2000

Electronic Notary System and its Certification Mechanism

Shinichi Nakahara
NTT Information Sharing Platform Laboratory

Electronic Notary System and its Certification Mechanism

Shinichi NAKAHARA
NTT Information Sharing Platform Laboratory,
1-1 HIKARINOOKA YOKOSUKA KANAGAWA, Japan

Abstract

We have developed a prototype electronic notary system (CYNOS : CYber NOtary System). CYNOS proves facts by providing the evidence (notary token) of events and/or actions that could be used to solve disputes between entities. It is a signature-based system and uses various security techniques to enable the timely certification of entities and fair and highly reliable delivery. It also cooperates with our CA (CANP : Certification Authority for secure Network Platform) through the network.

This paper describes CYNOS with regard to its service, functions, and mechanism. The ability of CYNOS to support the non-repudiation service and some issues on system management are discussed.

The additional requirements that are needed if the certification mechanism is to realize practical notarization functions are addressed.

1. Introduction

The popularity of EC(Electronic Commerce) and EDI(Electronic Data Interchange) on the Internet raises several fears such as eavesdropping, counterfeiting, spoofing, and repudiation. The major countermeasures are cryptography, digital signatures, CA(Certification Authority), and NA(Notary Authority), respectively. In particular, safe and reliable EC needs a certification and notarization mechanism to prevent repudiation. Certification ensures the genuineness of an entity before trading. Notarization safely stores the evidence of events and actions during trading for a long term and subsequently certifies the fact by presenting formatted evidence (notary token). Namely, certification and notarization are prior and post countermeasures that can ensure truly safe e-Commerce. Some international standards have been established [1][2][3] and several drafts are being studied.[4][5][6] CA and NA are briefly addressed in these documents, and they note that CA and NA are both a kind of Trusted Third Party (TTP). The secure delivery mechanism has been studied as one of the main techniques of notarization [7][8].

In recent years, the simple certification or notarization service has become popular, and many organizations now provide this service in both public and private fields (ex. ValiCert.com, Surety.com, e-Parcel.com, NetDox.com etc.). Some provide the time-stamping service, some offer secure delivery service. However, many of them do not distinguish the creator from the sender nor store the data itself for a long time, nor prove the action(creation, sending, receiving). Obviously, we believe that no truly commercial notarization service is available yet.

This paper addresses the usefulness of CYNOS as a true notarization system and discusses some of the issues of CA and NA systems based on our experience in developing CYNOS and a CA system(CANP). A new approach to keeping the consistency of a genuine entity is proposed.

The aspects of system operation and maintenance are not addressed here.

2. Secure and trusted services and mechanism of CYNOS

2.1 Overview of CYNOS

CYNOS is a typical TTP whose features are the provision of various notarization services, strict certification of all participants, issuance of notary tokens, and high availability.

Fig.1 shows a typical CYNOS configuration. CYNOS consists of notary server, web sever, fire wall, and client agent. The real-time CA (CANP) and time server are external plug-in functions. The notary server includes evidence data base and secure signing device (signer) which is tamper proof and works in the same security domain. The platform is UNIX based and includes OLTP (On-Line Transaction Program)and Database system, both of which enhance its availability.

The user, CANP, and time server may be connected through the Internet. The HTTP protocol is suitable for establishing synchronous communication among user, CYNOS, and CANP.

search

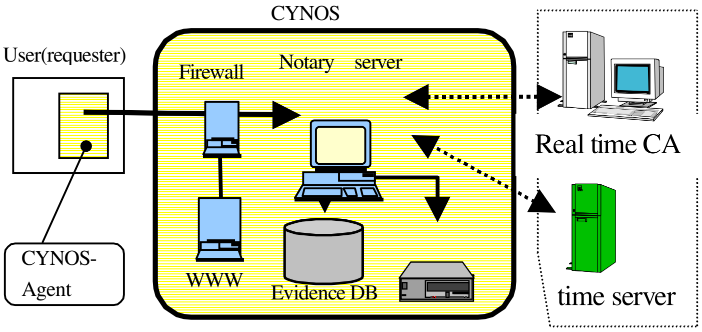


Fig.1 Typical configuration

2.2 Notary services of CYNOS

a) Existence notarization service

This service stores evidence proving the existence of a piece of data and its possessor; the evidence consists of a distinguishing name(DN), digital signatures, authentication time, data, etc. (See Fig. 2). The remarkable difference from the well-known time-stamping service is that CYNOS needs the document itself and the digital signatures of the creator and the requester as shown in Fig.3. Notarization must process the data itself and define and treat the creator (who is responsible for the contents) and requester as different personalities. Encrypted communication is adopted between client and server using ESIGN for digital signature, FEAL for encryption, and EC-DH for key exchange, all of which are NTT created algorithms.

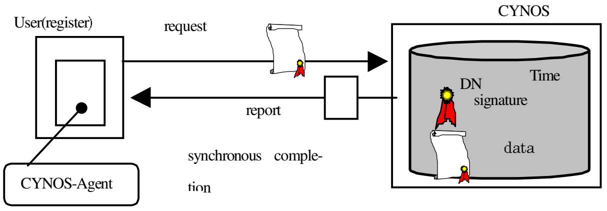


Fig.2 Existence notarization service

b) Delivery notarization service

This service stores the evidence of the delivery and the reception by the intended recipient as well as the existence of the data and the originator. The evidence consists of the DN of relative entities, the digital signature information, authentication time, the data, receipt from the recipient etc. This service uses either synchronous or asynchronous operation depending on the phase and entity. A sender submits the data with digital signatures using the format specified in Fig.3 together with certification information of the recipient (e.g. recipient DN, CA.-DN, mail address). This phase is asynchronous. The sender receives a claim check for the notarization service synchronously, but delivery is not guaranteed. The authentication of every participant is done by using CANP before the attention of data existence is submitted to the recipient. The specified recipient submits a request for the data to CYNOS. Fig. 4 shows the process of delivery transaction and protocol between the CYNOS server and recipient using an encryption technique. Fig. 5 shows the details of decryption and creating a signature of the data in the receptionist's CYNOS-Agent.

When the recipient takes the encrypted data from the CYNOS server, the receipt is automatically generated and returned to the CYNOS server in some continuous transactions involving the CYNOS-Agent that corresponds to the transmitted data (Fig.4). The receipt consists of a digital signature of the received data(plain text) by using the recipient's secret key. With regard to this process, we considered the problems possible such as terminal disconnect or timeout during delivery process, which may raise the situation whereby the whole

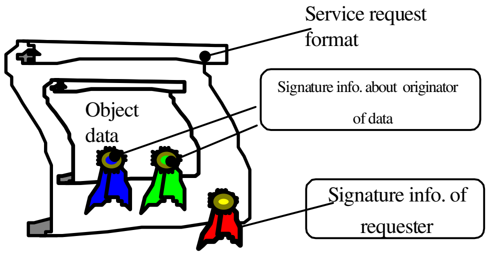

Service request format
Object data
Signature info. about originator of data
Signature info. of requester

Fig. 3 Request format and signature of entities

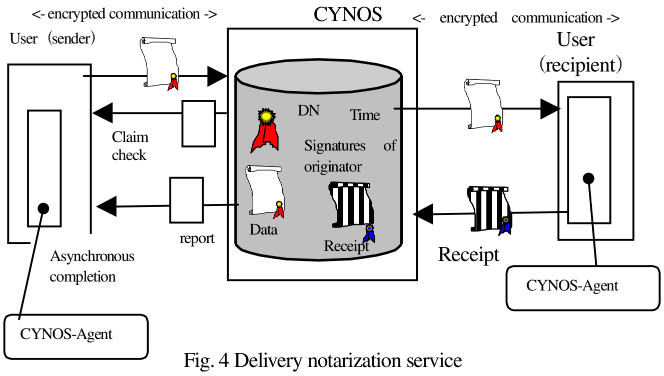


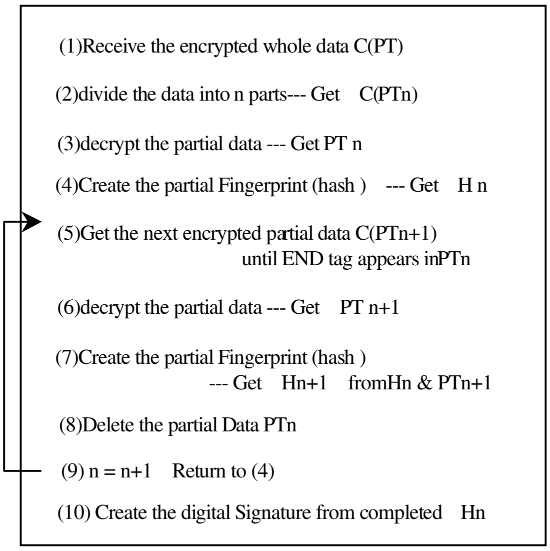
Fig. 4 Delivery notarization service

search

plain data is left on the recipient's terminal without the receipt being returned. When the data is valuable, this situation means that unauthorized data leakage has occurred and it is a kind of repudiation(The recipient could insist on delivery failure despite getting the data.). And it enable the recipient to get some valuable information without paying any fee by canceling the transaction.

Against these fears CYNOS adopts a remarkable protocol(See Fig.5) that includes encryption of the data on the server, division of the encrypted data into some pieces and serialized decryption and creating the piece of digital signature and assembling of the recipient's digital signature on the recipient terminal without leakage of information. The secret of this process is to delete immediately the used piece of plain data for signature (property (8) in Fig.5).

In this mechanism the CYNOS-Agent plays a very important role. At the entity's terminal, security operations (generating digital signature, encryption, key exchange, decryption, verification of the signature, access to the CA) are done by the agent implicitly. In addition, at the recipient's terminal, the user's digital signature for the data(including sender's signature) is automatically generated as above, and attached to the data which is then sent to the CYNOS server in one action. This phase is synchronous. Namely, the CYNOS-Agent conceals the cryptographic operations and represents all transactions as one controlled transaction. This approach reduces the success of any attack by the user and realizes a well controlled protocol between user and CYNOS.



(1)Receive the encrypted whole data C(PT)

(2)divide the data into n parts--- Get C(PTn)

(3)decrypt the partial data --- Get PT n

(4)Create the partial Fingerprint (hash) --- Get H n

(5)Get the next encrypted partial data C(PTn+1) until END tag appears inPTn

(6)decrypt the partial data --- Get PT n+1

(7)Create the partial Fingerprint (hash) --- Get Hn+1 fromHn & PTn+1

(8)Delete the partial Data PTn

(9) n = n+1 Return to (4)

(10) Create the digital Signature from completed Hn

[Legend]
PT : Plain Text ,
PT n : n th. partial Plain Text
C(PT) : encrypted PT
Hn : n th. hash value

Fig. 5 Process in the recipient CYNOS-Agent

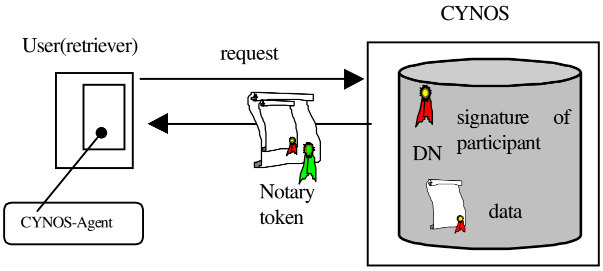


Fig. 6 Certification of facts service

c) Retrieve the certification of facts --- notary token

CYNOS issues a notary token as the certification of facts (see Fig.6); it contains the evidence stored in CYNOS after each notarization event and is accompanied with a signature of CYNOS. Users can retrieve the notary token by using the request format to confirm the notarized data, events, actions, and related information. We say that the original data is stored in CYNOS, so the notary token is understood to be a copy of the original data. The notary token is time sensitive as well as a public key certificate. This means a notary token has a finite life time and the signing key for the token of CYNOS also shares those properties. To extend the CYNOS life time CYNOS has multi-private keys and the signing key for long term storage differs from that for token; all keys are concealed safely (c.f. subclause 2.3 d)).

2.3 Accountability of the stored evidence

CYNOS adopts various mechanisms and functions to increase the accountability of evidence and CYNOS itself.
Some important items are as follows,

a) Strict authentication of entity at the notarization process

CYNOS currently recognizes five kinds of entities: a register (sender), a responsible entity for the registered data, a recipient, qualified person (not implemented), and access permitted entity. CYNOS requires the digital signature of the entity making the access without exception. In all services and in each entity's environment (i.e. related terminals and the server) CYNOS verifies entity genuineness of the attached digital signatures and public key certification. In particular, the digital signature of the responsible entity is a mandatory item for the data to be notarized. The responsible entity for data is the originator and/or a collaborator or a approver for the contents.

In the verification process, CYNOS dynamically uses our real time CA (CANP) whose important features are synchronous response and real time updating of the public key status (generated, revoked , expired). Real time CA is a severe requirement imposed by NA.

As demanded, CYNOS can cooperate with multi-CAs that individually certify different entity attributes.

b) Authorization time

The time of CYNOS server's system clock, which is periodically adjusted against a secure external time source, is adopted as the authorization time. There are several choices as to the authorization time (time of request reception or signature completion or data stored or request completion etc.). CYNOS uses the time of data storage after all participants finish their actions. For example, the authentication time of the delivery notary service is the time when CYNOS just stores the evidences in its data base after the receipt including the signature of recipient is verified on CYNOS server.

CYNOS does not care about the time specified by the user. It is assumed that the user accepts the CYNOS authentication time.

c) Stored evidence

CYNOS can store various evidence about who, when, what, where, and how. "Who" is represented as a digital signature and associated information. "When" involves authorization time. "What" is the stored original data. "How" addresses the requested service and the recipient's receipt. "Where" is defined implicitly as the network on which CYNOS exists.

d) Security technique

To realize adequate security, digital signatures, encryption, and secure key delivery are set between the user and CYNOS server under the CYNOS-agent's control. The CYNOS server uses a tamper proof signature device, a FIPS 140-1 level 3 device, which protects the private key hard and prevents it from being compromised. Also the device includes some signature keys, that is, current private key and reserved key. At least two signing keys are prepared for the functions of communication and storage, respectively. This enables a operator to smoothly change the private key. As a countermeasure to hardware faults, the private keys are backed up in second storage with encryption by Triple-DES. Also we prepare the Key Management System to recover the secret Triple-DES key in case with key destruction.

2.4 Mechanism for enhancing the system and service reliability(availability, trust)

Various countermeasures are used to increase the system and service reliability of CYNOS as a TTP. They include using the OLTP(On-Line Transaction Program)and Database system, providing a synchronous communication method, adopting the mirrored disc and duplex system, setting a firewall, controlling user access, and collecting various logs for audit. They guarantee consistent and atomic transactions, ensure high availability, and protect CYNOS against malicious access. They contribute to the realization of highly reliable services of CYNOS. This is our solution to the problem of long term storage.

3. Some remaining issues and some of our approaches

3.1 Continuous accuracy of a entity

As mentioned above CYNOS performs strict verification of all entities of trade when notarizing data, but the passage of time weakens the accuracy of their authenticity. We have devised a verification mechanism to prevent this. We set a fixed and permanent identification code (FID) for every entity and store and maintain the relation between DN and FID in the CANP server. The consistency is managed by the registration authority(RA) in the CANP. For example when a DN of a certain entity ""A" changes, "A" reports to RA which manages the history of DN and relation of the current DN and FID and old DN.

CYNOS always refers the history of specified DN by the requester to RA when it verifies the notarized data. CYNOS veriifies the accuracy of every participant related to the notarized data even if the public key certificates of participants have expired.

We do this by setting CA and NA at the same site to ease the operation and management load of our certification mechanism.

3.2 Releasing evidence tokens that are outdated

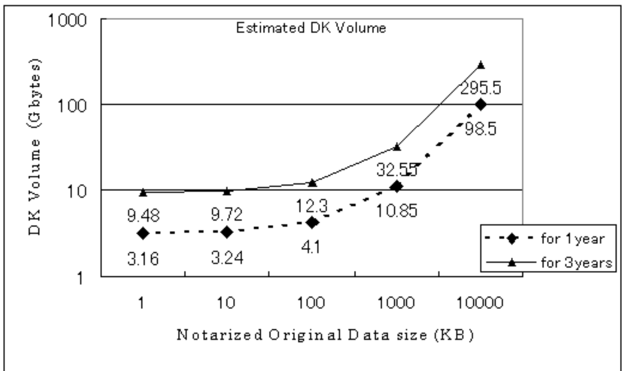
search

CYNOS can customize the stored period as a system policy (Usually from 1 year to 10 years). Outdated data is saved onto secondary storage such as ODK(Optical disk) or DAT.

The only solution to retrieving old data via on online service is to extend the storage capacity. The large scale notary service needs a break through to manage this problem.

3.3 Volume estimate and management of evidence

The storage volume of a notary system increases monotonically because all evidence must be kept in the NA for long periods. Our estimate of disk volume is shown in Fig.7. It is assumed that each service requires the storage of notarized data as well as the evidence addressed in clause 2.1; 5000 notarization services are processed in one year. The target data size ranges from 1KB to 10MB. The dotted and solid lines plot the estimates for one year and three year storage, respectively. These plots include the work area for OLTP and Database system as well as notarized data.. This figure shows that, even under such a moderate load, CYNOS needs from 3 to 300Gbytes and the storage volume increases nonlinearly. Moreover, the total volume proportionally increases against storing term. The required capacity is beyond our expectation. Terabyte(TB) data control is considered to be an exceptionally data warehouse service, but even a moderately sized notarization service will need TB storage.
The storage device and its control, data back up onto secondary media(e.g. DAT, ODK, DVD), and its safe storage(media) of terabytes of data are important items demanding further study.



Note) 5000 Notarization service/year
1 data stored /service

Fig.7 Trial Estimate on the requried capacity of the NA(CYNOS) system

4. Discussion

4.1 Implication of CYNOS

CYNOS has the functions needed to store sufficient evidence on events and actions. The services are suitable for real electronic commerce because the data itself is stored together with related information. Some time stamping services can provide a data existence proof service where the evidence server adds the authentication time to the fingerprint of the data and issues a certificate with digital signature. [6][9] CYNOS is different in that it offers strict certification of all entities and high accountability of the evidence as is described in clause 2.3. A notary service supports arbitration and adjudication, which demand the storage of the data itself together with other evidence. The approach of CYNOS, which is intended for TTP and high reliable real electronic notary systems, lightens the user's burden and offers efficient proof.

4.2 Key compromising

To avoid the key compromising we use the special tamper proof device (c.f. subclause2.3). To separate the communication signature key and storage signature key and back up the encrypted all private key enhance the reliabiliy of the CYNOS system. In addition we never disclosure the public key of storage signature. And some spare private keys help the key update. For example overlapping the 2 private key will enable to exchange its private keys smoothly. On the notary service the revocation of notary token merely occurs except of compromising the NA's communication private key. In that case CYNOS halts the retrieving and verifying notary token. But the original data is safe in the CYNOS data base.

4.3 New services

The next advance will be an agreement notarization service because most commerce involves the agreement of the participants. This can be realized as an extension of the delivery notarization service. Technically speaking, in addition to this paper, work-flow control and management, document sharing and management, interactive cooperation among competent qualified persons, users, attorneys, and NA will give essential and useful hints on notary system requirements.

5. Summary

This paper introduced our prototype notary system and showed that it can safely store evidence for electronic commerce based on data exchange.

We showed that existing certification mechanisms including CA fail to keep the consistency of entities. Our approach uses the lifetime identification of each entity by a responsible registration authority. Further study on the certification mechanism is needed to realize the mature digital signature based electronic society.

The monotonic increase in storage volume is an unsolved issue. Commercial notary systems would require strict control of TB(Terabyte) volumes.

References

1. ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8, "Information technology – Open System Interconnection – The Directory : Authentication framework", Nov. 1993.
2. ISO/IEC 10181-4 , "Non-repudiation framework ", 1997
3. ISO/IEC 13888-1-3 , "Information technology – security techniques – Non-repudiation", Dec. 1997.
4. ISO/IEC PDRT 14516 " Information technology – security techniques – Guidelines on the use and management of Trusted Third Party services", (SC27 N2317)
5. PKIX, Internet X.509 Public Key Infrastructure Data Validation and Certification Server protocols (DCS), 1999 http://www.ietf.org/html.charters/pkix-charter.html
6. ISO/IEC WD 18014 "Time Stamping Services", (SC27 N2323)
7. Jianying Zhou, Dieter Gollman, "A fair Non-repudiation protocol",0-8186-7417-2/96 IEEE, 1996
8. N.Asokan, Victor Shoup, Michael Waidner, "Optimistic Fair Exchange of digital signatures", In 4th. ACM Conference on Computer and Communication Security, pages 6-17,1997
9. A.Takura,S.Ono,S.Naito,"Secure and Trusted Time Stamping Authority", Proceedings of IWS'99,pp. 123-128, 1999