authority-Management

After the identification it is needed to determine whether the user is authorized to access the required service or not. In case of financial institutes, the user authorities can be very complex. These are built up out of the following combinations of variables:

- *Access to own account, with various methods.* With the use of the central identification module the possibility is given for the customer to access the account in different various ways. The sales channels and the relating authentication methods are contained by the central system.
- *Access to other's account, with various methods.* Managing the legal relations between users is an especially complex task of the financial service. The difficulty of this relationship is that most of the time the bank has to control the access of non-customers.
- *Access to an account in various roles.* There can be several kinds of relationships between the bank and the user. A customer can be the leader of the company; for example, who has his/her account at the bank, at which his/her company has it, too. With the knowledge-based customer-management it is possible for him/her to use his/her digital signature as a company-customer as well as for handling his/her private account.

[15] Among the identification methods used nowadays the electronic signature has some new features, it is really worth talking about them. The e-sign is the first kind of identification method (of course only after the handwriting) that the international law seems to support. The establishment of the PKI technology service provider (CA=Certificate Authority) is quite expensive. In practice this means that most of the organizations using this kind of identification does not develop their own solution, but connect to external, specialized identification systems, which generate and store the electronic signature of the customers. So this technology prescribes the demand of connecting to an external CA among the identification modules in case of the drafted black box conception.

- *Management of co-signatories.* The centarlized system enables to handle more than one signatory in a way that this has not to be managed by the client-application. The central module stores the incoming operations. When more than one signatory are needed, the operation stays pending until the authentication of all the signatures is made. This special status has to get an interpretation in the channel system of course.[16]

C. Function-Authorization

The function-authorization of the identified and authorized user depends on some factors influencing the risk-management. These are

- the limit of products/services usage, adjusted to the customer or the channel,
- the 'strength' of the identification used, which is correlated with the authentication method (see earlier).

These pieces of information are practical to store in a central, multidimensional function-risk database. The values of the matrix have to be defined partly according to the fraud expectations of the organization and partly to the requirements of the business service level.

During the identification process the system calculates a scoring value relying upon the attributes of the service protected and the strength of the identification. The task of the function-authorization is the harmonization of the calculated scoring value and the predefined level of function-risk in advance.

7. Connection to External Systems – Uniformed Transaction Messages

The central authentication system has two essential relationships towards other information systems. One of them is a relationship used for managing and answering identification messages, while the other is the relationship of the occasionally applied external identification modules and databases. The first connection has standardized communication, containing uniformed messages, where from the direction of the medium appears a message describing the transaction of the customer. The message has to contain the following information:

[16] With the solution given by the central identification module it is possible to handle cases when the co-signatories cannot be at the same place at the same time. For example in a case, when one of the signers prepares the transfer on the computer and sends it to the bank. The central identification module will register the order, but the transfer still cannot be sent, because the authentication is not complete yet. As the other signer calls the bank, gives the identification code of the transfer to the administrator, and authenticates himself (for example with a one-time used password), the authentication will be accepted by the identification module. After finishing the second identification the module informs the channel system, that the transfer is ready to be sent.

- the type of transaction
- the value of the transaction (if there is any)
- the method of identification
- the identification message
- the code of the media used

The uniformed transaction message has an advantage, that all the connected delivery channel systems can use the same data format for customer authorization. With the help of this solution we can reduce the built-in logic in all delivery systems: under the process of authentication they can act as a pure data tranfer system between the costumer and the black box.

The other group of relationships between systems describes the relationship with external databases. It can be a CA service or a connected database of customers. These are once defined relationships depending on the circumstances.

8. Summary

The establishment of the central identification system sketched out has multi-level advantages for the organization:

- significant reduction of administration, the users' service access control becomes adjustable through only one central system,
- the media independent authority-management of customer-relationships enables to summarize the usage limits of different channels, which creates a quite new way of risk-management in the organization [5].
- the central identification makes it possible that the way of identification can be independent from the type of the medium.[17] This way the cross-use of the sales channels becomes extraordinarily extended.

The appearance of the factors mentioned in the organization establishes the basics of the knowledge-based customer service. The customer-information based service enables the organization through the improvement of sales, radical changes in risk-management, and a significant increase in the level of customer loyalty. All this means for the enterprise the possibility to reach higher ROE and ROA[18] level, than the competitors in the market have. At the end, these become a guarantee for a long-distance presence on the market.

[17] In case of having an own ATM operating system, the organization becomes able to manage cash withdrawal service not just on bank card basis, but for example with the use of the Internet banking service username and a password combination.

[18] ROE = Return on Equity, ROA = Return on Asset

References

[1] DOYLE, P., Leveraging Trust for a New Era in Financial Services, Baltimore Technologies, 2001.
[2] BUCK, S. P., Secure M-commerce: Now or Ever, The Future of Financial Services, 2001.
[3] TUNSTALL, J., The Evolution of the Global Trust Authority, Global Trust Authority, 2001.
[4] STOREY, D., Securing Financial E-business with Practical PKI, RSA Security, 2001.
[5] BARLOW, S., Embedding Risk Management at Prudential plc, The Future of Financial Services, 2001.
[6] DEDMAN, R. D., Exploding the New Revenue Stream of Internet Financial Sevices, Lafferty, 2001.
[7] Biztonságos bankolás, E-finance Magyarországon, *Pénz a Hálón*, **2** (2001).
[8] A biztonság magasiskolája, E-finance Magyarországon, *Pénz a Hálón*, **2** (2001).
[9] ERDŐSI, P., A hazai informatikai biztonsági helyzet és az elektronikus aláírás, Alma Mater, 2001.
[10] EGERSZEGI, K., Informatikai biztonsági perspektívák Magyarországon, Alma Mater, 2001.
[11] The Unexpected eEurope, Accenture, 2001.
[12] Banking Technology Solutions 2000/2001, PriceWaterhouseCoopers, 2001.
[13] DUNSIRE, I., How to Get your Wires Uncrossed, Retail Banker, 2001.
[14] 2001/35 Az elektronikus aláírásról szóló törvény.