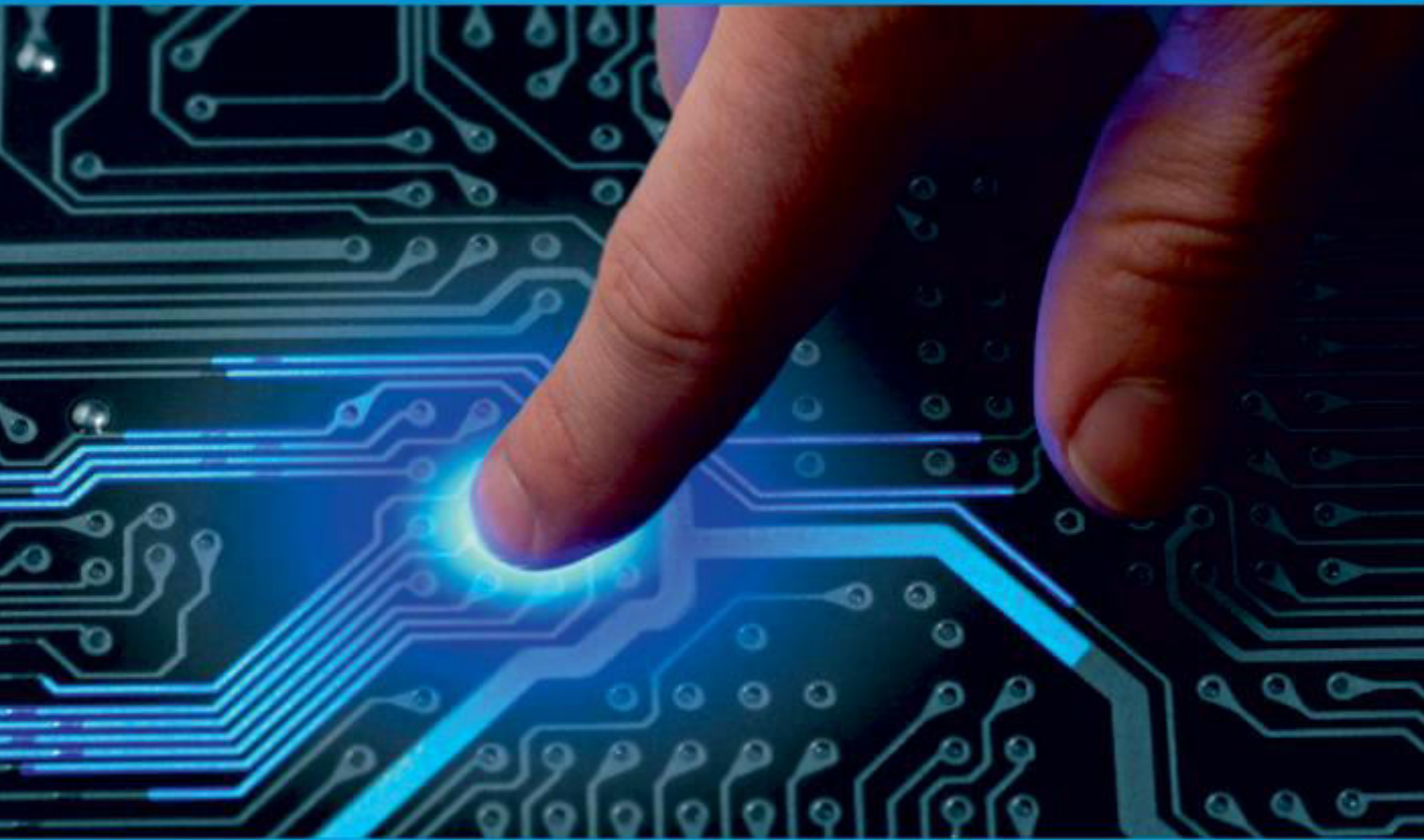
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

Website to Create Digital Signatures and Sign PDF

Pratik Chopade, Mrunalini Patil, Kanchan Patil, Omkar Khutwad, Mahesh Satpute, Mangesh Patekar

Head of Department, Department of Computer Science, JSPM'S Rajashri Shahu College of Engineering, Pune, India

Guide, Department of Computer Science, JSPM'S Rajashri Shahu College of Engineering, Pune, India

Lecturer, Department of Computer Science, JSPM'S Rajashri Shahu College of Engineering, Pune, India

Student, Department of Computer Science, JSPM'S Rajashri Shahu College of Engineering, Pune, India

ABSTRACT: Think of a document that has legal value. Such a document may contain important information about rights and obligations, in which you must verify its authenticity. You don't want people deny the obligations they have written. In addition, this document must be valid posted, viewed and maintained by different people. In different places in the flow of work, in different places from time to time, the document may be modified, either voluntarily, for example to add additional signature, automatically, for example due to a transmission error, or intentionally, if someone wants it create a fake from the original document. Over the centuries, we have tried to solve this problem by putting a so-called 'wet ink signature' on paper. Today, we can use digital signatures to ensure: Text Authenticity — we want proof that the document has not been changed somewhere in the flow of work, authenticity of the text — we require proof of the authorship of the document that we think you are (not someone else), Non-disclosure — we require assurance that the author will not deny his or her identity.

KEYWORDS: E-sign pdf, digital signature, Authentication, Integrity.

I. INTRODUCTION

A digital certificate contains a digital signature of the issuing authority so that anyone can verify that the certificate is genuine. This seems to be more common now in the making of the internet
A digital signature can be used for any type of message, transaction and the like, whether encrypted or not, just to make sure the recipient is sure of the sender's identity and that the message has arrived complete. The hash value of a message when encrypted with a person's private key is his digital signature in that e-Document. The digital signature of a person therefore varies depending on the document and the document thus ensuring the authenticity of each word in the text. As the signatory's public key is known, anyone can verify the message with a digital signature.

II. DIGITAL SIGNATURE

Here are some definitions of digital signature: A digital signature is an electronic signature that verifies the authenticity of the sender of a message, or a document signer and possibly confirms that the original content of the incoming message or document is unchanged. The use of cryptography is a key message A secret key is used, indicating that the signature must have been made by the owner of that key. A secure hash has been signed for the entire document, so that any changes to the document do not apply to the signature. A phrase (similar to John J. Jones) is encrypted with the sender's secret key à and is attached as a signature to the encrypted message to verify who the sender (or he) is. A digital signature or a digital signature scheme is a mathematical system that demonstrates the authenticity of a digital message or document. A valid digital signature gives the recipient reason to believe that the message was created by a known sender, and that it was not changed during shipping. Digital signatures are often used for software distribution, financial transactions, and in some cases where it is important to detect fraud and fraud. From the descriptions above we see that digital signature is a word-for-word encryption for the sender with his or her private key (signature), and removes the encryption clause for the recipient with a public key (verification signature) when sending data through an open channel.Attached data, or cryptographic modification, is data that allows the data recipient to verify the source and integrity of the data and to protect against fraud.

III. METHODOLOGY

The website design is done according to the official Material Design pattern from Google. Documents in .pdf, .doc, .docx format are accepted for importing. For downloads, we already have a signed document and a certificate with the extension .aaa, which holds the public key and signature of the document. When identifying a uploaded file, the document filing parameters and its certificate. In the case of a successful verification, we receive a certificate of authenticity of the document. If not - notice that we have an illegal document.

The system uses the following processes:

- upload data of various formats to the application;
- document signing;
- construction of a signing certificate;
- document authentication.

The algorithm for creating EDS and key production was performed in the signature class (utils package). Generating hash function and creating signature using the RSA algorithm is provided in JDK (java. Security package) classes. In the code of this category namespace, their purpose is clear (main generation, to create hash function, etc.) [8].

When you sign a selected document, the public key generated by the digital signature of the document, using a specific algorithm, is generated in the JSON format of the form:

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

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

Converted JSON is written to be a * .aaa format text file in the download folder on the device and represents it as a certificate.

IV.CONCLUSION

Digital signatures are an important achievement in cryptography. Wherever there is a smart card the use of a digital signature is almost a must. Digital signature is very different and is one of the most effective ways to protect your worries about what you have done.

A digital signature is a very effective way to get all your financial payments to get more comfort in dealing with various business and financial matters. This way you will not have to worry about going through the motions of traditional transactions using signatures.

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 Margozis A 2012 Utility` Sysinternals. Spravochnikadministratora (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 Inženernyjvestnik 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)

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING