Proc. IEEE 32nd Annual 1998 International Carnahan Conf. On Security Technology

A Smartcard-based Framework for Secure Document Exchange

Chung-Huang Yang[1], Shy-Ming Ju[1], T.R.N. Rao[2]
[1]Dept. of Information Management, National Kaohsiung First University of Science and Technology,
Yenchao, Kaohsiung, Taiwan 824, R.O.C.
[2]CACS, University of Southwestern Louisiana, Lafayette, Louisiana 70504-4330, U.S.A.

ABSTRACT

The advancement of information and communications technology, especially the Internet, has created opportunity to improve the administrative efficiency and service quality in governments of many nations. Official documents in Taiwan, Republic of China (R.O.C.) are traditionally sent to their corresponding recipients through the postal service, but official document could not be securely transferred in the open network using off-the-shelf email systems. In this paper, we present our effort in integrating smartcard-based security services (confidentiality, authentication, and non-repudiation) into XML-based document exchange systems.

INTRODUCTION

The R.O.C.'s "Electronic/Network-based Government" is a major national initiative plan augments the "National Information Infrastructure" (NII) program [1]. One of this initiative's objectives is to facilitate the exchange and integration of document and information between different agencies [2] and the Internet is being used as the communication system to exchange information between all sectors of society. However, due to the lack of communication security services and the export control of U.S.A. and many nations, sensitive official documents could not be securely transferred between and within governmental agencies over the Internet using off-the-shelf email systems (such as the browsers) [3].

XML (Extensible Markup Language) [4, 5] is a recommendation of the World Wide Web Consortium (W3C) and is a subset of the ISO-8879 SGML (Standard Generalized Markup Language). XML is designed to make it easy to define document types, to author and manage documents, and to transmit and share documents across the Web. It specifies a standard method for describing the structure of a document and the attributes of the elements in that document. We adopted XML so that the official documents could be easily exchanged between different computer platforms.

The email systems and the documents they carry are susceptible to vulnerabilities, or threats, such as the leakage and modification of document contents, the impersonation of legitimate users. Our smartcard-based system uses both public-key cryptography and private-key cryptography to provide privacy, authentication, non-repudiation, proof of submission, proof of delivery, audit, and message sequence integrity during document exchange.

Smartcard, or smart card, is a plastic card with an embedded microcomputer chip. The dimension of a smartcard is about the size of an ordinary credit card, which can be easily carried around in a wallet. Smartcards are much more difficult to duplicate than magnetic strip cards and cryptographic functions can be implemented inside these cards. Although smartcard itself has limited computing power and memory capacity, with proper design of the internal functions, the same card could, in addition to document exchange, be used for personal identification, electronic commerce, etc.

Before a document could be encrypted and sent to a recipient, the originator needs to get and validate recipient's public-key; upon receiving a digitally signed document, the recipient also need to get and validate the originator's public-key. Since both public-key and private-key cryptographic techniques require the management of cryptographic keys through trusted channels and untrusted channels (the Internet), an infrastructure is needed to support the generation, distribution, and authentication of these keys on a wide scale. We use smartcard extensively to provide cryptographic key management and support the required infrastructure.

This research was supported in part by the National Science Council, Republic of China, under grant NSC 87-2418-H-327-003, and by the Science and Technology Advisory Group, the Executive Yuan, Republic of China.

THE SECURE DOCUMENT EXCHANGE SYSTEM

Our secure document exchange system, as shown in the Figure 1, is comprised of the Document Exchange (DE) Stations and the Security Management Center.

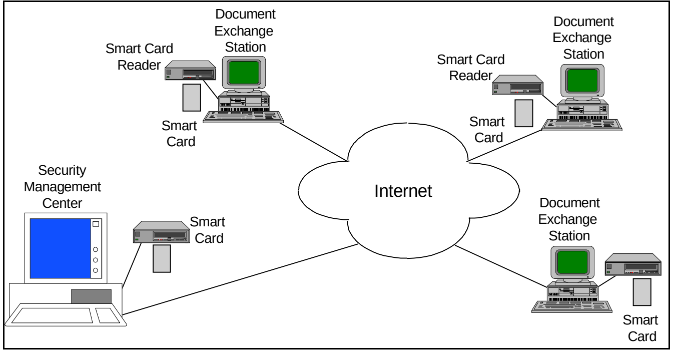
Document Exchange Station
Smart Card Reader
Smart Card
Document Exchange Station
Smart Card Reader
Smart Card
Security Management Center
Smart Card
Internet
Document Exchange Station
Smart Card

Figure 1. The secure document exchange system

Each DE Station, which is responsible for sending and receiving documents, is equipped with a smartcard reader. The RSA [6], SHA [7], DES [8], and triple-DES [8] cryptographic algorithms are implemented inside the card to provide security functions for digital signature and digital envelope. The card itself is protected by the PIN (personal identification number) and the personalized PIN on each card is setup by the card issuer. The card will lock itself after some attempts of wrong PIN input.

Here we will give a typical example how an XML document is protected and transferred over the Internet. As illustrated on Figure 2, the originator or sender is assumed to have the XML document at hand. At Step ①, the document will be appended with a digital signature that will protect the document against modification or impersonation and provide sender authentication based on non-repudiated public-key technology. To generate the signature, the sender will insert his/her smartcard into smartcard reader, input the correct PIN, then the application software will communicate with smartcard and let the card itself generate the signature based on the document's one-way hash value and the sender's RSA private-key that was stored inside the smartcard. The one-way hash function SHA is currently used with the RSA to provide digital signature and other signature algorithms, such as NIST's DSA [9], could be loaded in the card's EEPROM area as needed.

At Step ② and ③, to provide document confidentiality during transmission, application software at the sender site will randomly generate a bit stream and use it as the encryption key (so-called *session key*) to triple-DES encipher the digitally signed document. Then the session key will be further enciphered using receiver's RSA public-key. The encrypted document with the encrypted session, called a digital envelope, will be sent to the intended receiver using the simple mail transfer protocol (SMTP) [10].

It is not important to keep the value of the receiver's public-key confidential, but the sender has to be assured that the obtained public-key is the correct one for the intended receiver. How can one be sure that the obtained public-key information is correct? To solve this requirement, we may use a public-key file, which contains public-keys for all the possible senders and receivers, and securely install this public-key file to each DE stations upon system startup. This approach is suitable for small groups of parties involved. However, there are two major drawbacks: it is difficult to revoke or update any existing public-key and it is difficult to add new public-key for new user. Since an estimated 7,000 government agencies would exchange documents, we need a different approach.

Public-key infrastructures (PKI) [11] are comprised of supporting services that are needed for using public-key technologies on a large scale. A public-key certification system works by having a certification authority (CA) for generating and managing public-key certificates. Each certificate [12] contains a public-key value and information about a particular person, agency, and other entity that holds the corresponding private-key. The certificate is digitally signed by the issuing CA, using CA's private-key, and stored inside the user's personalized smartcard.

We could have multiple CAs, each CA services a set of users and issues certificates for those users. Depending largely on how the trust relationship between CAs is arranged, the PKI provides a method for validating a complete certification path traversing multiple CAs from the CA that's certifying other party's public-key to a root CA whose public-key has already been held in each DE station. At present, our PKI involves a tree-structure of CAs with each CA node certifying its children nodes while being certified by its parent node. This top-down hierarchical structure allows easy implementation and each party only need to hold a copy of the top-level CA's public-key. This also reflects the hierarchical structure of our government.

Upon receiving the digital envelope, the recipient decrypts the session key with his/her RSA private-key, then uses the session key to triple-DES decrypt the signed XML document. At the final step, the receiver recomputes the SHA one-way hash value of the received XML document, and also uses the sender's RSA public-key to decrypt the received digital signature. Then, the receiver compares these two values, if they match, the receiver is assured that the document did indeed come from the claimed sender and is intact during transmission.

Sender's public-key, given in the certificate form, could be attached in the XML document together with a chain of certificates from issuing CA toward root CA. The receiver might also retrieve sender's certificate via on-line directory query from the Security Management Center. The certificates do not have to be delivered via secure channels because they are self-protecting and digitally signed by CA. Since a public-key certificate has a limited valid lifetime and might be revoked prior to the expiration of its validity period, the receiver also needs to acquire a most recently-issued certificate revocation list (CRL) that is digitally signed and time-stamped. The receiver should retain the digital signature of the transferred XML document along with the related certificates and CRL. In the event the sender later denies sending the document, the receiver can furnish the retained data for non-repudiation verification.

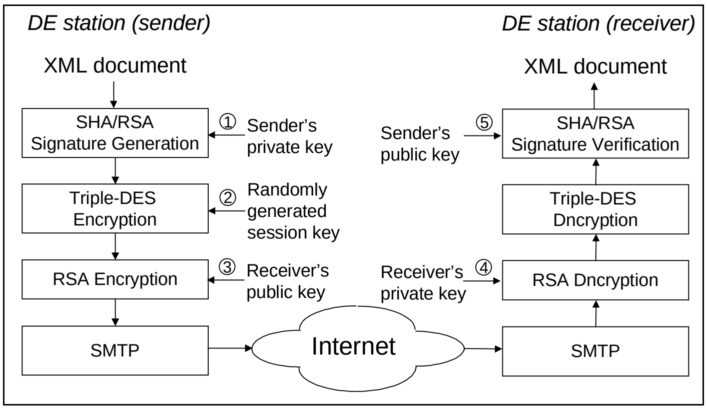

Figure 2. Processing a secure XML document

The Security Management Center is responsible for auditing and various security management such as issuing smartcards, acting as a public-key CA, regularly publishing CRL, and maintaining distribution lists. A distribution list identifies a set of recipients and could be used when a document is sent to a group of recipients. For instance, a document might want to be sent to all government agencies in the Department of Education.

The Security Management Center may act as a trusted third party and provide certified document service, the same idea as certified mail from the postal service. In this case, the sender transmits the document, or hash value of the document, to the Center who generates a digital signature over a data stream containing the document content, the identity of the sender, and optional information such as a time stamp. The Center returns this signed data to the sender who in turn forwards it to the receiver for use as a non-repudiation evidence.

The smartcard IC chip we adopted is the Hitachi H8/3111 [13] that offers an 8-bit RISC-like microprocessor, 14-Kbyte ROM, 8-Kbyte EEPROM, 800-byte RAM, and an arithmetic coprocessor. We developed an ISO-7816 compliant operating system for the smartcard IC and implemented the RSA, SHA, DES, and triple-DES cryptographic algorithms to fit our security needs. The ROM area of the chip is used for operating system while the EEPROM is used for personalized data and for optional cryptographic algorithms or other application programs. The specific cryptographic algorithms were chosen based on the technical requirements made for the government citizen's card [14].

The built-in arithmetic coprocessor features 576-bit ABR^{-1} *mod N* Montgomery modular multiplication [15], but the modular exponentiation operation for RSA algorithm has to be implemented by assembly codes. The size of RSA key in our implementation ranges from 512 bits up to 1024 bits, configurable by the card issuer.

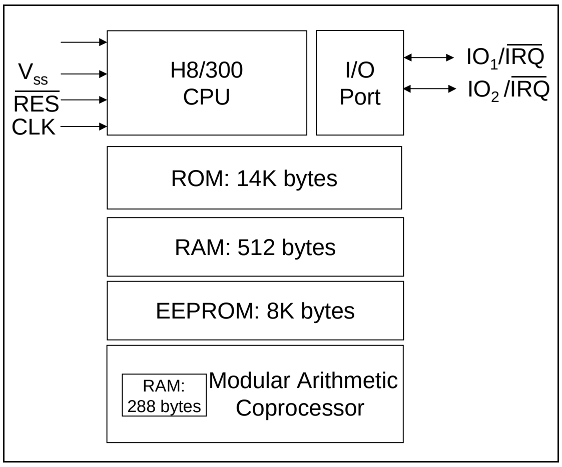

Figure 3. Block diagram of Hitachi H8/3111 smartcard IC

CONCLUSIONS

Public-key infrastructure is essential for the viability for large-scale secure document exchange. The multi-purpose smartcard has ISO-7816 compliant operating system with SHA, triple-DES, and 1024-bit RSA cryptographic algorithms inside. We have presented a design of smartcard-based infrastructure for the XML-based document exchange systems, where communication security services are made an integrated part of the systems. Our system uses both digital envelope and digital signature of the public-key and private-key cryptography to provide confidentiality, authentication, and non-repudiation security services.

REFERENCES

[1] The 1997 edition of the R.O.C. White Paper on Government Computerization, English web page: http://www.rdec.gov.tw:10080/white86/white86e.htm.

[2] C. H. Yang, S. L. Yen, H. D. Liu, K. Liu , B. S. Jeng, K. Y. Chang, M. S. Chang, Y. L. Cheng, J. L. Liang, and D. M. Shien, "Secure Official Document Mail Systems for Office Automation," *Proc. 31st Annual 1997 International Carnahan Conf. On Security Technology*, October, 1997, Australia, pp. 161-164.

[3] Shy-Ming Ju, "An SGML-based Office Document Exchange and Management," *Proc. SGML/XML Europe '98*, 1998, pp. 269-282.

[4] Extensible Markup Language (XML) 1.0, W3C Recommendation, February 10, 1998. http://www.w3.org/TR/REC-xml.

[5] Frequently Asked Questions about the Extensible Markup Language, http://www.ucc.ie/xml/.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, Feb. 1978, Vol. 21, No. 2, pp. 120-126.

[7] National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standard, FIPS PUB 180-1, April 1995.

[8] National Institute of Standards and Technology, *Data Encryption Standard*, Federal Information Processing Standard, FIPS PUB 46-2, December 1993.

[9] National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standard, FIPS PUB 186, May 1994.

[10] Jonathan B. Postel, *Simple Mail Transfer Protocol*, RFC 821, 1982.

[11] Warrick Ford and Michael S. Baum, *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*, Prentice Hall, 1997.

[12] ITU-T Recommendation X.509 "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework," 1993.

[13] *Hitachi Single-Chip Microcomputer H8/3111 Hardware Manual*, Hitachi Ltd., 1996.

[14] *Request for Proposal for IC Card with Combined National ID and Health Insurance Card Functions (Citizen's Card)*, R.O.C. Executive Yuan IC Card Planning &Promotion Task Force, June 1998. English web page http://www.gsn.gov.tw/eng/iccard/erfp0610.html.

[15] Peter L. Montgomery, "Modular Multiplication without Trial Division," *Mathematics of Computation*, pp. 519-521, 1985.