Authentisierung und Autorisierung in Logistik und Gesundheitswesen

Dr. Roman Gumzej

Fakultät für Logistik der Universität Maribor

Globalisierung und Sicherheit

- Der vorliegende Beitrag befasst sich mit informationeller Sicherheit in den Bereichen
  - Logistik und
  - Gesundheitswesen.
- Verfahren zur Authentisierung und Autorisierung der beteiligten Personengruppen und Vertriebsunternehmen sowie deren Lieferungen werden vorgestellt.
- Kritisch für die Vertraulichkeit von Daten ist beidseitige Authentisierung, die gewöhnlich durch dritte Personen bzw. Institutionen gewährleistet wird (Zertifizierung).
- Die EU erließ dazu 2010 die Verordnung (EU) Nr. 185/2010, in der der Begriff des *bekannten (vertrauenswürdigen) Versenders* eingeführt wurde.

Recherche der Bundesvereinigung Logistik

1. Die Gesetzgeber in Europa und den USA haben seit 2001 umsichtige Vorkehrungen zur Erhöhung der Sicherheit im Passagier- und Frachtbereich getroffen.
2. Die Verlässlichkeit der Ausführung dieser Bestimmungen zur Gewährleistung „sicherer Lieferketten“ hängt entscheidend von der Qualifikation und Überwachung des verantwortlichen Personals ab.
3. Die an den Sicherheitsprozessen Beteiligten, bspw. Luftfahrtunternehmen als Letztverantwortliche, Flughäfen, reglementierte Beauftragte, das Luftfahrtbundesamt sowie ggf. die Bundespolizei und andere, sind derzeit noch nicht hinreichend vernetzt. Hier gibt es Handlungsbedarf bei allen Beteiligten.
4. Die generelle Datenlage ist zu verbessern und die systematische Datenerhebung und -auswertung zu regeln. Sicherheit für Leib und Leben geht vor datenschutzrechtlichen Bedenken.
5. Ein deutliches Mehr an Sicherheit bringt höhere Kosten mit sich und verlangsamt logistische Prozesse.

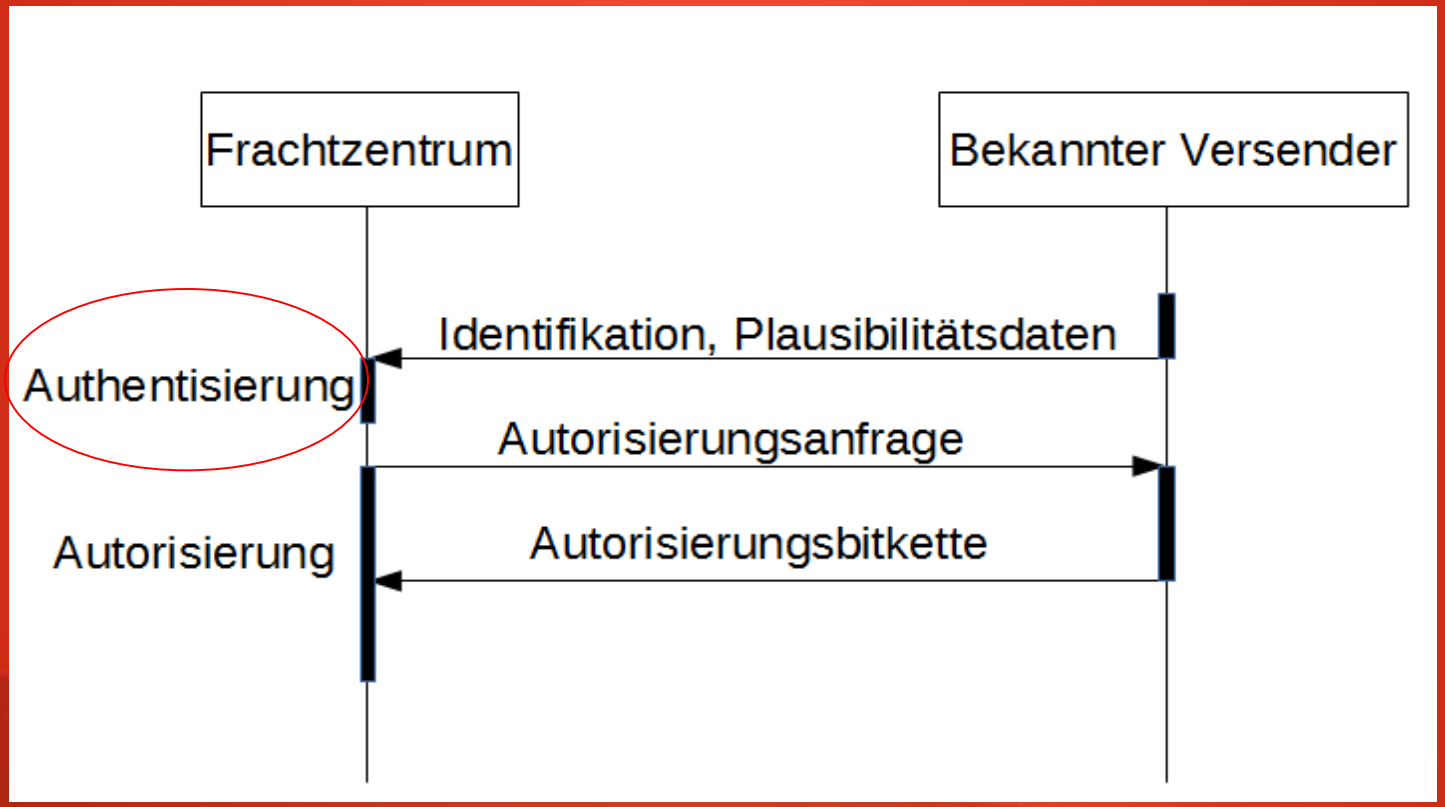
Recherche der Bundesvereinigung Logistik

6. Die technischen Möglichkeiten zur Durchleuchtung von Fracht sind weiterzu-entwickeln; nur so können Sicherheitsstandards weitgehend kostenneutral weiter angehoben werden.
7. Weil es weder nach europäischem noch nationalem Recht bislang Vorgaben gibt, Transit- oder Transferfracht zu kontrollieren, besteht Handlungsbedarf.
8. Die Zuverlässigkeit der Einhaltung von Sicherheitsstandards in Drittstaaten ist zu überprüfen und bei Feststellung sicherheitsrelevanter Mängel sind Konsequenzen zu ziehen.
9. Hundertprozentige Sicherheit kann es nicht geben, denn vor kriminellen und terroristischen Machenschaften lassen sich weder nationale noch internationale Lieferketten vollständig schützen.
10. Jede Form von Aktionismus schadet der ernsthaften Bearbeitung dieses wichtigen Themas.

Automatisierte Authentisierung und Autorisierung von Transporteinheiten

- Aufgrund gesetzlicher Bestimmungen und des zunehmenden Gefährdungspotentials müssen Transporteinheiten, insbesondere vor ihrer Verladung auf Flugzeuge oder Schiffe, auf Sprengstoff durchsucht werden.
- Das bedeutet zusätzlichen Aufwand, der in Lieferketten sogar mehrfach erforderlich werden kann und so die Transportkosten erhöht und logistische Prozesse verlangsamt.
- Um mehrfache Durchsuchungen von Transporteinheiten nach ihrem ursprünglichen Beladen zu vermeiden, wurden in den Verordnungen (EG) Nr. 648/2005 und Nr. 185/2010 die Konzepte zugelassener Wirtschaftsbeteiligter, bekannter Versender sowie reglementierter Beauftragter für Produzenten, Distributoren und Versandzentren, insbesondere Luftfrachtzentren eingeführt.
- Das Kernproblem der Authentisierung und Autorisierung von bekannten Versendern verschickter Transporteinheiten besteht darin, diese ohne großen Aufwand (automatisch) als solche erkennen und schnell weiterleiten zu können.

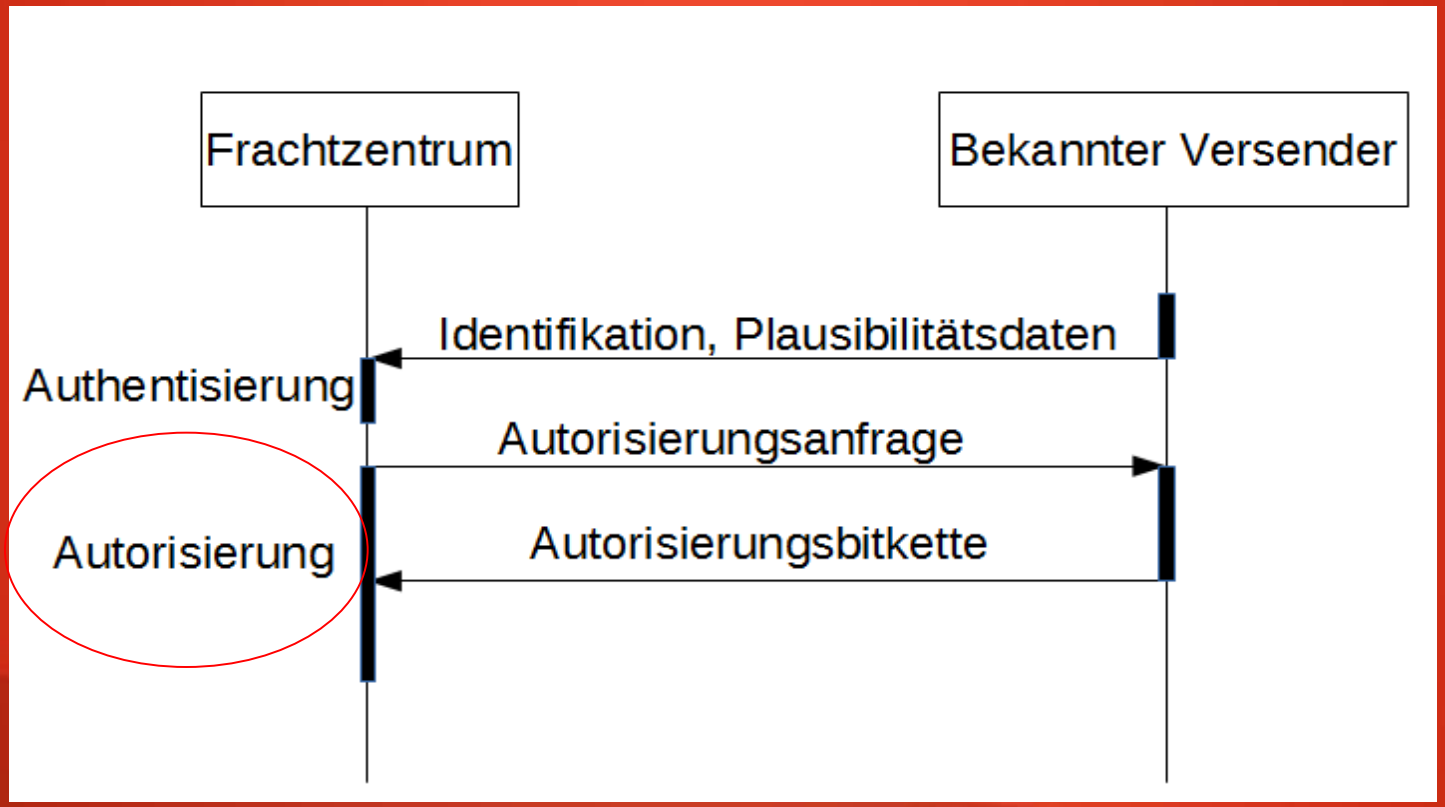
Lösungsansatz - Logistik



Automatisierte Authentisierung von Transporteinheiten

1. Bevor ein bekannter Versender eine Transporteinheit an einen reglementierten Beauftragten verschickt, kündigt er dies letzterem durch Übermittlung der Identifikation der Transporteinheit und von Plausibilitätsdaten an.
2. Bei Eintreffen der Transporteinheit im Frachtzentrum des reglementierten Beauftragten wird sie dort authentisiert. Ihre Identifikationsdaten werden abgelesen und die Einheit wird aussortiert, sofern sie nicht avisiert worden ist oder ihre Plausibilitätsdaten widersprüchlich sind.

Lösungsansatz - Logistik



Automatisierte Autorisierung von Transporteinheiten

3. Sofern die Transporteinheit und ihr Versender korrekt als solche erkannt worden sind, sendet das Frachtzentrum eine verschlüsselte Autorisierungs-anfrage an alle dort bekannten und akkreditierten Versender, und zwar verschlüsselt mit dem aktuellen Einmalschlüssel der Kommunikation mit dem bekannten Versender, der die Transporteinheit avisiert hat. Dieser ist als einziger in der Lage, die Nachricht sinnvoll zu entschlüsseln.
4. Dieser bekannte Versender schickt als Antwort auf die Anfrage einen Teil der Autorisierungsbitkette (AC), die das empfangende Frachtzentrum mit der Autorisierungsbitkette der Transporteinheit vergleicht und letztere im Fall autorisiert, dass beide Teile übereinstimmen. Anderenfalls wird davon ausgegangen, dass die Transporteinheit manipuliert wurde, weshalb sie als nicht vertrauenswürdig aussortiert wird.

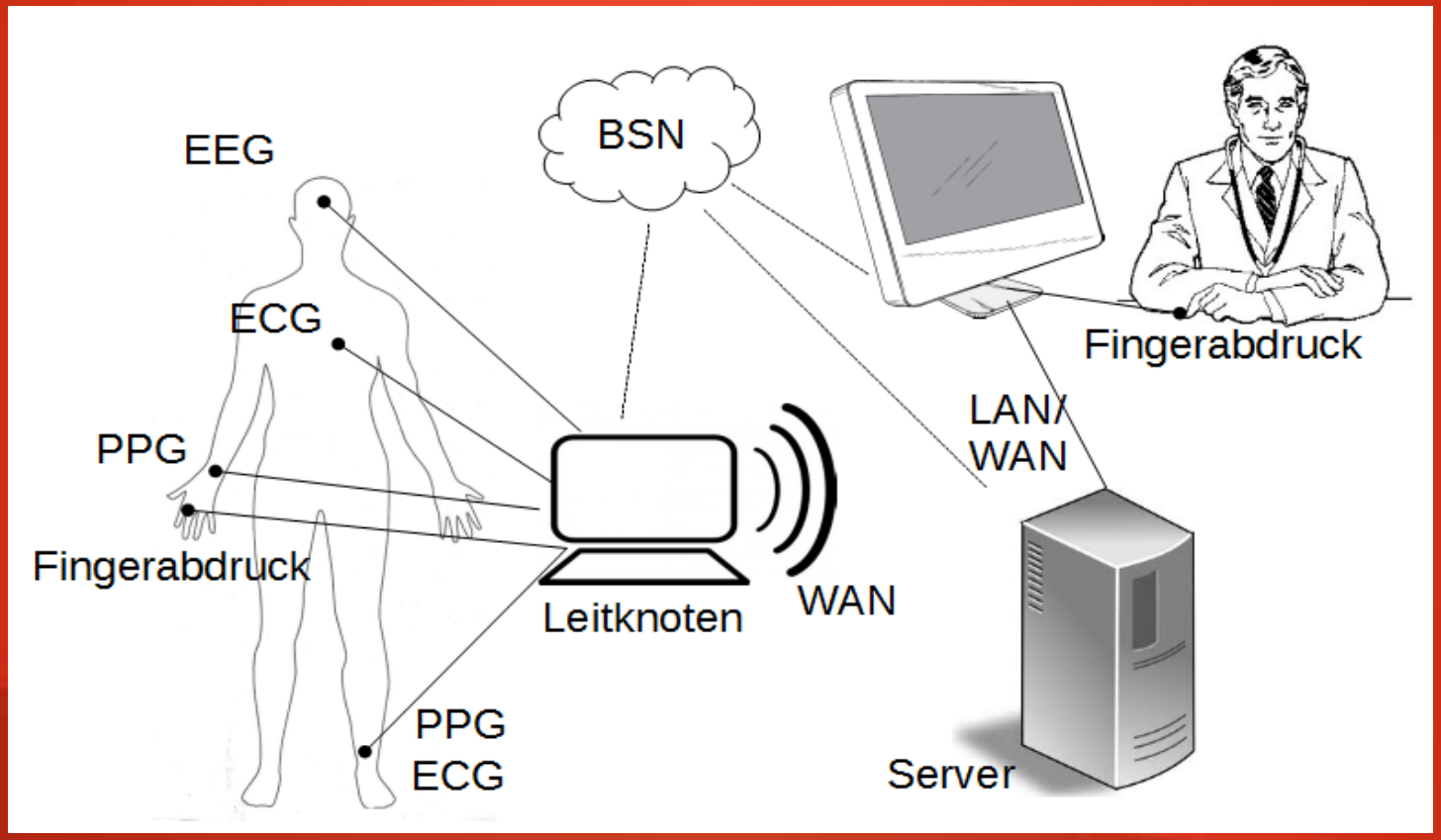
Authentisierung und Autorisierung im Gesundheitswesen

- Immer häufiger fallen diagnostische Befunde unmittelbar in elektronischer Form an.
- Diese Daten werden elektronisch weitergeleitet und –verarbeitet, bevor ein Arzt eine Diagnose stellen kann.
- Die Diagnosen sowie alle daraus resultierenden Handlungen werden ebenfalls elektronisch in der medizinischen Patientenakte abgelegt.
- Auf diese wird von verschiedenen Stellen aus zugegriffen: von Arztpraxen oder Krankenhäusern, um Befunde auszufertigen oder Rezepte auszustellen, bis hin zu Krankenkassen und anderen Versicherungsgesellschaften.
- Obwohl der Zugang zu medizinischen Daten gewöhnlich durch Passwörter geschützt ist, kommt es oft vor, dass dabei aus verschiedensten Gründen Sicherheitslücken entstehen.
- In der Konsequenz ermöglicht solches Verhalten uneingeschränkten unbefugten Zugang zu unseren Daten, die dann in verschiedensten Weisen missbraucht werden können.

Automatisierte Authentisierung und Autorisierung im Gesundheitswesen

- Aus den erwähnten Gründen wäre es besser, auf ein automatisiertes Authentisierungsverfahren wie bspw. RFID-basierte Smartcards zurückzugreifen.
- Da Herumtragen solcher Karten jedoch umständlich ist und sich ihr Verlust und Missbrauch nicht ausschließen lässt, bieten sich in der Medizin bereits eingeführte biometrische Verfahren auf der Grundlage unverlierbarer Merkmale zur Authentisierung und Autorisierung unmittelbar an.
- Der Einsatz biometrischer Verfahren bietet sich auch deshalb an, weil einige in der Medizin ohnehin schon zu diagnostischen Zwecken genutzt werden und entsprechende Geräte somit bereits vorhanden sind.
- Man braucht sie nur noch sinnvoll einzusetzen, um die Vertraulichkeit der im Verkehr zwischen Patient und behandelndem Arzt anfallenden Daten aufrecht zu erhalten und den Zugang zu Gesundheitsakten zu sichern.
- Biometrie wird als Authentisierungsmittel auch von der Telemedizin und bei Einsatz juxtakorporaler, d.h. am Körper installierter, Sensornetze benutzt.

Lösungsansatz - Gesundheitswesen



Automatisierte Authentisierung im Gesundheitswesen

1. Bevor ein Knoten einen Datenaustausch mit einem medizinischen Server startet, kündigt er dies dem Server durch Übermittlung seines Identifikators und von Plausibilitätsdaten an, verschlüsselt mit dem aktuellen Einmalschüssel der Kommunikation zwischen Knoten und Server.
2. Die Plausibilität der eintreffenden Anfrage wird überprüft; sofern die Plausibilitätsdaten widersprüchlich sind, wird die Kommunikation abgebrochen.

Automatisierte Autorisierung im Gesundheitswesen

3. Anderenfalls sendet der Server eine verschlüsselte Autorisierungs-anfrage an alle ihm bekannten und akkreditierten Knoten, und zwar verschlüsselt mit dem aktuellen Einmalschlüssel der Kommunikation mit dem anfragenden Knoten.
4. Dieser Knoten beantwortet die Anfrage mit seinem Entitäts-identifikator, den der empfangende Server mit seiner Datenbank abgleicht und die Kommunikation mit dem Knoten im Falle der Übereinstimmung beider Identifikatoren autorisiert. Anderenfalls wird der Knoten als manipuliert wahrgenommen, weshalb die Kommunikation als nicht vertrauenswürdig abgebrochen wird.

Automatisierte Authentisierung und Autorisierung im Gesundheitswesen

- Bei erfolgreicher Autorisierung eines BSN-Knotens oder Terminals wird in der Datenbank des Servers die elektronische Patientenakte geöffnet, mit der im weiteren Verlauf der Kommunikation bis zu deren normalem Abschluss diagnostische Daten verschlüsselt mit den aktuellen Einmalschlüsseln der Kommunikation zwischen Knoten und Server ausgetauscht werden.
- Wird die Übertragung unterbrochen, so muss sie unter Verwendung desselben Protokolls erneut aufgebaut werden.
- Falls sich die Autorisierung auf ein Terminal bezieht, verläuft die weitere Kommunikation mit dem Server ebenso, nur ist in diesem Fall darauf zu achten, nach jeder Anfrage die Verbindung nach einer bestimmten Zeit automatisch abzubrechen, damit sie dann explizit wieder neu aufgebaut werden muss.
- Bei einer Direktverbindung eines BSN-Knotens mit einem Terminal, wie sie in der Telemedizin erforderlich ist, muss das Terminal selbst die Möglichkeit haben, das Autorisierungsprotokoll und den späteren verschlüsselten Datenaustausch durchzuführen.

Zusammenfassung

- Mit der zunehmenden Informatisierung unseres Alltags steigt auch der Bedarf an Sicherheit der so genutzten Dienste und an Vertraulichkeit der im Zusammenhang mit ihnen übertragenen, gespeicherten und bearbeiteten Daten.
- Im vorliegenden Beitrag wurden Ansätze zum Schutz der in zwei besonders sicherheitskritischen Anwendungsbereichen anfallenden Daten vorgestellt mit dem Ziel, ein Umfeld zur sicheren Erfassung und Speicherung der Daten sowie zum vertraulichen Umgang mit ihnen für beide Anwendungsgebiete zu schaffen.
- Mit den beschriebenen Methoden lassen sich beteiligte Personen und Transport-einheiten sicher authentisieren und autorisieren.
- Die Methoden lassen sich leicht auf andere Bereiche und ähnliche Anwendungen, z.B. in der öffentlichen Verwaltung oder bei der Fernsteuerung automatisierter Anlagen und Betriebe, übertragen.