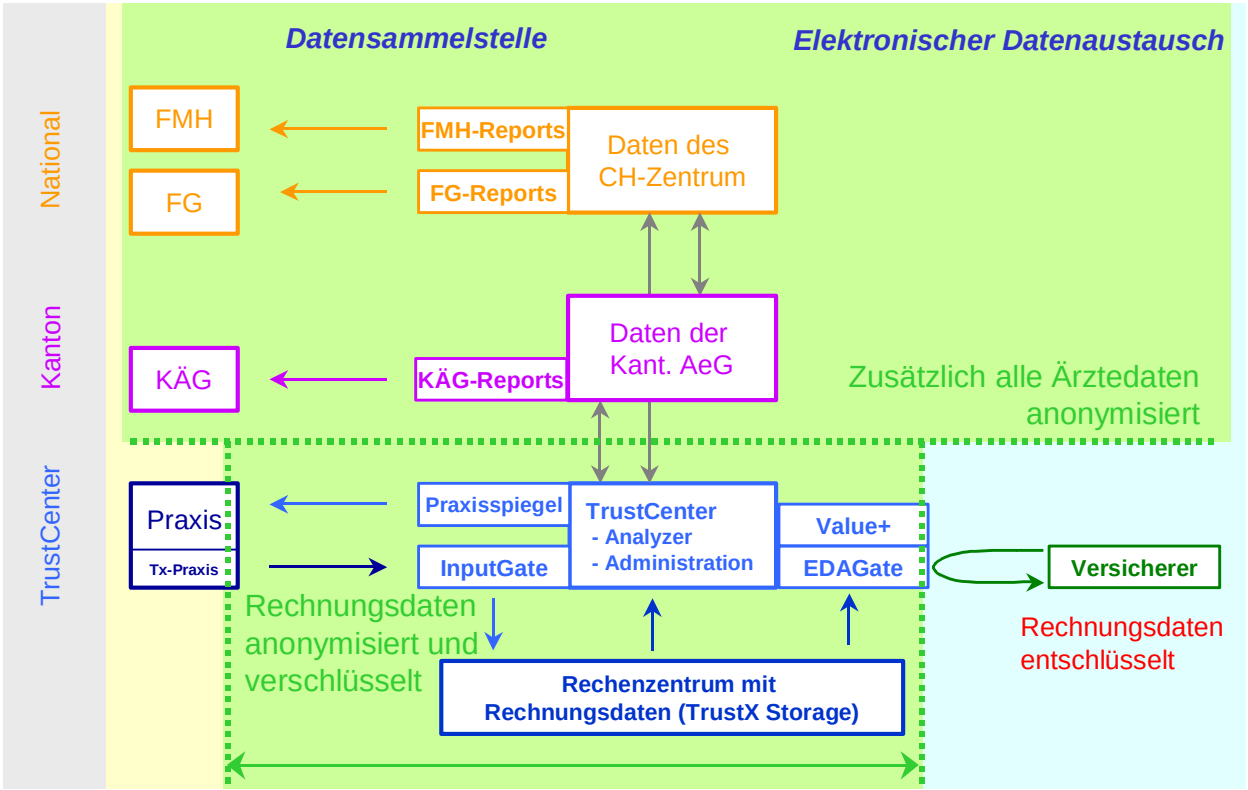
Anonymisierung und Verschlüsselung in TrustX

1. Übersicht über das Gesamtsystem TrustX



TrustX ist ein Administrations-, Analyse- und Auswertungssystem für die 11 TrustCenter der Schweiz und besteht aus einer Reihe von Modulen (siehe auch www.trustx.ch). Das System hat neben administratorischen Aufgaben zwei Hauptfunktionen: "Daten sammeln für statistische Auswertungen" und "elektronischer Datenaustausch". Dazu liefern die Arztpraxen Rechnungsdaten an das InputGate ihres TrustCenters. Diese elektronischen Rechungen werden durch TrustX-Praxis in der Arztpraxis anonymisiert und verschlüsselt.

Im InputGate des TrustCenters wird der Rechnungsdatenstrom entsprechend der beiden Hauptfunktionen von TrustX aufgetrennt.

- Für den Datenstrom "Daten sammeln" und die daraus erstellten statistischen Auswertungen werden nur anonymisierte Rechnungsdaten gespeichert und verwendet.
- Für den Datenstrom "elektronischer Datenaustausch" werden stark verschlüsselte Rechnungsdaten verwendet. Diese werden erst nach der Anforderung der Rechnungen durch die Versicherer im eDA-Gate des TrustCenters entschlüsselt und SSL-gesichert ausgeliefert.

Arztpraxis ⇨ IG TrustCenter

⇨ **anonymisierte Daten für Statistik**

⇨ **verschlüsselte Daten für elektr. Datenaustausch**

2. Verschlüsselung und Anonymisierung in der Arztpraxis

Die elektronischen Rechnungen werden wie erwähnt in der Arztpraxis bezüglich Personendaten des Patienten durch TrustX Praxis verschlüsselt (für elektronischen Datenaustausch) und anonymisiert (für Statistik). Dies bedeutet folgendes:

Verschlüsselung

Zur Verschlüsselung werden RSA-Verfahren verwendet. Diese gelten als sehr sicher und basieren auf privaten und öffentlichen Schlüsseln (Schlüssellänge 1024 Bit). Zur Verwaltung der öffentlichen Schlüssel wird die Public Key Infrastructure (PKI) von Health Info Net (www.hin.ch) verwendet. Die HIN PKI ermöglicht eine einfache und automatisierte Verteilung und Aktualisierung der öffentlichen Schlüssel / Zertifikate.
Die Rechnungsdaten werden durch TrustX-Praxis in der Arztpraxis mit dem öffentlichen Schlüssel des gewählten TrustCenter verschlüsselt. Eine Entschlüsselung ist nur mit dem privaten Schlüssel des TrustCenters und mit einem Entschlüsselungsmodul möglich. Dieses Modul ist im eDA-Gate implementiert und nicht zugänglich.

Ausschnitt von verschlüsselten Patienteninformationen in einer XML-Rechnung:

```
<trustx:data type="patient">MIAGCSqGSIb3DQEHA6CAMIIFLQIBADGCAxUwggEDAgEAMGwwZjEUMBIGA1UEAxML
  Z2F0ZS5oaW4uY2gxGzAZBgNVBAoTEkhlYWx0aCBOZXR3b3JrcyBBRzESMBAGA1UE
  BxMJS3Vlc25hY2h0MRAwDgYDVQQIEwdadWVyaWNoMQswCQYDVQQGEwJDSAICAfYw
  DQYJKoZIhvcNAQEBBQAEgYBHjbOXsLmH4JE+fD1FDXfg0yDhmthEHVcQzSrtGMLt
  2QxgRP6TNiEeaEht8zW3yyNzS9qoGxqvf4oXJwoH1ciqo7IiLTqG7OQC2GFRQtMQ
  MlHzSDf/GL+MJA4l1fKGk8wePSEFJJuAu6OrdRy5iEQMxl026yvpjouYg9cahxcC
```

Anonymisierung

TrustX Praxis anonymisiert nach der Verschlüsselung die entsprechenden Patienteninformationen in der elektronischen Rechnung, so dass eine Entschlüsselung dieser Datenfelder nicht mehr möglich ist.
Um anonymisierte Rechnungsdaten trotzdem patientenbezogen auswerten zu können, wird vor der Anonymisierung aus den Personalien ein nicht umkehrbarer Hash-Code (unique_id) erzeugt, der als Patienten-Identifier verwendet werden kann. Dieser anonyme Identifier wird analog der vom BFS für die "Statistik der stationären Betriebe des Gesundheitswesens" vorgeschlagen Methode bestimmt.

Ausschnitt aus anonymisierter XML-Rechnung:

```
- <invoice:patient gender="male" birthdate="1990-01-01T00:00:00" unique_id="a075d5b275a028d01c95395230c915">
  - <invoice:person>
      <invoice:familyname>XXXXXXXX</invoice:familyname>
      <invoice:givenname>XXXXXXX</invoice:givenname>
    - <invoice:postal>
        <invoice:street>XXXXXXXXXXXXXXXXXX</invoice:street>
        <invoice:zip>9999</invoice:zip>
        <invoice:city>XXXXXXXXXX</invoice:city>
      </invoice:postal>
    </invoice:person>
  </invoice:patient>
```

3. Sicherung des Transports via Internet durch HIN

Die Rechnungsdaten werden für den Transport durch das Internet zusätzlich HIN ASAS streckenverschlüsselt (SSL mit Authentifikation beider! Partner). Siehe dazu auch www.hin.ch. Damit ist ein sicherer Transport durch das Internet gewährleistet und zwar von der Arztpraxis zum InputGate des TrustCenters und vom eDA-Gate zum Versicherer.

4. Vertragliche Regelungen

Neben technischen Massnahmen zur Gewährleistung des Datenschutzes bestehen zudem zwischen allen Partnern Verträge, welche den vertraulichen Umgang mit Daten DSG-konform regeln.