A Security Extension for the Standard SCP-ECG Based on Metadata

Óscar J Rubio, Álvaro Alesanco, José García

Communication Technologies Group (GTC), Aragón Institute of Engineering Research (I3A),
University of Zaragoza, Spain

Abstract

This paper analyzes the structure and content of the SCP-ECG standard to further design a tailor-made security extension. It is proposed to limit the access privileges of the users by means of role-based profiles (teaching/research, examination, diagnosis, storage) which are implemented with cryptographic elements (ciphering, digital certificates and signatures). A new security section is added to extend the SCP-ECG and the remaining sections are ciphered. The application implemented to test this proposal showed its ability to authenticate users, protect the integrity of the files and the privacy of the confidential information, with a low impact on the file size and access time.

1. Introduction

There are several standards for the storage and exchange of electrocardiograms (ECGs), intended for different applications (diagnosis, home care, emergency) and using different coding formats (binary, XML). The most widespread are the Standard Communication Protocol for computer-assisted electrocardiography [1] (SCP-ECG, international ISO standard), the HL7 aECG [2] (American ANSI standard) and the DICOM supplement 30 [3] (American NEMA standard). All of them dedicate most of their fields/sections to store structured data, called metadata, related to the patient, to the test or reserved for future use. Part of these metadata can also be used to protect the medical files against attacks of eavesdropping, forgery and manipulation. Using metadata for this purpose ensures an optimal integration with the protocol, although it entails two drawbacks: the file size raises (slightly) and it is not possible to use steganography to hide information, since the structure of protocols is public.

Current legal regulations (e.g. the HIPPA [4], the PIPEDA [5], the Digital Signature laws) establish three essential security requirements to be fulfilled by medical protocols:

1. **Guaranteeing the integrity** of the ECG and its associated data. Any small change in the duration, amplitude or shape of an interval of the signal may change substantially the physician's diagnosis, putting the patient at risk.
2. **Authenticating the agent** who protects the ECG file. Digital certificates allow the authentication of agents and users and checking the integrity of the file by means of a digital signature.
3. **Protecting the privacy of the patient**. The confidential data of the patient should only be accessed by his/her cardiologist/s and by those authorised by the consent of the patient (e.g. researchers and teachers). Besides all access to the ECG file should be recorded to uphold the principle of transparency.

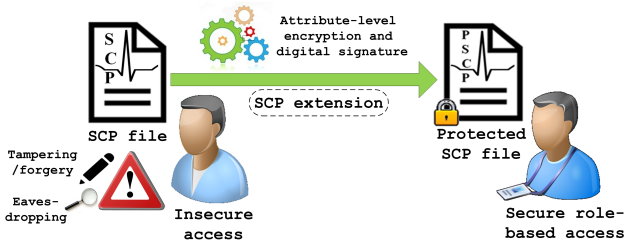

Figure 1. Aim of the SCP-ECG security extension.

DICOM and HL7 dedicate two working groups and several publications to define standardized security measures in line with these requirements: digital signatures, secure communications, audit trail and node authentication, role-based access control, risk management frameworks, attribute-level encryption and secure electronic online storage. Although SCP-ECG is a standard supported by most manufacturers of ECG devices and very spread due to its flexibility, it does not implement any security measure. As illustrated in Fig. 1, the aim of this work is to design a simple and robust security extension of this protocol, implementing attribute-level encryption, digital signature and role-based access profiles, by means of metadata. Finally this extension will be implemented and evaluated.

2. SCP-ECG and access profiles

The SCP-ECG is a protocol promoted by the European Committee for Standardization (CEN) with the purpose of

reaching interoperability among most ECG devices. Currently it is integrated within the ISO/IEEE 11073 family. This measure intends to extend the interoperability to other medical devices. This standard defines a binary encoding and procedures for ECG signal compression, to reduce the final file size. Although the SCP-ECG was designed to store tests of 12 leads of short duration, it also allows a different number of leads and it has been adapted to other environments, such as real-time transmission.

2.1. Separation of contents

The SCP-ECG is divided into 12 different sections, encoded by its own rules and preceded by a common header. Regarding their contents, five different groups may be distinguished:

- Section 0: this stores the **pointers** to the beginning of the remaining sections in the file. This section is considered as public since it does not contain any information itself.
- ***A****, Section 1 - tags 0-3, 5, 14-26, 31*: these tags contain the identification of the patient and the physician/s, institution/s and device/s involved in the acquisition, analysis and diagnosis of the ECG. They must be treated with strict confidentiality since they can identify the patient (directly or indirectly) in a file full of his/her health data.
- ***B****, Section 1 - tags 4, 6-13, 27-30, 32-35, 255*: these contain general information about the patient (e.g. age, height) and health data (e.g. medical history, drugs). This part (together with parts ***C*** and ***D***) may be used to conduct researches about the risk factors of a variety of heart diseases. Regarding privacy issues, these data itself do not identify the patient.
- ***C****, Sections 2-6*: these identify the leads present in the file (*Section 3*) and store **the ECG signal data** (*Section 6*), which may be kept as uncompressed raw data or alternatively compressed by different methods. The compression ratio which can be achieved ranges from less than 2-4:1, when only using Huffman tables (*Section 2*), or up to 6-20:1 when combining second-order differences (using *Sections 4* and *5*) with Huffman encoding and downsampling, at the cost of lower signal quality. This information can not be used against the patient for his/her identification since biometric recognition based on the signal would require another ECG of that patient, so no new information is obtained.
- ***D****, Section 7-11*: these sections can be optionally added to include:

1. global **measurements** (*Section 7*) and measurements from each lead separately (*Section 10*);
2. the **diagnostic** interpretation **of the ECG** record (*Section 8*), which must be consistent with the manufacturer interpretive statements (*Section 9*) and the universal ECG interpretive statement codes and coding rules (*Section 11*); These data interpret or help to interpret the ECG, so if the patient is identified (***A***), this information must be considered as highly confidential.

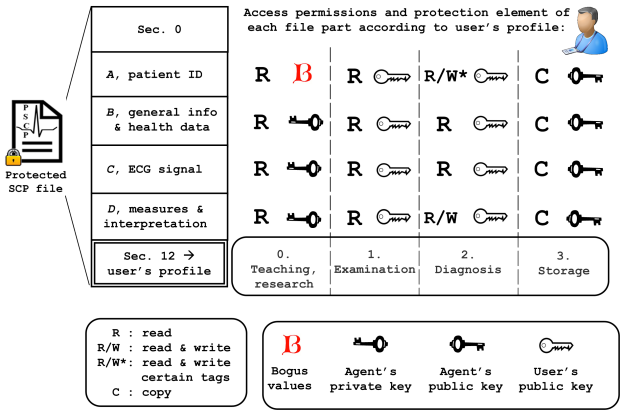

Figure 2. Security specifications of the SCP-ECG access profiles.

2.2. Role-based access profiles

Since the SCP-ECG can be divided into four parts (***A***, ***B***, ***C*** and ***D***) that can be protected independently (attribute/part-level encryption), it is possible to define different access profiles according to the professional role of the user. Fig. 2 depicts the security element that protects each SCP-ECG part and the user's access permission to them. It will be applied a kind of ciphering, called public, to protect the integrity and the authenticity of the contents and another kind of ciphering, called private, when their privacy is also protected. The proposed profiles are:

0. ***Teaching/research***
   - Use: to disclose those parts useful for teaching/research (***B***, ***C*** and ***D***).
   - Security: ***A*** is replaced with bogus values, public ciphering for ***B***, ***C*** and ***D***.
   - Privileges: reading.
1. ***Examination***
   - Use: to allow clinicians caring for the patient to read all parts.
   - Security: private ciphering.
   - Privileges: reading.
2. ***Diagnosis***
   - Use: to complement the file with analysis data, such as the delineation of signal fiducial points or the diagnosis of the cardiologist who interprets the ECG.
   - Security: private ciphering.
   - Privileges: reading all parts, writing ***D*** and *tags 15, 17, 19-20* of part ***A***, which identify the analyzing device, department, institution and physician.
3. ***Storage***
   - Use: secure storage.
   - Security: private ciphering.

• Privileges: making protected exact copies of the file, with no permission to interpret, write or modify the plaintext.

3. SCP-ECG extension

Since security is not addressed in any existing section of the standard, an entirely new section (numbered 12) is proposed. We call this new files Protected SCP-ECG and propose the extension .pscp to distinguish from the regular SCP-ECG format.

3.1. Section 12 structure

The new section defines the options (access profile, ciphering algorithms and parameters) that the agent uses to build the Protected SCP-ECG file.

Like the rest of the SCP-ECG sections, this is divided into two parts, **the header**, which is common to all the sections, and **the data part**, which adopts the structure corresponding to Section 1 to permit the storage of several fields of variable length. Each field is described by its tag (1 byte), its length (2 bytes) and its value (up to 65535 bytes).

Finally, the corresponding pointer to Section 12 is added in Section 0 to address the new section, indicating Section ID number, length and position.

3.2. Section 12 content

The tags included in Section 12, depicted in Tab. 1, enable the security measures under this extension:

• Integrity and authenticity by means of a digital signature (tag 3). For its obtaining, it is necessary to make a digest of the file by using a hash function (tag 2) and cipher it with the the private key of the agent, loaded from a password-protected file. The user will verify the digital signature by using the public key of the user, extracted from his/her public certificate (tag 1).

• Privacy, in four complementary ways:

– Replacing private data that the user is not allowed to access with bogus values (profile 0).

– Performing public ciphering (profile 0): it is necessary to choose a symmetric cipherer (tag 4) and replace the original sections with the ciphered counterparts.

– Performing private ciphering (profiles 1-3): it is necessary to choose a symmetric cipherer (tag 4) and replace the private sections with the ciphered counterparts. In this operation it is also necessary to load the certificate of the user, generate a random symmetric key (tag 5) for the symmetric cipherer and encrypt it with the public key of the user. Only that user will be able to recover the symmetric key and decipher the confidential sections.

Table 1. Structure and content of the Protected SCP-ECG Section 12 Data Part.

Tag	Length	Value (parameter data)
0	1 byte	**Access profile** Value — Type 0 — Teaching/research 1 — Examination 2 — Diagnosis 3 — Storage
1	length[1]	**Certificate of the agent** (PEM encoding): The certificate must be X.509, any version. RSA [6], DSA [7], ECDSA [8] public key algorithms are allowed for access profiles 0-2 (tag 0), only RSA for profile 3.
2	1 byte	**Hash function ID** Value — Algorithm 0 — SHA1 **1 — SHA2 512** 2 — RIPEMD 160 3 — RIPEMD 256 It is recommended to use SHA2 512.
3	length[1]	**Digital signature**, DS = Enc(PrKa, hash(SCP-ECG)) This is the encryption of the hash using the private key of the agent (initially DS = blank). At the user's end the DS is used to verify the integrity of the data and authenticate the agent. The length of the DS depends on the agent's certificate type (tag 1).
4	1 byte	**Ciphering algorithm ID** Value — Algorithm **0 — Rjindael (AES)** 1 — Twofish 2 — RC6 3 — Blowfish 4 — 3DES Rjindael is the preferred option: it was chosen as the Advanced Encryption Standard [9] by the National Institute of Standards and Technology after a contest.
5	length[1]	**Encrypted secret random key**, eKs = Enc(PbKu, Ks) This is generated with a secure random function and encrypted with the public key specified in the user's certificate, PbKu. Thus, the length of this field depends on the user's certificate type. This field is not present in profile 0 (tag 0).
6	25·n bytes	**Secure access record**, SAR Each entry is composed of: Byte — Name — Type — Notes 1 to 15 — **Certificate issuer, Common Name** — ASCII 16 to 20 — **Certificate serial number** — Integer 21 — **Type of access** — Integer — Allowed values: 0 to 3 22 to 25 — **Request date** — Integer — Seconds since January 1, 1970, 00:00:00 GMT For profiles 0-2 there is only one entry, for profile 3 there may be several.

[1] The length of these fields is specified in Tab. 2.

– Including a Secure Access Record (SAR, tag 6) to identify the user (profiles 0-2) and maintain the privacy principle of transparency (profile 3).

4. Implementation and use

The access profiles described in Sec. 2.2 can be easily managed using a GUI application that we have implemented, openly available at `http://sourceforge.net/projects/pscp`. It is also available as an applet for integration in web pages. Both versions have been written in Java, so they are compatible with most devices. The application is used in the first place by the agent, who replaces his/her SCP-ECG genuine files by the protected counterparts using profile 3. When an authorised user requests an ECG, the agent prepares a Protected SCP-ECG file by using the most adequate profile according to the role of the user. Finally the user receives the protected file and access its contents by means of the application.

5. Evaluation and conclusions

This proposal relies on cryptography and it is compatible with 5 different ciphering algorithms, 3 hash functions and the main public key algorithms (RSA, DSA and ECDSA), to have replacement in case that any of them becomes vulnerable in the future. The use of attribute/part-level encryption to support role-based access control and digital signatures to detect corruption of contents implies that agents who protect SCP-ECG files and users who access them must have their own digital certificates.

The ciphering of the SCP-ECG parts severely distorts the ECG waveform and the rest of the data. We chose randomly 30 SCP-ECG from `www.openecg.net` and calculated the normalized cross correlation, $corr \in [0, 1]$, between all pairs of metadata and signals from different files. Related signal pairs, such as leads from the same patient record, obtained $corr$ values higher than 0.6 while unrelated signal (and metadata) pairs obtained values close to 0. As expected, the $corr$ values between pairs of original signals/metadata and their ciphered counterparts were also close to 0, showing the decorrelation power of ciphering.

On the other hand, the security extension of SCP-ECG files also results in a different file size and it delays the access. Protecting a file takes typically 0.5-1 s (1.5-3 s if it is done from a PSCP-ECG since it implies unprotecting and protecting again) and access a PSCP-ECG typically takes 0.5-1 s. Besides, the addition of Section 12 increases the size of the file. As it is shown in Tab. 2, the main factors are the agent's certificate type (tag 1), which also determines the length of the DS (tag 3), and the user's certificate type, which fixes the encrypted symmetric key length (tag 5). For profile 3 the number of entries in tag 6 may grow substantially, so we propose limiting this field to the last 40 accesses (1 KB). The size of Section 12 ranges from 0.69 (profile 0 with agent's cert EC 192, -no user's cert- and 1 entry in tag 6) to 3.83 KB (profile 3 with agent's cert=user's cert RSA 4096 and 40 entries in tag 6). Since we estimate that the average size of a SCP-ECG file is 31 KB, the overhead is $\simeq$ 2-12%.

Table 2. Typical size (KB) of Section 12 fields.

Agent's cert type	Tag 1	Tag 3	**User's cert type**	Tag 5
EC 192	0.6	0.05		
EC 224	0.6	0.06	RSA 1024	0.13
EC 239	0.6	0.06	RSA 2048	0.26
DSA 1024	1.1	0.05	RSA 4096	0.51
DSA 2048	1.6	0.05		
DSA 4096	2.6	0.05	Tags 0, 2, 4	Tag 6
RSA 1024	0.9	0.13		
RSA 2048	1.1	0.26	0.012	$0.025 \cdot$
RSA 4096	1.8	0.51		$\#entries$

Neither the delay nor the overhead are obstacles for the integration in e-health platform, since both are low or moderate and the standard is mainly designed for store & forward transmission. This proposal allows to add security to the SCP-ECG, which will result in a wider use.

Acknowledgements

This research work has been partially supported by projects TIN-2011-23792/TSI from the Ministerio de Ciencia e Innovación (MICINN) and the European Regional Development Fund (ERDF).

References

[1] Standard Communication Protocol for Computer-assisted ElectroCardioGraphy, ISO 11073-91064:2009. `http://tinyurl.com/86qzf6t`, 2009.

[2] Health Level 7 Annotated ECG, ANSI standard. `http://tinyurl.com/7fldgw4`, 2004.

[3] DICOM Waveform Supplement 30: Waveform Interchange. `http://tinyurl.com/7tlxbbt`, September 2000.

[4] The Health Insurance Portability and Accountability Act (P.L.104-191), 1996. Enacted by the U.S. Congress.

[5] The Personal Information Protection and Electronic Document Act, `http://tinyurl.com/4mn4wof`, 2000. Enacted in Canada.

[6] RSA Laboratories. PKCS 1: RSA Cryptography Standard `http://tinyurl.com/76oms`, June 2002.

[7] Kravitz DW. (FIPS PUBS 186: Digital Signature Standard (DSS), `http://tinyurl.com/2pxg3h`, May 1994.

[8] Certicom Research. Standards for efficient cryptography, SEC 1: Elliptic Curve Cryptography, Version 2.0,`http://tinyurl.com/6sqlb3d`, May 2009.

[9] Daemen J, Rijmen V. FIPS PUB 197: Advanced Encryption Standard, `http://tinyurl.com/qksc6`, Nov. 2001.