Electronic digital signature

A I Dzhangarov¹ and M A Suleymanova²

¹ Department of Programming and Information and Communication, Chechen State University, Sheripova Street 32, Groznyy 364093, Russia
² Department of Business Informatics, Chechen State University, Sheripova Street 32, Groznyy 364093, Russia

E-mail: dzhangarov1995@gmail.com

Abstract: The object of this article is an electronic digital signature that allows to identify the author of the document. An electronic digital signature is some details of the source document obtained by converting information using special cryptographic algorithms. In addition to determining the author, it also allows to check the accuracy of the information and evaluate its distortion from the moment of the formation of the signature itself. As part of the scientific work, a software product was created that was able to sign electronic documents using one of the well-known cryptographic algorithms, and the prospects for the development of this direction were also analyzed. Despite the fact that the electronic signature has not yet become widespread, there is a high probability that its widespread adoption in public and private institutions is expected in the very near future.

1. Introduction
Electronic digital signature (EDS) is a cryptographic software that is necessary to solve the following tasks:

- analysis of the document and verification of its integrity;
- concealment of confidential data and development systems;
- initialization of the author of information exchange.

The concept of EDS is based on the transition from paper to electronic documentation and automation of workflow systems, by reducing the processing time of documents. As mentioned, the EDS provides the ability to identify an individual who has signed an electronic document. It can be said that the EDS is an analogue of both a handwritten signature and an analogue of a paper signed document. It is also worth noting that such a signature has its own regulatory framework that governs the use of digital signatures in state self-government bodies, in municipalities and in the hands of private business owners [1].

2. Purpose and use of EDS
An electronic digital signature performs the following functions:

1. ensuring the integrity of the document. If during the transfer of an electronic document it is changed, corrected, then the electronic signature automatically becomes invalid. This is due to the fact that the digital signature is formed on the basis of the very first version of the signed document;
2. accurate confirmation of authorship. In a document signed by electronic digital signature, the author cannot be changed. Since when creating an EDS, a private key is generated, which is only with
the author. Therefore, the presence of a digital signature under the document guarantees authorship of the owner of the signature;

3. the provision of evidence. In order to confirm the availability of a working digital signature, the author only needs to provide the public and private keys that he receives at the time of creating the electronic digital signature [2].

Thus, one can conclude that the digital signature provides a high degree of data protection, which is extremely important in the modern realities of digital espionage and the existence of various methods of data interception. Therefore, such signatures are already used in banking systems, public procurement, when registering real estate, in the judiciary, in trading systems, customs declarations, and so on.

However, one cannot fail to mention an important feature - documents with electronic signature have legal force and are recognized as equivalent to paper documents only when it is established by federal law or documented by agreement of the parties [3].

3. EDS Creation Algorithms

There are several varieties of algorithms for creating electronic digital signatures: symmetric, asymmetric and combined.

The symmetric encryption algorithm uses a single key (secret information consisting of a set of numbers and letters) for encryption and decryption. The key must be kept secret by the owners, it is assumed that there is a third trustee. The document is considered approved after encryption with its secret key and transfer to a third party [4].

Asymmetric encryption algorithm is considered the most common. It uses a cryptosystem with a public key, a pair of public-private keys.

Combined, it is also hybrid, encryption combines the advantages of the above algorithms. The result is an asymmetric cryptosystem using public and private keys. Moreover, all of the above schemes are modified and new types of digital signatures appear: group, undeniable, trusted, and so on.

For a more complete understanding of the process of creating EDS, one can consider the step-by-step application of the algorithm:

1. A document of arbitrary size is divided into blocks (512 bits each);
2. the so-called hash function is applied (or a compression function that converts input information into a bit string of a specified length);
3. the length of the document and the checksum (the number of processed bits) are calculated and a unique set of characters (key) is assigned [5].

4. Software implementation of EDS based on RSA algorithm

In the course of research related to electronic digital signature, a mobile application based on the RSA algorithm using the hash function was also developed. The application was developed in the Java programming language in the integrated development environment Android Studio 3.1.2 [6].

At the beginning the RSA algorithm can be considered, which consists of several stages:

1. Key generation process:
   • creates a pair of simple distinct numbers \( p \) and \( q \);
   • module is calculated \( n = p \cdot q \);
   • the Euler function is calculated by the formula \( e : \begin{cases} 1 < e < \varphi(n) \\ (e, \varphi(n)) = 1 \end{cases} \);
   • the closed exponent \( d \) is calculated: \( d = e^{-1} \mod \varphi(n) \Rightarrow de = 1 \mod \varphi(n) \);
   • a pair of numbers form a public key;
   • a pair of numbers form a private key;
2. Signature formation:
   • \( m \) - message;
using a hash function from message $m$, we get a set characters: $h = H(m)$;

- the signature is formed: $\text{sign} = h^d \mod n$;
- a message is transmitted with an electronic digital signature $(m, \text{sign})$.

Then a certificate is formed, where the information is placed in the form of a public key $(e, n)$ and signature $\text{sign}$. The certificate is transmitted to the recipient separately from the signed document.

3. signature verification:
- a message is received from the electronic signature $(m, \text{sign})$;
- the hash function of the original message is calculated: $h = \text{sign}^d \mod n$;
- the hash function of the received message is calculated: $H(m)$;
- equality $h = H(m)$ is checked, if equality is confirmed, the signature is correct, otherwise it is not true [7].

However, that is not all. The scientific novelty of the study is that the existing and basic RSA method was supplemented by elements of the El-Gamal encryption method. This cryptosystem is an improved version of the encryption of the Diffie-Hellman method (cryptosystem with public key, based on the difficulties of computing discrete logarithms). A feature of the El-Gamal method that it has not been patented and is freely available for use. The described method has one noticeable advantage over other encryption algorithms - the presence of a probabilistic encryption scheme. When calculating a pair of numbers, a random value $k$ is also set, which is within the lower and upper boundaries of the specified pair of numbers.

Therefore, at the first step, before calculating the number $n$, additional calculations are performed: for a pair of numbers $p$ and $q$, a random number $k$ is given that satisfies the following condition $- p-1 < k < q-1$. Then, respectively, the numbers $a$ and $b$ are calculated by the following formula: $e = p^k \mod q, \ n = q^k \mod p$. Due to this, the general scheme obtains the probabilistic nature of encryption, and since probabilistic encryption schemes exhibit greater strength compared to schemes with a specific encryption process, the proposed method is more reliable.

5. Application Software Features
The developed mobile application is designed in accordance with the MVP (Model - View - Presenter) pattern, which involves the distribution of code into layers (levels). The structure of the project is presented below:

![Project structure](image.png)

Figure 1. Project structure.
When creating the application, the following libraries were used:

- appcompat-v7;
- cardview-v7;
- rxandroid;
- rxjava2;
- dagger2.

The design of the application is made according to the official Material Design pattern from Google. Documents in .pdf, .doc, .docx format are accepted for entry. At the output, we already have a signed document and a certificate with the extension .aaa, which stores the public key and the signature of the document. When identifying the uploaded file, the input parameters are the signed document and its certificate. In the case of a successful verification, we receive a confirmation of the authenticity of the document. Otherwise - a notice that we have an illegitimate document.

The program implements the following processes:

- loading data of various formats into the application;
- the signing of the document;
- the formation of a signature certificate;
- document authentication.

The algorithm for creating EDS and key generation is carried out in the Signature class (utils package). Generating a hash function and creating a signature using the RSA algorithm are provided by the classes included in the JDK (java. Security package). In the code of this class for the names of methods, their purpose is clear (key generation, creating a hash function, and so on) [8].

When signing the selected document, the generated public key and digital signature of the document, using a specific algorithm, are generated in the JSON format of the form:

```
{"public_key": "<generated key>", "signature": "<document digital signature>"}.
```

The generated public key and digital signature are written in Base64 format. And the JSON format text itself is also converted to Base64 for greater reliability [9].

The converted JSON is written to a *.aaa format text file in the Download folder on the device and it represents itself as certificate.

![Application interface](image)

**Figure 2.** Application interface.
In the application itself (Figure 2), when "Sign Document" button is selected, it is proposed to download the document from the device’s catalog and after selecting the necessary document, it will be assigned an electronic digital signature. The “Check Document” button also offers the download of existing and already signed documents to verify the integrity of the digital signature.

6. Conclusion
Electronic digital signature is already successfully used by leading companies and government agencies. According to statistics, approximately 17% of world GDP is traded using EDS, which is about twelve trillion dollars a year. EDS is also actively used in the field of electronic document management and with its help millions of documents are signed per day.

Such statistics once again indicate that this tool is quite in demand. The fact that almost all modern electronic document management systems use this software product also emphasizes this. Based on this, it can be concluded that in the future the need for digital signatures will only increase and the market for electronic digital signatures will develop rapidly [10].

References
[1] Riham Al T and Amr M 2014 Integral Distinguishers for Reduced round Stribog (Concordia Institute for Information Systems Engineering)
[2] Kircanski A 2012 Rebound attacks on Stribog (Concordia Institute for Information Systems Engineering)
[3] Network Working Group R Rivest 1992 MIT Laboratory for Computer Science and RSA Data Security, Inc
[4] Russinovich M and Margozi A 2012 Utility` Sysinternals. Spravochnik administratora (Microsoft Press)
[5] Pogorelova B A and Sachkova V N 2006 Dictionary of cryptographic terms Pod red (M.: MCzNMO)
[6] Dawn M 2016 What is a Digital Signature. What It Does, How It Works (Cryptomathic)
[7] Magomedov I A, Mezhieva A I and Suleymanova M A 2018 Inženernyj vestnik Dona 4 5334
[8] Gabriel Henry 2015 The History of Electronic Signature Laws (Isaac Bowman)
[9] Dawn M 2014 Is the NIST Digital Signature Standard DSS legally binding (Cryptomathic)
[10] Dawn M 2016 The difference between an Electronic Signature and a Digital Signature (Cryptomathic)