Trustworthiness in Distributed Electronic Healthcare Records – Basis for Shared Care

Bernd Blobel
Otto-von-Guericke University Magdeburg, Medical Faculty
Institute for Biometry and Medical Informatics
Leipziger Str. 44, D-39120 Magdeburg, Germany
bernd.blobel@mrz.uni-magdeburg.de

Abstract

Shared Care is the common answer to the challenge for improving health system's quality and efficiency. This development must be accompanied by implementing shared care information systems moving to extended electronic healthcare record systems which are distributed and have to be interoperable too. Comprehensive communication and co-operation between healthcare establishments is increasingly using the open Internet. Regarding the sensitivity of personal medical data due to legal, ethical, social and psychological implications, such communication and co-operation must be provided in a trustworthy way. The HARP project launched and funded by the European Commission specified and offered a solution for distributed, component-based, trustworthy applications based on Internet technology. Specifying and implementing Enhanced Trusted Third Party (ETTP) services, the HARP solutions concern secure authentication as well as authorisation of principals. By associating role profiles and security attributes to standard Web-based interactions, HARP provides an initial degree of 'automation' in building certified secure medical Internet-based applications deploying established paradigms such as object orientation, component architecture, Secure Socket Layer (SSL) protocol, and XML standard. The solution has been demonstrated and evaluated in a clinical study environment.

1: Introduction

Seeking for improvement of quality and efficiency in healthcare, specialisation and de-centralisation combined with extended communication and co-operation seem to be the proper solution. Such model of providing comprehensive care for patient by different persons, belonging to different organisations, using different methods at different time is called the Shared Care Paradigm. Shared care must be supported by information systems being distributed and interoperable as well.

All relevant medical information as well as related non-medical information derived from the former one is contained in healthcare records. Derived non-medical information concerns, e.g., materials, billing. Therefore, healthcare records are the informational basis for any communication and co-operation within, and between, healthcare establishments (HCE). Information systems supporting shared care based on medical records are electronic healthcare record (EHCR) systems being distributed too. For providing information and functionality needed, EHCR must be structured and operating appropriately.

Because personal medical data are highly sensitive, communication and co-operation in distributed networking systems must be established in a trustworthy way.

2: Security Models for Healthcare

For keeping development and maintenance of comprehensive healthcare information systems manageable from the security's point of view, the real systems' complexity should be simplified by grouping system components and services needed in a proper way. For that reason, a generic set of models has been developed and introduced which has been meanwhile widely accepted including standardisation activities provided within ISO and CEN. The generic models relevant in that context are the domain model, the generic security model and the layered security model.

A domain is characterised by components of a system grouped by common organisational, logical, and technical properties. This could be done for common policies (policy domains), for common environments (environment domains), or common technology (technology domains) [1, 2].

A policy describes the legal framework including rules, regulations and ethical aspects, the organisational and administrative framework, functionalities, claims and objectives, the principals (human users, devices, applications, components, objects) involved, agreements, rights, duties, and penalties defined as well as the technological solution implemented for collecting, recording, processing and communicating data in information systems. For de-

scribing policies, methods such as policy templates or formal policy modelling might be deployed.

Regarding the flexibility in handling properties and policies, the domain is of a generic nature, consisting of subdomains and building superdomains. The smallest domain is the working place or sometimes even a specific component of a system (e.g., of a server machine). The domain will be extended by chaining subdomains to superdomains forming a common domain of communication and co-operation, which is characterised by establishing an agreed security policy. Such transaction-concrete policy has to be negotiated between the communicating and co-operating principals, which is also called policy bridging.

For dealing with distributed systems, two security concepts have to be supported: the concept of communication security between two or more principals (e.g., components) and the concept of application security within one component. Communication security services comprise strong mutual authentication and accountability of principals involved, integrity, confidentiality and availability of communicated information as well as some notary's services. As result of the authentication procedure, authorisation for having access to the other principal has to be decided. Application security services concern accountability, authorisation and access control regarding data and functions, integrity, availability, confidentiality of information recorded, processed and stored as well as some notary's services and audit.

3: Concepts for Roles and Authorisation

Because it is impossible to assign authorisation and access rights within extended domains to any principal specifically, principals are grouped for assigning authorisation and access rights according to the role group members play. Grouping is performed according to defined attributes characterising the group. Such attributes could be qualifications and skills as prerequisites for assigned roles, commonly accepted groups (general professions, legally-defined or regulation-defined groups), etc. For enabling open systems and communication across the border, efforts have been undertaken to harmonise attributes by SDOs (Standard Developing Organisations), e.g., by establishing an international healthcare profession nomenclature [3, 4].

For assigning authorisation and access control to specific principals as group members, attribute certificates must be bound to ID certificates. The Public Key Infrastructure (PKI) needed has been standardised internationally by ISO with the recently approved ISO TDS 17090 "Public Key Infrastructure" [5] and at European scale by CEN/ISSS (Comité Europeéan de Normalisation/Information Society Standardisation System) and ETSI (European Telecommunications Standards Institute) with the European Electronic Signature Standard Initiative (EESSI) [6]. Beside the technical harmonisation, the European Union established also a legal harmonisation for establishing electronic signatures: the EU 99/93/EC "Directive on Electronic Signatures". Contrary to the harmonisation for ID-related certificates, attributes such as specialty, subspecialty and medical disciplines as well as related authorisations (rights and duties) are mostly different. If, e.g., prescriptions are a privilege for Germany's doctors, in Norway this activity is performed by nurses. Therefore, before an agreed terminology and ontology has been introduced, the services (acts) being provided are a better characteristic for defining harmonised roles. Such services are, e.g., observation, physical examination, prescription, nuclear treatment, surgical treatment, anaesthetic preparation, collection of specimen, order, billing.

There are several ways for binding key-related ID certificates to key-less attribute certificates: the monolithic approach, the autonomic approach, and the approach of chained signatures. In the monolithic approach, the attribute certificate is part of the ID certificate. In the autonomic approach, some relevant information in the ID certificate is referred to bind with the attribute certificate. In the binding approach using chained signatures, the ID certification authority's signature is referred to bind with the attribute certificate. The mentioned ISO TDS 17090 fixed the first approach [5].

Figure 1 presents the author's HL7 Human Resources information model adopted and presented to the Interoperability Summit of OASIS, CORBA, and other SDOs for managing personnel information including roles, authorisation, certificates and prerequisites.

Considering roles, two specialisation of roles might be distinguished: organisational or structural roles on the one hand and functional roles on the other hand. Organisational roles are established by relationships between entities such as organisations and/or persons. Functional roles are created by acts.

The structure-related role of an HP defines his/her position in the organisational hierarchy of the institution reflecting responsibility and competence of the professional. This schema is a rather static one. With respect to the access control procedures it describes a mandatory model. For this paper out of scope examples of structure-related (organisational) roles of organisation are Naming Authority, Registration Authority, Certification Authority, Physician's Chamber. Examples for structure-related (organisational) roles of healthcare professionals (HCP) in health care systems reflecting decreasing access rights are: medical director, director of clinic, head of the department, senior physician, resident physician, physician, medical assistant, trainee, medical student, head nurse, and nurse.

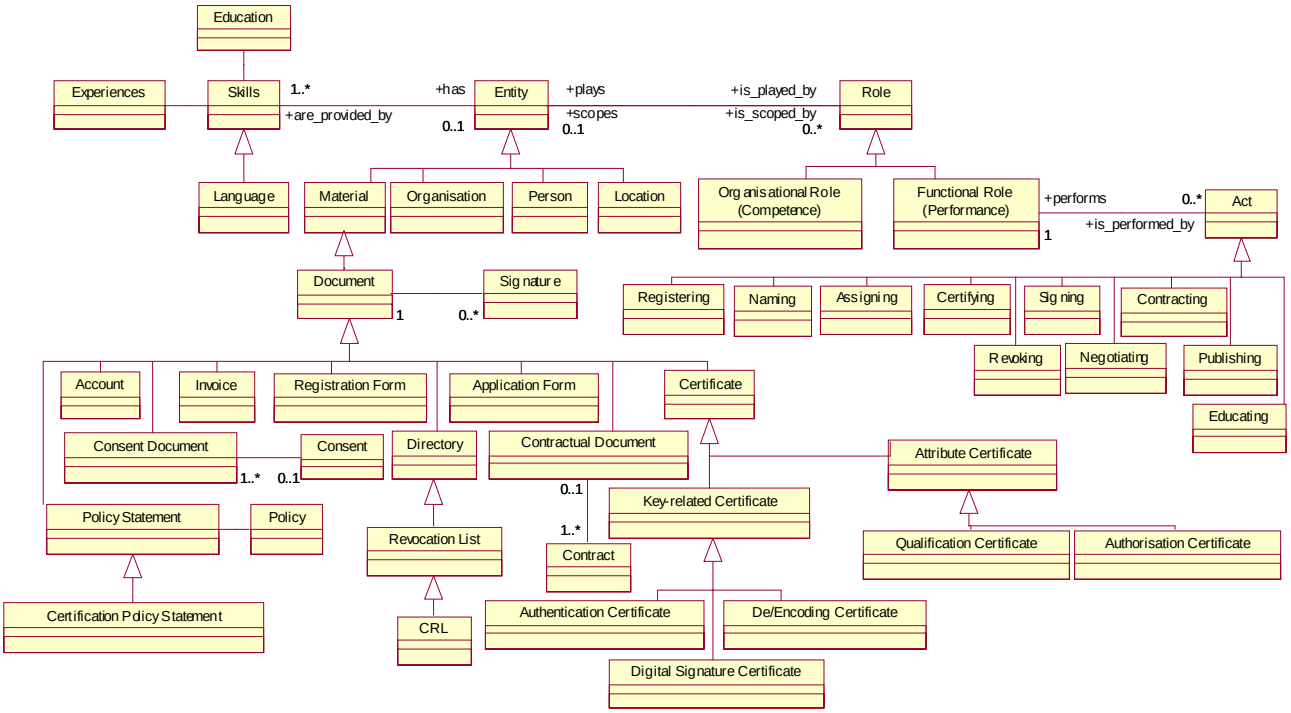

Figure 1. HL7 Human Resources (Class Hierarchy) Information Model

The function-related role of an HP immediately reflects the position in the healthcare process, i.e., the concrete HCP-patient relationship. It represents a highly dynamic relation, which follows discretionary model approaches. Examples for function-related roles in health care systems reflecting decreasing access rights are: **c**aring doctor (responsible or reliable doctor[1]), member of diagnostic team, member of therapeutic team, consulting doctor, referring doctor, attending doctor, family doctor, attending nurse.

Both roles define the rights and duties of an HP in an Health Care Establishment (HCE). Because HPs fulfil obligations in both the organisational and the functional framework, the resulting access control model combines these two views. According to the codes of conduct, the data protection legislation and the European Data Protection Directive, in most of the democracies the function role dominates the access control model in health information systems. Details are given in [7].

4: EHCR Standards

As kernel of health information systems, EHCR has to meet requirements investigated, e.g., in the context of several EHCR projects. Managing objects, an EHCR arises as dynamic process from clinical practice. It performs a complex workflow connected with medical acts. The EHCR is based and supports electronic communication between all parties involved. It documents any diagnostic and therapeutic measures in a standardised structure. Reducing or avoiding redundancy, an EHCR facilitates an optimised unambiguous presentation of medical concepts, preserving the original context and enabling new ones. It reflects chronology and accommodates future developments and views. For managing an EHCR system, the architecture of such distributed and highly complex component system as well as its behaviour (functionality, set of services) must be designed appropriately. The CEN prENV 13606 “EHCR communication” defines in its part 1 an extended component-based EHCR architecture. Such an extended architecture is mandated to meet any requirements through the EHCR’s complete lifecycle. Distributed component-based EHCR systems enable the aggregation of those components needed in a specific context. Beside this single model approach, a dual model approach is currently under international development, not influencing the security-related statements made however [8].

5: Authorisation and Access Control Services

For managing a highly distributed EHCR architecture, distributed component technology is the king’s way for developing a serviced architecture that provides any services needed to run an EHCR system properly, such as patient identification, patient record information location,

[1] In the health care system of several countries (e.g.UK), the family doctor is (or is intended to be, e.g., in Germany) the reliable doctor.

authorisation and access control dedicated to actors in the EHCR context.

For dealing with authorisation and access control services in component-based information systems, different approaches have been developed. These services are components themselves offering specific behaviour depending on the policy established within the domain and its corresponding principle as well as actual requirements. Acknowledging that only the policy but not the services is domain-specific, the CORBAmed Task Force specified a domain-independent Resource Access Decision (RAD) Service. This facility realises de-coupling of authorisation logic from application logic. This allows application development being independent from a particular access control policy.

The RAD service extends the underlying security infrastructure that provides both authentication of users the ability of an application to protect any resources stewarded by application logic. It supports the naming of resources and the definition of patterns for resource names in a standardised format to facilitate management of fine-grain access control policy at the level of granularity required by an application end-user community. It also allows the definition of arbitrary operations on these resources and the independent protection of those operations. The framework provides administrative interfaces that allow access control policy engines to be "plugged in", thus accommodating integration of existing policy engines and/or user written policy evaluators. The RAD framework was designed for accommodating environments with multiple policies established, e.g., administrative policies, legal policies, etc. Therefore, the understanding how to locate and to combine policies for making access decisions is needed. The facility manages authorisation and access control meeting both organisational and functional roles. Modelling the security related basic use cases of component-based information systems, the use cases

- PolicyManagement,
- UserManagement,
- RoleManagement,
- UserAuthentication,
- PatientConsent,
- CommunicationInitialisation,
- InformationRequest,
- AccessControl,
- InformationProvision,
- InformationTransfer, and
- Audit

can be separated [9].

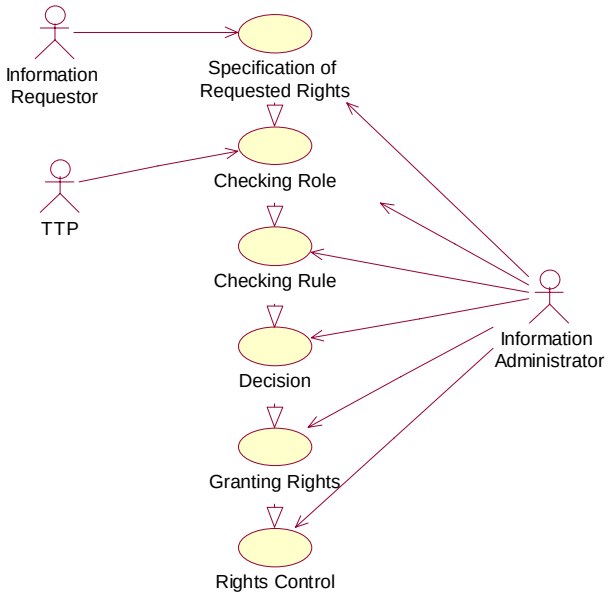

Figure 2. Security-Related Basic Use Case AccessControl

These basic use cases can be refined as shown in figure 2 for the Access Control basic use case example and in figure 3 refining the decision sub-component according to the RAD specification.

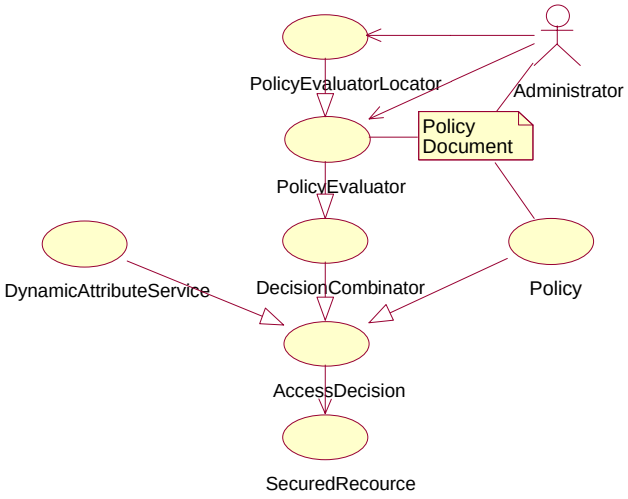

Figure 3. Refined Use Case ResourceAccessDecision

6: Security Infrastructure Enabling Healthcare Networks

The trustworthy environment needed for healthcare communication and co-operation is based on specification and implementation of the aforementioned security serv-

ices. Most of these services deploy cryptographic algorithms. For applying asymmetric algorithms such as RSA or elliptic curves, e.g., to provide services for both communication security and application security, such as authentication, accountability, integrity and confidentiality, a security infrastructure has to be established. In Europe, such Public Key Infrastructure (PKI) is based on token for storing the private keys and for processing (signing and verifying) the digital signature mechanism and encoding/decoding as well as on appropriate Trusted Third Party (TTP) services.

At both the European and the German national level, smart cards for health professionals have been standardised as proper token [3, 4]. These Health Professional Card (HPC) standards specify 3 keys for authentication, digital signature and encoding/decoding information or symmetric session key as well as corresponding key-related certificates, but also attribute certificates certifying the card holder's role-defining attributes. For enhancing flexibility in policy and role definitions as well as in role/attribute assignment, especially attribute certificates should be stored and managed on a specific attribute server. Also the legal, organisational and functional infrastructure framework has been specified in Europe as mentioned already.

Supported by several European project's results, the first German demonstrator of an Internet-based secure healthcare network following these standards has been implemented by the Magdeburg Medical Informatics Department. Exploiting experiences about secure communication using strong authentication, encryption, etc. over analogue lines since 1993 or over ISDN lines since 1995, the infrastructure based on HCP and TTP services started its routine use in 1999. This open network aims to facilitate shared care of cancer patients in the region, therefore it is called ONCONET Magdeburg / Saxony-Anhalt. ONCONET enables secure communication of any sensitive multimedia information, but also some application services like secure information retrieval from cancer registry by authorised HP using predefined or free Structured Query Language (SQL) queries. More details about ONCONET can be found in [10].

Regarding the aforementioned application security issues of registries concerning application services (implemented components with their data, operations, restrictions, etc.), following problems could occur. Registries might be organised centrally or decentrally. The former are characterised by separating the site recording information and therefore being responsible for it from the site storing and offering information retrieval. If a registry is centrally organised, the problem of trust whether policy and following authorisation and access rights are correctly enforced occurs. If the registry is decentralised, the management of the entire system requires an adequate architectural solution which isn't in place normally. However, even nowadays Web solutions using component distribution do not support policy enforcement.

For enhancing clinical registry's functionality, specification and implementation of enhanced EHCR interoperability, clinical studies and measures for quality assurance such as quality assurance studies are currently under development. Like the current ONCONET, also these applications have to be trustworthy, interoperable and shall run at the open Internet. They have to use the security infrastructure of HPC and TTP services. Any proprietary architecture shall be avoided.

7: The HARP Cross Security Platform

Real interoperability leads to a closer connection of both communication and application security services. Within the European HARP project funded by the European Commission within the Information Society Technologies (IST) Programme, partners from Greece, Germany, Norway, United Kingdom and The Netherlands specified, developed and implemented enhanced security solutions and TTP services for Internet-based communication and applications [11]. The HARP project's objective is building up entirely secure applications in client-server environments over the Web.

To provide platform independence of solutions in HARP as a real three tiers architecture, the design pattern approach of developing a middleware-like common cross platform called HARP Cross-Security Platform (HCSP) has been used. In HCSP, platform-specific security features have been isolated. Using an abstraction layer, communication in different environment is enabled. According to the component paradigm, an interface definition of a component providing a platform-specific service specifies how a client accesses a service without regard of how that service is implemented. So, the HCSP design isolates and encapsulates the implementation of platform-specific services behind a platform-neutral interface as well as reduces the visible complexity. Only a small portion The solutions concern secure authentication as well as authorisation of principals even not registered before, deploying proper Enhanced TTP (ETTP) services [11]. Especially, it helps to endorse policies by mapping them on processing components. Figure 4 demonstrates the HARP ETTP compared with a traditional TTP.

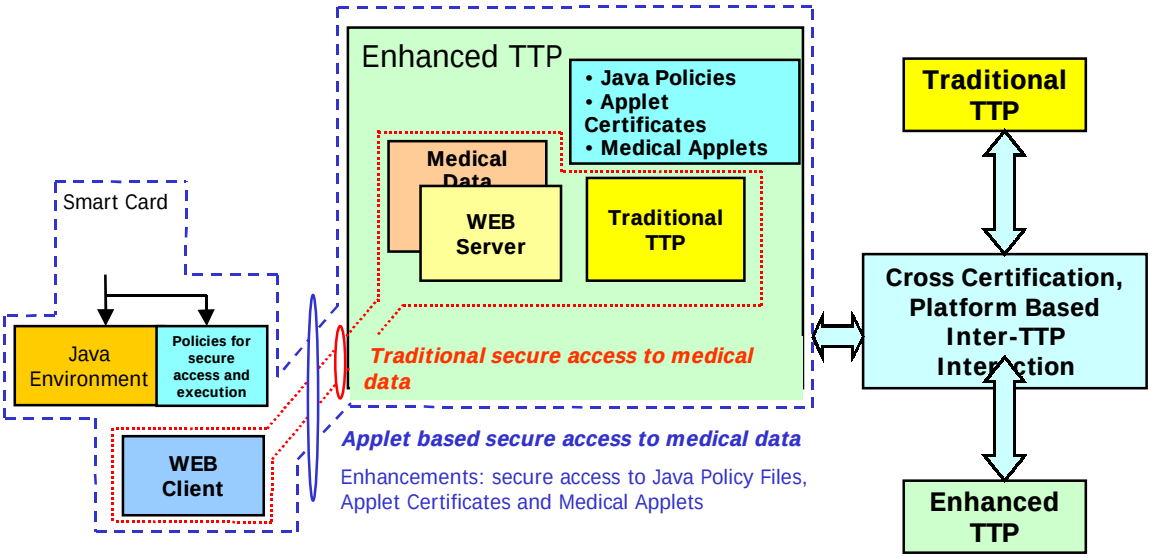

Figure 4. HARP Enhanced TTP vs Traditional TTP [11]

HARP's generic approach implements several basic principles.

HARP's embedding security into any application to be instantiated over the web-based environment outlined above is based on object oriented programming principles. It is based on Internet technology and protocols solely. The trustworthiness needed has been provided by applying only certified components which are tailored according to the principal's role. In fine-grained steps, it establishes its complete environment required, avoiding any external services possibly compromised. After strong mutual authentication based on smartcards and TTP services, the security infrastructure components are downloaded and installed to be used for implementing the components needed to run the application as well as to transfer data input and output. The SSL protocol deployed to initiate secure sessions is provided by the Java Secure Socket Extension API. The applets and servlets for establishing the local client and the open remote database access facilities communicate using the XML (Extended Markup Language) standard set including XML Digital Signature. Because messages and not single items are signed, the messages are archived separately for accountability reasons meeting the legislation and regulations for health.

Policies are dynamically interpreted and adhered to the components. All components applied at both server and client site are checked twice against the user's role and the appropriate policy: first in context of their selection and provision and second in context of their use and functionality.

Applet security from the execution point of view is provided through the secure downloading of policy files, which determine all access rights in the client terminal. This has to be seen on top of the very desirable feature that the local, powerful, and versatile code is strictly transient and subject to predefined and securely controlled download procedures. All rights corresponding to predefined roles are subject to personal card identification with remote mapping of identity to roles and thereby to corresponding security policies with specific access rights.

For realising the services and procedures described, an applet consists of the subcomponents GUI and interface controller, smartcard controller, XML signing and XML processing components, communication component applying the Java SSL (Secure Socket Layer) extension, and last but not least the data processing and activity controller. Beside equivalent subcomponents and an attribute certificate repository at the server side, policy repository, policy solver and authorisation manager have been specified and implemented as a "light weight RAD".

After exchanging certificates and establishing the authenticated secure session, servlet security is provided from the execution point of view through listing, selecting and finally executing the components to serve the user properly. By establishing an authenticated session that persists for all service selections, a single-sign-on approach can be realised.

In the server-centric approach, a web-accessible middleware has been chosen based on its support of basic security functionality, e.g., MICO/SSL., Apache Web server with mod_ssl, Apache JServ, and Apache Jakata Tomcat.

The next figure (Figure 5) exemplifies a logic for assigning and authorising a user regarding both organisational and functional roles [12, 13].

User_role (user, role, unit, validity_flag) ←
User_position (user, position, unit) ∧
Unit_role (role, position, unit, object_type, actor)

Role_authorisation (role, unit, object_type, transaction, state) ←
Unit_role (role, position, unit, object_type, actor) ∧
Transaction_mode (object_type, transaction, state, action)

Figure 5. Logic for Assigning and Authorising a User [12]

Combining the server-centric approach of HCSP, its server-centric approach and the network-centric VPN behaviour, the completely distributed HARP Cross Security Platform can be designed as shown in figure 6.

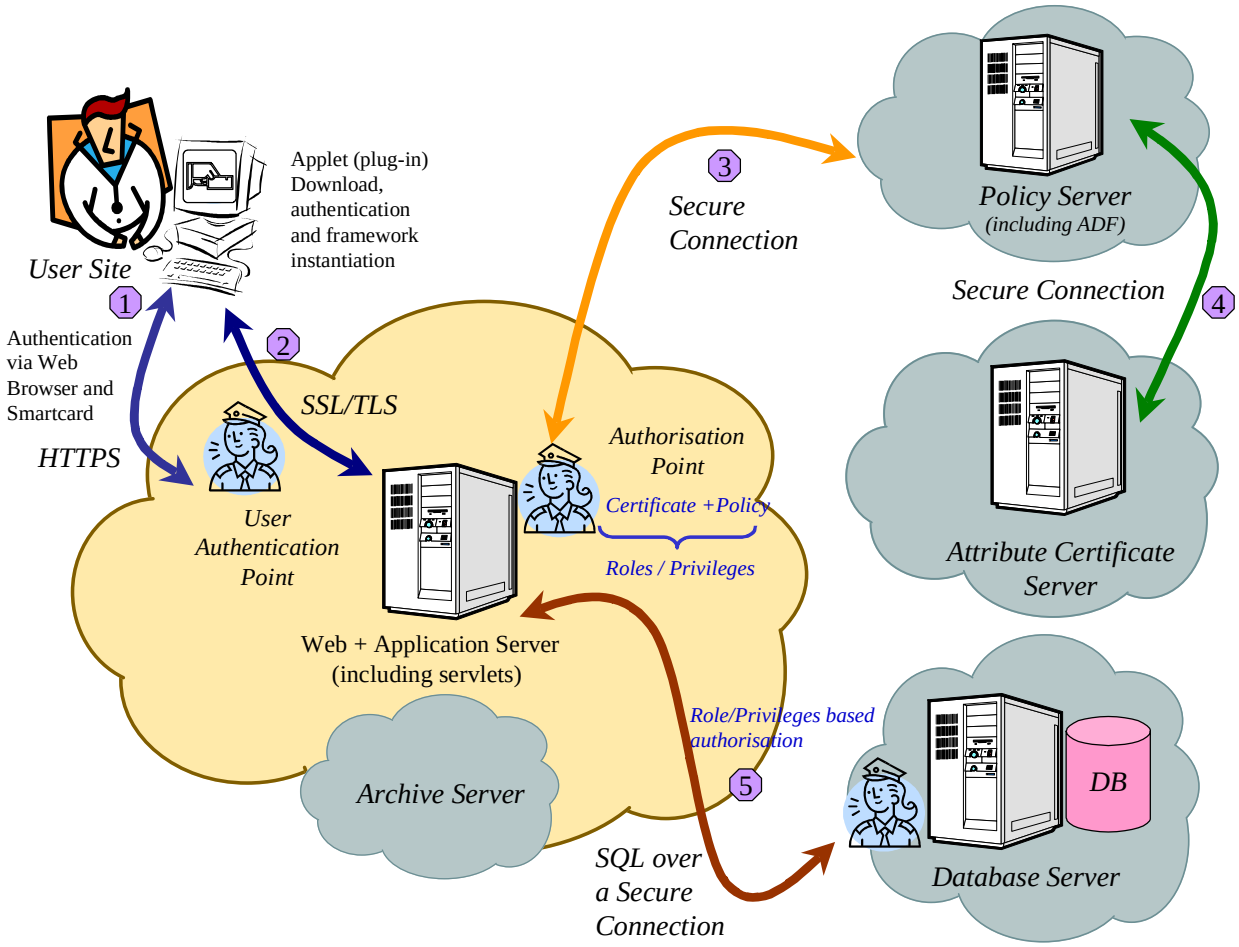

Figure 6. HARP Cross Security Platform [11]

8: The Clinical Study HARP Demonstrator

Clinical studies can be interpreted as an EHCR subsystem. According to CEN prENV 13606 "Electronic Healthcare Record Communication", Part 1 "Extended Architecture" it comprises with a Folder Original Component Complex. Therefore, clinical studies which claim increasing importance in the context of improving quality and efficiency of diagnosis and therapy are an acceptable model for evaluating the HARP Cross Security Platform as an trustworthy EHCR approach.

To establish clinical studies, components for remote data entry must be distributed to authorised parties. Fur-

thermore, these components perform comprehensive services for quality assurance (QA), e.g., plausibility checks and more. The components' functionality must be different according to the different user's roles. In that context, study partners (documentation instances) collecting information, documentation personnel recording data, QA team members (proof instances) checking the information, and the study co-ordinator managing the roles, rules, procedures, etc. fixed in the policy must be served establishing different rights (create, read, write, update, delete) on the one hand and granting rights on the other hand. Finally, a study council has to be included which defines and controls the policy agreed upon.

The clinical study schema presented has been applied to a quality assurance study in paediatric endocrinology performed at the German national level (Figure 7).

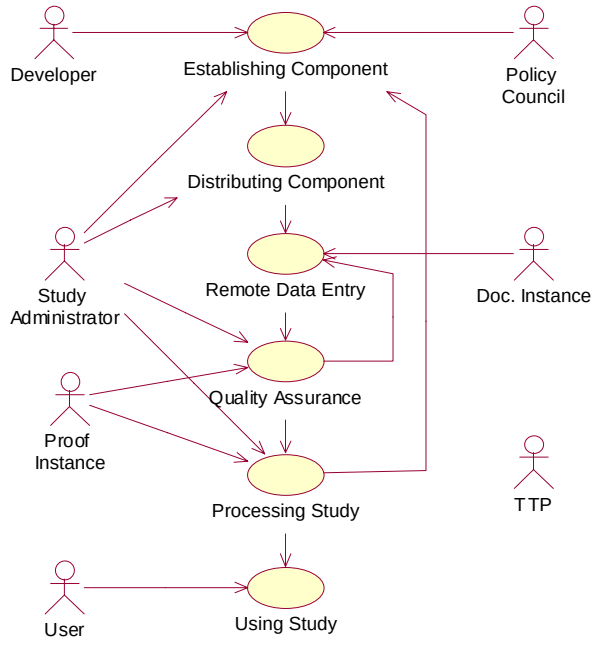

Figure 7. HARP Clinical Study Demonstrator Use Case Diagram

9: Conclusions

The HARP project's objective is building up open and entirely secure applications in client server environments over the Web by embedding the fine grained security into the application. Within a real three tiers architecture, the HARP solutions concern secure authentication as well as authorisation of principals even not registered before deploying proper Enhanced TTP (ETTP) services. By associating role profiles and security attributes to standard Web-based interactions, HARP provides an initial degree of 'automation' in building secure medical Internet-based applications. Moreover, it clearly separates and demarcates security and policy related issues according to the component paradigm. This enables administrative bodies acting as 'policy councils' to define off-line and according to the standing legislation all procedural regulations without entering into implementation details. Standard security mechanisms such as, e.g., SSL and IPsec are accommodated. Applets and servlets are generic easing any client as well as supporting any given database schema. Therefore, the HARP solution offers open XML driven client-server interactions. Specification and implementation of components are facilitated by an XML-specified component generator.

The HARP demonstrator presented has been developed using UML (Unified Modeling Language) and the Rational Rose ® methodology. This direction will be enhanced by developing further graphic and model tools as a comprehensive HARP development environment.

In the near future, the HARP approach will be improved by adopting other open specification such as specific CORBAmed services.

10: Acknowledgement

The author is in debt to the European Commission for funding as well as to the international and national HARP project partners for their support and their kind co-operation.

11: References

[1] Blobel B, Bleumer G, Müller A, Louwerse K, Flikkenschild E, Ottes, F: Current Security Issues Faced by Health Care Establishments. ISHTAR Project HC 1028, Deliverable 09 (Final), February 1997; see also Barber B (edr.): Implementing Secure Healthcare Telematics Applications in Europe - ISHTAR. Studies in Health Technology and Informatics, Vol. 66. IOS Press, Amsterdam 2001

[2] OMG: The CORBA Security Specification. Framingham: Object Management Group, Inc., 1995, 1997.

[3] CEN TC 251 prENV 13729: Health Informatics - Secure User Identification – Strong Authentication using Microprocessor Cards (SEC-ID/CARDS). Brussels, 1999.

[4] The German HPC Specification for an electronic doctor's license. Version 1.0, July 1999. http://www.hcp-protocol.de

[5] ISO DTS 17090 "Public Key Infrastructure" Part 1 - 3. ISO, 2001.

[6] Council of Europe: 99/93/EC: Directive on Electronic Signatures. Strasbourg, 1999.

[7] Blobel B: Modelling for Design and Implementation of Secure Health Information Systems. International Journal of Bio-Medical Computing **43** (1996) S23-S30.

[8] Thomas Beale: An Interoperable Knowledge Methodology for Future-proof Information Systems. Deep Thought Informatics Pty Ltd, 2001.

[9] Blobel B, Roger-France F: A Systematic Approach for Analysis and Design of Secure Health Information Systems. International Journal of Medical Informatics **62** (3) (2001) pp. 51-78.

[10] Blobel B.: Onconet: A Secure Infrastructure to Improve Cancer Patients' Care. Eur. J. Med. Res. 2000: 5: 360-368.

[11] The HARP Consortium: http://www.ist-harp.org

[12] O Y.-L, A life-cycle based authorisation expert database system in artificial intelligence in medicine, In: W. Hom et al. (Eds.), Lecture Notes in Artificial Intelligence 1620, pp. 153–157. Springer, Berlin, 1999.

[13] Blobel B: Application of the Component Paradigm for Analysis and Design of Advanced Health System Architectures. International Journal of Medical Informatics **60** (3) (2000) pp. 281-301.