Takao Namiki; Kazutsuna Yamaji; Toshiyuki Kataoka; Noboru Sonehara

Time Stamping Preprint and Electronic Journal Server Environment

In: Petr Sojka and Thierry Bouche (eds.): Towards a Digital Mathematics Library. Bertinoro, Italy, July 20-21st, 2011. Masaryk University Press, Brno, Czech Republic, 2011. pp. 19--23.

Persistent URL: `http://dml.cz/dmlcz/702599`

Time Stamping Preprint and Electronic Journal Server Environment

Takao Namiki[1], Kazutsuna Yamaji[2], Toshiyuki Kataoka[3], and Noboru Sonehara[4]

[1] Department of Mathematics, Hokkaido University
nami@math.sci.hokudai.ac.jp
[2] R & D Center for Academic Networks, National Institute of Informatics
yamaji@nii.ac.jp
[3] R & D Center for Academic Networks, National Institute of Informatics
kataoka@nii.ac.jp
[4] Information and Society Research Division, National Institute of Informatics
sonehara@nii.ac.jp

Abstract. The exchange of preprints and journals plays an important role to communicate new research ideas and results in many academic fields. Distribution of preprints and journal articles by electronic file via the Internet has become a primary method in addition to paper publication. Electronic preprints and articles in the paperless era should be certified in terms of existence proof and tamper resistance because they are easily modified by their site administrator. We developed a secure preprint and electronic journal service environment that uses an electronic signature and timestamp technique.

Keywords: long-term electronic signature, electronic signature, timestamp, preprint, archives.

1 Introduction

In the last decade electronic preprints and mathematical journals become an infrastructure of mathematical researches, however, it is not familiar to us that electronic files of articles should be preserved with its timestamp because we might assure community of the originarity even if the modified versions were floating. On the other hand, in order to establish the priority of research ideas and results, preprints are published in several research fields. For example, arXiv.org, which is operated by Cornell University Library, is a major preprint server that covers physics, mathematics, non-linear science, computer science, quantitative biology, and statistics [1]. Moreover, while many universities operate local preprint servers, the security of these digital documents may be at risk. Currently, most preprints still have the printed issue in addition to digital file distribution. In this dual publication scheme, the printed issue is regarded as the trusted original version. However, in paperless publication, it is difficult to distinguish a copy from the original. Electronic journal has the same problem. That is, the security level of the preprint and journal article files has to be raised in order to protect the research results. In the field of business, the security of

Petr Sojka, Thierry Bouche (editors): DML 2011, Towards a Digital Mathematics Library, pp. 19–23.
ISBN 978-80-210-5542-1

digital documents containing patentable ideas and intellectual property are guaranteed by means of an electronic signature and timestamp technique [2]. These technologies can be applied to academic publishing to ensure reliable digital content. This study proposes a secured preprint server environment using EPrints 3 software and describes its application to the mathematical preprint and electronic journal service at the Hokkaido University.

2 Long-term Electronic Signature

The electronic signature (ES) ensures integrity and signer of a document. An ES (Figure 1) is composed of signature policy, other signed attributes and digital signature [3]. The digital signature is created from an encrypted hash value of a digital document. The recipient (client application) can detect a falsification of the document by comparing hash values calculated from the original document and decrypted from the digital signature [4]. The timestamp (TS) technology guarantees existential evidence of digital documents [5]. The combination of ES and TS, as indicated by ES-T in Figure 1, ensures the authenticity of the digital documents.

The ES and TS, each of which is based on the digital signature technology, have a validity period and revocation functions against compromise of the hash algorithm and leak of the private key. However, the temporary nature of these functions causes a problem for long-term preservation. To solve this problem, a long-term signature has been proposed [3]. This signature format embeds a complete certificate and revocation references shown as ES-C in Figure 1; therefore, ES and TS can be verified even after the signature expires. This study employed international standard RFC3126 as a long-term signature format and applied it to the article PDF documents.

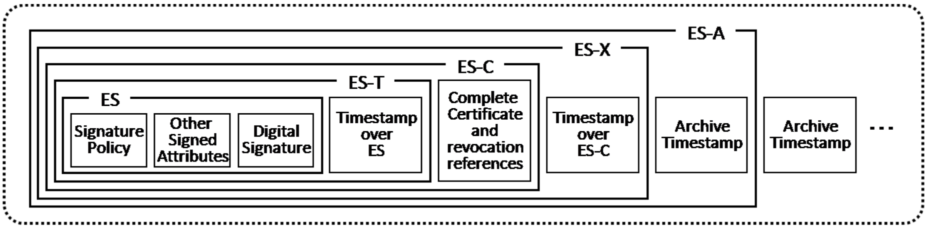


Fig. 1. Long-term signature format defined by RFC 3126 [3]

3 Application for Preprint Server

3.1 System Environments

The system architecture of the developed preprint and electronic journal server environment is shown in Figure 2. Application of the long-term signature requires a certification authority (CA) server and long-term signature server. The CA issues a digital certificate to a user who would like to register a document on the server. CA was established by NAREGI-CA which is an open source software originally developed for grid computing [6]. NAREGI-CA provides a variety of utilities including key generation, certification issuance, verification, and storage. The long-term signature server obtains a timestamp token from the time stamping authority managed by a trusted third party. EPrints 3 was chosen for the server software.

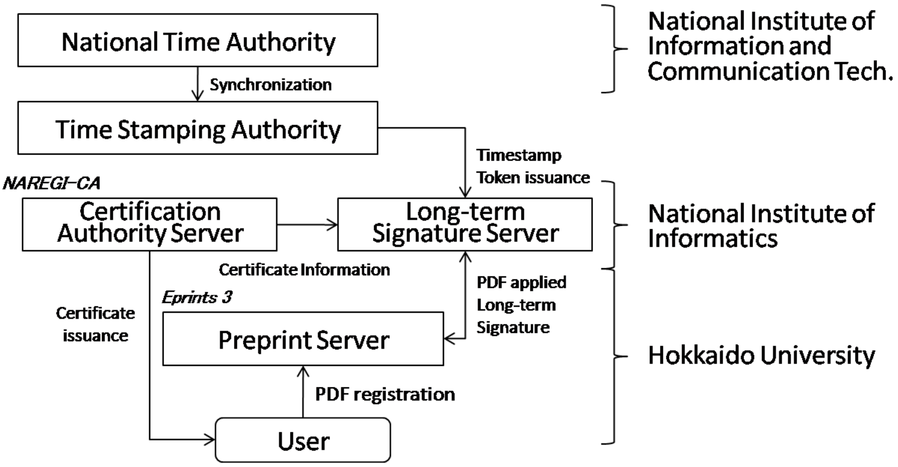


Fig. 2. System architecture of the server environment

3.2 Data and Work Flow

To attach a long-term signature to an article, a registrant must do the following procedure.

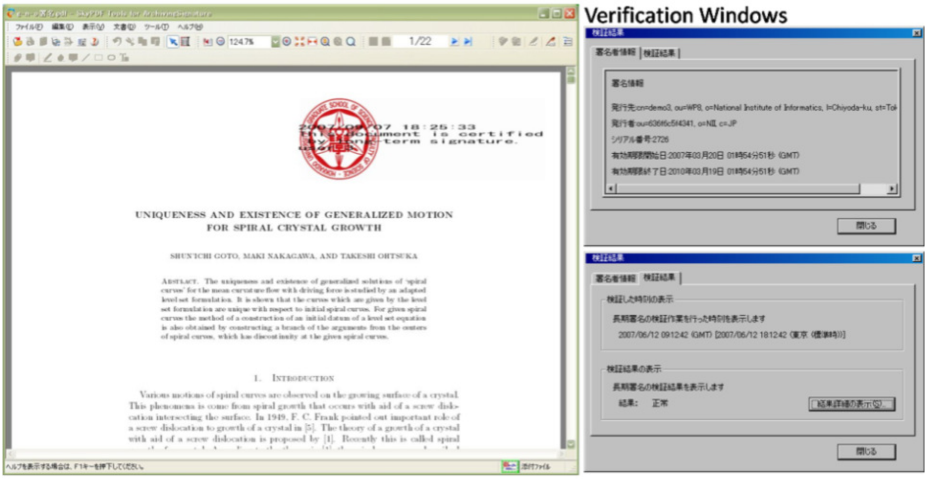
1. Obtain a digital certificate
2. Prepare an article PDF
3. Attach an electronic signature using the digital certificate to the article PDF
4. Register the article PDF file on the server

Once the PDF file has been registered, the following steps will be performed automatically.

1. The server sends the PDF file to the long-term signature server.
2. The long-term signature server obtains a timestamp token from the time stamping authority and applies it to the PDF file.
3. The server obtains the above PDF file.
4. The server makes the PDF file public.

In the EPrints system, the moderator receives an email whenever a new item has been submitted. This workflow is executed by utilizing the perl script named send_alerts. The procedures from 5 to 8 are inserted just before the workflow. Besides the additional task that the article registrant needs to apply an electronic signature, the proposed system does not have more manual operations than the conventional one.

An example of an article PDF secured by a long-term signature is shown in Figure 3. The emblem of the Hokkaido University and minimum information for the long-term signature are superimposed on the article. The position, size, and form of this information can be customized by the client application. The long-term signature can be verified, as shown on the right of the Figure 3.


Verification Windows
ファイル(F) 編集(E) 表示(V) 文書(D) ツール(T) ヘルプ(H)
124.7%
1/22
ヘルプを表示する場合は、F1キーを押下してください。
添付ファイル
検証結果
署名者情報
検証結果
閉じる
結果詳細の表示(S)...

2007/0?/07 18:25:33
This document is certified
by long-term signature.

UNIQUENESS AND EXISTENCE OF GENERALIZED MOTION FOR SPIRAL CRYSTAL GROWTH

SHUN'ICHI GOTO, MAKI NAKAGAWA, AND TAKESHI OHTSUKA

ABSTRACT. The uniqueness and existence of generalized solutions of 'spiral curves' for the mean curvature flow with driving force is studied by an adapted level set formulation. It is shown that the curves which are given by the level set formulation are unique with respect to initial spiral curves. For given spiral curves the method of a construction of an initial datum of a level set equation is also obtained by constructing a branch of the arguments from the centers of spiral curves, which has discontinuity at the given spiral curves.

1. INTRODUCTION

Various motions of spiral curves are observed on the growing surface of a crystal. This phenomena is come from spiral growth that occurs with aid of a screw dislocation intersecting the surface. In 1949, F. C. Frank pointed out important role of a screw dislocation to growth of a crystal in [5]. The theory of a growth of a crystal with aid of a screw dislocation is proposed by [1]. Recently this is called spiral

署名情報

発行先:cn=demo3, ou=WP8, o=National Institute of Informatics, l=Chiyoda-ku, st=Tok

発行者:ou=636f6c5f4341, o=NII, c=JP

シリアル番号:2726

有効期限開始日:2007年03月20日 01時54分51秒 (GMT)

有効期限終了日:2010年03月19日 01時54分51秒 (GMT)

検証した時刻の表示

長期署名の検証作業を行った時刻を表示します

2007/06/12 09:12:42 (GMT) [2007/06/12 18:12:42 (東京 (標準時))]

検証結果の表示

長期署名の検証結果を表示します

結果: 正常

Fig. 3. Example of preprint PDF file guaranteed by long-term signature and its verification results

4 Conclusion

Since the EPrints system stores the registered file under the certain directory of the OS file system, the proposed system simply transfers the file between EPrints and the long-term signature server. This process can be used in different systems.

In Japan, the university public key infrastructure (UPKI) project is in progress, and it will be one of the key technologies of the cyber science infrastructure (CSI) framework promoted by the National Institute of Informatics. That is, the security of digital contents will be ensured by means of digital certificates issued by the UPKI project. We believe that this scheme of enhanced security will accelerate the exchange of scholarly content via the Internet and will boost scientific research and education activities.

Finally we remark that the long-term signature framework works well in electronic journals without print edition because titles of small scale electronic journals are published from small publishers in mathematics. We have already experimented in Hokkaido Mathematical Journal, volume 38, no. 2. As access to this journal is restricted by IP address for subscribed institution, we place a PDF file of the issue on the URL: `http://www.math.sci.hokudai.ac.jp/~nami/note/hmj38-2-1.pdf` to access it from any place.

References

1. McKiernan, G. (2000). *arXiv.org: the Los Alamos National Laboratory e-print server.* The International Journal on Grey Literature 1(3): 127–138.
2. Haber, S. and Stornetta, W. S. (1991). *How to time-stamp a digital document*. Journal of Cryptology 3(2): 1432–1378.
3. Pinkas, D., Ross, J. and Pope, N. (2001). *Electronic Signature Formats for long term electronic signatures.* IETF RFC 3126.
4. Housley, R. (2004). *Cryptographic Message Syntax (CMS).* IETF RFC 3852.
5. Adams, C., Cain, P., Pinkas, D. and Zuccherato R. (2001). *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).* IETF RFC 3161.
6. Miura, K. (2006). *Overview of Japanese science Grid project NAREGI* Progress in Informatics 3: 67–75.
7. Millington, P. and Nixon, W. J. (2007). *EPrints 3 Pre-Launch Briefing* Ariadne 50.
8. Sakauchi, M., Yamada, S., et al. (2006). *Cyber Science Infrastructure Initiative for Boosting Japan's Scientific Research.* CTWatch Quarterly 2(1): 20–26.