A Proposed Solution for Managing Doctor's Smart Cards in Hospitals Using a Single Sign-On Central Architecture

Christian Mauro Ali Sunyaev Jan Marco Leimeister Andreas Schweiger Helmut Krcmar

Technische Universitaet Muenchen
Information Systems
Boltzmannstrasse 3
85748 Garching b. Muenchen, Germany
{mauro, sunyaev, leimeister, schweiger, krcmar}@in.tum.de

Abstract

This paper describes a single sign-on solution for the central management of health care provider's smart cards in hospitals. The proposed approach which is expected to be an improvement over current methods is made possible through the introduction of a national healthcare telematics infrastructure in Germany where every physician and every patient will automatically be given an electronic health smart card (for patients) and a corresponding health professional card (for health care providers). This introduction will cause changes in many existing health care administrative processes. The example process of writing a discharge letter is used in the paper to compare two existing approaches for integrating the new smart cards to the proposed single sign-on approach. Based on the findings we support a centralized single sign-on card management approach which allows us to exploit possible process improvements now and in the future. In closing we outline further application potentials of the described approach for management of smart cards in health care and, in particular, in hospitals.

1. Introduction

The use of networked information technology across the boundaries of institutions and sectors is a potential opportunity for increased efficiency and better delivery of health care [7]. It creates numerous possibilities such as improved communication between health care providers and patients [12], smoother transfer of information across electronic boundaries [16], lower costs [10], increased access transparency, and improved treatment quality and safety [9]. An essential step towards the implementation of this system will be the introduction of an electronic healthcare smart card (eHC) for patients and a counterpart health professional card (HPC) for care providers. These cards will form an essential part of the comprehensive and nation-wide telematics infrastructure currently being developed. At the time this paper is being written, practice tests in selected regions of Germany are in progress. The eHCs will be mandatory for every German citizen. Furthermore, each healthcare provider will be required to have an HPC card. Both cards will have a clearly defined structure and set of functionalities. Thus, it will not be possible to add additional functionalities or to create additional certificates. This makes it very difficult to use the cards for further purposes.

The creation of these cards leads to considerable adaptations to everyday work processes of care providers in hospitals. Because these changes are so pervasive, this allows us the possibility of reengineering the given processes and to possibly deploy a new and viable solution for the management of the smart cards in hospitals. Such a solution would potentially achieve improvements in current processes both in terms of efficiency and effectiveness. For this purpose we need to take into account the requirements of an adequate and seamless integration of the HPC into business processes and the given IT infrastructure [14, 17]. The central issue needing to be addressed is the missing support of the efficient deployment of a comprehensive amount of smart cards. Smart Carts are typically used for different purposes such as single sign-on (SSO) access to systems or as company identification cards. Thus, there is expected to be a large number of them already in use in any typical health care facility such as a hospital.

This paper is structured as follows: In Section 2 we describe the forthcoming nation-wide German telematics infrastructure in more detail. In Section 3

1530-1605/08 $25.00 © 2008 IEEE

the new smart card based processes are shown on a typical administrative process that is commonly carried out in clinical practice. Since there already exist other approaches for managing clinical smart cards, we outline these in Section 4. Section 5 presents the description of our proposed smart card management solution which is a centralized approach. In order to demonstrate the advantages of our proposed approach, we compare it to the other approaches in Section 6. In Section 7 we discuss the advantages of the proposed approach over the other approaches.

2. The German Health Telematics Infrastructure

Advances in communication infrastructure have aided the introduction of the electronic patient card in Germany. A telematics infrastructure is used as the basis for this mandatory electronic patient card system. Figure 1 depicts an abstract overview of the architecture to be used for Germany's forthcoming nation-wide health system. This infrastructure was created by an institution called gematik (we refer to this infrastructure as gematik when comparisons are performed in this paper) In general, the gematik infrastructure connects existing information systems of various service providers and health insurances via a common network. The requirements for the development of this infrastructure are derived from legal constraints, current standards, and the demands of the participating stakeholders.

Primary systems (e.g. a hospital information system) of service providers (i.e. general practitioners or hospitals) are connected to the communication infrastructure (CI) by a special component namely a so-called connector. This connector communicates with the primary systems and the card terminals for the eHC, the HPC and the secure module card (SMC). SMCs are used to create secure connections either between components (e.g. between a VPN Box and the CI) or smart cards. The communication between the connector and the card terminals is transparent to the user and is encrypted automatically. The connector is connected to a so-called VPN box (virtual private network unit). Connection to the communication infrastructure is established via an access gateway. Access gateways allow only registered users to access the communication infrastructure. A certificate within the used access node enables the mapping to an appropriate VPN. A special user role is associated with the mapping to a dedicated VPN. The service gateway contains a list specifying the mapping between possible roles and rights for using the application services. These rights specify which services of the user's VPN can be used. Access gateways and service gateways communicate via a trusted backbone, with components mutually authenticating themselves and connecting via a VPN. These measures allow only those users possessing the appropriate roles the power to execute application services which then invoke these services via access gateways. Dedicated VPNs are capable of calling infrastructure services.

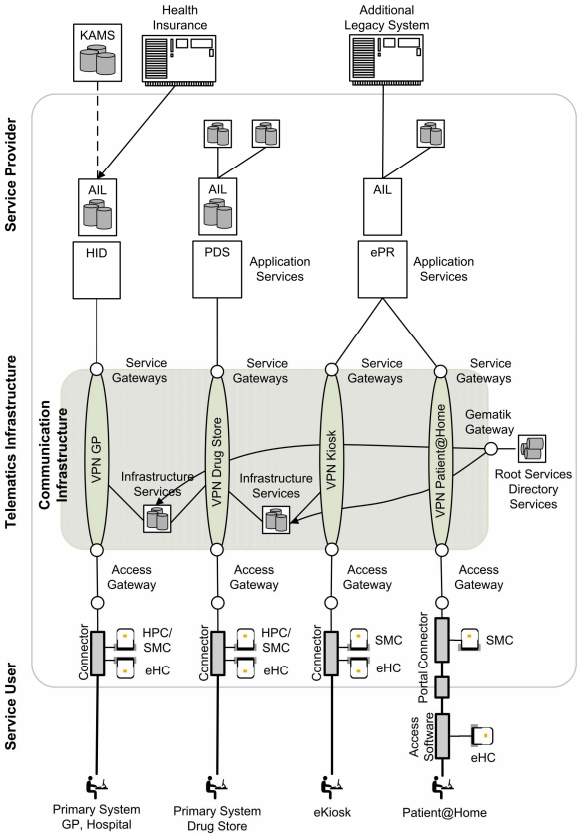

Figure 1. Architecture of the German health telematics infrastructure [13]

Application services, such as access to an electronic patient record (ePR), a prescription data service (PDS), or a health insurance data service (HID), can be called via service gateways. Application services access relevant data via a common access and integration layer (AIL). This layer implements a common rights management for the access to data which allows for mapping of appropriate rights to users. The AIL layer also hides the actual distribution of data and implements storage transparency. This encapsulation facilitates the future extension for the integration of external systems since the interfaces of the application services will not need to be adapted. For this instance a so-called gematik gateway allows access to root and

directory services which are necessary for the administration of the network.

The user is not faced with the complexity of the telematics infrastructure. He or she uses the new functionality via a graphical user interface front end of the hospital information system (this means that every manufacturer has to adopt existing software to the new telematics infrastructure). Depending on the selected solution for managing this infrastructure, the user has to insert a smart card and type in a PIN from time to time. It is this need for inserting the eHC or HPC card plus typing a PIN that will be used in evaluating each potential infrastructure solution for this health care system.

3. Induced Process Changes

3.1 General Changes

The introduction of the eHC implies changes in medical processes. The HPC will especially become an essential part of everyday work in hospitals. Medical information about a patient can only be accessed by using the HPC in connection with the HPC authentication PIN (PIN.AUT). Furthermore, all medical documents will have to be signed by physicians using the HPC in connection with the signature PIN (PIN.SIG). The usage of different PINs for authentication and signature is already defined in the HPC specification. Dealing with these processes requires the physician to spend more time handling the HPC and the PINs, especially if there also exist additional smart cards (e.g. for Single Sign On requirements (SSO)). The process of issuing a discharge letter is one of the typical processes physicians perform frequently. We use this discharge process to demonstrate the described card insertion and PIN typing activity.

3.2 Discharge Letter Process

The conventional process of issuing a discharge letter is shown on the left side of Figure 2.

Figure 2 illustrates work processes using an extended EPC notation. The notation is derived from the well-known Event Driven Process Chains [EPC, 8].[1] Functions are represented by rectangles with rounded corners and denote tasks. Events (left out in our modified notation) trigger functions and show their completion.

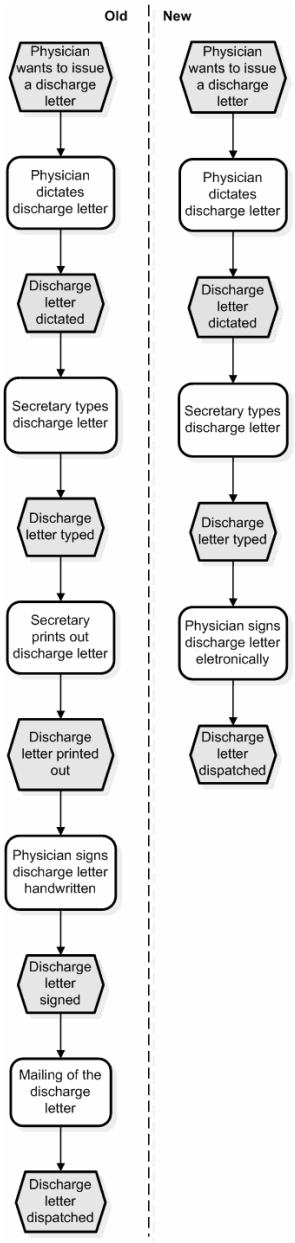

Figure 2. Old and new discharge letter process

Nowadays physicians usually dictate discharge letters. A secretary is responsible for typing and printing the letter. Physicians sign the document, and afterwards, the letter can be mailed to the family doctor.

In the new process (right side of Figure 2) the discharge letter is signed electronically. This means that printing the letter is no longer necessary. In addition there is no need to mail the document. The

[1] For an overview of references on the EPC notation see e.g. the publication list of the Special Interest Group on Process Modelling with EPCs at the German Informatics Society website (http://www.epk-community.de/).

letter is stored within the health telematics infrastructure and is thereby directly accessible by the family doctor.

At first glance the new process looks quite simple and several prior steps can now be omitted. The process change means that now the physician has to sign the discharge letter electronically. Thus, the doctor has to login on a computer, insert a personal HPC and type a PIN.AUT and a PIN.SIG. If an SSO card is required for the login, the physician has to handle two smart cards both with PINs. Furthermore, every time a physician changes a workstation, the cards need to be removed and inserted in the new workstation. In addition the input of different PINs is again necessary (SSO PIN, PIN.AUT, and PIN.SIG). Since physicians are highly mobile, moving from patient to patient, this creates a significant amount of busywork in the physicians' day. Therefore, an adequate smart card management solution has to be introduced, which simplifies the described work process.

4. Existing Approaches for Managing Smart Cards in Hospitals

According to the telematics rules to be introduced, every physician will receive a new Health Professional Card and has to use it for authentication and authorization of activities such as signing prescriptions, accessing electronic patient records, etc. There now exist two basic management approaches for smart cards in hospitals (The Decentralized Approach and the VerSA Approach). We will describe and contrast these two approaches and use them to suggest a third new approach: The universal clinic card approach.

4.1 The Decentralized Approach

The decentralized approach is the "official" solution, currently being tested in selected regions in Germany (with reduced range of functions). According to the complete health telematics infrastructure specification [3], every workstation has an SICCT (Secure Interoperable ChipCard Terminal) component (Figure 3, right side). An inserted HPC card permits its owner to perform processes such as signing prescriptions or accessing patient data. Communication with the central telematics infrastructure (CTI) is facilitated by the connector. When a person leaves the workstation, the HPC is ejected and must be removed.

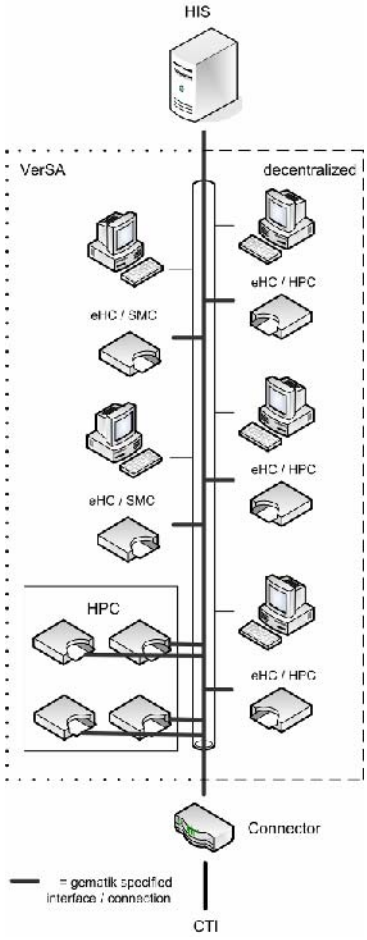

Figure 3. VerSA (left) and decentralized approach (right)

4.2 The VerSA Approach

The VerSA concept [1] ("Verteilte Signatur Arbeitsplätze", an acronym meaning distributed signature workstations) has been developed by the German Federal Association of Pharmacists. This approach (Figure 3, left side) requires the HPC to be inserted into a central server card terminal. Each workstation is equipped with an SICCT component. A secure connection to the HPC is established via SMCs (which are inserted at the SICCT). This allows the user to make use of the functionality that is normally provided by the HPC without actually needing to physically insert the card in each workstation.

Currently no hardware has been built for this concept. Thus, it cannot be tested or practically compared with other solutions.

4.3 Disadvantages

The problem with these existing two approaches is that they are not specifically designed for hospitals' needs. They may work fine for a general practitioner with a small number of computers and therefore a small number of expensive SICCTs. In hospitals a multitude of SICCTs would be needed. In addition, besides the HPC, other smart cards will often be in use for operating other functions of the hospital. Thus, the user may have to handle more then one smart card and may also be faced with other controls for system access. These disadvantages motivate developing a new approach that considers the special needs of hospital environments.

5. The Clinic Card Approach

For a better handling of the multitude of smart cards, a completely centralized approach for smart card management in hospitals (Figure 4) has been developed. The approach is based on a smart card management unit (SCMU, also called smart card safe) which stores HPCs in a secure way as well as a multifunctional smart card (so called clinic card (CC)) which has a well-defined association to an HPC. The overall idea is: The aforementioned smart card unites all functionalities of other already deployed smart cards and therefore reduces the number of smart cards to be handled by the medical personnel.

At the beginning of a workday the user puts his HPC (and maybe further signature cards) into the SCMU. After that he or she only needs a CC and CC PIN for all purposes. To avoid queues and to be able to manage a large number of users, there can be many SCMUs, distributed throughout the medical complex. In addition the mechanism for placing cards in the SCMU should be very easy and quick.

5.1 Technical Architecture

The system consists of the following four components (Figure 5): SCMU, CC, card middleware, and connector. SCMU and CC (via the middleware) are accessed by the connector which only acts as the central access point for the hospital information system (HIS). The connection to the telematics infrastructure is established via the VPN box.

The SICCT interface of the SCMU and the main parts of the connector are specified by the gematik requirements. In addition customized functionalities are necessary for the Clinic Card Solution. Thus the SCMU and the connector each have distinct subunits which perform the gematik connection and the customized functionality.

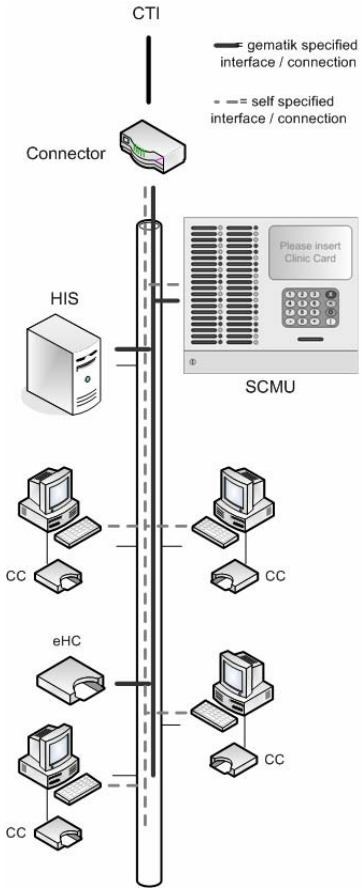

Figure 4. Central management approach

5.2 Smart Card Management Unit

From a technical point of view, the SCMU is a multislot SICCT terminal. eHCs, HPCs, and SMCs are to be read exclusively by SICCT components. The SICCT interface describes the interaction with the connector. In addition a self-defined interface is necessary for the remote access to the HPC. The SCMU is provided with removal protection for inserted HPCs. An authorized removal is therefore only possible with the associated CC in combination with the CC PIN.

The user interface is quite simple. After inserting the CC and the corresponding CC PIN, the SCMU assigns a free card slot (noticeable on a flashing green LED). If the HPC is inserted the LED switches to solid green. The authentication PIN and the signature PIN of the HPC will be requested and stored encrypted on the HPC (which is the only allowed storage place according to German signature laws) for later usage.

The insertion of the PIN is done via a PIN-pad (similar to numeric pads on ATM machines) with coaching from screen displayed messages. The encryption keys are cut into two pieces: One half will be held inside the SCMU, the other half will be stored on the CC. After this process, the LED switches to red, indicating a busy card slot. In addition the CC will be ejected and must be removed by the user. (Otherwise the CC will be retracted and stored in a special box inside the SCMU.)

Because the SCMU acts as a central unit and holds multiple important chip cards, it must be made readily available to users. Thus, it is established with a redundant power supply as well as redundant network interface cards. In addition a software module on the connector monitors every SCMU. Furthermore, mechanisms are available for securely (i.e. access is only possible by authorized personnel) removing the inserted cards in case of a problem.

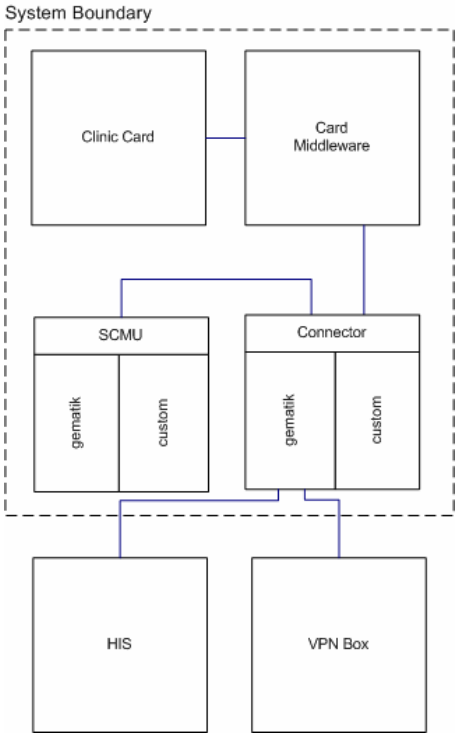

Figure 5. Component overview

5.3 The Clinic Card and Card Middleware

Once the HPC is inserted in the SCMU, at the user's workstation remote access to the HPC is possible with the use of the CC. The user only has to type in the CC PIN to use the functionality of the HPC. The CC PIN can also be used for initiating signatures. Alternatively, biometric data or RFID tags could be used as authorization mechanisms. In addition further applications can be used with the CC, such as SSO or canteen billing. For these purposes contactless identification systems like Legic (www.legic.com) or Mifare (www.mifare.com) can be integrated in the CC. In short, the user has one single smart card available for all needs. The CC can be read by a normal card reader in combination with the middleware installed on the workstation.

5.4 Connector

As shown in Figure 5, the connector has interfaces to internal and external components of the system. One important aspect of the Clinic Card Solution is that the interface to the HIS remains unchanged (in relation to the gematik requirements). Thus, the solution can be integrated into the hospital's IT infrastructure independently of the given HIS. This is essential because many different HIS exist in Germany [11].

Only a small modification to the conventional connector is necessary for using it in the context of the presented solution. Thus, it is relatively trivial and inexpensive to create a connector that is compatible with the proposed Clinic Card solution.

5.5 Remote Access

The SCMU acts like the usual SICCT component until an authentication failure occurs. This means, that a function needs a PIN insertion. For an HPC, this can be a PIN.AUT or a PIN.SIG. The complete remote access process is shown in Figure 6.

As a first step, the user chooses a function inside the HIS that needs an HPC access (1+2). The HIS calls the corresponding connector service (3). All this is transparent to the user. The connector tries to access the needed card (4). If a PIN is required for access, the SCMU responds with an authentication failure (5). Up to now, the process is identical to the other solutions (except for the location of the HPC). Because the presented solution doesn't need an SICCT component connected to the workstation, the PIN has to be typed directly at the workstation (6). However, instead of the HPC PIN, the CC PIN will be requested (7). After the user correctly types the PIN, the half key (saved on the CC) will be transmitted over secure connections to the connector (8). The connector now is able to initiate the authentication by transmitting the half key to the SCMU (9). Within the SCMU the half keys can be recombined with the encrypted half key stored at the SCMU. The combined key can then be used to decrypt the HPC PIN saved on the HPC. The PIN can now be used for authentication and the result of the card access will be sent to the connector (10). Finally, the connector forwards the result to the HIS (11) which

can finalize the called user function and present the result to the user (12).

This process looks quite complicated, but this is not a fault of the presented solution but a result of the way the telematics infrastructure and especially the connector work. Fortunately this process is transparent to the user. The user simply requests an HIS function, types the needed CC PIN and continues with the task.

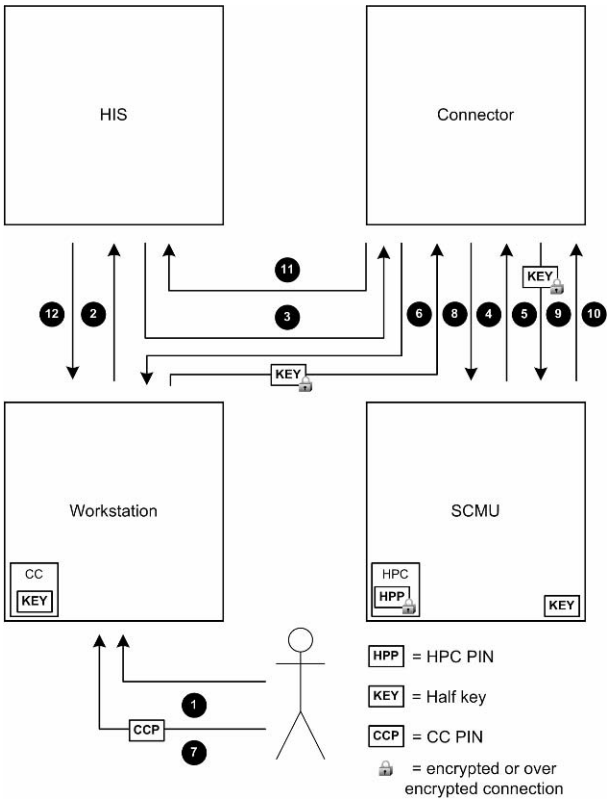

Figure 6. Remote HPC Access.

5.6 Unique Characteristics of the Central Approach

Initially, the centralized solution looks similar to VerSA, but there are some significant differences:

- No HPC PIN is transmitted through the network.
- At the workstations no expensive SICCT components are necessary. A conventional card reader will suffice (except for the patient check in workstations where patients´ eHCs have to be read).
- No SMCs are necessary inside the card terminals.
- Conventional card readers can be connected to the workstations instead of connecting them to the network. Thus no additional network ports are necessary.
- A multifunctional smart card (the CC) is in use.

The first three points are made possible by the use of a special remote access to the stored cards. As one can see on the second point, the eHC is not integrated into the presented solution yet because there are some legal issues to resolve. In addition, at this point in time, it is not foreseeable whether integration of eHC access makes sense. However, the integration of the eHC can be done at a later date with a simple software update.

5.7 Discharge Letter Process

This section again takes up the process of issuing a discharge letter that was described in Section 3.2. Assuming that an SSO card is used, the differences between the described approaches are shown in Figure 7.

The process begins at a point when the user is not yet logged in on a workstation. Thus, depending on the approach used, different mechanisms for logging in are necessary. As one can see, using the decentralized approach requires the insertion (and removal) of two different cards and the typing of three different PINs. The VerSA solution requires less busywork because the HPC is inserted in the server terminal and only the SSO card must be inserted every time the user switches to a different workstation. Nevertheless, the user still has to enter different PINs for the login process, the HPC authentication PIN and the signature PIN. The central approach requires only one smart card and only one PIN entry at a given workstation. This enables the physician to finish the process of issuing a discharge letter much faster (in comparison to the other approaches).

6. Comparison of the presented approaches

6.1 Evaluation Framework

Different evaluation methods exist for health care information systems [6]. For evaluating the described approaches, we make use of an evaluation framework introduced by [2] and [15]. According to this framework, the dimensions objects (approaches for card management), criteria (hardware requirements, session management, usability, additional value-adding aspects), and method (comparative procedures) are each handled separately in the evaluation.

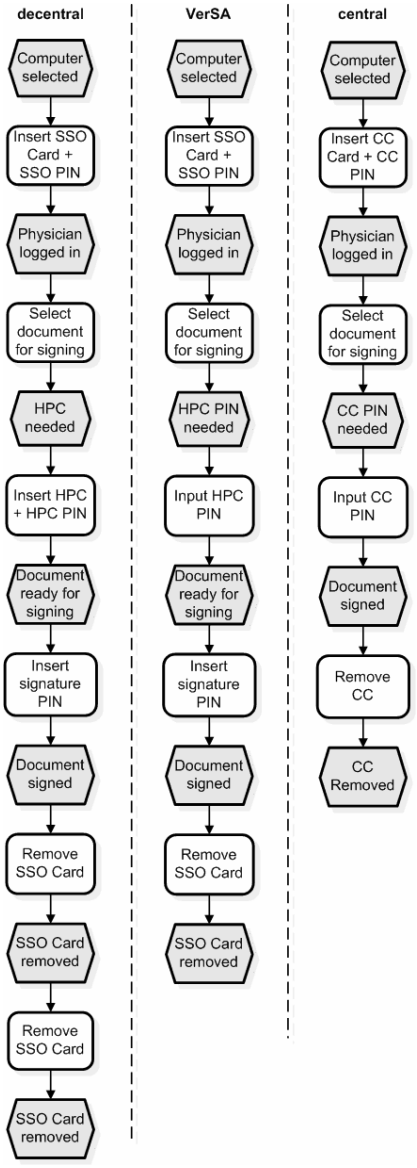

Figure 7. Discharge letter process comparison

6.2 Hardware Requirements and Integration

The decentralized gematik approach requires gematik-certified SICCT components to be installed at each workstation. Network enabled card terminals (connection via LAN) necessitate an additional network connection for each workstation. This can lead to a further extension of the given network infrastructure. Virtual card terminals (connections to the PCs) do not require their own network connection. However, the installation of special software, which is capable of exporting the SICCT interface is necessary [5].

The central VerSA concept requires, in addition to the decentralized approach, a server card terminal to be installed in order to provide central access to the HPCs. The amount of necessary server terminals is dependent on the number of employees and the spatial layout of the hospital. For a secure PIN transfer via the network there is also an SMC that is needed for each card terminal.

By pursuing the central clinic card approach there arise costs for obtaining the management components, the clinic cards and the card application management system (CAMS). The CAMS manages the data and applications stored on the CC. Furthermore, additional expenses are incurred for the purchase of the card reader terminals and the installation of the necessary terminal software.

The actual expenses for obtaining the hardware are dependent on a set of factors. Among these are the number of medical employees in a particular health care facility and, the expected market price for SICCT components (which will drop as demand increases). Since there can currently be no exact quantitative calculation of these basic conditions, we make the following assumption for the intended comparison: The expected hardware costs are comparable to each other. Therefore, in terms of hardware requirements, there is no advantage of one approach over another.

From an objective point of view there is a slightly bigger software and system effort when integrating VerSA or the Clinic Card Solution, because in addition to the placement of card terminals at each workstation, the server terminals have to be installed and configured. When using the Clinic Card Solution there is also an additional effort for the creation of CAMS. But as mentioned before, the German health telematics infrastructure is still in test stage. After tests are completed, a nation wide rollout of the system will begin. There will be a huge effort on the part of hospitals to integrate the new processes and hardware. Thus, the slightly bigger effort when integrating the Clinic Card Solution is not relevant.

6.3 Session Management

If an HPC is inserted into the card terminal, a set of actions for session management purposes is necessary [4]. Central approaches provide the advantage that this effort has to be carried out only once. In contrast, decentralized approaches require the repetition of these actions at each insertion of the HPC. As a result, every time a health care provider leaves one workstation, the actions described above need to be redone at the next workstation.

With the VerSA approach we need to consider that logical connections between SMCs and HPCs need to be established. Both the SMC and the HPC are capable of establishing only a limited number of connections. If this number is exceeded, previously established connections need to be closed. Therefore, parts of the session management need to be repeated again. When deploying the central clinic card approach, this problem does not arise, since no logical connections on the basis of SMCs for PIN transfer are necessary. In this respect the clinic card solution has advantages in comparison to the gematik and VerSA approaches.

6.4 Usability

The decentralized approach has the disadvantage for each user that the HPC authentication process has to be redone every time a new workstation is used. As a result, additional work steps are necessary especially for highly mobile physicians. Furthermore, there is a security risk because the HPC could be left unintentionally in one of the workstation card terminals. Centralized approaches provide a secure safekeeping for the HPCs throughout the workday. Additionally, the HPC can be used remotely, which leads to a simplification of work processes. If the multi-functional clinic card is deployed, the user has to handle only one card. This reduces busywork and increases security, especially in the hospital domain. The central approach has an enormous advantage with respect to usability in comparison to the gematik approach. Health care providers will especially benefit as well with respect to time savings and convenience.

6.5 Further Value-adding Aspects

Both the decentralized and the VerSA approaches are designed for HPC applications only. Therefore, no further value-adding scenarios can be supported. However, the central clinic card approach is capable of supporting a broad spectrum of use cases in hospitals. The clinic card can, in the proposed solution, be substituted for all deployed smart cards or contact-free media. Thus, with a single card, a person can open doors automatically, enter restricted parking garages, pay for canteen purchases, or sign on to various hospital management systems. Combining access to all of these functions on a single smart card reduces costs and supports the user in trivially managing a broad spectrum of applications.

7. Conclusion and Outlook

Table 1 summarizes the derived evaluation from Section 6. It is evident that the selection of adequate infrastructure fundamentally affects the possible benefits of smart card applications in hospitals. This is why such a selection decision should be made carefully. Furthermore, Table 1 shows that the single sign-on clinic card solution has significant advantages over present concepts described above, suggesting that the small amount of additional development to deploy this system is worth the extra effort and will reap benefits in a short time.

Table 1: Concepts for central management of smart cards in hospitals

Concept / Criteria	gematik Approach	VerSA Approach	Clinic Card Solution
Hardware Requirements	O	O	O
Session Management	-	O	+
Usability	O	+	+
Additional Value-adding Aspects	-	-	+
Legend: + most suitable O suitable - not suitable			

The clinic card solution we described is capable of being extended for use in accessing personal electronic health care records if electronic patient cards are deposited in the central smart card management unit and patient agreement is given. In particular, the introduced solution has the potential of providing a truly seamless healthcare system.

8. References

[1] ABDA, VERSA – Verteilte Signatur Arbeitsplätze: Ein Überblick, 2002. on: http://www.wuv-gmbh.de/media/versa_abstract.pdf, accessed on 04.04.2007.

[2] Gappmair, M.; Häntschel, I., Die Evaluierung von Workflow-Management-Systemen in Laborstudien, In: Wirtschaftsinformatik – Ergebnisse empirischer Forschung, Hrsg.: Grün, O.; Heinrich, L.J. Springer, Wien, New York 1997, p. 63-77.

[3] gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Einführung der Gesundheitskarte: Gesamtarchitektur Version 0.2.0, 2006, on: http://gematik.de/upload/gematik_GA_Gesamtarchitektur_V0_2_0_1281.pdf, accessed on 06.04.2007.

[4] gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Einführung der Gesundheitskarte: Konnektorspezifikation Version 1.0.0, 2007, on: http://gematik.de/upload/gematik_KON_Konnektor_Spezifikation_V1_0_0_1573.pdf, accessed on 06.04.2007.

[5] gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, Einführung der Gesundheitskarte: Spezifikation eHealth-Kartenterminal Version 1.3.0, 2007, on: http://gematik.de/upload/gematik_KT_eHealth_Kartenterminal_V1_3_0_1574.pdf, accessed on 06.04.2007.

[6] Häkkinen, H., Turunen, P., Spil, T.A.M., Information in Health Care Process – Evaluation Toolkit Development, Proceedings of the 36th Hawaii International Conference on System Sciences, Hawaii, 2003.

[7] Haux, R. (2005): Health information systems - past, present, future. In: International Journal of Medical Informatics, (2005).

[8] Keller, G.; Nüttgens, M.; Scheer, A.-W., Semantische Prozeßmodellierung auf der Grundlage „Ereignisgesteuerter Prozessketten (EPK)“. Universität des Saarlandes, 1992.

[9] Kuhn, K.A.; Wurst, S.H.R.; Bott, O.J.; Giuse, D.A. (2006): Expanding the Scope of Health Information Systems Challenges and Developments. In: IMIA Yearbook of Medical Informatics, (2006), S. 43-52.

[10] Krcmar, H. (2005): Informationsmanagement. Springer, Berlin, Heidelberg, New York 2005, p. 213-217.

[11] Krcmar, H.; Leimeister, J.M.; Klapdor, S.; Hörmann, C., IT-Management im Krankenhaus: Die Sicht der IT-Entscheider: Eine empirische Studie zur Ermittlung von Herausforderungen und Trends für das IT-Management in deutschen Krankenhäusern. Technische Universität München, Lehrstuhl für Wirtschaftsinformatik, 2007.

[12] Michel-Verkerke, M.B., Schuring, R.W., Spil, T.A.M., Workflow Management for Multiple Sclerosis Patients: IT and Organization, Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii, 2004.

[13] Projektgruppe FuE-Projekt "Lösungsarchitektur": Die Spezifikation der Lösungsarchitektur zur Umsetzung der Anwendungen der elektronischen Gesundheitskarte, Version 1.0 vom 14. März 2005: Projektinternes Glossar, on: http://www.dimdi.de/de/ehealth/karte/download/egk_glossar_v1-0.pdf, accessed on 14.03.2005.

[14] Schweiger, A.; Sunyaev, A.; Leimeister, J.M.; Krcmar, H. (2007): Toward Seamless Healthcare with Software Agents. In: Communications of the Association for Information Systems, Vol. 19 (Article 33), p. 692-709.

[15] Spil, T.A.M., van de Meeberg, H.J., Sikkel, K., The definition, selection and implementation of a new Hospital Information System to prepare the hospital for the electronic future: An example of project based education, Proceedings of the 32nd Hawaii International Conference on System Sciences, Hawaii, 1999.

[16] Sunyaev, A.; Leimeister, J.M.; Schweiger, A.; Krcmar, H. (2008): IT-Standards and Standardization Approaches in Healthcare. In: Encyclopedia of Healthcare Information Systems. Editors: Wickramasinghe, N.; Geisler, Publisher: Idea Group, 2008, to be published.

[17] Zöller, A.; Rothlauf, F.; Paulussen, T.O.; Heinzl, A., Benchmarking of Multiagent Systems. In: Multiagent Engineering. Hrsg.: Kirn, S.; Herzog, O.; Lockemann, P.; Spaniol, O. Springer, Berlin, Heidelberg 2006, p. 557-574.