Sicherheitsstandards für Authentifizierungen mittels biometrischer Verfahren – das EU-Projekt BioHealth

Demski H[1], Pharow P[2], Hildebrand C[1]
[1]*Institut für Medizinische Informatik, GSF – Forschungszentrum für Umwelt und Gesundheit, Deutschland*
[2]*eHealth Competence Center, Universität Regensburg Medical Center, Deutschland*
demski@gsf.de

Einleitung und Fragestellung

Das von der EU geförderte Projekt BioHealth (Security and Identity Management Standards in eHealth including Biometrics: Specific Requirements having an Impact on the European Society and on Standardisation) [1] unterstützt Kenntnis und Verbreitung existierender Standards im Bereich eHealth. Dabei werden neben der Datensicherheit das Identitätsmanagement und der Einsatz entsprechender biometrischer Verfahren als eine den Datenschutz unterstützende Technologie (Privacy-Enhancement Technology) [2] in diesem sensitiven Bereich besonders berücksichtigt.

BioHealth begleitet die Verbreitung und Einführung bestehender Standards durch gezielte Maßnahmen. Lücken in vorhandenen Standards, die z.B. aufgrund spezieller neuer oder bislang nicht berücksichtigter Anforderungen der Anwender entstehen, und Hindernisse bei der praktischen Umsetzung von Standards sollen identifiziert werden. Die Weiterleitung der Anforderungen der Nutzer an die relevanten Einrichtungen (Standardisierungsgremien, politische Einrichtungen) und der Einsatz von Empfehlungen und Standards sowohl auf europäischer als auch auf nationaler Ebene sollen unterstützt werden. So werden der Bekanntheitsgrad, das Vertrauen und die Akzeptanz in die Standardisierungsaktivitäten auf europäischer Ebene und darüber hinaus gefördert. Durch aktive Teilnahme an Workshops und Beiträgen auf relevanten Konferenzen, z.B. im Bereich eHealth, Chipkarten, Biometrie, Public Key Infrastruktur, eGovernment und Sicherheit wird eine breit gefächerte Zielgruppe von den Arbeiten und Ergebnissen des BioHealth Projektes profitieren. Auf diese Weise wird auch ein besserer Bezug zur Praxis hergestellt, um den von Nutzern oft vorgebrachten Bedenken über eine gewisse "Praxisferne" der Standards selbst und der Standardisierungs- bzw. Normungsgremien Rechnung zu tragen und letztlich die Umsetzung von existierenden Standards in reale Lösungen zu erleichtern. Viele der europäischen Projektpartner sind bereits seit langer Zeit aktiv in internationale Standardisierungaktivitäten eingebunden. Aus nationaler und auch aus europäischer Sicht erlaubt eine weit reichende Standardisierung die Harmonisierung von Sicherheitslösungen in eHealth-Anwendungen und stellt dadurch auch deren Interoperabilität sicher. Dies ist momentan für Deutschland aufgrund der vielfältigen Aktivitäten zum Aufbau der Rahmenarchitektur und der Telematikinfrastruktur für die elektronische Gesundheitskarte (eGK) und den Heilberufsausweis (HBA) von besonderem Interesse.

Material und Methoden

Um seine europäischen und nationalen Ziele zu erreichen, wird BioHealth:

- Die Ergebnisse vorhandener Standardisierungsaktivitäten bezüglich Sicherheit und Identitätsmanagement sowie den aktuellen Stand der zugehörigen Technologien identifizieren und analysieren.
- Den Versuch unternehmen, alle relevanten Interessenvertreter (z.B. Versorger, Gesundheitspersonal, Patienten, Krankenversicherungen, Gesundheitsbehörden) in die Aktivitäten einzubinden.
- Auf regionaler, nationaler und europäischer Ebene Treffen mit den betroffenen Personengruppen organisieren und Informationen verteilen, um Harmonisierung und Interoperabilität voranzutreiben.
- Die speziellen europäischen Anforderungen im Bereich eHealth-Sicherheit identifizieren und darauf hinwirken, sie mit denen aus eGovernment, eBusiness und eTransport zu harmonisieren, um so möglichst frühzeitig eine Abstimmung der verschiedenen Aktivitäten in nationalen, europäischen und internationalen Standardisierungsgremien im Bereich Sicherheit und Identifikation zu ermöglichen.
- Ethische und rechtliche Aspekte berücksichtigen und mit den Anwendern diskutieren.
- Eine Umgebung schaffen in der es europäischen Experten auch außerhalb des Projektrahmens ermöglicht wird sich zu treffen, Erfahrungen auszutauschen und Empfehlungen zu formulieren.

Der Schwerpunkt wird dabei auf innovativen Ansätzen wie RFID und Maßnahmen zum Rollenmanagement (z.B. mittels biometrischer Authentifizierung) liegen. Die Bewertung biometrischer Authentifizierungsverfahren ist aufgrund der restriktiven Gesetzgebung in Bezug auf den Datenschutz und den Schutz der Privatsphäre sowie auch in ethischer Hinsicht in ganz Europa von großer Bedeutung.

Die integrierte Versorgung bedingt einen Zugriff verschiedener am Versorgungsprozess beteiligter Akteure auf die Krankenakte des Patienten. Dabei ist ein entsprechendes Identitätsmanagement [3] erforderlich, um einen sicheren, gesicherten und rollengesteuerten Zugang auf die über verschiedene Einrichtungen verteilten Informationen zu ermöglichen. Das Identitätsmanagement – oder besser das Management von Eigenschaften bestehender Identitäten – dient dem Ziel einer sicheren Verwaltung von strukturellen und funktionalen Rollen im Zusammenhang mit Identitäten, z.B. der Benutzer eines Systems. Es ermöglicht die Identifikation und Verifikation der Nutzer während eines Authentifizierungsprozesses und stellt im Kontext der Authentifizierung weitere Informationen über den Benutzer bereit. Dabei können die Nutzer durchaus mehrere abgeleitete Identitäten besitzen, die den verschiedenen Situationen und Rollen angepasst sind. Die mit einer bestimmten Identität verknüpften Informationen (z.B. die Rollen) können sich im Lauf der Zeit verändern und müssen sorgfältig verwaltet werden. Ein Teil der Nutzerinformationen kann informell sein (z.B. funktionale Rollen) und sich häufig ändern. Andere Teile wie z.B. bestimmte Beziehungen zu anderen Personen oder strukturelle Rollen innerhalb der eigenen Organisation sind über einen gewissen Zeitraum stabil. Letztere können im Rahmen der Sicherheitsinfrastruktur auch in Attributzertifikaten abgelegt werden, die dann an die Identität (z.B. abgebildet als Public-Key-Zertifikat) gebunden sind. Identitäten, die mit strukturellen Rollen innerhalb von Organisationen verknüpft sind, haben in der Regel auch einen Bezug zu bestimmten festen und langfristigen Aufgaben, Verantwortlichkeiten und speziellen Rechten, die den permanenten Zugriff auf bestimmte Ressourcen erlauben. Der internationale Standard ISO/IEC 24760 „A Framework for Identity Management" [4] zielt darauf ab, einen universellen Rahmen für die Definition von Identitäten und die sichere, zuverlässige und vertrauliche Verwaltung der Identitätsinformationen zu schaffen. Die in Erarbeitung befindlichen Standards ISO TS 21298 „Functional and Structural Roles" [5] sowie ISO TS 22600 „Privilege Management and Access Control" [6] ergänzen die Betrachtungsmöglichkeiten in geeigneter Weise, da sie die Rollen, deren Management und ihre Beziehungen zu den Identitäten abbilden helfen.

Die Biometrie stellt automatisierte Methoden für die Identifikation und die Verifikation von Personen, basierend auf deren physiologischen (z.B. Gesicht, Fingerabdruck, Handgeometrie, Iris) oder verhaltensspezifischen (z.B. Handschrift, Stimme) Merkmalen, bereit. Biometrie wird somit als Schlüsseltechnologie für die sichere Identifikation von Personen und die Verifikation (Überprüfung) der Identität von Personen gesehen [7]. Die Europäische Kommission hat ein neues Internetportal [8] eröffnet, das unter anderem die Entwicklung einheitlicher Richtlinien für die Nutzung biometrischer Verfahren adressiert und deren Einsatz unter Gewährleistung von Interoperabilität und Datenschutz vorantreiben soll. Andererseits wird Biometrie auch kritisch gesehen. So lösen unter anderem die Frage der Zugänglichkeit zu den Mechanismen (bestimmte Personen werden unter Umständen von der Nutzung ausgeschlossen, weil sich ihre Identität biometrisch nicht prüfen lässt; eine Person ohne Hände kann kein handgeometrisches Erkennungsverfahren nutzen.) und auch potentielle Bedrohungen durch eine zentrale Datensammlung im Sinne der Identifizierbarkeit von Individuen oder auch des Missbrauchs einmal erfasster Daten Bedenken aus. Außerdem stehen dem weiten Einsatz biometrischer Verfahren im Moment noch technische Schwierigkeiten im Wege. So liegen die Anteile der zu unrecht zurückgewiesenen berechtigten Personen (FRR – False Rejection Rate) und der fälschlicherweise akzeptierten unberechtigten Personen (FAR – False Acceptance Rate) noch immer zu hoch für einen Masseneinsatz. Da diese Technologien auch im Gesundheitsbereich immer wichtiger werden, gilt es Datenschutzaspekte hinsichtlich der Rechte des Benutzers ausreichend zu adressieren und deren Belange ernst zu nehmen. Die Einführung von durch biometrische Verfahren unterstützten Authentifizierungsverfahren erfordert eine umfassende Information und Diskussion auf allen Ebenen, um den Bedenken über

den Einsatz dieser Technologie gerecht zu werden. Besonders im Bereich eHealth gilt es passgenaue Lösungen zu erreichen, die den speziellen europäischen Anforderungen an die Sicherheit im Gesundheitsbereich gerecht werden.

Ergebniserwartungen

Der Workshop "Sicherheitsstandards für Authentifizierungen mittels biometrischer Verfahren – das EU-Projekt BioHealth" stellt die Arbeit des Projektes vor und gibt anhand verschiedener Vorträge einen Einblick in die laufenden Standardisierungsaktivitäten mit Bezug auf das genannte Thema. Die Präsentation soll auf die Arbeit des BioHealth-Projektes aufmerksam machen, einen Überblick über die aktuellen Arbeiten an relevanten Standards geben und durch Diskussionen den bidirektionalen Wissenstransfer zwischen Vertretern von Standardisierungsgremien einerseits und potentiellen Anwendern von Standards andererseits verbessern helfen.

Literatur

[1] http://mirc.gsf.de/biohealth - zuletzt zugegriffen am: 29.03.2006

[2] Borking JJ, Raab CD. Laws, PETs and other Technologies for Privacy Protection. Journal of Information, Law & Technology (JILT) 2001; Issue 1.

[3] RAPID Project Report. Overall Roadmap 'Privacy and Identity Management'. 21.08.2003. URL:https://rami.jrc.it/roadmaps/rapid/overall.pdf - zuletzt zugegriffen am: 29.03.2006

[4] ISO/IEC NP 24760. Information Technology -- Security Techniques - A Framework for Identity Management.

[5] ISO/CD 21298. Health informatics -- Functional and structural roles

[6] ISO PRF TS 22600. Health informatics -- Privilege management and access control

[7] Petermann T, Sauter A. Biometrische Identifikationssysteme - Sachstandsbericht. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). 2002

[8] European Commission, Directorate General Justice, Freedom and Security. B-1049 Brussels, Belgium, Office No LX-46 01/43. URL: http://europa.eu.int/comm/justice_home/fsj/privacy - zuletzt zugegriffen am: 29.03.2006.