

# xChange - Dokumentation

Gerry Weirich

28. Juli 2008

## Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
<b>2</b>	<b>Voraussetzungen und Technik</b>	<b>2</b>
2.1	Umfang der Daten . . . . .	2
2.2	Datentransport . . . . .	2
<b>3</b>	<b>Anwendung</b>	<b>3</b>
3.1	Auswahl des Empfängers und des Übertragungsmodus . . . . .	3
3.2	Auswahl der zu übertragenden Daten . . . . .	5
3.3	Ergebnis der Ausgabe . . . . .	5
<b>4</b>	<b>Probleme und Lösungsansätze</b>	<b>5</b>
4.1	Duplizität . . . . .	5
4.2	Aktualität und Diskrepanz . . . . .	6
<b>5</b>	<b>Verschlüsselung</b>	<b>6</b>
5.1	Voraussetzung . . . . .	7
5.2	Exportvorgang . . . . .	7
5.3	Authentizität . . . . .	7
<b>6</b>	<b>Technische Informationen</b>	<b>7</b>
6.1	Grundlagen . . . . .	7
6.2	Implementationsdetails . . . . .	8

## 1 Einleitung

Mit der Implementation von SGAM.xChange macht Elexis einen weiteren Schritt hin zur universellen elektronischen Krankengeschichte: xChange ermöglicht es Elexis-Anwendern<sup>1</sup>,

---

<sup>1</sup>und theoretisch auch den Anwendern anderer KG-Programme, aber Elexis ist bisher die einzige, die das Konzept umgesetzt hat

Patientendaten untereinander auszutauschen. Dies können Daten fast beliebigen Detailgrades von einzelnen Laborwerten, Überweisungen, Berichten, bis hin zur kompletten KG sein.

Sgam.xChange entstand auf Initiative der Arbeitsgruppe Sgam.Informatics, welche auch die Entwicklung eines Pilotprojektes finanzierte<sup>2</sup>. Der Standard ist offen und kostenlos erhältlich und kann daher von jedem interessierten Hersteller implementiert werden (Die konkrete Implementation wird in den meisten Fällen selbstverständlich nicht kostenlos sein, aber es müssen keinerlei Lizenzgebühren an Sgam.Informatics bezahlt werden – die Kosten entstehen allein durch die Programmierarbeit des jeweiligen Programmherstellers. Es wurde beim Entwurf des Standards auf einfache und damit preisgünstige Implementierbarkeit geachtet). Die vorliegende xChange - Implementation ist eine Weiterentwicklung des Pilotprojektes, wobei vor die Stabilität und die Benutzerfreundlichkeit erheblich verbessert wurde.

## 2 Voraussetzungen und Technik

Die Basisfunktionalität ist in Elexis ab Version 1.4 enthalten. Für die Zusammenstellung der Daten und für den eigentlichen Transport sind Plugins oder externe Programme notwendig. Für die technischen Hintergründe sei auf Abschnitt 6 verwiesen.

### 2.1 Umfang der Daten

Personalien, Laborwerte, Briefe, Konsultationstexte, Diagnosen und Medikation können vom Basisprogramm transportiert werden. Daten, welche von Plugins verwaltet werden, können nur dann in den xChange-Transport eingebunden werden, wenn es für diese Plugins xChange-Adapter gibt. Die von Elexis selbst bereitgestellten Plugins wie Befunde, Omnivore oder Molemax werden im Zuge des normalen Update-Prozesses ohne weitere Kosten xChange-fähig werden. Bei Fremdplugins wenden Sie sich bitte an deren Hersteller.

### 2.2 Datentransport

Da wir hier mit sensiblen Patientendaten hantieren, muss dem Datenschutz besondere Beachtung geschenkt werden. Die exportierten Daten gelangen in einen Container (Eine Datei mit der Endung '.xchange'). Dieser Container ist zwar nicht ohne Hilfsmittel lesbar, aber er ist nicht verschlüsselt. Er darf daher nur auf gesicherten Wegen transportiert werden - man kann in auf einem Datenträger wie einem USB-Stick oder einer CD dem Patienten selbst mitgeben, oder man kann ihn über einen gesicherten Kanal wie ASAS per E-Mail transportieren. **Keinesfalls** darf man eine .xchange-Datei über unverschlüsselte E-Mail transferieren, und man sollte sie auch keinesfalls nach dem Versand auf dem eigenen PC belassen. Sie sollte vielmehr möglichst umgehend gelöscht werden.

---

<sup>2</sup><http://www.primary-care.ch/pdf/2007/2007-16/2007-16-169.PDF>

Eine viel bessere Methode bietet xChange mit der Technik der direkten Verschlüsselung des Containers an. Diese Methode braucht eine zusätzliche Software (GnuPG) und etwas mehr Bereitschaft des Anwenders, sich zusätzliche Kenntnisse anzueignen, erfüllt dafür dann aber höchste datenschützerische Anforderungen. Der Container ist in diesem Fall eine Datei mit der Endung '.xchange.gpg', welche die Daten in einer dem Stand der Technik entsprechenden verschlüsselten Form enthält. Ein solcher Container ist nur für den rechtmässigen Empfänger entschlüssel- und importierbar. Die Anwendung dieser Methode wird im Kapitel 5 genauer behandelt.

### **3 Anwendung**

Wenn Sie ein Export-Plugin installiert haben, können Sie mit Rechtsklick auf einen Patienteneintrag die Option 'KG Exportieren' wählen. Es erscheint ein Dialog, in dem Sie angeben können, welche Daten Sie exportieren wollen, und in welcher Form Sie sie an wen senden wollen, S. Abb. 1.

#### **3.1 Auswahl des Empfängers und des Übertragungsmodus**

Da Patientendaten besonders schützenswert sind, benötigen Sie im allgemeinen die Erlaubnis des Patienten. Elexis kann natürlich nicht prüfen, ob Sie diese Erlaubnis haben, aber Sie sind zumindest gezwungen, bei jedem Export zu deklarieren, ob Sie die Erlaubnis des Patienten explizit bekommen haben, oder ob Sie sie implizit haben (z.B. bei einem Notfalldienst-Bericht an den Hausarzt oder bei einem Überweisungsschreiben an einen Facharzt), oder ob in diesem Fall kein Einverständnis nötig ist. Klicken Sie das entsprechende Feld an (diese Angabe wird in der übertragenen Datei mit gespeichert).

Dann können sie einen Empfänger für die Daten auswählen. Wenn Sie keinen Empfänger auswählen, dann haben Sie nur die Option 'Unverschlüsselte Datei' anwählbar. Wenn Sie einen Empfänger anwählen (er muss als Kontakt vorhanden sein), dann hängen die verfügbaren Optionen davon ab, was über diesen Empfänger bekannt ist. Wenn eine E-Mail-Adresse angegeben ist, dann haben Sie auch die Möglichkeit 'Unverschlüsselte E-Mail'. Denken Sie daran, dass Sie Patientendaten aus Datenschutzgründen niemals über eine unverschlüsselte E-Mail-Verbindung senden dürfen. Daher darf diese Option nur ausgewählt werden, wenn sowohl Sie als auch der Empfänger eine ASAS-Mailadresse verwenden. Wenn sowohl Sie als auch der Empfänger ausserdem im Besitz eines xChangeKeys sind, dann stehen auch die Möglichkeiten 'verschlüsselte Datei' und 'verschlüsselte E-Mail' zur Verfügung. Eine solche E-Mail bzw. Datei darf auch über ungesicherte Mailverbindungen (ohne ASAS) transferiert oder auf anderen ungesicherten Wegen transportiert werden, da nur der Empfänger in der Lage ist, sie zu entschlüsseln. Das Konzept der gesicherten Übertragung mit xChangeKey ist unter Verschlüsselung (Kapitel 5) näher erläutert.

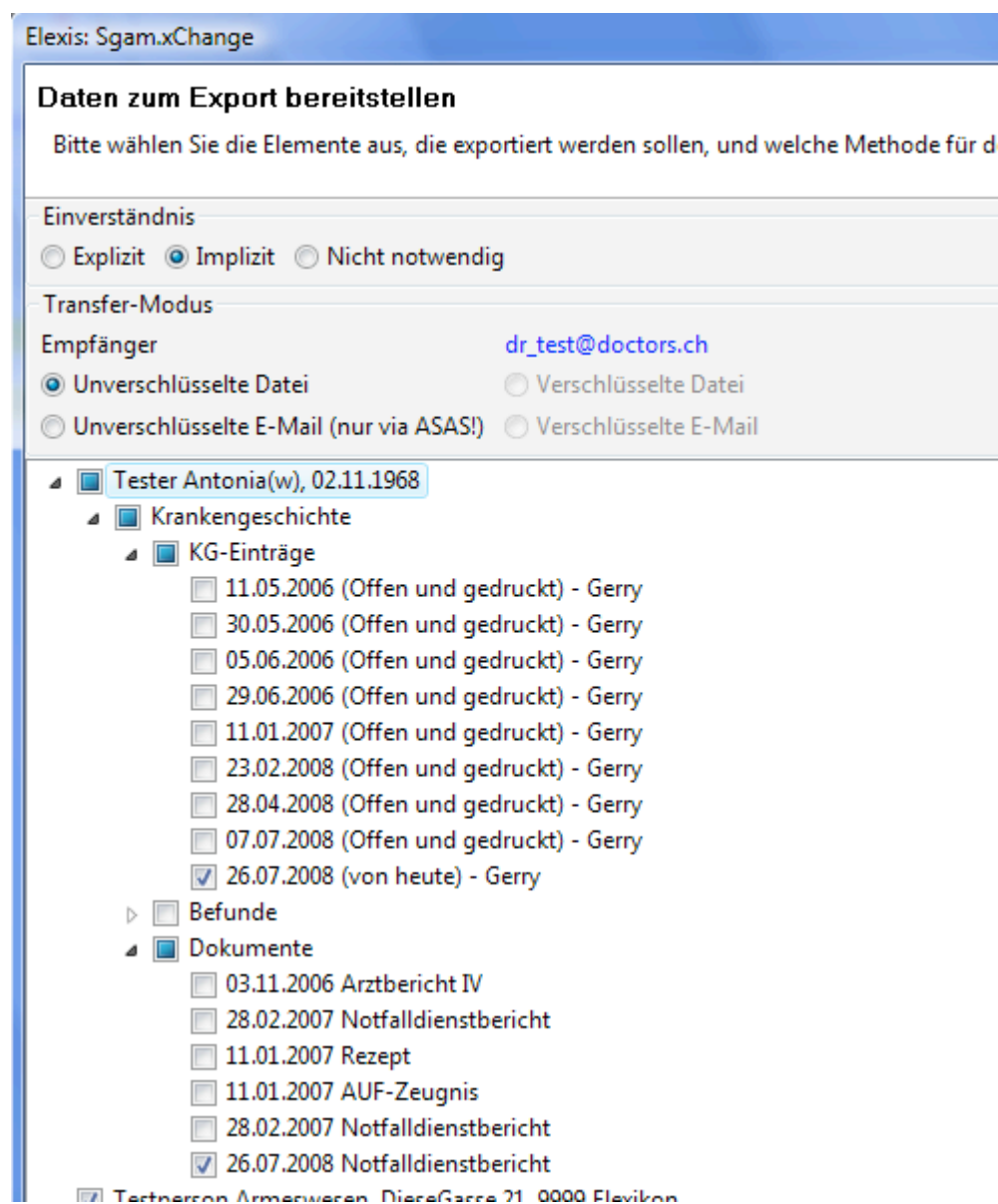


Abbildung 1: Exportauswahl

```

<?xml version="1.0" encoding="utf-8" ?>
- <xChange:xChange xmlns:xChange="http://informatics.sgam.ch/xChange" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:schemaLocation="http://informatics.sgam.ch/xChange xchange.xsd" timestamp="2008-07-26T10:21:22" id="x4fda0f6d1a7121dc4b483"
  origin="cd8987aec2f3e4b43788" destination="undefined" responsible="cd8987aec2f3e4b43788">
  <xChange:header creatorName="Elexis" creatorID="ch.elexis" creatorVersion="1.3.2" protocolVersion="1.0.1" language="de" authorization="implicit" />
- <xChange:contacts>
- <xChange:contact id="f545f4a171b7f3093c6285" type="person" lastname="Tester" firstname="Antonia" sex="female" birthdate="1968-11-02">
  - <xChange:xid uuid="f545f4a171b7f3093c6285">
    <xChange:identity domain="www.elexis.ch/xid" domainID="f545f4a171b7f3093c6285" quality="localAssignment" isGUID="true" />
  </xChange:xid>
  <xChange:address street="Hinterdorf 2" zip="9998" city="Krankenhausen" country="CH" description="default" />
  <xChange:contactref description="Freund" refID="x123.45.678" />
  <xChange:contactref description="Hausarzt" refID="cd8987aec2f3e4b43788" />
  - <xChange:medical>
  - <xChange:anamnesis>
    - <xChange:episode beginDate="2006-05-30" id="x8081640b600e160cb4499" name="D50.0 Eisenmangelanämie nach Blutverlust (chronisch)">
      <xChange:diagnosis codesystem="ICD-10" code="D50.0" />
    - <xChange:insurance dateFrom="2006-05-11" reason="disease" companyref="f545f4a171b7f3093c6285">
      <xChange:contract />
    </xChange:insurance>
  </xChange:anamnesis>
  </xChange:medical>
  </xChange:contact>
</xChange:contacts>

```

Abbildung 2: Ausschnitt aus xChange-Datei (XML)

## 3.2 Auswahl der zu übertragenden Daten

Wie Sie in Abb 1 sehen, können Sie den vorher ausgewählten Patienten, alle damit zusammenhängende Kontakte, sowie die KG des Patienten separat zum Einschluss in den Transfer auswählen. Wenn Sie beispielsweise nur einen Notfalldienstbericht oder eine Facharztanmeldung senden wollen, dann genügt, es, den entsprechenden Brief und/oder den dazugehörigen Konsultationseintrag und die dazugehörigen Befunde auszuwählen. Wenn Sie das gesamte Dossier senden wollen, z.B. weil der Patient den Wohnort wechselt und zu einem neuen Arzt geht, dann können Sie den gesamten Patienteneintrag auswählen. Wenn Sie eine Rubrik markieren oder demarkieren, werden jeweils alle darunterliegenden Einträge automatisch mitmarkiert bzw. mit demarkiert.

## 3.3 Ergebnis der Ausgabe

Die angegebenen Daten werden dann in eine xChange-Datei exportiert. Eine xChange-Datei besteht aus einer XML-Datei, wie im Ausschnitt in Abb. 2 dargestellt, sowie den beigefügten externen Dokumenten. Diese Datei wird dann je nach gewähltem Modus verschlüsselt und gespeichert oder direkt per E-Mail versandt.

# 4 Probleme und Lösungsansätze

## 4.1 Duplizität

Wann immer Daten von einer Krankengeschichte in eine andere importiert werden, stellt sich die Frage: 'Ist dieser Datensatz bereits vorhanden?' Beispielsweise könnte der Patient, dessen Daten von Dr. X zu Dr. Y transferiert werden, schon früher einmal bei Dr. Y gewesen und in dessen KG erfasst worden sein. In diesem Fall muss das System erkennen, dass derselbe Datensatz schon vorhanden ist und muss neue Daten an diesen anhängen, anstatt denselben Patienten ein zweites Mal zu erstellen. Dies ist schwieriger, als es auf den ersten Blick scheinen mag: Lisa Müller bei Dr. X kann Elisabeth

Müller-Meier bei Dr. Y. sein. Die AHV-Nummer kann sich wegen Heirat oder Einbürgerung geändert haben. Die Adresse kann einmal als Rudolfstrasse 17 und einmal als Rudolfstr. 17a erfasst sein, die Plz einmal als 8200 und einmal als 8203. Sie sehen, es gibt im Grunde keine 'wasserdichte' Methode, um immer zu erkennen, dass ein bestimmter Patient schon vorhanden ist<sup>3</sup>. xChange sieht ein mehrstufiges System vor, das nebst Name, Vorname und Adresse auch die Xid in die Erkennung einbezieht (s. dazu auch <http://www.elexis.ch/jp/content/view/214/45/>). Dennoch kann diese Erkennung aus prinzipiellen Gründen nicht in allen Fällen völlig sicher sein.

Wenn das Importmodul zweifelsfrei erkennen kann, dass ein bestimmter Datensatz schon existiert, dann werden die Daten aus dem Import nur ergänzt. Wenn der Importer 'merkt', dass ein Datensatz möglicherweise schon vorhanden ist, dann wird er eine Rückfrage stellen und Sie bitten, die Entscheidung zu treffen, ob die Daten ergänzt oder neu erstellt werden sollen, oder ob dieser Datensatz ganz übersprungen werden soll. In allen anderen Fällen wird der Importer den Datensatz als neu importieren, was, wie oben ausgeführt, dazu führen kann, dass manche Daten nachher doppelt vorhanden sind.

## 4.2 Aktualität und Diskrepanz

Angenommen der Importer erkennt, dass 'Testperson Armeswesen' von Dr. X. zweifelsfrei dieselbe Person ist, wie die gleichnamige Patientin von Dr. Y.<sup>4</sup> Nun hat der zu importierende Datensatz aber eine andere Adresse oder ein anderes Geburtsdatum, als der vorhandene Datensatz. Der Importer kann nun nicht automatisch erkennen, welche Daten korrekt sind. Vielleicht hat sich die Adresse geändert oder das Geburtsdatum wurde entweder bei Dr. X oder bei Dr. Y falsch erfasst. In einem solchen Fall wird der Importer eine Rückfrage stellen, ob die vorhandenen oder die neuen Daten behalten werden sollen.

## 5 Verschlüsselung

Mit der xChange Verschlüsselung können die zu transportierenden Daten auf eine Weise verschlüsselt werden, dass niemand ausser dem rechtmässigen Empfänger<sup>5</sup> sie lesen kann. Dieses Kapitel beschränkt sich zunächst auf die praktischen Aspekte der xChange-Verschlüsselung. Die theoretischen Grundlagen dazu finden Sie im Abschnitt 6.

---

<sup>3</sup>Falls dermaleinst wirklich eine eindeutige und lebenslänglich unveränderliche Sozialversicherungsnummer eingeführt wird, und falls diese Nummer auch zum Zweck des Datenabgleichs verwendet werden darf, dann wird dieses Problem keines mehr sein. Im Moment sind wir allerdings noch nicht so weit

<sup>4</sup>beispielsweise anhand der identischen AHV-Nummer oder einer identischen Krankenkassen-Mitgliedsnummer

<sup>5</sup>Auch Sie selbst können eine einmal verschlüsselte xChange-Datei nicht mehr entschlüsseln, ausser Sie sind selber der Empfänger.

## 5.1 Voraussetzung

Die Verschlüsselung von xChange-Daten ist nur dann möglich, wenn sowohl der Sender als auch der Empfänger der Daten im Besitz eines xChangeKeys sind. Ein solcher Schlüssel kann bei Elexis oder einer anderen autorisierten Abgabestelle bezogen werden. Elexis erkennt beim Export automatisch, wenn der angegebene Empfänger über einen xChangeKey verfügt<sup>6</sup>. Ausserdem müssen Sie das Programm 'GnuPG' installiert haben, das es kostenlos bei <http://www.gnupg.org> für Windows, Linux und MacOS-X zum download gibt.

## 5.2 Exportvorgang

Wenn sowohl xChangeKey als auch das GnuPG-Programm gefunden wird, haben Sie bei den Exportoptionen (Vgl. Abb. 1) auch die Möglichkeit 'verschlüsselte Datei' oder 'verschlüsselte E-Mail'. Nach dem Klick auf 'OK' werden Sie aufgefordert, das Passwort für Ihren xChangeKey einzugeben. Alles andere funktioniert genau gleich, wie beim 'gewöhnlichen' Export. Wenn Sie glauben, verschlüsselter Export müsste möglich sein, aber die entsprechenden Optionen sind trotzdem nicht anwählbar, dann können Sie 'Test' anklicken. Elexis zeigt dann an, welche Voraussetzungen für die Verschlüsselung vorhanden resp. nicht vorhanden sind.

## 5.3 Authentizität

Mit der xChange-Verschlüsselung bekommen Sie noch einen zweiten Benefit quasi 'gratis' mitgeliefert: Jedes so übertragene Dokument erhält Ihre elektronische Signatur (diese ist Teil des xChangeKeys). Ganz ohne HealthProfessionalCard<sup>7</sup> oder andere teure Gerätschaften können Sie also mittels SGAM.xChange gesicherte und authentifizierte Datenübertragung gewährleisten.

# 6 Technische Informationen

## 6.1 Grundlagen

Eine kurze Einführung in die verwendete Verschlüsselungstechnik finden Sie hier:

<http://www.elexis.ch/jp/content/view/81/63/>

Ein xChangeKey ist 'unter der Haube' einfach ein Schlüsselpaar nach OpenPGP-Standard<sup>8</sup> resp. rfc 4880<sup>9</sup> plus eine Verwaltungssoftware, die den Anwender davon befreit, sich selber um die Details der Schlüsselgenerierung und des Schlüsseltransfers zu kümmern - beim SGAM xChange Pilotversuch hatte sich gezeigt, dass dieses Schlüsselhandling eine relativ grosse Hürde darstellte.

---

<sup>6</sup>Voraussetzung: Es muss eine Verbindung zum Internet bestehen.

<sup>7</sup>Für diese bezahlt die FMH aus ihren Mitgliederbeiträgen ca. eine Million Franken pro Jahr!

<sup>8</sup><http://de.wikipedia.org/wiki/OpenPGP>

<sup>9</sup><http://tools.ietf.org/html/rfc4880>

In der aktuellen xChange-Version wird das Schlüsselhandling automatisiert. Es genügt für den Anwender, einen xChangeKey zu beantragen, den Rest erledigt die Software und die auf einem internet-Server lokalisierte Infrastruktur. Der xChangeKey dient zur Signatur und zur Ver/Entschlüsselung. Der xChangeKey wird Ihnen auf einem Datenträger zugestellt, hat ein anwenderfreundliches Installationsprogramm und wird durch ein von Ihnen zu wählendes Passwort gesichert, damit keine unbefugte Verwendung durch Dritte, die Zugriff auf Ihren PC haben, möglich ist. Die öffentlichen Schlüssel aller xChange-Teilnehmer werden auf dem Server verwaltet und für Transfers bereitgestellt. Elexis fragt diesen Server automatisch ab, wenn eine xChange- Datei verschlüsselt übermittelt werden soll.

Da die Errichtung und Bereitstellung dieser Infrastruktur und das Management der automatischen Schlüsselverwaltung von jemandem erstellt und gepflegt werden muss, kann diese Dienstleistung im Gegensatz zum manuellen Schlüsselmanagement der alten xChange-Version nicht mehr gratis sein. Es steht Ihnen aber weiterhin frei, selber einen Schlüssel zu erstellen und mit Ihren xChange-Partnern 'von Hand' auszutauschen, dann können Sie xChange weiterhin kostenlos benutzen. (Dasselbe gilt natürlich auch, wenn Sie ganz auf die eingebaute Verschlüsselung verzichten und Mails grundsätzlich via ASAS transferieren. Es liegt dann aber komplett in Ihrer Verantwortung, die manchmal etwas kryptischen ASAS-Meldungen korrekt zu interpretieren damit Sie realisieren, wenn eine bestimmte Mailverbindung gar nicht verschlüsselt wird.).

Die definitiven Bedingungen für die xChangeKeys sind noch nicht festgelegt, aktuell können sie noch kostenlos direkt bei admin (at) elexis.ch bezogen werden. Längerfristig wird der Preis wohl in der Region von ca. CHF 30.- pro Jahr liegen.

## **6.2 Implementationsdetails**

Der Datenfluss aus der Elexis-Datenbank in einen xChange-Transport ist in Abb. 3 schematisch dargestellt. Wie Sie sehen, wird der Transport vom Elexis.Kern angestossen und xChange-fähige Plugins erhalten Gelegenheit, die von ihnen verwalteten relevanten Daten einzubringen. Am Ende sorgt ein Transporter-Plugin dafür, dass die exportierten Daten in der korrekten Weise aufbereitet werden. Als Anwender wählen Sie lediglich mit Hilfe des Menüs, das bei Rechtsklick auf den Patienten erscheint, den gewünschten Transporter aus. Hier als Beispiele die Transporter für xChange-Transport und für Ausdruck der Daten.

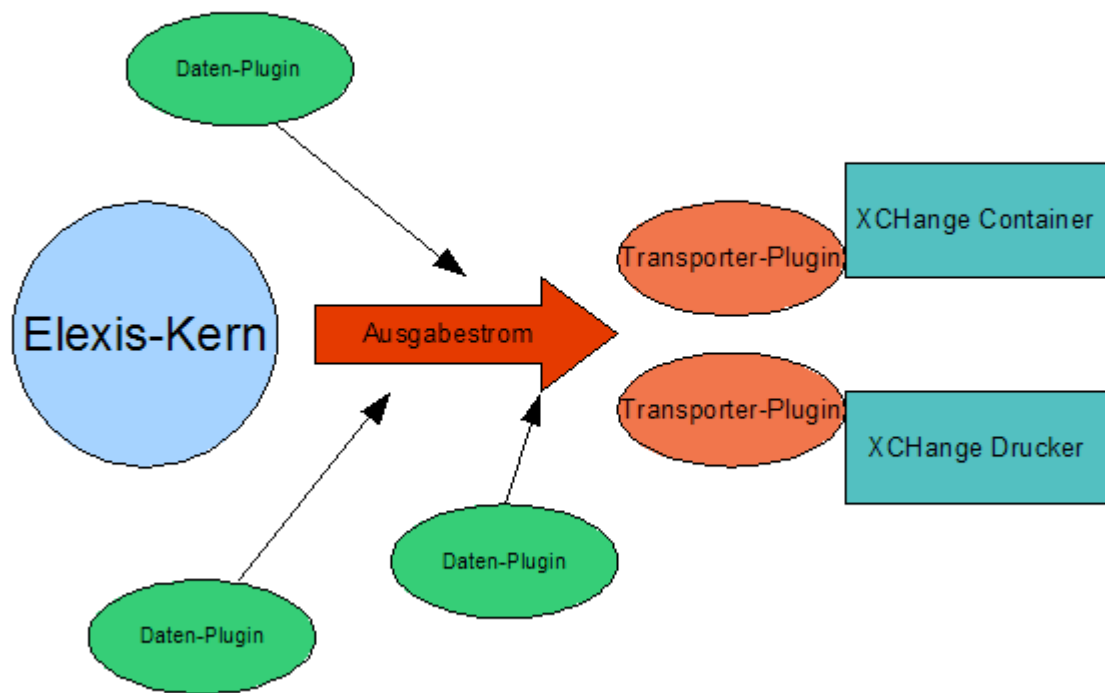


Abbildung 3: Datenfluss in xChange