THE SECURED MANAGEMENT OF ELECTRONIC DOCUMENT SERVICES FOR CLOUD SERVER BASED ON DIGITAL ELECTRONIC SIGNATURE MODEL

Krishna Bikram Shah
Department of Computer Science and Engineering, Nepal Engineering College, Nepal

Abstract

Recently, it often talks about electronic signature (ES) in the cloud. Basically, this topic is discussed by IT-experts. However, with the development of electronic document management services (EDF), subject matter experts - accountants, secretaries, auditors and others - began to engage in the topic of cloud ES. In this paper, the secured management of electronic document services for cloud server was proposed based on digital electronic signature model. A cloud-based electronic signature indicates that your private ES key is stored on the certificate authority's server and that the signing of documents takes place there. It is accompanied by the termination of relevant contracts and powers of attorney. Actual confirmation of the signer's identity occurs, as a rule, using SMS authentication. To work with a cloud-based electronic signature, you do not need to install an electronic signature certificate or special tools for working with it. This means you won't waste time figuring out how it all works.

Keywords:

Electronic Signature, Document, Management, Cloud Server, ES Key, Certificate, SMS, Authentication

1. INTRODUCTION

The need for an accountant to use Cloud ES depends on the mode in which he works. If you are often out of the office, or, for example, work in a company that provides accounting services (accounting outsourcing), cloud-based ES will help you sign documents from anywhere. No need to install additional software [1]. However, despite the ease of use, not all companies are ready to take advantage of this opportunity. We will consider all the pros and cons of using a cloud-based electronic signature so that you can choose for yourself whether you need it or not. Also consider who might actually need such a signature [2]. Cloud electronic signature is cheaper than usual. This is because you don't need to buy a cryptographic information protection tool (CIPF) and a token (a flash drive with a certificate) [3]. As a rule, taking into account their acquisition, the price of a certificate rises by 2-2.5 times. At the moment, there are no common and free solutions for using non-cloud electronic signatures on mobile devices [4]. In this regard, a big advantage of cloud-based electronic signature is that you can work from any computer, tablet, smart phone with Internet access [5].

It is not physically signing the document. It should understand that in the case of a cloud-based electronic signature, the private part of the key, confidential and belonging only to you, is located on the certificate authority's server [6]. Of course, this will be documented, and the servers are securely protected. But here it all depends on the company's security requirements and policy regarding signing documents [7]. If it is important to you that the owners of the private keys themselves sign the documents, then cloud-based electronic signature is not for you. In this situation, you need to decide how much you trust the CA and the servers that store the private keys [8]. It can use cloud-based ES only in services with integration of certificate authority software. In the case of Cloud ES, this is because the private key is stored on the CA server [9]. It can use such a private ES key to sign for the service, which can then send a request to the CA server to generate an electronic signature. At the moment there are many services and it is clear that not all of them can provide integration with CA software. It turns out that you only need to use Cloud ES with certain services [10]. To work with other services, you need to purchase another ES certificate, and there is no guarantee that these services will support cloud-based electronic signature [11].

A qualified electronic signature should be used to generate and verify the regulator. A simple verification may not be sufficient to control the embedding of cryptographic information security in the particular information system where a cloud-based electronic signature is used [12]. Currently, companies that develop information security tools are concerned with increasing the security of user authentication when confirming the signing of a Cloud ES document and encrypting data when it is sent over the Internet [13-14]. And according to the developers only the signature is eligible. It offers a qualified upgraded cloud-based ES at relatively low cost and authentication via SMS with login + password and one-time password [15-17]. Application security is directly related to the user's access to the phone. Today, this risk is gradually decreasing, as it is an increasingly common practice among users to install a primitive password protection on the phone [18].

2. RELATED WORKS

Cloud signature in today's understanding belongs to the category of enhanced unqualified signature. Most of the work done by it is consistent with the concept of legally inscribed as an enhanced signature. But at the same time, this signature is not certified by the FSB as a controller responsible for the security of signatures based on cryptographic methods [1]. Currently, a document signing scheme in the cloud looks like this: documents are signed on a DSS (Digital Signature Server) server using keys stored in the HSM (Hardware Security Module). At the same time, user access to HSM is, as a rule, based on the use of non-cryptographic authentication systems [2].

Cloud electronic signature is a convenient, mobile and simple tool, but not very flexible. In terms of security, it is better to store the private key on a secure server than to keep a token in a drawer. First, those who often work outside their office in the office [3]. The lawyers and auditors who frequently meet with clients were important executives and directors signing documents from anywhere. For them, cloud-based electronic signature will become an indispensable assistant in their work [5]. Also, a lot depends on the company's policy. If a company is moving towards cloud technologies, for example, storing documents, using

services for internal and external document management, electronic signatures are often cloud-based. Otherwise, cloud-based electronic signature is not required for accountants, clerks and other employees who usually do not leave the office during work [8]. They can purchase an ES private key and ES certificate in the usual way, from a carrier that can be used to exchange most services with counterparties and government agencies [10]. The purpose of this work is to analyze scientific publications and laws in the field of electronic signature and its subspecies - cloud electronic signature. The implementation of this goal is carried out by solving tasks [12].

3. PROPOSED MODEL

With the active information of all spheres of life in modern society, the transition to cloud computing and services is being implemented. Public services are already running on cloud services due to their high performance for mass use by citizens. Cloud Signature Security Login Bank. Transferring workflow to cloud storage is also suitable for a small dynamically growing business. In the process of such exchange, the question of security and efficiency of using cloud signature arises. Cloud signature can be actively used in areas such as:

- Internet banking or mobile banking systems that require the use of a qualified electronic signature;
- Websites of public services, electronic reporting systems;
- E-commerce systems;
- Electronic document management systems

Cloud Electronic Signature is a computer system that provides access via the network to the creation, verification of ES and the possibility of integrating these functions into the business processes of other systems.

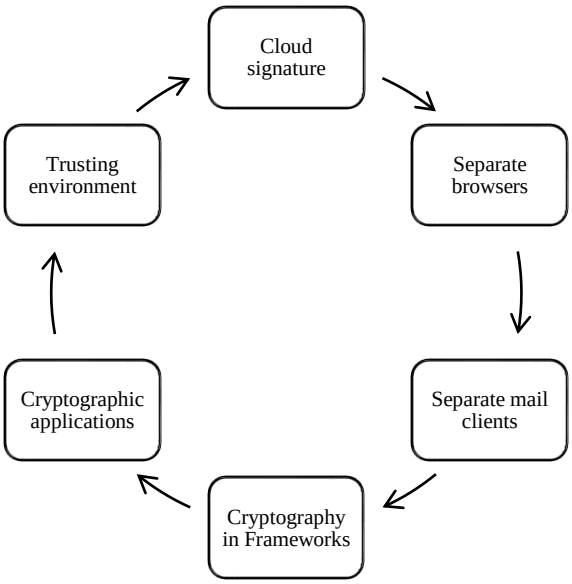

Fig.1. Essence of an electronic digital signature

A cloud-based electronic signature has all the characteristics of an electronic signature, except that it is not stored on a token or computer, but on the Internet - on a special secure server, in the cloud. Cloud ES means that your ES private key is stored on the certificate authority's server and documents are signed. On the one hand, the fact that the signing of keys and documents occurs on the server side reduces the cost of the entire ES system, on the other hand, the key is private and must be kept only by its owner. The Legal regulation was creating the relations in the field of use for the electronic digital signature. The concept and essence of an electronic digital signature as an electronic analogue of a handwritten signature is significant. This was shown in the Fig.1.

- Cloud signature
- Separate browsers with encryption
- Separate mail clients with encryption
- Cryptography in Frameworks, Platforms, Interpreters
- Desktop cryptographic applications
- Guidelines for creating a trusting environment

Cloud ES is usually cheaper than regular ES, which is due to the fact that there is no need to purchase a token with a cryptographic information security tool and certificate. For people who are far from IT, using cloud signature is easy: there is no need to install an ES certificate and special tools to work on a workstation. It can work with Cloud ES from anywhere in the world, from any device with an Internet connection. However, there are also disadvantages like changing and storing the key on the server. The servers are securely protected, but the violation of the confidentiality of the key and its alienation from the owner make Cloud ES ineligible, i.e. not confirmed by a certificate issued by an accredited certification authority. A Cloud ES service developed for one information system, as a rule, is not suitable for another. In other words, the user bears the burden of having the signing key for each computer. The proposed model was shown in the Fig.2.

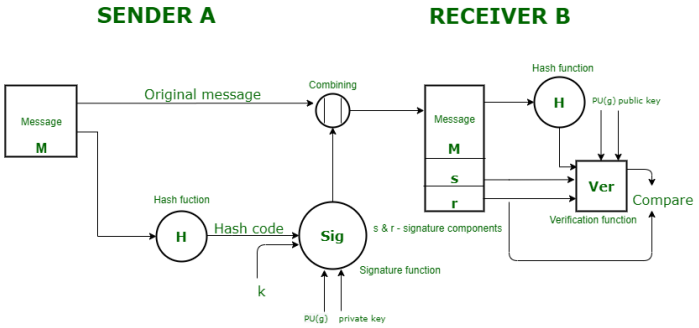

Fig.2. Proposed digital Electronic Signature model

Two-factor authentication with an additional input of a one-time password is provided to the user via SMS (OTP-via-SMS). The main problem is identifying the user's identity and is protected for cloud signing. To access the cloud service, a person uses a login-password. This, of course, is not enough. It needs to know exactly who is logged in under this login-password. You can use it by sending your fingerprint to the server over an unencrypted connection. The key factor will be "unencrypted connection" because we have no mechanisms for cryptographic information security. In this case, it is one of the main objectives of the EP being. A reliable cryptographic was the way to determine the author of an electronic document. Such an approach is justified only for inter-enterprise electronic document management systems where a DSS/HSM-based solution is implemented at the level of participating enterprises. In this case,

the outgoing documents in the common system are processed according to the usual rules, and the storage of keys in a secure cloud is implemented for the convenience of employees.

4. RESULTS AND DISCUSSION

The proposed digital electronic signature model (DESM) was compared with the existing qualified electronic signature service (QESS), block chain-based cloud data management (BCDM), Cloud-Based Electronic Signature Authentication (CESA) and the Integrated Electronic Signature Service (IESS)

Browsers based on the open-source Mozilla Firefox and Chromium projects use NSS or Open SSL as the crypto kernel. The Open SSL supports crypto algorithms. For NSS, there are also improvements that provide support for new crypto algorithms. Some time ago, full-featured browsers with support for encryption appeared on the market. Such a solution has a great, currently unclaimed, potential, as it allows you to create secure static WEB clients for computers with high security requirements. This was shown in the Table.1.

Table.1 . Comparison of Browser management

Inputs	QESS	BCDM	CESA	IESS	DESM
100	50.96	56.34	64.25	53.69	86.85
200	49.67	55.59	59.63	50.29	86.75
300	49.92	55.62	59.63	50.65	86.68
400	50.05	56.44	60.10	51.84	86.64
500	49.97	56.53	60.30	51.71	86.60
600	49.98	56.66	60.56	51.69	86.57
700	50.33	57.08	61.19	52.12	86.55

Another advantage of this browser is its "portability". Due to the availability of secure USB tokens with flash memory, secure solutions were developed, in which the most important operations with the private key are carried out on the "board" of the USB token, and the browser is protected in its flash memory from change. Such a solution, in addition to a high level of security, is very convenient to use.

Private mail clients with cryptography allow you to implement correspondence protection using electronic signature and message encryption for subscriber / group of subscribers (S / MIME). This solution is convenient for use in systems built according to the "point-to-point" principle, in which information is exchanged directly between subscribers, and the server is used only for message routing. This was shown in the Table.2.

Table.2. Comparison of P2P routing Management

Inputs	QESS	BCDM	CESA	IESS	DESM
100	50.10	55.28	60.92	50.37	86.86
200	49.60	55.28	59.83	50.11	86.75
300	48.85	54.45	58.69	49.54	86.69
400	48.85	55.18	59.05	50.68	86.64
500	49.90	56.29	60.58	51.70	86.60
600	50.18	56.69	61.22	51.94	86.57
700	49.46	56.12	60.64	51.29	86.55

The platform contains a set of cryptographic classes that provide mechanisms for extension by third-party algorithms. The most well-known solution on the market for extending the Microsoft.Net platform with crypto algorithms is the Crypto Pro product. NET, this is a plugin for CryptoPro CSP. Installing CryptoPro.NET allows using crypto algorithms, for example, in WEB services based on ASP.NET, SOAP services in MS. Silverlight client browser applications. This was shown in the Table.3.

Table.3. Comparison of Cryptographic Management

Inputs	QESS	BCDM	CESA	IESS	DESM
100	58.39	46.75	85.43	49.21	88.86
200	60.05	52.61	78.59	55.39	88.75
300	60.50	51.47	77.30	56.88	88.69
400	55.81	52.61	75.16	60.12	88.64
500	55.42	53.49	76.73	59.40	88.60
600	55.58	54.69	78.35	59.27	88.57
700	56.32	56.34	80.15	60.54	88.55

An open source library that implements its own cryptographic classes for the Microsoft.NET platform. The library supports both basic cryptographic algorithms, taking into account GOST 28147-89, GOST R 34.10-2001, GOST R 34.11-94, and encryption formats PKCS#7/CMS, PKCS#10, X.509. In addition, according to the developers, the library supports the Gates format with cryptographic algorithms. This was shown in the Table.4.

Table.4. Comparison of Separate libraries Management

Inputs	QESS	BCDM	CESA	IESS	DESM
100	54.45	51.21	70.18	49.79	89.86
200	55.16	53.97	70.39	52.83	89.75
300	55.09	52.99	69.13	53.37	89.69
400	52.48	53.91	67.94	55.67	89.64
500	52.75	54.91	69.52	55.73	89.60
600	52.97	55.70	70.77	55.77	89.57
700	53.03	56.23	71.68	56.18	89.55

The Java cryptography architecture allows you to expand the set of cryptographic algorithms supported on the platform. Due to the high prevalence of Java, many developers of cryptographic tools offer certified JCP providers.

5. CONCLUSION

The use of cloud signature is one of the steps in the development of the latest information technologies, which is our approach to a convenient digital future. However, there is still work to be done in this area. State guarantees in the form of a certificate of compliance with information security requirements of cloud electronic signature tools are required. It is appropriate to develop and implement a standard for the use of cloud-based electronic signature. Definition of electronic signature generation, application technologies and principles, standard cryptographic

algorithms etc. should be ensured. The concept of signature key certificate and verification of its authenticity, appointment of electronic document management systems and electronic digital signature, and using hash functions are improves the document security. The Symmetrical and asymmetrical scheme and different types of Asymmetric Electronic Signature Algorithms are generating a private key and obtaining a certificate.

REFERENCES

[1] Joseph Idziorek and Mark Tannian, "Exploiting Cloud Utility Models for Profit and Ruin", *Proceedings of IEEE International Conference on Cloud Computing*, pp. 33-40, 2011

[2] Tao Xiang, Jia Hu and Jianglin Sun, "Outsourcing Chaotic Selective Image Encryption to the Cloud with Steganography", *Digital Signal Processing*, Vol. 43, pp. 28-37, 2015.

[3] G.U. Devi and G. Supriya, "Encryption of Big Data in Cloud using De-duplication Technique", *Research Journal of Pharmaceutical Biological and Chemical Sciences*, Vol. 8, No. 3, pp. 1103-1108, 2017.

[4] K. Goyal and P. Supriya, "Security Concerns in the World of Cloud Computing", *International Journal of Advanced Research in Computer Science*, Vol. 4, No. 4, pp. 976-997, 2013.

[5] B. Poornima and T. Rajendran, "Improving Cloud Security by Enhanced Hasbe using Hybrid Encryption Scheme", *Proceedings of World Congress on Computing and Communication Technologies*, pp. 312-314, 2014.

[6] Chang Liu, Jinjun Chen, Laurence T. Yang, Xuyun Zhang, Chi Yang, Rajiv Ranjan and Ramamohanarao Kotagiri, "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates Parallel and Distributed Systems", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 25, No. 9, pp. 2234-2244, 2014.

[7] Tram Truong-Huu and Chen-Khong Tham, "A Novel Model for Competition and Cooperation among Cloud Providers", *IEEE Transactions on Cloud Computing*, Vol. 2, No. 3, pp. 251-265, 2014.

[8] X. Li and L. Shu, "EdgeCare: Leveraging Edge Computing for Collaborative Data Management in Mobile Healthcare Systems", *IEEE Access*, Vol. 7, pp. 22011-22025, 2019.

[9] I. Aciobanitei, M.L. Pura and V.V. Patriciu, "Sabres-A Proof of Concept for Enhanced Cloud Qualified Electronic Signatures", *Proceedings of International Conference on Communications*, pp. 103-108, 2020.

[10] Y. Lee and U. Lee, "Issues and Concerns: Record Management in Cloud Services", *Proceedings of International Conference on Computer Applications and Information Processing Technology*, pp. 1-6, 2017.

[11] Lu Huang, Hai-Shan Chen and Ting-Ting Hu, "Survey on Resource Allocation Policy and Job Scheduling Algorithms of Cloud Computing", *Journal of Software*, Vol. 8, No. 2, pp. 480-487, 2013

[12] Hui Zhang, Guofei Jiang, Kenji Yoshihira and Chen Haifeng, "Proactive Workload Management in Hybrid Cloud Computing", *IEEE Transactions on Network and Service Management*, Vol. 11, No. 1, pp. 90-100, 2014.

[13] M.A. Tawfeek, A. El-Sisi, A.E. Keshk and F.A. Torkey, "Cloud Task Scheduling Based on Ant Colony Optimization", *Proceedings of International Conference on Computer Engineering and Systems*, pp. 64-69, 2013.

[14] Haiying Shen and Guoxin Liu, "An Efficient and Trustworthy Resource Sharing Platform for Collaborative Cloud Computing", *IEEE Transactions on Distributed and Parallel Systems*, Vol. 25, No. 4, pp. 862-875, 2014.

[15] D. He, S. Zeadally and H. Wang, "Certificateless Provable Data Possession Scheme for Cloud-Based Smart Grid Data Management Systems", *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 3, pp. 1232-1241, 2017.

[16] M. Sutharasan and J. Logeshwaran, "Design Intelligence Data Gathering and Incident Response Model for Data Security using Honey Pot System", *International Journal for Research and Development in Technology*, Vol. 5, No. 5, pp. 310-314, 2016.

[17] J. Kennedy and R. Eberhart, "Particle Swarm Optimization", *Proceedings of IEEE International Conference on Neural Networks*, Vol. 4, pp. 1942-1948, 1995.

[18] R. Kohli, Y. Kumar and S. Jain, "An Improvised Model for Securing Cloud-Based E-Healthcare Systems", *Proceedings of International Conference on IoT in Healthcare and Ambient Assisted Living*, pp. 293-310, 2021.