

Editorial

Sehr geehrte Leserinnen,
sehr geehrte Leser,

das Gesundheitswesen ist heute ein Datenwesen: IT-Systeme speichern und sichern Patientendaten und machen sie verfügbar. Unverzichtbar sind Daten-systeme auch bei der medizinischen Dokumentation. Das Krankenblatt am Bett wurde durch den PC ersetzt. Ärzte arbeiten mit dem Laptop auch von zu Hause aus und kommunizieren untereinander mit Smartphones wie dem BlackBerry®.

Der Internist greift von irgendwoher übers Netz beispielsweise auf Radiologiedaten zu. Grenzenlose Datenverfügbarkeit definiert ihrerseits aber auch enge Grenzen: Patientendaten müssen vertraulich behandelt werden. Datenschutz ist gerade im Gesundheitswesen ein besonders sensibles Thema, wie die Schlagzeilen über die jüngsten Datenschutzskandale gezeigt haben. Krankenhäuser können das Patientenvertrauen behalten, indem sie die Patientendaten wirkungsvoll schützen und dies nachweisen. Die gestiegenen Datenschutzerfordernisse haben zur Entwicklung multifunktionaler Sicherheitssysteme geführt. Wer in zentral gemanagte Schließanlagen investiert, baut heute die Zukunft gleich mit ein. Intelligente Mitarbeiterausweise öffnen Mitarbeitern die Türen, erleichtern ihre Arbeit, gewährleisten den sicheren Datenzugriff und bieten in Verbindung mit einer Festplattenverschlüsselung den denkbar besten Power-Off-Schutz auch für Laptops.

Auch bei der Verschlüsselung von E-Mails auf Smartphones kommen Karten zum Einsatz. Kartenmanagement-Systeme der neuesten Generation helfen darüber hinaus im Alltag, wenn beispielsweise ein Mitarbeiter einen neuen Ausweis bekommt oder seinen Ausweis vergessen hat. Was vor einiger Zeit noch unmöglich schien, ist heute zum höchsten Standard geworden. Die neuen Single-Sign-On-Lösungen bieten den im Gesundheitswesen erforderlichen Schutz, decken die Sicherheits- und Workflow-Anforderungen moderner Kliniken vollständig ab und lassen sich einfach integrieren.

Herzlichst, Ihr

Ralf Bunger
IDpendant GmbH

P.S. Vergessen Sie nicht, uns vom 18.-21. November auf der MEDICA 09 in Düsseldorf zu besuchen. Sie finden uns in Halle 15 Stand G49. Mehr Details und wie Sie zu einer Eintrittskarte kommen, steht auf Seite 4.



Fünf Trends, warum Sie jetzt handeln sollten!

Ralf Bunger, IDpendant GmbH, Deutschland

In kaum einem anderen Wirtschaftssektor gab es in den letzten Jahren so viele Veränderungen wie in der stationären Betreuung und Pflege von Patienten. Technologien wie die Telemedizin, Ärztenetze und (Online)-Zusammenarbeit zwischen multidisziplinären Facharztpraxen erschließen neue Möglichkeiten, stellen aber auch neue Herausforderungen. Dieser Artikel soll Ihnen Impulse geben, welche Neuerungen und Trends Sie bei der Planung Ihrer (IT-)Strategie für Klinik und Krankenhaus berücksichtigen sollten.

Trend 1

Novelle des Bundesdatenschutzgesetzes

Spätestens seit der Bundestag die Änderungen am Bundesdatenschutzgesetz oder BDSG bestätigt hat, sollte das Thema Daten-

schutz – und insbesondere der Schutz von Patientendaten – ganz oben auf der Liste der Verantwortlichen in Krankenhäusern, Spitälern, Pflegeheimen und Arztpraxen einen Platz eingenommen haben. Es sind weniger die angehobenen Bußgelder (§43 BDSG, nun maximal 50.000 € bzw. 300.000 € für Verstöße gegen das BDSG) sondern eher die in §42 BDSG fest geschriebenen Pflichten zur persönlichen oder indirekten Informationspflicht vermutlich Geschädigter. Sollten durch Fahrlässigkeit, Vorsatz oder zu schwachem Datenschutz allgemeine Patientendaten unrechtmäßig Dritten bekannt werden, so muss jeder Betroffene persönlich oder durch die Schaltung einer Anzeige in einer überregionalen Tageszeitung über den Vorfall in Kenntnis gesetzt werden. Ein solcher Vorfall kann sehr schnell zur existenziellen Bedrohung werden, da der Imageschaden erheblich ist und zudem

Bußgelder die knappen Budgets belasten würden.

Trend 2

Mehrwertanwendungen für Ausweiskarten

Viele Kliniken und Hospitäler hatten für Einführung von Heilberufe-Ausweis (HBA) und Gesundheitskarte signifikante Investitionen geplant – andere wollten oder mussten unsicher gewordene RFID-Technik wie Mifare in ihren Firmenausweisen austauschen. Die hierfür geplanten Technologien bieten – auch ohne den HBA – ein großes Potenzial an Mehrwertanwendungen, die zum einen zur operationalen Effizienz als auch zur Anwenderfreundlichkeit der PC-Systeme im OP und in den Behandlungsräumen beitragen können. Ein besonders viel versprechender Ansatz ist die para-

lle Einführung einer vereinfachten Anmeldeprozedur für die Anwender, ein so genanntes Single-Sign-On oder SSO. Hier wird ein am PC angeschlossener Kartenleser verwendet, um den Anwender anhand seiner Ausweiskarte zu identifizieren und mit einer PIN zu authentifizieren. Alle eventuell notwendigen weiteren Anmeldeprozeduren werden dann durch das SSO automatisch vorgenommen, was eine erhebliche Entlastung der Mitarbeiter verspricht. Ganz nebenbei wird der kritische Zugriff auf Patientendaten (siehe Trend 1) durch starke Authentisierung mittels Karte und PIN abgesichert und der Anwender muss sich nur noch eine PIN statt vieler, ständig wechselnder Passwörter merken. Ergänzend wirkt hier ein Session-Management, so dass Ärzte und Pflegepersonal denselben PC im schnellen Wechsel nutzen können.

Weiter auf Seite 2 ->

Evolution bei der Krankenbetreuung – Revolution bei der Pflegedokumentation

Andreas Ropertz, CIS Leader, GE Healthcare, Deutschland



Eine der größten Herausforderungen und zugleich Ursache für einen Großteil der Überstunden und Mehrarbeit in deutschen Krankenhäusern ist der hohe Dokumentationsaufwand in der Pflege. Selbst die Einführung moderner Krankenhaus Informationssysteme (KIS) und der vermehrte Einsatz von moderner Technik bei Ärzten und Pflegepersonal hat nur teilweise zu Erleichterungen geführt. Fortschritte im Bereich der mobilen Datenerfassung von Patientendaten und deren unterschiedlicher Weiterverarbeitung eröffnen nun in Kombination mit moderner Ausweisteknik und damit einhergehenden Komfortfunktionen

neue Arbeitsweisen – und leisten damit einen entscheidenden Schritt hin zu höherer Dokumentationsqualität und weniger Dokumentationsaufwand!

Dokumentation vor Ort

Kernstück der neuen Technologie zur Pflegedokumentation ist ein bettseitiger Arbeitsplatz mit modernem, auf Berührung reagierendem Display das die direkte Aufnahme und Dokumentation aller relevanter Informationen ermöglicht. Diese Panels können durch eine Kabelverbindung die gerade erfolgten Eingaben ohne Verzögerung zur

zentralen Weiterverarbeitung oder Auswertung zur Verfügung stellen – Ärzte und Pflegepersonal können somit zeitnah von ihren (entfernten) Arbeitsplätzen wichtige Details abfragen und bearbeiten, oder neue Anweisungen für die tägliche Pflege einfügen. Unter Nutzung einer Webstation und einer verschlüsselter Verbindung (VPN) kann sogar über das Internet Zugriff auf die Informationen genommen werden. Für den Fall, dass der behandelnde Arzt von zu Hause oder von unterwegs Details überprüfen möchte oder Analyseergebnisse aus dem Labor Prüfung der Medikation oder Pflege anzeigen.

Sicherheit und Komfort im Fokus

Da die Sicherheit der Patientendaten oberste Priorität hat, die erforderlichen Sicherheitsmaßnahmen jedoch oft zu Lasten der Anwenderfreundlichkeit gingen, haben führende Unternehmen für das Patientendaten Management (GE Healthcare) und Sicherheitstechnik (IDpendant) eine innovative eine sichere und komfortable Kombination ihrer Technologien entwickelt. Das Zusammenspiel der Centricity® Applikationen von GE mit den benutzerfreundlichen Single-Sign-ON (SSO) Systemen der IDpendant erfüllt sowohl die strengen Anforderungen an Datenschutz und Datensicherheit, als auch die hohen Erwartungen des Pflegepersonals und der Ärzteschaft hinsichtlich Bedienkomfort und Funktionalität. Der



Anwender kann sich bequem mit seiner Ausweiskarte an den Arbeitsplatz- oder den Bettseitensystemen anmelden und hat sofort direkten Zugriff auf alle seine Applikationen. Alleine die Nutzung der SSO-Funktion zur transparenten Anmeldung erleichtert den Umgang mit den Anwendungen deutlich – die automatische Abmeldung bei Inaktivität oder beim Entfernen des Ausweises sorgt gleichzeitig für hohe Sicherheit!

Mehrwert für Patienten, Belegschaft und Verwaltung

Die intelligente Kombination neuer Technologie sichert einerseits die Investition in umfangreichen Patientendaten-Management-Systeme, deren Funktionalität sanft erweitert wird. Andererseits wird das Arbeitsaufkommen des Pflegepersonals und der Ärzteschaft direkt reduziert und

die Belegschaft spürt deutlich die Entlastung – sowohl bei der manuellen Dokumentation als auch bei der Nutzung der Informationstechnik. Letztlich kommen die Komfortfunktionen bei IT-Nutzung und der Dokumentation direkt den Patienten zu Gute, da mehr Zeit für ihre direkte Betreuung und Pflege bleibt und weniger Zeit mit Administration und Dokumentation verbracht werden muss. Ein besserer Pflegestandard, höhere Dokumentations- und Informationsqualität und die generelle Entlastung der Mitarbeiter führen zu weniger Fehlern und somit zu besseren Behandlungsergebnissen. ■

Info zum Unternehmen:

GE Healthcare IT beschäftigt sich seit mehr als 15 Jahren mit der elektronischen Dokumentation in der Klinik. GE Healthcare IT hat in dieser Zeit sein IT-Produktportfolio über RIS, PACS und kardiologische Bildverarbeitungssysteme hin zur Integration von Dokumentationssystemen für die Intensivstation, die Anästhesie und das OP-Management erweitert. Die Integration aller bei der Behandlung des Patienten anfallenden Daten gibt dem Kliniker die Sicherheit im Qualitäts- und Risikomanagement. www.ge.com

Fortsetzung Artikel „Fünf Trends, warum Sie jetzt handeln sollten!“ von Seite 1

Trend 3

Datenschutz durch Verschlüsselung

Ein ebenfalls durch Trend 1 stark beeinflusster Themenkomplex ist die Nutzung mobiler Rechner und Datenträger wie USB-Sticks. Lokal zur Analyse vorgehaltene (Patienten-) Daten auf diesen Laptops und Speichermedien stellen ein großes Risikopotenzial dar, dem durch eine rigorose Pflicht zur Verschlüsselung betrieblicher Daten entgegen gewirkt werden kann. Auch hier bietet sich der neue Dienstaussweis als multifunktionaler Alleskönner an: Ohne die Ausweiskarte kann zum Beispiel ein hausinternes Laptop nicht gestartet bzw. dessen Inhalte nicht gelesen werden. Die zur Anwendung kommende Festplatten- bzw. Medienverschlüsselung ist jedoch zwingend in zentrale Management-Systeme einzubinden, um ungewollten Datenverlust durch Zerstörung der Ausweiskarte zu vermeiden. Einen

besonderen Minitrend stellen hierbei die bereits etablierten Ausweiskarten mit kontaktloser Technik dar, die – als kostengünstige Alternative – teilweise ebenfalls erweitert werden können.

Trend 4

Sicherheit über Grenzen hinweg

Nicht nur Ärzte in Bereitschaft und Belegschaft im Notdienst sondern auch kooperierende Facharztpraxen oder Laboratorien nutzen die neuen Möglichkeiten der (mobilen) Datenkommunikation. Immer häufiger werden durch den Einsatz von Telemedizin und interdisziplinäre Diagnostik Patientendaten außerhalb des eigenen Netzwerks benötigt – sei es am Heimarbeitsplatz der Ärzteschaft oder in den Privatpraxen niedergelassener Hausärzte. Eine sichere Kommunikation über so genannte Ärztenetze oder Extranets kann ebenfalls unter Nutzung von Ausweiskarten für Anmeldung und Verschlüsselung etabliert werden. Eine vorausschauende Betrachtung solcher Einsatzszenarien kann jetzt Ein-



sparpotenziale sichern, da teure Individuallösungen in Zukunft vermieden werden. Kann man dann den Zutritt zu Gebäuden und Sicherheitsbereichen (Personalabteilung, Archiv) mit einbinden, freuen sich Auditoren und Prüfer über ein ganzheitliches Sicherheitskonzept.

Trend 5

Mit (IT-)Strategie planen

Gerade in Zeiten knapper Budgets sollte jede Investition wohl überlegt sein. Vor dem Hintergrund maßgeblicher gesetzlicher und technischer Änderungen ist es jetzt mehr denn je von Bedeutung, Technologie-Investitionen aufeinander abzustimmen und Mehrwerte aus notwendigen Neuschaffungen zu generieren. Nutzen Sie die Chance und informieren Sie sich jetzt über die Möglichkeiten zur Integration mittelfristig kostensparender Techniken und entwickeln Sie eine passende Strategie. Je nach Budgetlage können Sie dann fundierte Entscheidungen über notwendige und sinnvolle (Zusatz-) Investitionen fällen. ■

Kriterien bei der Auswahl von Terminals für den Basisrollout

Antworten auf viele offene Fragen

Uwe Harasko, Produktmanager ZF Electronics GmbH, Auerbach

Der Basis-Rollout (der elektronischen Gesundheitskarte) bringt neue Herausforderungen für die IT-Abteilungen der Krankenhäuser. Die vorhandenen Informationen wie z.B. „Übersicht Gesundheitskarte“ der Deutschen Krankenhaus-Gesellschaft oder auch die „Themen-Landkarte eGK-Basis-Rollout“ der gematik beantworten nicht alle offenen Fragen, insbesondere hinsichtlich der Auswahl geeigneter Terminals. Neben der Basisfrage welche Terminals ein verwendetes KIS (Krankenhaus Informations-System) überhaupt unterstützt, sind Fragen zur Bauart, den vorgesehenen Betriebsparametern im Basis-Rollout und dem späteren Online-Betrieb sowie die Unterstützung durch Betriebssysteme nahezu unbeleuchtet geblieben. Folgende Kriterien sollen bei der Planung Licht ins Dunkel bringen:

1. Bauart

Es gibt derzeit zwei Bauarten von Terminals:

a) Standalone-Geräte

Bei den Standalone-Geräten gibt es derzeit neun zugelassene Terminals mit unterschiedlichen Ausprägungen

b) Tastaturbauform

Hier gibt es derzeit nur einen zugelassenen Anbieter. Die Auswahl der Bauform leitet sich hier natürlich vom Platzangebot am Einsatzort, der Bedienbarkeit des Terminals durch das Personal sowie von Zusatzfunktionen (Tastatur) ab.

2. Stromverbrauch

Kann das Terminal ausgeschaltet werden, oder hat es nur einen Standby-Modus? Die EU-Vorgaben zum Stromverbrauch für PC und Notebooks im Stand-by machen hier eine Berücksichtigung der Leistungsaufnahme notwendig. Nur komplett abschaltbare Terminals können hier als zukunftssicher gewertet werden.

▼ Cherry eHealth-BCS Tastatur G87-1504



3. Abdeckung der Anforderungen des Basis-Rollouts

a) Physikalische Schnittstellen

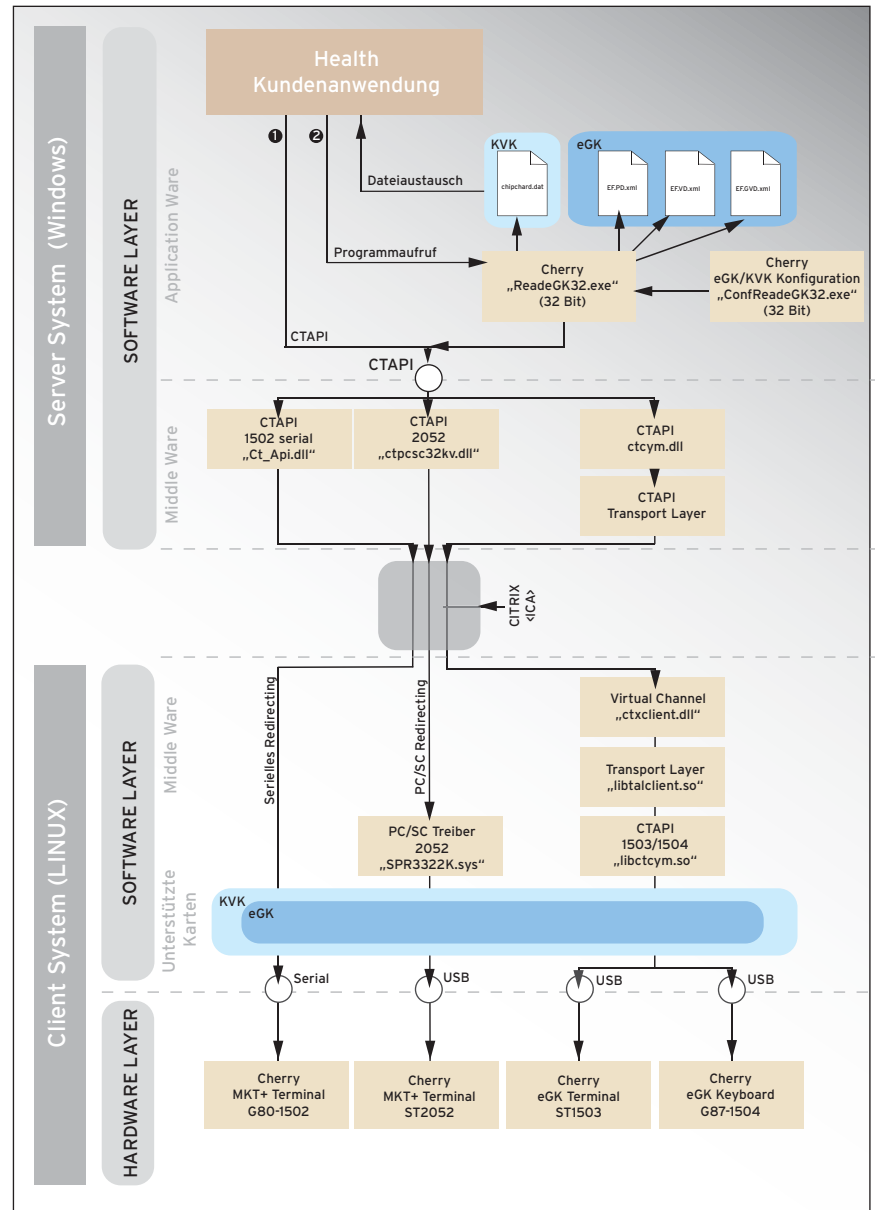
Normalerweise werden die Terminals über USB angeschlossen. Es gibt Terminals, die die USB-Schnittstelle nur über einen seriellen Adapter abbilden. Eine weitere Möglichkeit ist, die Ethernet-Schnittstelle schon im Basis-Rollout zu benutzen – ein Vorgriff auf die spätere Migration zum Betrieb direkt im LAN. Für diese Nutzungsart muss die verwendete CT-API, also die Kartenschnittstelle, dafür vorbereitet sein. Die direkte Verfügbarkeit von Terminals an der Netzchnittstelle erlaubt später eine einfachere Migration, sowie die unter 8. b) beschriebene Variante mit Translating Proxy. Dies ist eine weitere Möglichkeit, die Gesamtkosten zu optimieren. Zunächst ist für den Anschluss zu prüfen, ob an den Clients serielle und/oder USB-Schnittstellen vorhanden sind? Und werden diese Schnittstellen auch bei nachgekauften Geräten noch zur Verfügung stehen?

b) Treiber für verschiedene Betriebssysteme

Treiber für Microsoft Betriebssysteme sind für alle Terminals vorhanden, deren Nutzung an Thin Clients ist jedoch nicht immer gewährleistet. Einige Hersteller wie IGEL und Wyse haben sich dazu bereit erklärt, für ihre auf Linux basierenden Thin Clients entsprechende Images bereit zu stellen, die den reibungslosen Betrieb z.B. der Cherry Tastatur G87-1504 mit einem virtuellen Channel-Treiber unter Citrix sicher stellen. Linux-Unterstützung für normale Arbeitsplatzsysteme sollte gesondert abgefragt werden.

4. Client-Server-Unterstützung (Citrix, WTS)

Für eine flexible Anwendung im Krankenhaus ist eine Weiterleitung der Daten über ICA oder RDP notwendig. Es ist zu klären, auf welche Art die Daten weitergeleitet werden, und ob dies vom jeweiligen KIS-System unterstützt wird – die KIS-Hersteller (wie z.B. Agfa HealthCare)



▲ eHEALTH eGK/KVK Software Architektur. Linux Client – Windows Server. (G80-1502 | ST2052 | ST1503 | G87-1504)

unterstützen ihre Kunden bei der Umstellung auf die eGK mit gesonderten Newslettern zu diesem Thema. Des Weiteren kann z.B. für ORBIS ein Paket „eGK BASIS“ erworben werden, das über Anleitungen den Administratoren und Anwendern die notwendigen Arbeitsschritte für die Migration ausführlich erklärt.

5. Heterogene oder homogene Infrastrukturen

Zusätzlich sollte im Hinblick auf die Wartbarkeit der Systeme bewertet werden, ob es sinnvoll ist, eine Inte-

gration mit verschiedenen Terminals zu betreiben oder besser eine homogene Struktur aufzubauen, die sich einfacher verwalten lässt.

6. Belastung des Netzwerkes durch die Datenübertragung

insbesondere die Übertragung der Daten über ICA oder RDP kann bei einer größeren Anzahl von Terminals das Netzwerk deutlich belasten. Die meisten Terminals erledigen diese Weiterleitung über das PC/SC Redirect, da sie keine klassischen MKT Terminals sind, sondern über eine CCID-Schnittstelle verfügen,

welche die Daten über einen CT-API Wrapper anbietet. Die Cherry Terminals arbeiten hingegen ohne einen PC/SC Treiber und nutzen den USB-HID-Kanal. Ein eigener ICA/RDP-Kanal für die Abfrage der Daten von der eGK zwischen KIS und Terminal reduziert den LAN-Verkehr zudem drastisch. Diese Reduzierung erfolgt durch eine Bündelung der einzelnen Anfragen des Systems an das Terminal, das die Antwort ebenfalls gebündelt zurück überträgt.

Weiter auf Seite 5 ->

Fortsetzung Artikel „Kriterien bei der Auswahl von Terminals für den Basis-Rollout“ von Seite 3

7. Anbindung von Außenstellen

Die Anbindung von Terminals in Außenstellen über das Internet führt oft zu Problemen – bedingt durch die Latenzzeiten im Netz wird der Einlesevorgang der Patientendaten von der eGK oder KVK abgebrochen. Durch die in 6) beschriebene Konsolidierung mehrfachen Anfragen vor der Datenübertragung, kann die Überschreitung der Antwortzeiten vermieden werden. Die Wahrscheinlichkeit einer Störung beim Lesen der Daten wird hierdurch drastisch reduziert.

8. Abdeckung der Online-Phase

A: Anschluß am Konnektor

Die Online Phase sieht vor, die Terminals generell am LAN zu betreiben. Hierbei sind folgende Varianten möglich:

a) Direkt am LAN

(1) Separat angeschlossen

Dies setzt voraus, dass genügend Netzwerkanschlüsse vorhanden sind oder entsprechend zusätzliche Switches zur Verfügung gestellt werden, um die Terminals direkt verbinden zu können.

(2) Mit integriertem Switch

In die Terminals integrierte Switches führen zu einer größeren Menge an Computern hinter nicht fernwartbarer Switch-Hardware. Dies kann im Fehlerfall zu größeren Aufwänden beim Support führen, da die Terminals

nicht in ein Netzwerkmanagement System einzubinden sind.

b) Indirekt am LAN

Eine weitere Möglichkeit ist es, die Terminals über USB am Rechner angeschlossen zu verwenden. Für den Zugriff des Konnektors auf das Terminal wird hier mithilfe eines Translating-Proxi der Netzwerk-Anschluss des entsprechenden PC genutzt. Somit entfällt auch das Umstecken bzw. das Umrüsten des Terminals von der Offline- in die Online-Phase.

B: Bauform für Patienten-Transaktionen

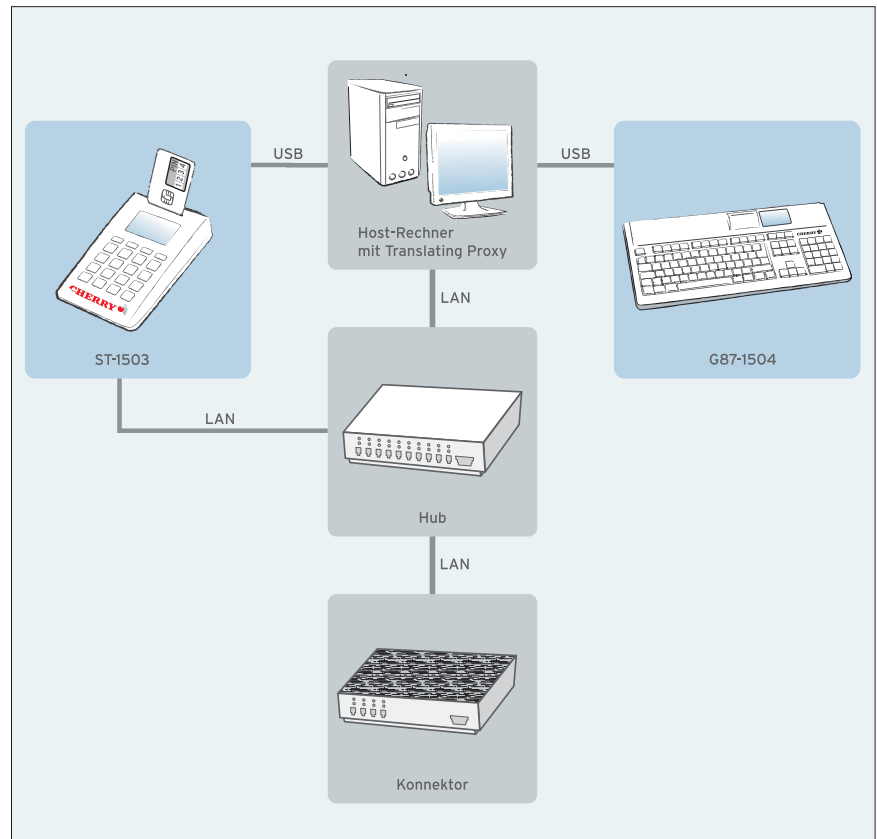
Im Online Betrieb wird es bei den Funktionen „Notfalldatensatz“ und „elektronische Patientenakte“ notwendig sein, dass der Patient seine PIN eingibt. Dazu ist folgendes zu beachten:

(1) Ist die Tastatur des Terminals dazu geeignet, dass Patienten ihre PIN eingeben können, auch wenn sie eine Sehschwäche oder anders gearbete Beeinträchtigungen haben? Sind die Tasten ausreichend groß und ist die Beschriftung deutlich lesbar?

(2) Gibt es für das Terminal einen geeigneten Schwenkarm, um das Terminal dem Patienten leicht verfügbar zu machen? Für den Einsatz der Cherry Tastatur-Lösung ist ein externes PIN-Pad zur Eingabe der Patienten PIN vorgesehen.

C: Firmware Update

Für die Online Phase muss bei allen eHealth-BCS Terminals ein Firmware-Update durchgeführt werden. Dabei stellt sich die Frage, ob das Upgrade vom BCS Betrieb im Basis-Rollout auf den Online Betrieb kostenpflichtig ist,



▲ Cherry Translating Proxy

oder in den Anschaffungskosten des Gerätes inkludiert ist (wie z.B. bei den Cherry Geräten). Ein weiterer Kostenfaktor ist die Auführung des Updates: Stellt der Hersteller ein Update Tool zur Verfügung mit dem die Terminals über das Netz zu aktualisieren sind oder muss dies lokal am Terminal vorgenommen werden. ■

Informationen zu Produkten oder technischen Spezifikationen erhalten Sie unter:

+49 (0) 1805-919109

MEDICA – Weltforum der Medizin



World Forum for Medicine

Düsseldorf
Nov. 18 – 21, 2009

Besuchen Sie uns vom 18. – 21. November 2009 auf der MEDICA

Wir laden Sie herzlich zu einem Messerundgang und einem Besuch an unserem Stand ein. Sie finden uns in Halle 15 Stand G49.

Wir zeigen Smartcard-Tastaturen im Einsatz mit der nach Kundenmeinung „genialsten Single Sign-On-Lösung“. Zusätzlich präsentieren wir vor dem Hintergrund der bevorstehenden Einführung der elektronischen Gesundheitskarte die umfangreiche eHealth-Produktpalette.

Fordern Sie unter irmgard.haertl@zf.com Ihren persönlichen Gutschein für eine Eintrittskarte zur MEDICA 09 in Düsseldorf an

Wir freuen uns auf Ihren Besuch bei der MEDICA!



Effizienz und Sicherheit im Gesundheitswesen – ein Widerspruch?

Politik gibt grünes Licht für Roll-Out der Gesundheitskarte – Chancen jetzt nutzen!

Sebastian Rohr, CTO und technischer Geschäftsführer, accessec GmbH, Groß-Bieberau



▲ Die elektronische Gesundheitskarte ersetzt die bisherige Krankenversichertenkarte

Nach vorübergehender Unruhe in der aktuellen Tagespresse wird die Einführung der elektronischen Gesundheitskarte (eGK) und des elektronischen Heilberufsausweises (HBA) nun fortgesetzt. Klärende Aussagen des Bundesgesundheitsministers Philipp Rösler geben den Kassen nun die notwendige Sicherheit, mit dem Roll-Out wie geplant voran zu schreiten und zukünftig auch Ausweise aus zu geben.

Nach dieser wichtigen politischen Weichenstellungen ist es für den Gesundheitsbereich unabdinglich, sich für die kommenden Jahre auf die anstehenden Veränderungen vorzubereiten, insbesondere durch die immer größere Rolle des Datenschutzes im Gesundheitswesen. Der fortgesetzte Druck die Kosten im Gesundheitsbereich zu reduzieren, kann nur durch Ausschöpfung von Synergiepotenzialen bei der Einfüh-

rung neuer Technologien gelingen. Die Nutzung eines multifunktionalen Dienst-Ausweises in Krankenhäusern und Kliniken bietet sich als Beispiel: Komfortfunktionen wie elektronischen Bezahlssystemen und die Konvergenz von physischer Sicherheit und IT-Sicherheit ergeben neue Anwendungsformen, die direkt zu Kosteneinsparungen und verbessertem Datenschutz führen. Der Ausweis ist hierbei der universelle Schlüssel, denn eine entsprechend konfigurierte Karte kann zur sicheren Freigabe von Patientendaten genauso verwendet werden, wie zum Öffnen von Türen oder für die Zufahrt zum Parkhaus der Klinik. Die bequeme und schnelle Anmeldung am PC über die Karte (und Eingabe einer PIN) begeistert die Mitarbeiter und die Ausweise erfreuen sich sehr schnell eine große Beliebtheit bei der Belegschaft.

Verschmelzung richtig nutzen

Weitere Synergien ergeben sich durch die Einbeziehung der physischen Sicherheit und der Zeiterfassung, insbesondere wenn die Belegschaft ihren Einsatzort häufig wechseln muss und unterschiedliche Systeme für Zeiterfassung und Zutrittskontrolle in den Liegenschaften vorhanden sind.

Vor der konvergenten Nutzung eines universellen Ausweises steht eine eingehende Analyse, welche Systeme eingebunden und welche gegebenenfalls ersetzt werden sollten. Der Schlüssel für die Verbindung der Systeme ist wieder der Ausweis: Bezahlssysteme (Kantine, Automaten) und Zutrittsberechtigungen können durch geschickte Wahl der Kontaktlos-Chips vereinhheitlich und individuell auf die Bedürfnisse angepasst werden. Die

derzeit notwendige Nutzung mehrerer Karten für verschiedene Gebäude und Liegenschaften kann bei geschickter Integration entfallen! Integrierende Management Systeme, wie z.B. das von der Firma newfrontiers entwickelte ONEaccess, sind in der Lage, mehrere lokale Systeme logisch zu verknüpfen und übergreifend zu verwalten. Ersatzinvestitionen und teurer Austausch von Systemen können vermieden oder minimiert werden.

Die Mitarbeiter nutzen bequem einen Ausweis für den Zutritt zu allen Liegenschaften und für den Zugriff auf die (IT)-Ressourcen.

integrierter HBA-Funktion! Für die erfolgreiche Einführung eines solchen kombinierten Ausweises und der damit verbundenen Systeme bedarf es einer genauen Planung und Erstellung eines detaillierten Anforderungsprofils – insbesondere wenn mehrere Liegenschaften und Systeme verbunden werden sollen. Schöpfen Sie die Synergiepotenziale voll aus und lassen Sie sich bei der Planung von erfahrenen Partnern begleiten – dann steht einer erfolgreichen Implementierung nichts im Wege. ■

Im Idealfall bedeutet das:

Verwendung der Karte zur Authentisierung an IT-Systemen, dadurch

- Erhöhung des Datenschutzes

Nutzung der Karte als Berechtigungsausweis für die physische Sicherheitswelt, dadurch

- bei Kartenverlust kein Austausch der Schließanlage notwendig

Nutzung der Karte als Bezahlssystem, Ergebnis:

- die Mitarbeiter führen die Karte immer mit sich

Vergabe aller notwendigen Berechtigungen durch ein zentrales System (z.B. ONEaccess), hierdurch:

- sofortiges Entziehen/Sperren der Berechtigungen durch diese zentrale Stelle möglich
- Reduzierung der administrativen Tätigkeiten durch einfachere Abläufe
- deutliche Kosteneinsparung durch geringeren Pflegeaufwand
- kostengünstige Umsetzung von ganzheitlichen Sicherheits- und Informationsschutzkonzepten

Die Vorteile der Verwendung eines multifunktionalen Ausweises liegen auf der Hand – ob mit oder ohne

Info zum Unternehmen:

Die accessec GmbH ist Spezialist für Sicherheitsstrategien und ganzheitliche Sicherheitslösungen welche die Bereiche IT-Sicherheit, physische Sicherheit, Chipkarten und USB Token umfassen. Insbesondere die Beratung zur Konvergenz zwischen Systemen der physischen und der IT-Sicherheit stehen im Fokus des Unternehmens. accessec ist an keinen Hersteller gebunden und bietet dadurch ein umfassendes Leistungsportfolio, von ganzheitlicher Betrachtung der kritischen Geschäftsprozesse bis hin zur individuellen Risikostruktur-Analyse. accessec entwickelt basierend auf den spezifischen Anforderungen der Kunden und deren Geschäftsprozessen ganzheitliche Sicherheitskonzepte und begleitet die Kunden bei deren Umsetzung. Und bietet neutrale und unabhängige Beratung zu allen Fragen rund um die Sicherheit im Gesundheitswesen. www.accessec.com

Impressum:

Herausgeber und verantwortliche Redaktion:

ZF Electronics GmbH
Cherrystrasse
D-91275 Auerbach/Opf.
Deutschland
Tel. +49 96 43 18 - 0
Fax +49 96 43 18 - 1545
info@cherry.de
www.cherry.de
und

IDpendant GmbH
Edisonstraße 3
85716 Unterschleißheim/München
Deutschland
Herr Ralf Bunger
Tel: +49 89 3700 110 22
Fax +49 89 3700 110 10
info@idpendant.com
www.idpendant.com

Layout:
kaba:design, Limburg

Alle Informationen und Nachrichten werden nach bestem Wissen erarbeitet. Die Veröffentlichung erfolgt ohne Gewähr. Irrtümer vorbehalten. Nachdruck, auch auszugsweise, nur mit Genehmigung des Herausgebers. Copyright 2009. Alle Rechte vorbehalten.

Über **IDpendant**

Die IDpendant GmbH ist Spezialist für Lösungen aus den Bereichen IT-Sicherheit, USB Token und Chipkarten. Weil Sicherheitsanforderungen sehr unterschiedlich sind, bietet IDpendant ein umfassendes Leistungsportfolio, das den individuellen Anforderungen von Firmen, und Institutionen gerecht wird. Das Portfolio reicht von Authentisierungstechnologien und IT-Sicherheitsprodukten über Card-Management-Systeme bis zu Lösungen aus dem Identity & Access Management (IAM). Damit ist IDpendant ein führender, unabhängiger Systemintegrator für IT-Sicherheitslösungen und schließt die Lücke zwischen Karten- und IT-Security Herstellern.

Über **CHERRY**

Cherry ist eine Marke der ZF Electronics GmbH. Das im Jahr 2008 akquirierte Geschäftsfeld Elektronikkomponenten, die ZF Electronics GmbH (vormals Cherry GmbH), entwickelt und produziert Computer-Eingabegeräte, Schaltsysteme, Sensorik und Steuerungen für die Automobilindustrie sowie Komponenten für Industrie- und Hausgeräteeinrichtungen. Insgesamt erwirtschaftete es im Jahr 2008 mit weltweit rund 2.800 Mitarbeitern einen Umsatz von 255 Mio. Euro. ZF ist ein weltweit führender Automobilzulieferkonzern in der Antriebs- und Fahrwerktechnik mit rund 63.000 Mitarbeitern an 125 Standorten in 26 Ländern. Der Konzern erwirtschaftete im Jahr 2008 einen Umsatz von 12,5 Milliarden Euro. Auf der Weltrangliste der Automobilzulieferer ist ZF unter den zehn größten Unternehmen.