DIGITAL SIGNATURE AND ORGANIZATION OF DECENTRALIZED AUTHENTICATION IN BUSINESS ENVIRONMENT

Tijana Talić, Gordana Radić, Zoran Ž. Avramović

Pan-European University APEIRON, Banja Luka, Republika Srpska, Bosnia and Herzegovina,
tijana.z.talic@apeiron-edu.eu

Contribution to the state of the art

DOI: **10.7251/JIT1901024T** UDC: **316.77:004.773]:658.14**

Abstract: Modern electronic communication is fast and efficient. It has never been easier to change the document's content. In this paper, we explain and show through practical work how it is possible to protect the data sent electronically in business communication by using decentralized authentication systems.

Keywords: authentication, digital signature.

INTRODUCTION

Security is a matter of trust. Should you take your security into your own hands or let someone else take care of it?

The problem of security and protection of computer systems is slowly becoming a business, actually, a service that is sold to you by companies outside your firm. This releases companies from employing professional staff and partially relieves their costs. These services often include: the purchase of a part of the hardware, especially firewalls, the software that works on them, installing and maintaining antivirus programs, various types of data backups, and even storing cloud databases that are maintained by specialized hardware, software, and team of experts. This is very interesting for our BiH conditions, especially when electricity goes down. This brings us back to the eternal question of who controls the controllers, or how much we can trust those companies. Even if these systems function properly, the fact is that a lot of damage can be caused by the lack of sender's authentication or the credibility of the electronic message.

Violating privacy, tracking the users and recording their habits is a perpetual topic in electronic communication. On the other hand, the presence of various kinds of malicious programs imposes the need to pay attention to security in every form of communication.

Modern electronic communication is fast and efficient. At the same time it has never been easier to change the document's content. This can be applied not only to electronic messages, but also to printed documents that are not particularly protected, for example, with a dry stamp, using special paper or in a similar manner. It is enough just to digitize the document, make a change in one of the available editors, and print it again. We had the opportunity to see how officers usually check the credibility of the stamps on paper by 'licking' them. This tells us more clearly that in the new age we have to use new techniques of signing and credibility verification.

Authentication

One of the main elements of authentication in electronic communication is a digital signature, whereby we need to distinguish the meaning of terms electronic and digital signature. One of the definitions states that an electronic signature is any sound, symbol or process that is electronically linked to a document-contract or record adopted by the signatory, indicating his or her intention of signing. The digital signature replaces the personal signature and confirms the sender's identity as well as the credibility of the sent message and is based on cryptographic algorithms and keys. Connecting a public key and identifying the person using it is one of the major issues in authentication. There are two approaches to solving this problem:

- Use of certification authorities (centralized system)
- Use of decentralized systems

WoT

The most well-known decentralized model of trust is the "Web of Trust" (WOT). WOT is a concept used in PGP and other OpenPGP compatible systems, best known as GnuPG (GPG) [4]. It does not rely on the certification authority hierarchy, but users sign certificates among themselves to confirm the public key connection with the person or entity specified in the certificate.

Key K is considered valid if two conditions are fulfilled:

1. It is signed with enough valid keys which means:
   b. It was signed by you personally,
   c. It was signed by a fully reliable key,
   d. It was signed by three keys with marginal trust.
5. The path's length of the signed keys that leads from the key K back to your key is five steps or shorter.

Besides signing a public key, each user must also be determined the level of trust (owner-trust) in the way he signs other keys. There are four levels of trust:

- unknown
- none
- marginal
- full

It is possible to adjust the length of the path, the number of marginally trusted keys and the number of fully trusted keys. The above listed numbers are default values used by GnuPG. The setting parameters are: marginals-needed, completes-needed, and max-cert-depth for the path's length from the key K back to your key.

It is important to note that the level of trust in user (owner-trust) must always be entered on our own, while the key validity can be calculated using the above mentioned method.

Web of Trust has a flexible approach to the problem of secure public key exchange. This approach allows you to configure GnuPG to reflect how it is used. In the extreme case, it is possible to request a multiple, shorter path from your key to key K. On the other hand, you may be satisfied with a longer path and perhaps with a shorter path from your key to key K as well. Requiring multiple short paths is a powerful guarantee that the key K is really valid.

The main problem is that if we need to confirm a large number of keys or we need to communicate with people, we do not know that this procedure requires user's immense engagement.

Therefore, the main problem of the WoT network is the validation of keys in case we want to establish communication with a large number of people. In this case, in order to provide less perfect but effective security solution, it is suggested to slightly loose the threat model instead of using theoretically perfect but practically very difficult rules. We achieve this by using the TOFU model (*trust on first use*).

TOFU

The TOFU model memorizes the key during the first contact and remembers the key usage statistics [5]. In the case that the key is changed, the TOFU declares both the key (old and new) as conflicting and requests interaction with the user to determine whether it is an attack or a regular key update. In the case of an attack, the attacking key will be declared defective, communication will be denied and, if necessary, other measures will be taken as well. If we find that it is a regular update of the sub keys in contact with the sender, both keys will be accepted as correct.

TOFU will also warn us on the first contact and we can easily recognize whether it's a mimicry attack or a real new contact.

WEB Key Directory

Web Key Directory is a new public keyword detection scheme that allows you to detect PGP keys by using an email address.

For example, if you are looking for the key of tijana@example.org, the key will be delivered from the following location:

https://example.org/.well-known/openpgpkey/hu/1xnth55nm69yzufx5jbdyh5hjzcbecbr

The web directory provides an easy way to discover public keys via HTTPS. It provides an infrastructure that significantly improves user's experience while sharing secure email and file messages.

Unlike the public key server, Web Key Directory does not publish email addresses. This is the authoritative source for your own domain.

It works in the following way:

- The sender's mail client checks the "well-known" URL on the recipient's domain.
- If the public key is available for this email address, it will be downloaded via HTTPS.
- The public key can now be used without further user's interaction.

The use of WKD is implemented in GPG from version 2.1.12 as well as by adding it to the main e-mail clients: Thunderbird / Enigmail 2.0, KMail from Version 5.6, Outlook with GpgOL from version 2.2.0, Mailvelope from version 3.0.0

The Web Key Directory is generally created and maintained through the web key service, but organizations or individuals can host only the web key directory without the web key service.

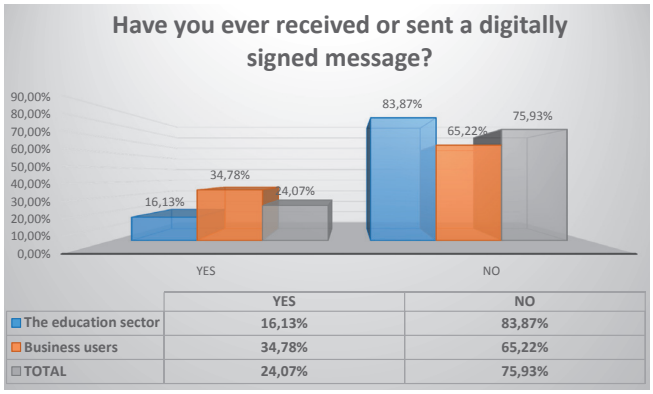
This is accomplished by using a flat file structure that should be re-created if the public message changes.

The thing is that files, whose hash address name is from corresponding domain, are created for each address of the corresponding domain with the help of GPG. It is necessary to have control over the web server of that domain. Created files are set up on the path. well-known / openpgpkey / hu / on the web server's domain. This is set up on the HTTPS server. It is necessary for the web server to be configured appropriately and to enable HTTPS communication and protect the directory from direct browsing. The client calculates hash addresses and searches for a file with that name on that path. If he finds it, then the matching public key is imported.

WKD is set up only for addresses from that domain and represents a unique authoritative key server of that domain.

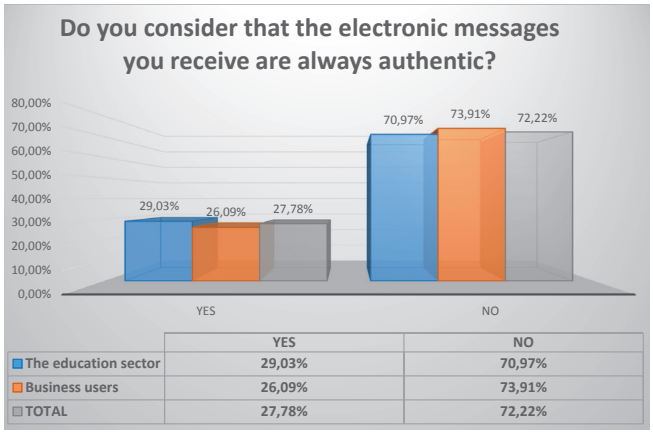
Current situation

The use of digital signatures in the business environment of BiH can easily be seen from the research diagram conducted in the work [1]. The survey covered two groups of business users: employees in the education sector and employees in the civil service.



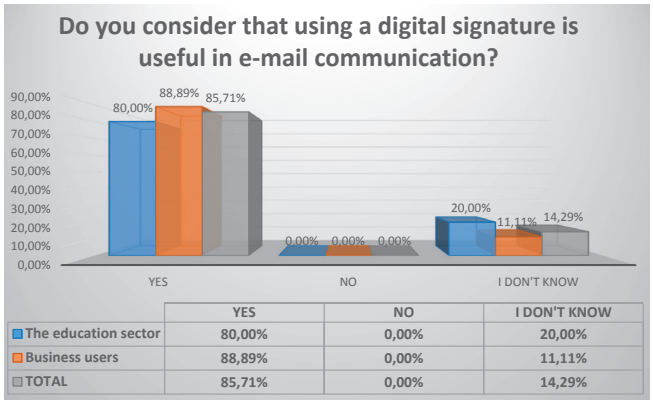
	YES	NO
The education sector	16,13%	83,87%
Business users	34,78%	65,22%
TOTAL	24,07%	75,93%

Figure 1. *Use of digital signature in business environment*



	YES	NO
The education sector	29,03%	70,97%
Business users	26,09%	73,91%
TOTAL	27,78%	72,22%

Figure 2. *Authenticity of electronic messages*



	YES	NO	I DON'T KNOW
The education sector	80,00%	0,00%	20,00%
Business users	88,89%	0,00%	11,11%
TOTAL	85,71%	0,00%	14,29%

Figure 3. *The importance of using a digital signature in electronic communications*

From Figure 1 we can conclude that a small number of business users use a digital signature. On the other hand, it is clear from Figures 3 and 4 that electronic communication is not always safe and messages sent electronically are not always authentic. The survey also shows that over 85% of respondents in our business environment agreed that the induction of authentication by using digital signatures makes business communication easier and more secure.

Organization Model in a Business Environment

Our model is based on a combination of web of trust and trust for first use (TOFU). This solution does not cover the entire world, but we will limit ourselves to everyday business communication in which we have the definite number of participants. Construction begins as WOT. In the case of a business entity, we will form the key that is related to the company. Although email is a strong identifier, we can create this key without using an email. We can also omit the encryption sub key so that this key is for signature and certification only. Let us call this key the main key of the company. With the main key we will sign all employees' keys. By signing the main key with complete trust, all employees will have mutually valid keys. The connection of the main key and employees' key is two-way and with full confidence. In this way, we saved the users within the company from a part of the work about the signing and certification.

We should not forget that all these keys must be synchronized with the key server.

Employees will deposit their secret keys and revocation keys in a secure location. Depositing private keys and keys for revocation to a secure location is extremely important as well as remembering the pas-phrase key. This is especially noteworthy since, during the performance of the experiment, we noticed that users are prone to lose keys or passwords for private key.

Let us observe the other organization that was arranged in the same way. It would be desirable that, if there is a business link between these two organizations, the administrators sign and certify the main keys with full confidence. Of course, the administrators will do this with detailed checks. What did we get with this?

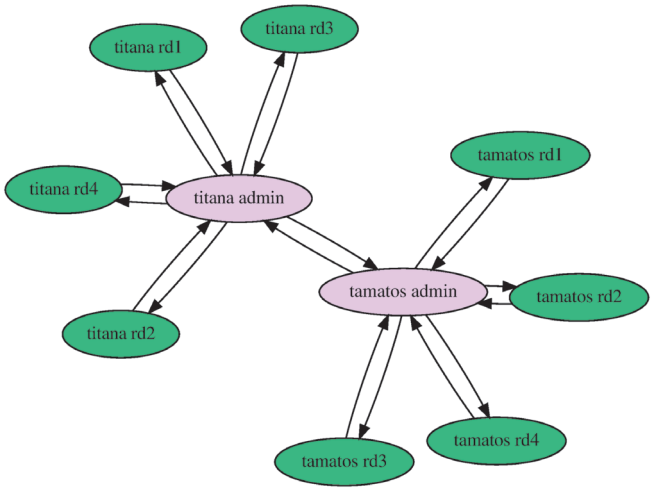


Figure 4. *The signature structure for Titana and Tamatos companies*

If a user from one company imports the main key of another company, WoT will automatically certify the main key of another firm. This key will be associated with unknown trust. If the user makes more effort and gives fully trust to the main key of another firm (based on a check made by administrators among them), then all users of another company certified with its main key are placed on the path shorter than 5 steps and signed with enough valid keys. In this way, we used WoT to identify known associates from close companies. In order to join a third company in this scheme, the previous steps should be repeated.

Automating and increasing reliability using WKD

Using the WKD, it is possible to automate the process of key manipulation additionally. New versions of GPG have built-in support for WKD application. Add-ons of the well-known mail clients are set to automatically check the existence of a key on WKD. After entering the recipient's address, these add-ons on Enigmail (Mozilla Thunderbird) and GpgOL (Outlook) automatically detect the keys to the WKD. This further reduces user's interaction.

Of course, IT administrators have to create web key directories and maintain them up-to-date. Combination of the automatization provided by WKD and web of trust increases the level of resistance to sophisticated attacks. When applying automation, we need to distinguish the way in which we

have come up with the appropriate public key. If a user explicitly enters an email address (for example, when encrypting), we know that the user intended to enter exactly that email address. On the other hand, if we get the key through the WKS to check the signature (for example, we use WKS to find the key for varalica@example.org), then we should not be convinced that the key is reliable and the message is authentic.

The third engine of this system is TOFU. It practically checks the system all the time. It also tracks and collects key usage statistics and most importantly, it detects the conflict. In case of TOFU conflict detection, both keys are declared defective and user's interaction is necessary.

This can be applied in organized systems with an IT administration. Of course, this is often not the case. In such, and in all other situations, we will use the TOFU scheme. It is necessary to emphasize the importance of establishing the first contact. It is desirable that the keys exchange is performed with a secure channel, or by combining multiple communication modes.

Our solution requires from customers to use the TOFU + PGP settings to validate the keys. This setting calculates validity according to WoT and TOFU rules and sets the higher one. In some cases it is advisable to set the settings so that the TOFU does not provide any evaluation of the key validation, and the TOFU is only used for conflict detection. The result is an increase of the interaction level.

The defense of persistent and targeted attacks is not easy. Although this system has a high level of automatization, a certain level of user's training is needed to see some signals when it comes to targeted pirate attack or CEO fraud.

Conclusion

This model uses three essential components: WOT with its strict and precise rules is loosened by the usage of TOFU models and it is automatized by the usage of WKD. The model is not demanding to the end user.

Interaction with the user is reduced to a minimum. The purpose of this model is its usage in everyday communication where it gives a solid level of reliability, especially when defending from *man in the middle* attack and facilitating the detection of mimicry. For areas where communication reliability requirements are much higher, it is necessary to use different models and probably other tools.

The use of this model requires the existence of IT administrators, whether they are directly present in a business entity or engaged from outside, as well as a minimum education of users.

Bibliography

[1] Talić, T., "The use of digital signature in electronic communication in BiH - Research," *JITA - Journal of Information Technology and Applications*, vol. 7, no. 1, pp. 20-23, June 2017.

[2] Darxus,. (2002) sig2dot GPG/PGP Keyring Graph Generator. Available at: http://www.chaosreigns.com/code/sig2dot/, [Last accessed 01 May 2019]

[3] Talić, T., Decentralizovani sistemi autentifikacije u savremenoj komunikaciji, 2019, (Doctoral dissertation, PanEuropien University APEIRON, Banja Luka).

[4] wiki.gnupg.org,. (2018, Jun) *Automated Encryption.* Available at: https://wiki.gnupg.org/AutomatedEncryption, [Last accessed 10 May 2019]

[5] Walfield, H N. and Koch Werner, "TOFU for OpenPGP," in *EuroSec '16 Proceedings of the 9th European Workshop on System Security*, London, 2016.

[6] Gambetta, D., ""Can we Trust Trust?"," in *Trust: Making and breaking coopeative relations*.: Department of Sociology, University of Oxford, 2000, ch. 13, pp. 213–237.

[7] Böhme, R. and Grossklags Jens, "The security cost of cheap user interaction," in *Proceedings of the 2011 Workshop on New Security Paradigms Workshop, NSPW '11,* New York, 2011, pp. 67-82.

Submitted: May 24, 2019
Accepted: May 30, 2019

For citation

Talić T., Radić G., Avramović Z.Ž., Digital Signature and Organization of Decentralized Authentication in Business Environment, *JITA – Journal of Information Technology and Applications Banja Luka,* PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 9(2019) 1:24-28, (UDC: 316.77:004.773]:658.14), (DOI: 10.7251/JIT1901024T), Volume 9, Number 1, Banja Luka, june 2019 (1-48), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004