AUTHENTICITY AND INTEGRITY OF PORTABLE ELECTRONIC HEALTH RECORDS

Chung-Yueh Lien
Institute of Biomedical Engineering, National Yang-Ming University, No. 155, Sec. 2, Linong st. Beitou District, Taipei 112, Taiwan

Chia-Hung Hsiao
Department of Medical Informatics, Tzu Chi University, Hualien City, Taiwan

Lu-Chou Huang, Tsair Kao
Institute of Biomedical Engineering, National Yang-Ming University, Taipei, Taiwan

Keywords: Security, Portable electronic health record, Digital signature, Integrity, Authenticity.

Abstract: In this paper, we proposed a method to secure an electronic health record stored on a portable data storage media (CDs/DVDs, diskettes, flash drives). We applied cryptography to realize the authenticity and integrity of the portable health record. A manifest signature mechanism was used to reduce the computation time of the signing and verifying processes. A DICOM DIR consists of 166 DICOM MR images was tested as an example of a portable medical record. The performance of this method is faster than the regular digital signature mechanism.

1 INTRODUCTION

Electronic health records (EHRs) may be generated by hospitals, examination laboratories, insurance companies or patients themselves (Bates et al. 2003; Wang et al. 2004; Pharow & Bolbel 2005; Tang et al. 2006). To realize clinical data exchange between healthcare providers, a trusted conduit is needed for the EHR systems and users. The integrity and authenticity of EHRs can be validated using a digital signature mechanism (Ruotsalainen & Manning 2007; Schütze et al. 2006). A digest of the digital document is calculated from an irreversible one-way hash function. The hash check of digital data is commonly used on the Internet to prevent unauthorized modification. The digital signature can be implemented by a combination of the hash algorithm and public-key cryptography such as the RSA algorithm. When the RSA algorithm is used to calculate a digital signature, the signer encrypts the digest of the digital document with his/her own private key. The recipient, with access to the signer's public key then verifies the digital signature.

The implementation of EHRs has to conform to security regulations, laws and standards, such as Digital Imaging and Communication in Medicine (DICOM), Health Level 7 (HL7), World Wide Web Consortium (W3C), Health Insurance Portability Accountability Act (HIPAA) and ISO/TS 17090. According to the healthcare standards, a legal signed EHR must contain one digest, one digital signature and one timestamp signature. Under public-key infrastructure (PKI), the use of the RSA algorithm makes it possible to work with the certificate and trusted third party (TTP) to process inter-institutional applications such as the verification of an EHR and referral information (Lekkas & Gritzalis 2007). An EHR may contain hundreds of digital files, and then require the same number of digital signatures. However, it is impractical to implement these lengthy signing and verifying processes in the real world due to the high computation time.

In this paper, a manifest signature mechanism is proposed to reduce the computation time of the signing and verifying processes used when dealing

Lien C., Hsiao C., Huang L. and Kao T. (2008).
AUTHENTICITY AND INTEGRITY OF PORTABLE ELECTRONIC HEALTH RECORDS.
In *Proceedings of the First International Conference on Health Informatics*, pages 67-71

with a portable EHR. A DICOM DIR consists of 166 DICOM MR images was tested as an example of a portable EHR.

2 METHODS

We used a smart card system that supports the Microsoft Cryptography Service Provider (CSP) as the digital signature module. The use of the health professional card (HPC) with a smart card-based certificate is a good example and can be found in the healthcare environments of Taiwan (Yang et al. 2006), Germany (Schütze et al. 2006; Schurig, Heuser & Wedekind 2001), Belgium (France, Bangels & De Clercq 2007), etc. A health organization certificate card (HOC) holds the digital official seal of every health organization and can be used for EHRs exchange among organizations. The Health Certificate Authority Timestamping Authority (HCA-TSA) provides the timestamp service as the TTP.

2.1 The Characteristics of a Portable EHR

The flowchart of the security protection process is shown in Fig. 1. The clinical documents, integrated from various systems in a hospital stored in the portable storage media. The signed list has to be managed through the metadata that define these data in a portable EHR. The metadata has to identify the information, structures and formats to meet the needs of multimedia data exchange. The signed list is used to sign the clinical documents from the signing hospital; the documents described in the signed list will be signed using the hospital certificate with a digital time signature. According to the signed list, the digest values of the clinical documents are calculated and packaged as the digest of these documents. The hospital and TTP generate the digital signature and digital time signature to verify the authenticity of the clinical documents. The hospital certificate is used as identification on the exchanged clinical documents and to authenticate the source site, and the site receiving the data can then verify whether or not the exchanged clinical documents are valid. Table 1 summarizes the use of the characteristics of a portable EHR.

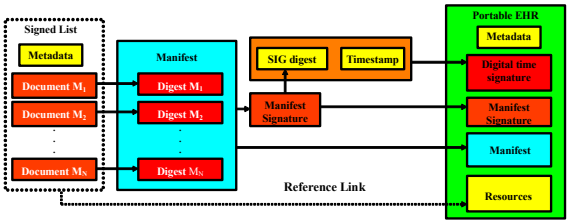

Figure 1: The characteristics of a portable EHR architecture.

Table 1: The use of the characteristics of a portable EHR.

Characteristics	Use
Metadata	Definition of the portable EHR
Signed List	Information of signed EHR
Digital Time Signature	Authenticity
Manifest	Integrity
Manifest Signature	Authenticity
Resource	The physical EHR structure

2.2 The Manifest Signature Mechanism

The manifest signature process is shown in Fig. 2. In the signed list, there are N documents M_1, M_2, ..., M_N need to be signed. For each file $Ref(M_n)=ID(M_n)^H(M_n)$ is calculated. The symbol '^' means cascade. $Ref(M_n)$ represents the metadata of M_n, and some information related to M_n can be defined in $ID(M_n)$, such as data type, creation time, purpose, etc., for exchange among various EHR systems. $H(M_n)$ is the digest of M_n, where H is the hash function, such as MD5, SHA1, etc. We can reconstruct $Ref(M_n)$ as the manifest of N documents' digest MD_D defined as:

$$MD_D = Ref(M_1)^Ref(M_2)^...^Ref(M_N)$$

Based on the RSA algorithm, using the signer's private key P_r to encrypt $H(MD_D)$, the digest value MD_D, as the digital sitnature of MD_D, we then define the digital signature process as follows:

$$SIG(MD_D)= RSA_{Enc}(P_r, H(MD_D)),$$

Where RSA_{Enc} is the RSA encryption function. $SIG(MD_D)$ is the manifest signature. We send the digest $H(SIG(MD_D))$ to a TSA to obtain a qualified digital time signature TSA_{SIG}, defined as:

$$TSA_{SIG} = RSA_{Enc}((P_{rTSA}, H(SIG(MD_D)||T_{SS}))$$

The symbol '||' represents the concatenation, P_{rTSA}, is the TSA's private key and T_{SS} is the Greenwich Mean Time (GMT) timestamp.

This is an efficient mechanism to ensure the integrity and authenticity of a portable EHR. From the aspect of data integrity, $Ref(M_n)$ ensures the

integrity of a document M_n. The manifest signature $SIG(MD_D)$ and the digital time signature TSA_{SIG} provide verification of the authenticity for the documents in the signed list and the T_{SS} confirms the synchronized time.

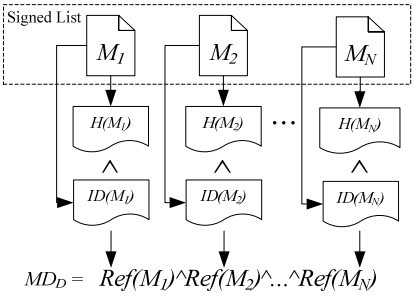

Figure 2: Manifest of the documents' digest process.

2.3 Performance Analysis of the Manifest Signature Mechanism

Assuming the time required for hashing, signing and digital time signature retrieval are T_n, T_r and S_n, respectively, where $1 \le n \le N$. The timestamp retrieval time depends on the network status; here S_n is just for reference. If we create digital signature for each document one by one, the total calculation time is:

$$T_{total} = \sum_{n=1}^{N} T_n + N \times T_r + \sum_{n=1}^{N} S_n$$

However, using the method proposed in this stuy, the total time will be reduced to:

$$T_{total} = \sum_{n=1}^{N} T_n + S_1 + T_r + T_M$$

T_M is the computation time of H(MD_D). The number of calculations needed for verification process is still the same. Table 2 shows the number of calculations in hashing, signing and digital time signature retrieval for different methods.

Table 2: Comparison of the number of calculations between the proposed method and the one-by-one method.

Operations	Calculation time	
	Proposed method (sec)	One-by-one method (sec)
Hashing	N+1	N
Signing	1	N
Digital time signature retrieval	1	N

*N is the number of documents in the signed list.

3 RESULTS

3.1 The Manifest Signature Architecture Implemented using XML

We tested an example of the manifest signatures of 166 DICOM MR images (packaged as DICOM DIR) to be signed using both our method and the one-by-one method regulated in the DICOM standards.

First, system will search all of files in selected folder and mark the URI of files to generate the signed list. According to the URI of the signed list, system will find the direction pathway of file and calculate the digest value of each file. The $ID(M_n)$ is created from the DICOM head tags such as Transfer syntax UID (0020, 0010), SOP Instance UID (0008, 0018)…etc, and we use XML encoding to present $Ref(M_n)=ID(M_n)^H(M_n)$.

Fig. 3 shows the $Ref(M_n)$ structure presented as XML. In Fig. 3, a unit of $Ref(M_n)$ is represented by the tag name "Reference". The attribute "URI" of <Reference> is the related directory pathway in addition to an identification of the resource file. $H(M_n)$ is represented by <DigestValue> and $ID(M_n)$ is represented by <DigestMethod Algorithm> and <Transforms>. Transforms means the namespace of this referenced document, which identifies the data format. In this example, the value in <Transform Algorithm> is urn:oid:1.2.840.10008.1.2.1, which expresses the explicit little endian coding for DICOM. This attribute can deal with different cases of different data formats for EHR exchange between hospitals; in addition, it can be extended for multiple data formats, which are defined by the user.

We reconstruct $Ref(M_n)$ as the manifest digest MD_D, and put MD_D into <Object> tag as the signing range of manifest signature and the attribute "Id" of <Manifest> is represent the identifier of MD_D. The cascade of the element in XML as the manifest of these DICOM files is shown in Fig. 4. We calculate $H(MD_D)$ and using HOC's private key to encrypt $H(MD_D)$ and generate the manifest signature $SIG(MD_D)$ complies with the W3C XML enveloped signature standard is shown in fig. 5. All value is encode by Baase64, the value "Object" in attribute "URI" of <Reference> means sign the <Object> described above, H($SIG(MD_D)$) is represented by <DigestValue>; the manifest signature is represented by <SignatureValue> the singing certificate is put in <X509Certificate> tag.

```
<Reference URI="SDY00000\PRS00000">
  <DigestValue>lujg6oNg+2lq+l7Gn+HTAw==</DigestValue>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
- <Transforms>
    <Transform Algorithm="urn:oid:1.2.840.10008.1.2.1" />
  </Transforms>
</Reference>
```

Figure 3: A unit of Ref(Mn) of one image in DICOM DIR.

```
- <Object>
  - <Manifest Id="DICOMDIRManifest">
    + <Reference URI="DICOMDIR">
    + <Reference URI="SDY00000\PRS00000">
    + <Reference URI="SDY00000\SRS00000\IMG00000">
    + <Reference URI="SDY00000\SRS00000\IMG00001">
    + <Reference URI="SDY00000\SRS00000\IMG00002">
    + <Reference URI="SDY00000\SRS00000\IMG00003">
    + <Reference URI="SDY00001\SRS00000\IMG00000">
    + <Reference URI="SDY00001\SRS00001\IMG00000">
    + <Reference URI="SDY00001\SRS00002\IMG00000">
    + <Reference URI="SDY00001\SRS00003\IMG00000">
    + <Reference URI="SDY00001\SRS00004\IMG00000">
    + <Reference URI="SDY00001\SRS00005\IMG00000">
    + <Reference URI="SDY00001\SRS00006\IMG00000">
          .
          .
          .
    </Manifest>
  </Object>
```

Figure 4: The manifest structure of DICOM DIR presented as XML.

```
- <SignedInfo>
  - <Reference URI="Object">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    - <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#base64" />
      </Transforms>
      <DigestValue>JPj9jG0PZxRHPtXbCvWGgw==</DigestValue>
    </Reference>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
  </SignedInfo>
- <KeyInfo>
  - <X509Data>
      <X509Certificate>MIIB/TCCAWqgAwIBAgIFygAAABQwDQYJKoZIhvcNAQEBBQAwVTE ...
    </X509Data>
  </KeyInfo>
    <SignatureValue>NhSWrLMWRFBfODsB1qvRymPQEbUVx1+XMaRBHxGapjbLMEAQY+lker9 ...
```

Figure 5: The manifest digital signature presented as W3C XML enveloped signature standard.

3.2 Performance Test

Table 3 shows a comparison of the operation time for test files by different methods. In the one-by-one method, each image has to be hashed, RSA encrypted and timestamp retrieved once, for which the total time needed was about 167.89 seconds. In the proposed method, however, the total time was reduced to 2.81 seconds. The demonstrating PC is a Pentium D 2.8 GHz, with 4 GB memory; the size of each image is about 516KB~1.58 MB; the total data size of the images is 82.3 MB; the type of the smart card is e-gate. The test of digital time signature time is retrieved from the Taiwan HCA-TSA.

Table 3: Comparison of the time needed for signing 166 DICOM MR images between the proposed method and the one-by-one method.

Operations	Calculation time	
	Proposed method (sec)	One-by-one method (sec)
Hashing	1.34	1.34
Signing	1.27	148
Digital time signature retrieval	0.2	18.55
Total time	2.81	167.89

4 DISCUSSION

If a portable EHR is to be exchanged with other organizations, the presence of a removable storage media is also required. To verify the authenticity of the EHR, the sender site creates the digital signature of the EHR as the organizational stamp. The receiver can then verify whether the EHR is valid by Certificate Authority (CA) and TTP. The digital signature created by the hospital and the digital time signature created by the TSA can record the authenticity of the EHR for inter-organization exchange. In terms of cryptography, the digital timestamp mechanism is not used to provide a qualified digital signature, but to certify a qualified time signature. Some infrastructures, such as patient identification, certificate management, and standards should be established as well. And some security issues should be noticed in implementation: e.g., data backup, audit trail, register loss, maintenance, recovery, etc.

A portable EHR contains clinical data and related setting data, the combination of these data can reconstruct representation of EHR. The signing range should contain all of the data related to clinical data. It is very important to ensure the integrity of representation of EHR. If only signing clinical data and related setting data is not singed, it could be happened in inconsistency of representation of EHR while setting data had been modified. The security protection of EHR should include all of data in portable storage media.

In general, most of the medical information standards and national regulations regulating the legal EHR do not use the manifest signature. If existing medical information digital signature rules are followed, as the practice is not feasible due to the high computational time of the signing and verifying processes. However, the signing time and timestamp retrieval time need to be reduced because a portable EHR may contain many clinical documents and

images, all of which need to be protected. For example, a study may contain hundreds of DICOM images, and following the DICOM standards in these cases is impracticable in real-world clinical operations. The manifest signature can be used not only for the exchange of EHR, but also for EHR long-term storage in hospitals.

Fast and reliable proof of authenticity and integrity is needed for security considerations when an EHR became portable. It is common that patients collect their own health records from different hospitals and manage the process by themselves. The implementation of a centralized health record containing personal health records is very difficult when taking into considerations of the physicians' intellectual property rights and patient privacy.

5 CONCLUSIONS

The computational time of this prototype is much lower than that of the one by one digital signature method. Following the existing medical information digital signature rules, the practice is not feasible. Using the proposed method, the computational time is reduced. In addition, this method can be used not only for the exchange of EHRs, but also for their long-term storage.

ACKNOWLEDGEMENTS

This work was supported by the National Science Council of Taiwan under Grant NSC 95-2221-E010-003.

REFERENCES

Bates, DW, Ebell M, Gotlieb, E, Zapp, J, & Mullins, HC 2003, 'A Proposal for Electronic Medical Records in U.S. Primary Care', *Journal of the American Medical Informatics Association*, vol. 10, no. 1, pp. 1-10.

France, FHR, Bangels, M & De Clercq, E 2007, 'Purposes of health identification cards and role of a secure access platform (Be-Health) in Belgium', *International Journal of Medical Informatics*, vol. 76, no. 2-3, pp. 84-88.

Lekkas, D & Gritzalis, D 2007, 'Long-term verifiability of the electronic healthcare records' authenticity', *International Journal of Medical Informatics*, vol. 76, no. 5-6, pp. 442-448.

Lekkas, D, Gritzalis, S & Katsikas, S 2002, 'Quality assured trusted third parties for deploying secure internet-based healthcare applications', *International Journal of Medical Informatics*, vol. 65, no. 2, pp. 79-96.

Makoul, G, Curry, RH & Tang, PC 2001, 'The Use of Electronic Medical Records: Communication Patterns in Outpatient Encounters', *Journal of the American Medical Informatics Association*, vol. 8, no. 6, pp. 610-615.

Pharow, P & Blobel, B 2005, 'Electronic signatures for long-lasting storage purposes in electronic archives', *International Journal of Medical Informatics*, vol. 74, no. 2-4, pp. 279-287.

Schurig, A, Heuser, H & Wedekind, R 2001, 'Introduction of the health professional card into the SAXTELEMED-Project', *International Congress Series*, vol. 1230, pp. 867-871.

Tang, PC, Ash, JS, Bates, DW, Overhage, JMS & Sands, DZ 2006, 'Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption', *Journal of the American Medical Informatics Association*, vol. 13, no. 2, pp. 121-126.

Wang, M, Lau, C, Matsen, FAIII & Kim, Y 2004, 'Personal health information management system and its application in referral management', *IEEE Transactions on Information Technology in Biomedicine*, vol. 8, no. 3, pp. 287-297.

Yang, CM, Lin, HC, Chang P & Jian, WS 2006, 'Taiwan's perspective on electronic medical records' security and privacy protection: Lessons learned from HIPAA', *Computer Methods and Programs in Biomedicine*, vol. 82, no. 3, pp. 277-282.

Zhou, XQ, Huang, HK & Lou, SL 2001. 'Authenticity and integrity of digital mammography images', IEEE Transactions on Medical Imaging, vol. 20, no. 8, pp. 784-791.