Privacy en security in het Landelijk Schakelpunt

Niels Sijm

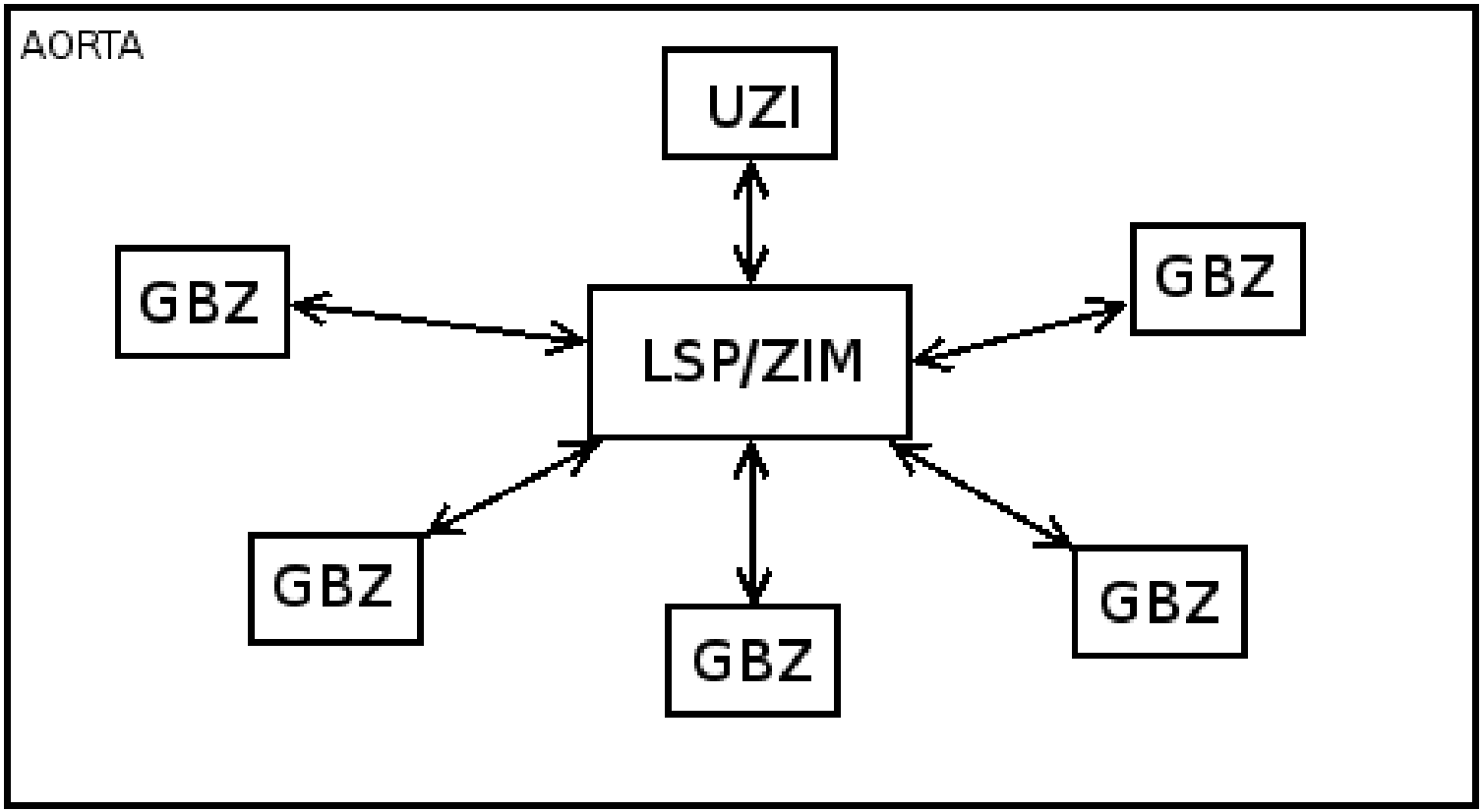
July 2, 2008

Inhoud presentatie

Inleiding Landelijk Schakelpunt

- Landelijk digitaal uitwisselen van medische informatie
- Vereiste voor invoering Elektronisch Patinten Dossier (EPD)
- Onderdeel van AORTA
- Ontworpen door Nictiz in opdracht van ministerie van VWS

Basale architectuur



Onderzoeksdefinitie

1. In kaart brengen architectuur en ontwerpbeslissingen LSP
2. Diepte-onderzoek naar verwijsindex

Taken en verantwoordelijkheden

- Authenticatie (zorgverleners, zorgsystemen en LSP)
- Autorisatie van zorgverleners
- Bijhouden en ontsluiten van verwijsindex
- Doorgeven van medische gegevens
- Bijhouden van een toegangslog

Authenticatie

- Authenticatieproces maakt gebruik van UZI-register
  - Unieke Zorgverlener Identificatie
  - UZI-pas is smartcard, beveiligd met pincode
  - Zorgapplicatie leest UZI-pas met card reader uit
- Verschillende X.509-certificaten
  - Authenticatie
  - Encryptie
  - Digitale handtekening
- Root van UZI-certificaten is Staat der Nederlanden Root CA

Autorisatie

- Autorisatie bij LSP afhankelijk van beroepsfunctie zorgverlener
- Patiënt kan in zorgprofiel toegang ontzeggen
  - Uitwisselen van medische gegevens totaal verbieden
  - Individuele zorgverleners toegang tot bepaalde medische gegevens verbieden
- Zorgaanbieder controleert omstandigheden
  - Behandelrelatie zorgaanbieder/patint
  - Noodzaak tot inzage patintgegevens
  - Noodsituatie
- Zorgverlener kan taken delegeren via interne mandateringstabel

Verwijsindex

- Verwijsindex centrale component van LSP
- Koppeling van patiënten aan dossiers van zorgaanbieders
  - Koppeling op basis van burgerservicenummer (BSN)
  - Dossierstukken uniek identificeerbaar via patiëntgegevens-id
- Scheiden van beheerverantwoordelijke en inhoudverantwoordelijke
  - Alleen beheerverantwoordelijke kan verwijzingen muteren
  - Beheerverantwoordelijke en inhoudverantwoordelijke vaak zelfde zorgaanbieder

Verwijsindex

- Bij aanmelden verwijzing wordt gegevenssoort vermeld
- Voorbeelden van gegevenssoorten
  - Adresgegevens
  - Diagnose
  - Labuitslag
  - Medicatieverstrekking
  - ...
- LSP houdt in autorisatieprotocol bij welke beroepsfuncties toegang tot welke gegevenssoorten hebben

Verwijsindex

- Ontsluiting via web services
- Technische infrastructuur web services
  - TCP/IP (transport)
  - HTTPS (authenticatie en encryptie)
  - SOAP (XML RPC framework)
  - HL7v3 (medische informatie)
- HL7v3 is gestandaardiseerd formaat voor uitwisselen medische informatie
  - Gebaseerd op XML
  - Wereldwijde omarmd door de gezondheidszorg

Doorgeven medische gegevens

- Centraal via LSP of tussen zorgaanbieders onderling
- Nictiz pleit voor uitwisseling medische gegevens via LSP
- LSP authenticeert communicerende zorgaanbieders
  - Zorgaanbieder authenticeren elkaar meestal niet
- End-to-end encryptie mogelijk; wordt vaak niet vereist
  - Berichten gaan leesbaar door LSP heen (!)

Bijhouden toegangslog

- Centraal bijgehouden door het LSP
- Gebruikersinteracties worden gelogd
  - In- en uitloggen zorgverleners
  - Opvragen index gegevens
  - Opvragen en versturen medische gegevens
  - Aan- en afmelden medische gegevens
- Toegangslog slaat geen medische gegevens op

Discussie en verder onderzoek

- Lijst met beschermde beroepstitels wellicht te grofmazig
- Uitwisselen van informatie vaak zonder end-to-end authenticatie
- Nictiz pleit voor uitwisselen medische gegevens via LSP
- Samenstelling sleutels in verwijsindex (information disclosure)