Constructing a secure HIPACS with Structured Reporting

Lutz Vorwerk*, Frank Losemann, Thomas Engel, Christoph Meinel

Institute of Telematics, Trier, D-54292

ABSTRACT

The specification of security features of the DICOM (digital imaging and communication in medicine)[4] standard is not clear where encryption and decryption are concerned. In the age of digital medicine, a growing need for secure transfer and storage of patient data is obvious. In medical science, the design of a PACS (picture archiving and communication system) is essential for storing digital images. This paper describes an alternative method of integrating encryption as a DICOM-conform mechanism in a PACS and via a DICOM-conform directory service in a HIS (hospital information system)/RIS (radiological information system). It is useful to integrate these systems in order to be able to merge existing patient data with DICOM images. The DICOM supplement SR (structured reporting)[5] is used for encryption and as an interface-specification for databases. SR also allows the definition of private coding schemes. It is possible to integrate security in a PACS by using one, private, coding scheme for encryption and a different coding scheme for decryption. The interface to the databases is a directory service that uses its attributes to store orders from databases and which retrieves orders for the databases. This method makes the construction of a secure HIPACS (hospital integrated picture archiving system) possible.

Keywords: PACS, structured reporting, security, object database, Java, DICOM, codes.

1. INTRODUCTION

This concept describes a way to use SR for encryption and as an interface specification for relational and object databases. The specification of SR allows to define coding schemes. These schemes are intended for coding findings with medical codes like SNOMED (Systematized Nomenclature of Medicine) or ACR (American College of Radiology). SR also allows the definition of private coding schemes. If one private coding scheme - the public key - is used for encryption and another coding scheme - the private key - is used for decryption of a DICOM document, it is possible to integrate security in the PACS. These coding schemes can be extended so that a certification mechanism can be added.

SR allows to integrate the DICOM model (PACS) with database models (HIS/RIS). Existing applications may use the new functionality represented as JAVA-applets by loading these applets into a browser and by operating them on a local database or file system where the unencrypted files are located. These encrypted files are then transferred by a DICOM protocol to the HIPACS or to another location which uses the applets to store the file. The decryption should only be used when an application uses an encrypted file. The code-attributes defined in supplement 36[7] which are intended for the specification of a medical coding scheme are used to store the encrypted data. Another possibility would be to define relationships of SR for those attributes which are not considered to have a medical code attribute. The unencrypted data is deleted or replaced during encryption and is being rewritten during the decryption process. It is important that fast performance for the algorithm decrypting and encrypting large data sets is ensured. Because of this, the image-data only gets encrypted when ordered.

The interface to the databases is a directory service evoked through the SR-'named types' which uses its attributes to store the search-, store-, delete- and retrieve-orders for the databases. The databases that are supported were managed in a list that containing information about the retailer, the product and the version of the database. The applications try to find out which database is connected to the system and store this information until the database is changed. There is an option to add new databases orders. The missing development of security concepts for DICOM is the reason why existing alternatives are being used and why we are presenting a concept to integrate security by encryption and decryption. The SR supplement 23 and the supplement 36 of the DICOM-standard provides a mechanism to form such an alternative. SR also provides the possibility to build a directory service which can be operated on different databases. This way, existing databases - object or relational - can be connected to a HIPACS, PACS, RIS or HIS. This method provides a quick way to scale these systems to the needs of the using institution. Finally, the integrated log mechanism of SR provides a way to control when and where a user or a modality has taken action.

*Correspondence: Email: vorwerk@ti.fhg.de; Phone: (+49) (0)651-97551-34; Fax: (+49) (0)651-97551-12

2. STRUCTURED REPORTING

In Europe, the workflow of a hospital is influenced by the so-called 'law regulating financial support for hospitals'. Therefore, hospitals must try to achieve a balance between patients' welfare and the economic budget of the hospital. The need to reduce costs by using information technology and increasing the patient care at the same time makes it necessary to think about the integration of a hospital information system (HIS) and/or a radiological information system with a picture archiving and communication system (PACS). The basic elements of the integrated system, called 'hospital integrated picture archiving system` (HIPACS), are the standard of digital imaging and communication in medicine (DICOM) and of health level 7 (HL7). DICOM is used to manage the transfer and use of digital images and data that belongs to the digital images. HL7 adds features that concern the transfer of medical data, i.e. patient data, like findings or reports. The standards HL7 and DICOM were integrated by trying to specify an interface called imaging system - information system (ISIS). A subset of this interface is used to specify a supplement of DICOM called 'structured reporting' (SR). The new features of SR enable DICOM to connect (DICOM) images, and existing reports of a person with images that belong to these reports. It is therefore possible to integrate text, audio, images, sequences of images, curves, diagrams and alphanumeric parameters. The presentation of the functionality from SR on an output device is ignored and has to be invented by the developer of the user-interface. As far as separation of structure and layout are concerned, the similarity of SR to the standard, generalized markup-language (SGML)[9] is obvious. To understand the SR, knowledge about DICOM is important. Therefore, we will, in the following, give a short overview about DICOM.

The use of computers in medical imaging and the development of applications that process images produced by imaging devices creates the problem of how to exchange images with related patient data between devices of different manufacturers. A common interface has to be specified for the devices and applications. This interface called DICOM makes it possible to connect devices, PACS and databases that contain diagnostic data. The DICOM-standard is accepted and used by many manufacturers.

The status of the standard is represented by the core. This core consists of parts which specify the required elements needed to develop and to understand a DICOM-conform application. The required elements are: the definitions of attributes, the representation of these attributes, the transfer of a set of attributes and the storing of these attributes in a file. A statement declaring which attributes defined in the DICOM-standard have been used and how they are being represented as well as additionally defined attributes that do not occur in the DICOM-standard has to be written. The statement is important for a user wanting to buy a DICOM application or a hardware with a DICOM interface. The statement serves as information about the interoperability of two DICOM interfaces. Interoperability may not be guaranteed if the statement is vague, incomplete, not precise or incorrect. Developers of DICOM-conform applications as well as manufacturers of DICOM-conform devices should take care to describe the features of their products thoroughly in order to increase the interoperability and acceptance of products that conform to the DICOM-standard. One aim of a such a standard is interoperability.

The core of the DICOM-standard may be extended by correction-proposals or supplements. The evolution of DICOM is achieved by the integration of accepted supplements that have reached the final stage and by the acceptance of correction proposals. There are two supplements concerning the integration of security in the DICOM-standard. Both are vague when specifying the transfer of encrypted data. There are some basic elements like digital signatures and authentication. The description of the use of digital signatures in adding an attribute that contains the hash-code to a set of attributes called module in the DICOM-standard is clearer than the description of encryption and decryption. Therefore, the use of digital signatures is not considered here . A module represents a piece of related information like the module 'patient' that contains all personal data of a patient. The problem for this solution of integrating digital signatures in the DICOM-standard is the modularity of the standard. An application without support for digital signatures may ignore the attribute that contains the hash code so that this attribute may get modified and the document may be transferred to a third application. This application contains a feature to verify digital signatures if they exist. It reads the document, estimates that there are no digital signature attributes and treats the data as unsigned. A problem of information getting lost is that it is dangerous for the transfer of data which must not be changed. To guarantee consistent exchange of data is one aim of digital signatures.

The other supplement of the DICOM-standard concerns the authentication of SOP and the specification of security policies. A SOP is a combination of a set of modules representing a DICOM document, called 'information object definition' (IOD) and a service that allows to work on the attributes of the modules and therefore, on the IOD.

Operations that move data from one point to another are an example for such a service. The authentication integrated through the supplement concerns the communication between two applications which support the service. This SOP itself is authenticated by the other application. This concept is very time-consuming because of the verification of the SOP that poses the request for authentication. The encryption of a connection between two applications is specified incompletely. There is no concrete definition of how to integrate encryption into the DICOM-standard. There are references for policies, but these policies require creativity from the developer.

Because of the current status of the two supplements we are currently thinking about alternatives of integrating encryption into the DICOM-standard. The growing need to integrate security in medical applications as a result of the increased use of computers in medicine makes it necessary to think about an alternative that can be realized quickly. This alternative is the SR together with the supplement of the specification to integrate medical coding in DICOM.

3. THE ALTERNATIVE: SR AND MEDICAL CODING

The DICOM-standard was enhanced by a supplement called structured reporting (SR). The SR defines a way to produce medical reports like, for example, findings. In practice, the production of a finding is achieved by using a dictaphone. The finding recorded on tape is transcribed by a secretary. The secretary shows the transcribed report to the physician who recorded the tape. The physician verifies the report and signs it. To reduce the amount of text, the physician uses a medical code. The code is often a standard-code like ACR (American College of Radiology) or SNOMED (systemized nomenclature of human medicine), but private codes of physicians who want their code to be understood only by themselves or by a group of persons they trust is also used. The supplement SR uses the supplements for coding medical data in a pre-defined scheme. In the definition of SR, there are four pre-defined kinds of reports which uses SNOMED as the default coding scheme. The text, the audio, the detail and the comprehensive IOD (information object definition). Other coding schemes are only permitted in a complex report of the four types of reports. Showing how to construct a coding scheme and how to integrate it in the definition of a report is important for understanding the way in which security gets integrated in DICOM over SR.

The structure of a SR report is complex[1,2,3]. This structure is represented in DICOM as IOD. In [5], there are four definitions for a report IOD. These four definitions will be described in the following. The simplest definition is the SR-Text-IOD. This definition possesses the features to reference other reports. The structure of a report in this definition consists of the following elements: A group of findings that contains information about the examiner and the time when the report and why the report is created. Elements of a group of findings are findings that represent observations made in a specific context. This context may be:

- an observer context describing which circumstances lead to the observation,
- a procedure context containing information about the requests which created the report,
- an observation subject context describing what has been observed,
- an observation category that adds characteristics to distinguish groups of findings.

The definition contains additional information about the patient, the study and the equipment and is restricted to text. This text can reference an image and/or is related to other text belonging to a specific category.

The SR-audio-IOD uses audio dictation instead of text and may reference images, overlays and wave forms. The SR-detail-IOD combines the features of the SR-test-IOD and SR-audio-IOD and allows additional classes like named types or codes within a report. The coding scheme defined for these three IOD is restricted to the SNOMED DICOM micro glossary (SDM). This coding scheme is a medical coding scheme that assigns medical code words to their descriptions. The intention of this paper is to use a private coding scheme in order to integrate the possibility to encrypt and decrypt defined parts of a DICOM-document. The fourth definition called `SR-comprehensive' allows to define a private coding scheme.

The comprehensive IOD possesses, as default coding scheme, SNOMED, but this can be replaced by another coding scheme. In the following, we want to describe the construction of a private coding scheme. This definition represents the whole functionality of the SR defined in [5] and has to be restricted according to our intention.

The first step is to estimate an appropriate coding scheme. To do this, it is necessary to understand how to build a medical coding scheme with the definition of [7] and then to do the transformation to a crypto-graphic coding scheme.

4. CODING SCHEMES IN DICOM

This section describes the SR point of view when building a coding scheme. To understand the integration of encryption in SR, the coding mechanism[7] used for medical coding schemes is described in general.

The first step of building a coding scheme is the definition of a baseline context group. This group represents a value set that consists of a set of attributes called 'code sequence attributes'. The values of these attributes are defined in a database with coding information called mapping resource. The baseline context group consists of values for a specific context. These values are called 'concepts' and use pick-lists which define the value-range for the context or action. The attributes of a specific context or action build a context group.

Concepts are templates that describe a concept through a set of properties. A set of templates builds a baseline template that represent a set of properties. These properties are values. A property is a piece of a concept. Concepts are connected via relationship types. With regard to medical coding schemes, each location has an identifier which is assigned to a description. This description is located in the mapping resource. There are additional identifiers in the database describing for diseases. Codes are used to give a short description of a finding. The problem is that only those people understand this cryptic code who have learned it. Our intention is for SR to take over the role of a translator from code to readable text. Why should SR not be used to translate a readable text into code using a coding scheme that represents an encryption method ?

4.1 INTEGRATION OF ENCRYPTION IN CODING SCHEMES

The integration of security in DICOM over the SR supplement is achieved by using coding schemes as keys. These keys are created by encryption algorithms selected through a mechanism called 'directory service' which is described in the following sections. All we need to do is to define a code scheme designator, a code value, a context identifier and a code-meaning stored in a record. The code-scheme designator gives the new private coding scheme a name. This name is the encryption scheme for the representation of the public key and the decryption scheme for the representation of the private key. The key is distributed on coding values. The defined terms of coding values are the digits 0 to 9. The context identifier is set to the algorithm from which the key pair is created. It is the unique identifier that identifies the entry in the directory service. In the code-meaning attribute, the name of the algorithm used to create the key pair is given. The code values are connected via relationships to a digit sequence that represents the public or private key. A first step can be the use of an existing algorithm to produce the key pair. After doing this, an application has to be written that transforms the key pair in the corresponding coding scheme. If the relationships were extracted and used as the key to the key we would have a new key pair for the code values and the relationships. This key pair can be used for working on the data.

The encryption process goes as follows: We define a third coding scheme that is used to encrypt attributes of the DICOM-standard in using the key pair created in the key creation process. The key is reconstructed as a sequence of digits and an encryption algorithm is chosen over the directory service represented here through SR in named-types records. The name of the algorithm is stored in the context identifier attribute of the coding scheme record. The encrypted data is stored as a sequence of digits connected via relationships stored in the code module of SR. According to the definition of DICOM-standard, some attributes must have a value. In order to delete the data from the attributes without affecting the definition, default values are stored in these attributes .

The decryption process looks for the private key of the user to decrypt the data, then it transforms the key pair and uses the information of the key and the encrypted data to find the algorithm for decryption. To find the algorithm, the directory service is used again. The data to be decrypted is stored in the attributes which belong to the encrypted data. The encrypted data will be deleted by this process.

4.2 THE ENCRYPTION METHOD

With the evolution of computer technology, the time to "crack" encrypted data will be reduced so that - according to the level of evolution- a new algorithm for encryption will have to be developed. A standard of encryption does not and will not exist. Therefore, a method has to be developed that allows to exchange an encryption algorithm without exchanging the whole application which uses this algorithm.

A first and simple method is to follow the same procedure that is used for the databases described in the next section. A header has to be defined that contains sufficient data to distinguish between the method of encryption and serves as an unique identifier for the encryption algorithm. This header will be stored in a directory service.

In DICOM, features concerning DICOM are negotiated between applications. This estimation feature is also used in other network protocols. If an application does not support a feature, this feature will not be used. To establish a communication, a default subset of features has to be defined in order to allow a communication between two or more applications. In the case of encryption, the possibilities are to encrypt the data with the default method or deciding to use the encryption algorithm supported by both partners of the communication. The algorithm to be used must not be available on the local system. It can be located elsewhere in the internet, referred to and described by a directory service. To integrate this service in DICOM, the SR is suitable since it allows to emulate a directory service which is DICOM-conform. Instead of defining a new class schema for a directory service, the named types of SR are used to store the data for the databases and the locations of encryption algorithms. A verification for validity of the links must be given to guarantee that the help applications represented by these algorithms are available. The advantage of the possibility to assign the method of encryption to the application lies, as has been shown, in the independence of the encryption algorithm. The feature for choosing the appropriate algorithm for encrypting the data puts the application on the security level that is needed. The characteristic of the algorithm is described in a 'named type' of SR so that the definition is independent from the encryption method.

5. THE DIRECTORY SERVICE

DICOM has some functionality features for constructing reports for findings. This functionality has the disadvantage that DICOM images can not be integrated with text or audio dictation which is needed for the generation of findings. One of the advantages of SR is the feature to manage external files that may be located somewhere in the internet. This kind of external link does not necessarily have to be a file, it might also be a link to a database. The kind of link is specified in the 'named types' of SR. A 'named type' called database - defined to represent the special characteristics - of the database is used to indicate which operations had to be performed in order to get data from or to put data to the referred database. The concept behind this is to use two applications:

One application is for the database having to be adapted to the database during installation. The configuration of this application includes the definition of a unique identifier, vendor and name of the database, operations to get data from and put data to the database, a kind of database (relative or object), the appropriate type of access and the appropriate type of operating system needed for the database. The vendor name and the product name serve as an identifier for the reusability of this configuration. The operations - which differ depending on the kind of access to the database - are used by the find operation, move operation and store operation by extracting the information from the corresponding attributes stored in the directory service. Ideally, this configuration should be automated in order to ease the installation of the application.

The other application is used to create, process or view reports. The applications may communicate via the DICOM protocol. The DICOM protocol orders like 'find' and 'move' can then be used to transfer the data between the applications. An option to disable the DICOM protocol is added for the case that the applications communicate only with applications supporting the DICOM protocol. The option to improve the message interchange between the applications by disabling the DICOM protocol is compulsory. The DICOM protocol is necessary when using a DICOM-conform image archive like a PACS. PACS are not always DICOM-conform. A central server which stores the new database definitions may be added. This central server is a dictionary for known databases and is used by the application assigned to the database to ease the adaptation of the application to the database.

To develop such a framework, one approach is to adapt an existing directory service based on X.500, DAP (direct access protocol) or LDAP (lightweight direct access protocol) to SR i.e. DICOM or to develop a new SR directory-service. We focus there on a scalable system that uses the DICOM protocol. As a result, we can conclude that we have a scalable directory service, i.e. a minimal directory service that conforms to the DICOM-standard. Existing directory services based on X.500[10] or LDAP are too big and not useful for the use on small systems. They can be used in a first step to quickly create an appropriate system by adapting the internal scheme of the directory service to DICOM. To integrate the DICOM protocol into existing directory services means to enhance the directory server and to modify the code of the server that conforms to X.500 but not DICOM.

The use of an existing directory service for SR depends on the need of the DICOM protocol. If there is a need for the DICOM protocol, a minimal directory service has to be created that conforms to X.500 or LDAP and, additionally, to

DICOM. LDAP specifies a layer which covers the TCP/IP protocol. The LDAP protocol uses BER (Basic Encoding Rules) of ASN.1 for byte protocol element coding, like the DICOM protocol.

6. AN OVERVIEW ON SECURITY

This section describes some aspects that are necessary to understand what security means when transferring data from one destination to another. There are different possibilities to protect data from third persons who want to read this data.

One way is to hide the data in other data. This concept is called steganography and is used for example in digital watermarking where data that belongs to an owner of an image is integrated in the image and protected against modification by using a digital signature. A digital signature builds a hash over the data that has to be signed. The hash is an encryption that is not reversible. The hash is encrypted with a private key. The private key is a secret key that can only be assigned to one and only one public key. The public key serves as a helping tool to exchange data with the owner of the assigned private key. To verify a digital signature, the hash is first decrypted with the public key and then it is checked whether the decrypted data (hash) matches the hash that has been generated by the data to verify if the data is changed.

Another way is to encrypt the data. That means to protect the data against modification and against information retrieval. The first step of such a method is the generation of a key. An algorithm patented in the USA which is has been declared 'secure' is Rivest Shamir Adleman (RSA). This algorithm is based on the problem of factoring large integers.

Another method is that of Diffi and Hellman. The algorithm computes discrete logarithms modulo a prime number. The renewal of patent will be processed by developing a health professional card[8].

A third method is that of using elliptic curves to compute the keys. The keys are shorter than in RSA and evoke, therefore, a smaller bandwidth and memory requirements.

With the key generation, a key pair is created: the public and the private key. The public key is now used to encrypt the data that can now only be decrypted by the owner of the private key. This method is called 'asymmetric encryption' because of the fact that one key is used for encryption and another one is used for decryption. Another method is called symmetric encryption. This method uses one key to encrypt and decrypt the data. It is less time-consuming but also less secure because the key can get deciphered by a crypto-analyst.

7. PUTTING IT ALL TOGETHER

Presently, all elements for building a secure HIPACS have been described. The core of the system is the SR, acting like a directory service. Its attributes are used to specify the mechanism which allows to operate with several databases which can be relational or object. In the case of a relational databases, the specification is similar to that of the JAVA interface to databases. In a first step, the interface to the relational databases can be this interface. For object databases, the ODMG (Object Database Management Group)[11] can be used.

The advantage of our concept is that the application has 'learned' the features of a proprietary databases by adding the access mechanism to the "knowledge" of the directory service.

The traditional method for connecting a database with an application is to install a driver for this database which offers the possibility of programming languages to access this database. Traditionally, relational databases are used where tables are combined via operators. The commands to find, store or delete data are defined in the database-query language called SQL. The interface between the relational database and the application which uses it receives commands as a string. Such an interface for relational databases is provided by the programming language JAVA[6]. But there are many proprietary database systems which do not conform to this interface. For these systems, a solution has to be found. A precaution is that the database must have the possibility to understand a text-file or stream which contains the commands of the query language used by this database. The commands are stored in the attributes and will be used as they are needed.

In addition, the location of the referred data in the database has to be reconstructed. The SR defines a mechanism which allows to reproduce the actions that have been performed to get this data. This mechanism is used in the case of an access to a relational database in order to log the actions that have to be performed to store or find specific data. Once stored, this procedure can be used to retrieve the data now contained as a reference in a report.

For object-oriented databases, a standard called ‘ODMG’ is accepted by several retailers of object-oriented databases. This interface specifies a query-language for object-oriented databases. Recently, a specification for JAVA has been published which is used by some retailers to write a JAVA interface for their database. This interface is new and here, proprietary systems exist as well. For the use of this concept, the object database has to also have the possibility to process a text-file or data stream that contains the commands for finding an entry. To find an entry as in using relational databases, the protocol mechanism of SR is used in order to reproduce the result.

Access to a DICOM-conform PACS is handled by storing the find-, store-, or move-operation used locating an entry. The ideal case is a PACS represented as a file system. In this case, only the uniform resource-locator (URL) has to be stored.

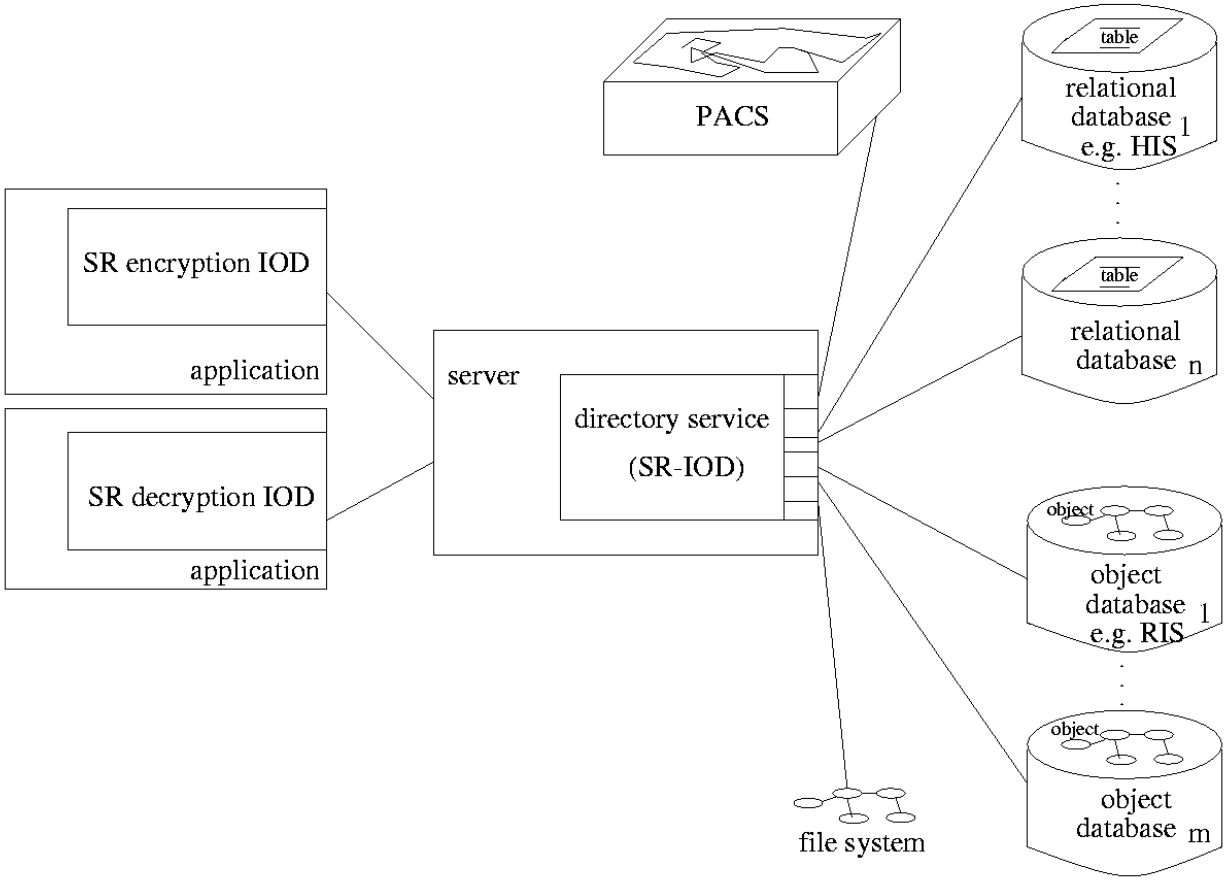

Figure 1: The joint components representing the proposal of a secure HIPACS.

The task of reproducing an order is taken over from an application that may be part of the directory server or stands alone and is referred to in the directory server in a special attribute. These applications are represented in Figure 1 as rectangles connected on one hand with the directory service and on the other hand with the databases, a PACS and a file system.

The integration of security in this system described in the sections above is the encryption and decryption of attributes of the SR-IODS. The SR encryption/decryption IOD uses cryptographic algorithms to generate the keys and encrypt or decrypt the attributes.

8. CONCLUSION

The constantly growing acceptance of computers in medicine causes a need for a common standard. A widely accepted standard for medicine is DICOM. In DICOM, there is no possibility to use existing data stored in relational or even object or proprietary systems. SR provides the features to connect existing systems to DICOM-conform systems. In such systems, data is transferred which should not be read by everyone who uses this system. Therefore, the need for security increases. In DICOM, this need evokes a specification of authentication and digital signatures, but this specification is not clear where encryption is concerned, since the specification has a recent and a first version.

An other way to integrate security in DICOM has been proposed in this paper. Here, the SR was used to construct a public and private key. These keys are then used to encrypt and decrypt the relevant data.

REFERENCES:

1. von Gehlen S. (Oldenburg), Vorwerk L., Jensch P., "Digitale Befunderhebung auf der Basis des DICOM Supplement Structured Reporting" in der Radiologie, in Biomedizinische Technik, Band 43 – Ergänzungsband 1, pp.46-47, 1998.
2. Lutz Vorwerk, Entwicklung eines Multimedia-Editors für die Befunderhebung in der Radiologie auf der Basis des DICOM Supplement Structured Reporting, (Master Thesis), Carl von Ossietzky Universität Oldenburg, November 1998.
3. S. von Gehlen, L. Vorwerk, M. Eichelberg, P. Jensch, A multimedia editor for radiological reports based on the DICOM Supplement Structured Reporting, CARS `99, Computer Assisted Radiology and Surgery, H.U. Lemke, M.W. Vannier, K. Inamura and A.G. Farman, 438-442, Elsevier, Paris, 1999.
4. *Digital Imaging and Communications in Medicine*, Teil 1-6. NEMA Standards Publication PS3.X, 1998.
5. Dr. Dean Bidgood and Ms Karen Kulda, NEMA-ACR and others. *Digital Imaging and Communications in Medi-cine (DICOM), Supplement 23: Structured Reporting (*Frozen Draft*)*, Supplement 23, Version 0.97 to NEMA PS 3.3, PS 3.4 and PS 3.6, 1997.
6. S. Hludov, L. Vorwerk, C. Meinel, *Intranet/Internet-basierte PACS*, Institut für Telematik e.V., Telemedizinführer Deutschland, Achim Jäckel, Deutsches Medizinforum (Minerva KG), Darmstadt, 1999.
7. Dave Snaveley*, Digital Imaging and Communications in Medicine (DICOM), Supplement 36: Codes and Controlled Terminology (Public Comment Draft)*, Supplement 36 to NEMA PS 3.3., 1998.
8. TeleTrust Deutschland e.V., Kryptographische Verfahren im Gesundheits- und Sozialwesen, 1998.
9. ISO (International Organization for Standardization), „ISO 8879:1986(E). Information processing -- Text and Office Systems -- Standard Generalized Markup Language (SGML)", First edition , International Organization for Standardization, 1986.
10. Computer network destinations, http://www.aloni.com/CND/CNDest.asp?TOCId=IPFamily&TopicID=X500, 1999
11. R.G.G. Cattell, Douglas Barry, Dirk Bartels, Mark Berler, Jeff Eastmann, Sophie Gmerman, David Jordan, Adam Springer, Hanry Strickland, Drew Wade, The Object Database Standard: ODMG 2.0, Morgan Kaufmann Publishers, Inc., 1997.