KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
PROGRAMŲ INŽINERIJOS KATEDRA

Valdas Šimas

Medicininių duomenų apsauga HL7 standarte

Magistro darbas

Darbo vadovas
doc. E.Karčiauskas

Kaunas, 2004

Turinys

Summary

That is not the secret that most of health insuranse institutions are still using hand-documentation methods for information helding, processing and transmission. The research shows that about 70% of international medical transactions are accompished with the help of the telephony, fax or paper. For example, only in Lithuania this percent is the whole 100. Only in very special cases medical information exchange invokes current technical solutions.
KMU centre of heart disease can be said is the beginner of the idea…The project started had to be extended to invoke all the medical Lithuanian institutions. With the help of KTU faculty of informatics the prototype for medical documents interchange was created.
Having the solution of medical documentation interchange, I defined the problem area as medical information security problems. The data security problem is not the new one in the world of computer science. But this problem is very important and the new one in the world of medicine. The only one medical information fault in medicine can reason the human's tragedy.
The first my step is to define medical information security strategy. This will be accomplished by the analyzing main information security services.
Having the defined strategy I will choose security technologies and will design the medical documentation security implementation. This work can be find in the analytical part of the current document.
Design part of the document will show the solution of medical document solution. This case study will prove that defined conclusions of analysis were right, After that, the next step is to integrate my implemented security strategy with the existing medical documentation interchange standard system.
I will accomplish the research to name the shortcomings of the medical documents security issues. That will help to define the/my main analysis and implementation mistakes.

1. Įvadas

Dokumento paskirtis

Šis dokumentas skirtas įvardinti pagrindines medicininės informacijos saugumo problemas. Atliekant probleminės srities analizę bus suformuluojami pagrindiniai reikalavimai duomenų saugumui ir aprašomi medicininių dokumentų apsaugos panaudojimo atvejai. Suformulavus duomenų apsaugos struktūra, bus atliekamas jos programinio realizavimo kelio tyrimas. Būtina atkreipti dėmesį, kad problemų sprendimui realizuoti pasirinktos technologijos turi būti suderinamos su jau sukurta HL7 medicininių dokumentų mainų sistema.

Pasirinkus reikalingas technologijas bei jomis realizavus jų - pagalba medicininių dokumentų apsaugos sprendimą, bus atliekamas sprendimo integracijos su esama programinę įranga, tyrimas bei eksperimentai. Apibendrinti tyrimų ir eksperimentų rezultatai, leis daryti išvadas ar tiriamojo darbo eigos kryptis buvo pasirinkta teisingai, ir kurias sukurtos sistemos vietas reikėtų tobulinti. Šio dokumento pabaigoje bus suformuluotos pagrindinės tiriamojo darbo išvados, kurios atspindės kiekvieną šio darbo iteraciją bei galutinį rezultatą.

Santrauka

Ne paslaptis, kad dauguma sveikatos apsaugos įstaigų vis dar naudojasi „popieriniais“ metodais informacijos kaupimo, apdorojimo ar perdavimo metodais. Sveikatos apsaugos sistemų tyrimai pasaulinių mastu rodo, kad 70 proc. visų informacijos transakcijų yra atliekama telefonų skambučiais, fakso aparatų ar popieriaus lapų, kuriuose pateikta reikalinga informacija, pagalba. Jeigu atliktume lokalesnį tyrimą, Lietuvos sveikatos apsaugos sistemų tyrimą, įsitikintume, kad šis skaičius praktiškai yra lygus 100 proc.. Tik labai išskirtinais atvejais informacijos mainai pasitelkia šiuolaikinius informacinius sprendimus ir yra vykdomi tik gydymo įstaigos viduje, nekalbant jau apie mainus tarp atskirų gydymo įstaigų.

Vieningos Lietuvos sveikatos apsaugos įstaigų sistemos sukūrimo idėjos iniciatoriumi santykinai galima laikyti KMU Širdies centrą. Jis užsibrėžė tikslą įdiegti vidinę įstaigos informacinę sistemą. Šis projektas ateityje turėjo peraugti į globalesnį mastą, tai turėjo būti žingsnis link vieningos Lietuvos sveikatos apsaugos įstaigų sistemos. Bendradarbiaujant su KTU Informatikos fakulteto Programų inžinerijos katedra, buvo sukurtas medicininių dokumentų mainų sistemos prototipas.

Sistemos prototipo šerdis yra medicininių dokumentų standarto HL7 panaudojimas. Šį standartą sudaro taisyklių ir reikalavimų rinkinys, skirtas aprašyti medicininiams dokumentams aprašyti. Tai yra

būtina, kad komunikuojančios sistemos galėtų priiminėti, atpažinti ir apdoroti informaciją, gautą viena iš kitos.

Programinis šio prototipo realizavimo sprendimas remiasi B2B architektūra. Tam buvo panaudotas BizTalk serveris ir jo komunikavimo, informacijos apdorojimo funkcionalumas.

Realizavus medicininių dokumentų mainų programinį sprendimą, kaip pagrindinę problemą, susijusią su medicinine informacija, iškėliau duomenų saugumo klausimą. Ši problema nėra naujiena informacinių technologijų segmente. Bet tai viena iš aktualiausių ir einamuoju momentu labiausiai linksniuojamų problemų sveikatos apsaugos segmente. Bet koks informacijos praradimas, „nutekėjimas“, sugadinimas ar jos negavimas gali turėti tragiškų pasekmių, ypatingai kai yra kalbama apie žmogaus gyvybę.

Vienas iš pirmųjų mano darbo uždavinių – sveikatos apsaugos informacijos apsaugos struktūros suformavimas. Ši struktūra bus kuriama analizuojant pagrindinius informacijos apsaugos servisus bei modeliuojant panaudojimo atvejus.

Pagal suformuluotą struktūrą bus parenkamos apsaugos technologijos bei projektuojamas medicininių dokumentų saugumo, pasitelkiant atrinktas technologijas, realizavimas . Tai darysiu analitinėje tiriamojo darbo dalyje.

Projektinėje dalyje, naudojantis pasirinktomis informacinėmis technologijomis bus realizuotas medicininės informacijos perdavimo saugumo pavyzdys. Pavyzdžio teigiamas rezultatas bus kaip įrodymas, kad pasirinkta tiriamojo darbo kryptis buvo teisinga.

Sekantis žingsnis – mano suformuotos saugumo strategijos ir jos realizacijos kelio integravimas su jau sukurta medicininių dokumentų mainų sistema. Šios integracijos trūkumam įvardinti, bus atliktas tyrimas. Tai padės nustatyti pagrindines problemų analizės bei realizacijos klaidas. Eksperimentinis integracijos rezultatų įvertinimas leis daryti išvadas ar tiriamas darbas buvo sėkmingas.

2. Analitinė dalis

Tiriamojo darbo tikslas

Pagrindinis šios magistrinio darbo dalies tikslas – išryškinti esmines duomenų saugumo problemas sveikatos apsaugos organizacijose, išanalizuoti saugumui keliamus reikalavimus, bei rasti sprendimus iškeltoms problemoms spręsti.

HL7 gali ir privalo remtis šiuolaikiškais apsaugos sprendimais ir standartais.

Viena iš šio tiriamojo darbo išvadų turėtų būti ar pavyko išspręsti problemas pritaikant egzistuojančius standartus ir kokios problemos liko neišspręstos.

Tiriamojo darbo apimtis

Einamuoju momentu, daugelis sveikatos priežiūros sistemų turi gana didelių duomenų apsaugos problemų. Gresiančios sveikatos sistemos reformos bei programinės įrangos gamintojų spaudimas verčia perprojektuoti naudojama medicininę programinę įrangą, atkreipiant dėmesį į apsaugos funkcionalumą. Chaoso prideda ir tose pačiose srityse egzistuojantis įvairiausi sprendimai. Sveikatos apsaugos organizacijos daugiau orientuojasi į „sričiai – būdingus“(domain - specific) apsaugos standartų servisus, kai tuo tarpu programinės įrangos kūrimo organizacijos pasisako prieš „medicinai – specifinių“ sprendimų naudojimą.

HL7 - medicininių dokumentų standartas

HL7 standartas – tai medicininių dokumentų standartas.

HL7 atsirado 1987 vystant elektroninių klinikinės, finansinės ir administracinės informacijos standartus tarp nepriklausomų gydymo įstaigų kompiuterinių sistemų; pvz., ligoninės informacinės sistemos, klinikinės laboratorijos sistemos[3].

Per paskutinius tris metus, HL7 narių skaičius išaugo iki 1700 ligoninių, gydymo priemonių pramonės ir nepriklausomų programinės įrangos gamintojų. HL7 standartas yra „palaikomas“ daugumos informacinių sistemų gamintojų ir šiai dienai yra naudojamas daugelyje Amerikos, Australijos, Austrijos, Belgijos, Suomijos, Vokietijos, Olandijos, Izraelio, Japonijos, Naujosios Zelandijos, Olandijos ir Jungtinės Karalystės sveikatos apsaugos įstaigų.

HL7 standartas apibrėžia susitarimus perduodant duomenis apie paciento registraciją, priėmimą, paleidimą ir perkėlimą, draudimą ir mokėtojus, užsakymus ir laboratorijos testų rezultatus, seselės ir

psichologo stebėjimus, dietos paskyrimus, vaistų užsakymus, tiekimo užsakymus, paskyrimo planavimus, problemų sąrašus ir k t.

Standarto „pritaikymas“ praktikoje leidžia ligoninėms kokybiškiau ir greičiau aptarnauti pacientus. „Popierinius“ informacijos mainų metodus kaip pavyzdžiui ligonio ligų kortelę, pakeičia informacijos užklausos ir atsakymai į šias užklausas. Pacientas yra apsaugomas nuo begalės biurokratinių procedūrų ir dokumentų pildymų. Informacija apie jo ligų istorija yra saugoma sveikatos apsaugos įstaigoje kurioje jis yra užsiregistravęs. Bet kuri kita sveikatos apsaugos įstaiga, norinti gauti informaciją apie ši pacientą, formuoja duomenų užklausą informacinei sistemai, saugančiai paciento duomenis ir gauna reikiama informaciją. Taip yra mažinamas sveikatos apsaugos darbuotojų darbo krūvis. Jie gali daugiau dėmesio sutelkti tiesioginių savo pareigų atlikimui.

Nepriklausomai nuo sveikatos apsaugos sistemose naudojamų informacinių sistemų, HL7 standartas apjungia jas visas. Standarto aprašomas medicininių duomenų formatas, yra atpažįstamas visų sveikatos apsaugos įstaigų. Būtinas reikalavimas, kad jų informacinės sistemos „palaikytų“ ši standartą.

Informacijos saugumo apžvalga

Kaip įžanga į mano tiriamąjį darbą aptarsiu bendrą informacijos saugumo padėtį.

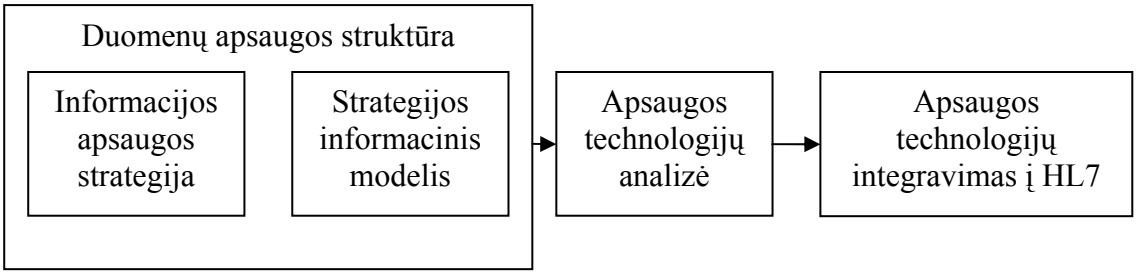
Informacijos surinkimas, analizė, funkcionalumo aprašymas, bei modeliavimas buvo pagrindinė projektų pradžios varomoji jėga. Dėl to informacinių sistemų saugumas, duomenų apsauga, taip pat ir privatumas, ypatingai sveikatos apsaugos segmente, likdavo ir lieka antrame plane. Ryšium su kompleksinės, multi-organizacinės sveikatos apsaugos programinės įrangos kūrimu, sistemų apsaugos svarba auga eksponentiškai. Transakcijų saugumo užtikrinimo reikalingumas, tapo akstinu kurti saugumo sprendimus.

Interneto atsiradimas įtakojo saugumo sprendimų susikoncentravimą ties individualiais kompiuteriais, programine įranga ar vartotojais t.y. atskirais vienetais, nuošalėje paliekant globalesnę sistemą. Dabar sveikatos apsaugos įstaigos ar finansinės institucijos, informaciją apsaugo, kurdamos privačius tinklus. Prisijungimas prie tinklo yra ribojamas – leidžiama tik patikimoms vartotojų grupėms. Vis dėlto, sistemos silpniausios vietos - ją naudojantis ar administruojantis žmonės, turintis priėjimą prie saugomos informacijos. Jie gali būti papirkinėjami ar jiems daromas spaudimas atskleisti slaptažodžius, „atidaryti duris“(suteikti priėjimą prie informacijos).

Reikalavimai sistemos saugumui ar duomenų saugumui yra panašūs – tiek Intranetui, tiek Ekstranetui ar Internetui jie vienodi. Tačiau daugiausia dėmesio yra skiriama Internetui, kuris sukelia ne tik nepasitikėjimą, bet ir labai paspartino aukštesnio lygio, saugumą užtikrinančių technologijų atsiradimą.

Saugumo struktūra

Tam, kad būtų galima pradėti tiriamąjį darbą, apsibrėžiu esminius dalykus į kuriuos koncentruosiuosi analitinėje dalyje. Šie dalykai tai duomenų saugumo struktūros sukūrimas susidedančios iš duomenų saugumo strategijos ir informacinio jos modelio. Suformavus duomenų saugumo struktūra, apžvelgsiu informacijos apsaugos technologijas, bei realizuosiu jų integravimą su HL7 standartu.



Paveikslas nr. 1. Tiriamojo darbo analitinės dalies etapai

Duomenų saugumo strategija

Saugumo strategija apima teisinius, organizacinius, struktūrinius, funkcinius, techninius, socialinius, etninius ir psichologinius aspektus apjungiamus su naujausiomis informacinėmis bei komunikacinėmis technologijomis. Stovėdama ant teisinio ir etninio, bei medicininės etikos pagrindo, strategija taip pat aprašo problemas, reikalavimus, sąlygas, įsipareigojimus, teises, bei pareigas surenkant, saugant, apdorojant ar grupuojant informaciją.

Aukštos klasės duomenų saugumo strategija yra ir turi būti geras pagalbininkas kasdieniame darbe. Taigi, vienas iš pagrindinių duomenų saugumo užtikrinimo aspektų yra saugumo strategijos sukūrimas ir įtvirtinimas. Tam, kad strategija duotų naudos, ji turi būti aiškiai suprantama, lengvai skaitoma visiems vartotojams bei administracijos darbuotojams.

Duomenų apsaugos informacinis modelis

Vieningas, analitinis konkrečios sistemos architektūros, visų apsaugos reikalavimų traktavimas yra reikalingas norint įvertinti apsaugos palaikymo galimybes. Duomenų apsaugos informacinis modelis tarnauja kaip pradinis taškas aprašinėjant ir analizuojant apsaugos reikalavimus. Pagrinde koncentruojantis ties architektūros apsaugos reikalavimais, informacinis modelis išskiria atskiras sistemos dalis į kurias būtina atkreipti dėmesį, norint sustiprinti apsaugos strategiją bei aplinkos faktorius įtakojančius strategiją.

Apsaugos informacinis modelis dažniausiai susideda iš:

- Pavyzdinių komponentų klasių(duomenų bazės, servisai)

- Aktyvių sistemos esybių klasių(vartotojai, rolės, programinė įranga, organizacijos)
- Pasyvių sistemos esybių klasių(pranešimai, pranešimų „dėžučių“)
- Bendrų sistemos apsaugos savybių
- Apsaugos savybių aprašančių kaip ir kodėl pasitikima naudojamu komponentu
- Komunikacijų apsaugos
- Atskaitomybės reikalavimų
- Grėsmių, atakų, pažeidžiamų vietų

Apsibrėžus duomenų apsaugos strategiją ir turint jos informacinį modelį galima nustatyti pagrindinį reikalavimų keliamų sveikatos apsaugos sistemoms rinkinį. Tai turėtų pagelbėti kuriant atviras ir lengvai integruojamas sistemas. Be to tiriamajame darbe aiškiai apsibrėžta strategija padės įvardinti svarbiausias problemas susijusias su duomenų apsauga. Kas vėliau pagelbės analizuojant egzistuojančias duomenų apsaugos technologijas bei jas integruojant į HL7 standartą.

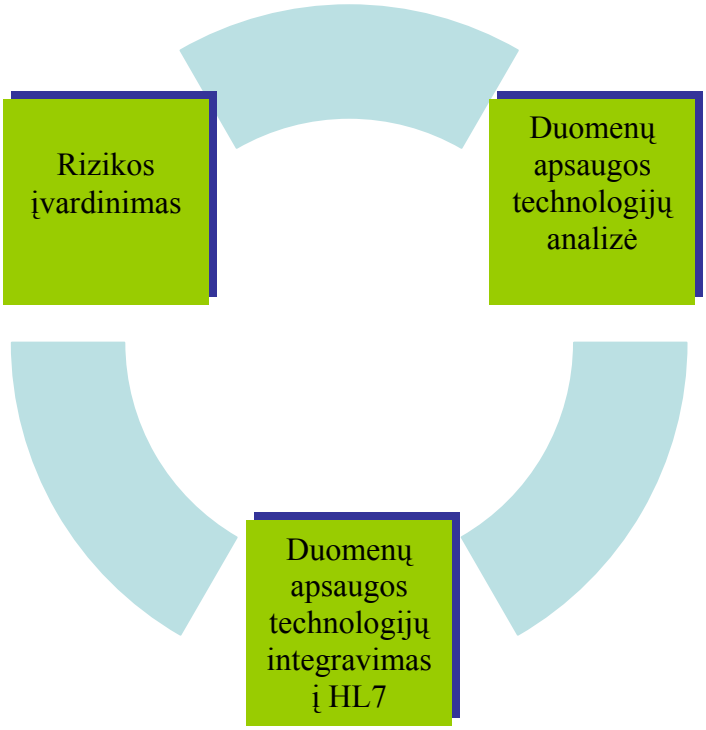
Duomenų apsaugos rizikos

Kuriant duomenų apsaugos struktūrą, ypatingą dėmesį atkreipiau į duomenų apsaugos pavojus ir šalutinius poveikius(grėsmės, silpnų vietų identifikavimas, atakos, kontrapriemonėms). Šių problemų apibendrinti pavyzdžiai:

- Atskleidimas
    - Pavojų demaskavimas
    - Pavojų užkirtimas
    - Išvados
    - Įsibrovimas
- Apgaulė
    - Maskavimasis
    - Falsifikacija
    - Išbrokavimas
- Griovimas
    - Kompetencijos stoka
    - Korupcija
    - Kliūtis
- Užgrobimas
    - Neteisėtas pasisavinimas

- Piktnaudžiavimas

Duomenų rizikos įvardinimas ir apibendrinimas, padės tolimesnėje tiriamojo darbo eigoje. Analizuojant duomenų apsaugos technologijas, būtina suformuluoti reikalavimus keliamus joms. Nesant aiškiai įvardintai informacijos rizikai, yra neįmanoma parinkti duomenų apsaugos problemų sprendimus.



Paveikslas nr. 2. Technologinių integracijų priklausomybė nuo duomenų apsaugos rizikos

Didžiąją dalį čia įvardinamų rizikos atveju galima rasti CERT(Computer Emergency Response Team) kaupiamuose pavojų duomenų saugyklose.

Duomenų apsaugos servisai

Toliau formuluodamas duomenų apsaugos strategiją, kaip vieną iš pagrindinių užduočių iškėliau pagrindinių apsaugos servisų įvardinimą. Apsaugos servisų tikslus aprašymas padės išskirti pagrindines duomenų apsaugos sritis į kurias būtina koncentruotis. Kiekvieną iš sričių laikydamas duomenų apsaugos problema, aš pasirinksiu pagrindines šio darbo problemas į kurias daugiausia koncentruosiu savo dėmesį.

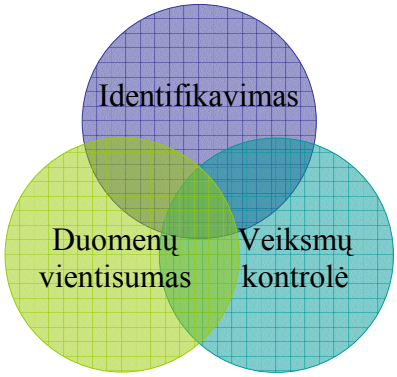
Nepriklausoma nuo realizavimo detalių ir dėl to reliatyviai pastovi komunikacijų ir programinės įrangos apsauga, koncentruojasi į šiuos apsaugos servisus:

- **Identifikacija ir autentifikavimas:** šis servisas „palaiko“ subjektų, tokių kaip žmogaus, organizacijos ar sistemos aprašymus, bei patvirtinimą, kad subjektas tikrai yra tas kuriuo dedasi.
- **Autorizacija ir prisijungimo kontrolė:** šis servisas kontroliuoja veiksmų teisių ir leidimų suteikimą subjektams. Bei vykdo veiksmų kontrolę remiantis subjektų apribojimais.
- **Integralumas:** esant įvairiems neteisėtiems prisijungimams prie sistemos ar bandymams gauti informaciją, šis servisas apsaugo duomenis nuo jų sugadinimo ar sunaikinimo.
- **Konfidencialumas:** šis servisas užtikrina duomenų neprieinamumą neautorizuotiems subjektams.
- **Atskaitomybė:** šis servisas užtikrina subjektų veiksmų kontrolę ir atsakomybę.
- **Patikrinimas, auditas:** vartotojų veiksmų stebėjimą užtikrina šis servisas.
- **Prieinamumas:** duomenų prieinamumą bei jų panaudojimo galimybę užtikrina prieinamumo servisas.
- **Veiksmų istorija:** šis servisas fiksuoja visus veiksmus atliktus su informaciją tam, kad užtikrinti subjektų veiksmų atsakomybę.

Kiekvienas iš šių apsaugos servisų atlieka svarbų vaidmenį užtikrinant medicininių dokumentų apsaugą. Dėl to dauguma sveikatos apsaugos duomenų standartų koncentruojasi būtent ties jais, norėdamos užtikrinti duomenų saugumą. Medicinos ir administracinės paskirties duomenų ar dokumentų apsikeitimui yra naudojami standartizuoti pranešimų formatai tokie kaip HL7, DICOM, xDT(BDT), EDIFACT. Apsikeitimo procesai yra įvardinami kaip žinučių apsikeitimas naudojant tinklus.

Tiriamojo darbo probleminės sritys

Kaip pagrindines šio tiriamojo darbo problemines sritis įvardinu: identifikacija ir autentifikavimas, integralumas ir veiksmų istorija.



Paveikslas nr. 3. Tiriamojo darbo probleminės sritys

Ties šiomis sritimis koncentruosiuosi nes jos atlieka svarbiausius vaidmenis užtikrinant duomenų mainų saugumą. Duomenų identifikavimas nustato informacijos savininką. Suteikia apie jį informaciją, kas vėliau duomenų mainų sistemai leidžia jį autorizuoti arba ne. Identifikavimo problemos išsprendimas, apsaugos informaciją nuo „nepatikimų“ vartotojų prisijungimo prie sistemos ir neautorizuoto duomenų panaudojimo.

Autorizavus duomenų savininką, yra tikrinama ar duomenis transportavimo metu nebuvo pažeisti, ar jų vientisumas yra toks pats kaip ir juos išsiunčiant. Šiuo atveju probleminė sritis yra duomenų vientisumas. Šios problemos sprendimo suradimas padės apsaugoti perduodamus duomenis nuo pažeidimų.

Bet kuri operacija su duomenimis, kaip pavyzdžiui duomenų užklausos, atsakymai į užklausas, užklausų gavimas, operacijų patvirtinimas, turi būti fiksuojama ir apie tai būtina informuoti visas komunikuojančias puses. Veiksmų kontrolės problemos išsprendimas padeda išvengti papildomų nesusipratimų ar įgalina kontroliuoti veiksmus atliekamus su informaciją.

Sveikatos apsaugos duomenų saugumo reikalavimai

Tiriant problemines sritis, susijusias su duomenų apsauga, ypatinga dėmesį reikia skirti jau atliktų tyrimų analizei. Dažnai pasaulinėje praktikoje egzistuoja rekomendacinio pabodžiu problemų sprendimų formuluotės. Kuriomis vadovaujantis galima ieškoti sprendinių savo iškeltiems uždaviniams.

Pateikiu dešimt pagrindinių reikalavimų keliamų gydymo įstaigų duomenų saugumui, suformuluotų IEEE(The Institute of electrical and Electronics Engineers):

- Prisijungimo kontrolė
- Apsaugos kontrolė, auditas ir monitoringas
- Duomenų peržiūra
- Kontrolė
- Sutikimas ir paskelbimas
- Išsaugojimas
- Žymėjimas
- Informacijos srautas
- Grupavimo kontrolė
- Patikima kompiuterinė infrastruktūra

SEISMED(The Secure Environment for Informatikon Systems in Medicine) gairės, paremtos dauguma Europos sveiktos apsaugos nuostatų, identifikuoja svarbiausias apsaugos vietas medicinos įstaigų sistemose. Jų brandus ir į verslą orientuotas požiūris pagrįstas informacinių technologijų sistemomis, žmoniškaisiais resursais ar valdymo praktika įvairiuose organizaciniuose lygiuose:

- Apsaugos strategija ir administravimas
- Fizinė apsauga
- Nesėkmių planavimas ir atstatymas
- Darbuotojų saugumas
- Apmokymai ir supratimas
- Informacinių technologijų valdymas
- Autentifikavimas ir prisijungimo kontrolė
- Duomenų bazės saugumas
- Sistemos priežiūra
- Įstatymų laikymasis

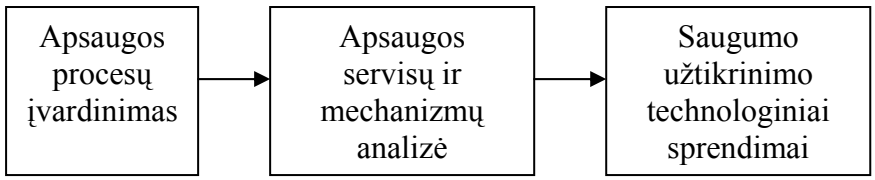
Norėdami skubiai integruoti medicininių duomenų apsaugą rekomenduojama:

- Individualus vartotojų autentifikavimas: kiekvienas vartotojas turi turėti unikalų prisijungimo vardą/slaptažodį.
- Prisijungimo kontrolė: sveikatos apsaugos įstaigų darbuotojai turi turėti galimybę gauti jiems reikiamą informaciją.
- Stebėjimas: kiekvieno prisijungimo prie duomenų ir operacijų su jais registravimas yra privalomas. Šie registrai privalo saugoti prisijungimo laiką, datą, informaciją apie peržiūrėtus duomenis ir su jais atliktus veiksmus. Ši informacija gali būti naudojama audito metu ar pacientui pareikalavus.
- Fizinė apsauga ir pažeidimų atstatymas: informacijos pateikimo terminalai privalo buti išdėstyti taip, kad juose pateikiama informacija nebūtų pasiekiama neautorizuotiems pašaliniams vartotojams. Jiems turi būti užkirstas priėjimas prie spausdinimo įrenginių ir elektroninių saugyklų.
- Nutolusių prisijungimo taškų kontrolė: nuotolinių prisijungimų saugumui užtikrinti pravaloma naudoti ugniasienes, pavienėmis sesijos, šifruotais slaptažodžiais.
- Išorinių komunikacijos procesų apsauga: Visa pacientus-identifikuojanti informacija, perduodant ją viešais tinklais, privalo būti šifruojama.
- Disciplinuota programinė įranga: virusus tikrinanti programinė įranga turi būti suinstaliuota kiekviename serveryje. Taip pat informacijos siuntimas į serverius iš interneto turi būti ribojamas.
- Reguliarus sistemos įvertinimas: kas mėnesi sistema privalo būti tikrinama ir audituojama, siekiant išsiaiškinti jos silpnąsias vietas.
- Būsimai medicininių duomenų apsaugos integracijai rekomenduojama:
- „Stiprus“ autentifikavimas: daugelį kartų naudojami tie patys slaptažodžiai ir identifikaciniai numeriai silpnina organizacijos sistemas. Autentifikavimą galima sustiprinti ar pagerinti programinį prisijungimą „suporuojant“ su „geležinėmis“ technologijomis – magnetinėmis, „protingomis“ kortelėmis ar įrenginiais reguliariai keičiančiais slaptažodžius. Artimoje ateityje bus pradedami naudoti(ir jau yra naudojami) pirštų antspaudai, veido skanavimas, balso analizė.
- „Enterprise-wide“ autentifikavimas: sveikatos apsaugos organizacijos paprastai naudoja įvairias sistemas. Dėl to reikalingas „vienkartinis“ prisijungimas – vartotojas autorizavęs save vieną kartą, gali naudotis bet kurią sistemą. Taip išvengiama pakartotinės autorizacijos.

- Prisijungimo validavimas: rolės privalo kontroliuoti tiek sistemos funkcionalumą tiek informacijos turinį.
- Išplėstas stebėjimas, auditas: visų sistemos dalių auditas.
- Elektroninis duomenų autentifikavimas: elektroninis parašas naudojamas įvedant informaciją ar norint ją „išgauti“. Kriptografinis skaitmeninis parašas padės užtikrinti, kad informacija nebus pakeista transakcijų metu.

Šiomis pateiktomis rekomendacijomis ir reikalavimais(priedas nr. 1, priedas nr. 2, priedas nr. 3), keliamais medicininių dokumentų saugumui, vadovausi formuluodamas medicininių dokumentų apsaugos struktūra.

Duomenų perdavimo apsaugos technologijų analizė



Paveikslas nr. 4. Duomenų saugumo užtikrinimo technologijų analizės seka

HL7 žinučių perdavimo saugumo problemos sprendimas pasaulyje

HL7(Health Level Seven) suformavo SIGSecure(Secure Transactions Special Interest Group) grupę kuri rūpinasi HL7 žinučių perdavimo saugumu. Daugiausiai dėmesio yra skiriama aplinkoms kurios dalyvauja atliekant informacijos mainus žinučių pagalba. Grupė didžiausias pastangas deda į egzistuojančių sprendimų integraciją. Taip siekiama užtikrinti informacijos perdavimo saugumą, išvengiant apsaugos strategijos standartizavimo. Apsaugos užtikrinimui naudojama autentifikavimas, šifravimas, elektronines parašas. Taipogi kaip viena iš galimų technologijų apsaugai - elektroninio pašto protokolas(S-MIME).

HL7 duomenų apsaugos reikalavimai

Sistemos komunikavimas tarpusavyje naudojant HL7 žinutes - HL7 apsaugos analizės dėmesio centras. Dėmesys nebus koncentruojamas ties informacijos elementų saugumo lygiais ar prisijungimo kontrolės sąrašais (išskyrus galimybę vykdyti informacijos mainus žinučių pagalba). Mūsų dėmesio centras – kaip žinučių maršrutizatoriai ar EDI tinklų sąsajos įtakoja saugumo problemą.

Analizuojant įgyvendinimo detales vietoj bazinių servisų aprašytų anksčiau, HL7 kreipia dėmesį į komunikacijos lygius: sąsają, tinklus, transportavimus(tiesioginiai), sesijas(programinė įranga naudojanti sesijas), ir programinę įrangą(buferinė programinė įranga, „store-and-forward“). Kiekvienam iš šių komunikacijos sluoksnių, HL7 adresuoja tam tikrus servisus: identifikaciją ir autentifikavimą, autorizaciją ir prisijungimo kontrolę, integravimą, konfidencialumą, atsakingumą, prieinamumą ir įvykių stebėjimą.

HL7 panaudojimo atvejų modeliai

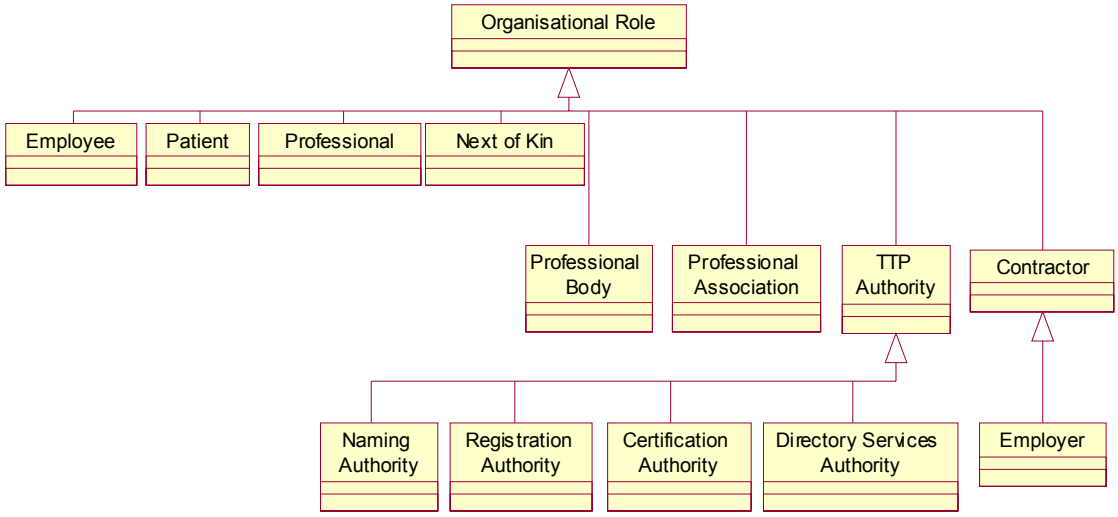
Norėdami detaliau įsivaizduoti medicininės dokumentų apsaugos svarbą sumodeliuosime informacijos mainų panaudojimo atvejus. Anksčiau apsirašyta duomenų saugumo struktūra ir panaudojimo atvejų modeliavimai leis tiksliau suformuluoti problemas bei parinkti sprendimus analizuojant bei integruojant informacijos apsaugos technologijas.
Panaudojimo atvejai:

Autentifikavimas

Autentifikavimo pavyzdys gali būti, vartotojo identifikavimas daugialypėje(keletas posistemių) sveikatos apsaugos sistemoje. Pavyzdžiui, gydytojas turi autentifikuotis norėdamas prieiti prie laboratorijos informacijos, vaistų panaudojimo informacijos ir prie rentgenologijos informacijos. Visi trys šie autentifikavimai – vienas veiklos procesas – paciento slauga. Praktikuojantis gydytojas privalo autentifikuotis prie keleto informacinių sistemų norėdamas gauti jam reikiamą informaciją. Deja, kai autentifikavimo procesas, esant įvairioms platformoms ar programinei įrangai, nėra koordinuojamas, informacijos paieškos procesas įtraukia daugybinį identifikacinių kodų bei slaptažodžių panaudojimą. Esant tokiai situacijai neįmanoma sukontroliuoti visos vartotojų informacijos organizacijos lygmenyje.

Autorizacija

Autorizacijos panaudojimo atvejo pavyzdys galėtų būti prisijungimo kontrolės matrica. Ji reguliuoja prisijungimą prie duomenų visos organizacijos lygmenyje. Esminis dalykas kad IT sistemos būtų apsaugotos visapusiškomis loginėmis prisijungimo kontrolėmis. Prisijungimas turi būti suteiktas teisėtiems vartotojams ir uždraustas visiems kitiems. Visos vartotojų grupės turi būti apibrėžtos prieš joms suteikiant tam tikras, veiksmų su sistema, teises. Pasiremdami grupių apibrėžimais, apsaugos mechanizmai turi kontroliuoti duomenų skaitymą, rašymą, koregavimą ar naikinimą. Bet koks šių kontrolių „apėjimo“ metodas yra draudžiamas. Sudarinėjant prisijungimo kontrolės matricas yra labai svarbu atkreipti dėmesį, kad kontrolės nestabdytų darbo procesų ir nesutrukdytų sveikatos apsaugos darbuotojams atlikti savo pareigos.



Paveikslas nr. 5. Autentifikavimo hierarchija

Privatumas ir konfidencialumas

Privatumo ir konfidencialumo panaudojimo atvejo pavyzdys yra „karšti“ debatai apie tai kam priklauso medicininiai įrašai. Privatus teisininkai vadovaujasi europietiška(daugelyje Europos valstybių) paradigma, kad pacientas kontroliuoja savo medicininius įrašus. Pas mus paciento medicininius įrašus koordinuoja sveikatos apsaugos įstaigos – laikydamos, kad paciento gydymo istorijos surinkimas ir kontroliavimas yra kaipo viena iš suteiktų paslaugų dalių. Informacija gali būti prieinama baudžiamosioms instancijoms, įstatymų numatyta tvarka ir patiems pacientams.Daugelyje valstybių prieinamumas prie tam tikros informacijos yra griežtai ribojamas. Pavyzdžiui:

- Priklausomybė nuo narkotikų ar alkoholio
- Psichinės negalios
- ŽIV
- Įvaikinimas
- Abortai

Taip pat pacientai turi teise gauti anoniminę medicininę pagalbą. Projektuojant sistema neturi būti atsižvelgiama į pacientų giminystės ryšius.

Auditas

Audito panaudojimo atvejo pavyzdys tai veiksmų kontrolė t.y. užtikrinimas kad visos paslaugos buvo suteiktos ir užklausų bei transakcijų vykdymo stebėjimas. Kaip pavyzdžiui, ligoninės pateikia krūvas sąskaitų draudimo bendrovėms už suteiktas paslaugas. Mokėtojas savo ruožtu turi reaguoti į pateikta sąskaita ir apmokėti per nurodytą laiką. Neįvykdžius savo įsipareigojimų yra skaičiuojami delspinigiai ar naudojamos kitos priemonės. Dėl to yra labai svarbu kad būtų stebimos visos transakcijos – tiek

sąskaitų „išstatymas“, tiek sąskaitų apmokėjimas. Kiekviena uždelsta diena tam tikrai pusei reiškia nuostolius.

Einamuoju momentu dauguma audito mechanizmų remiasi rankiniais metodais t.y. transakcijų įvykių fiksavimas ir pan. Dėl to labai sunku yra apibrėžti kas yra atsakingas už laikų neįvykdyta operaciją ar transakciją. Nesant globalios, laiko fiksavimo sinchronizacijos praktiškai neįmanomas organizacijos auditas. Operacijų su duomenimis fiksavimas yra reikalingas ne vien finansinėms operacijoms vykdyti. Duomenų mainai pastoviai vyksta tarp įvairių organizacijos padalinių ar tarp dviejų skirtingų sveikatos apsaugos įstaigų. Dėl to labai svarbus yra stebėjimas ir fiksavimas ar visos operacijos su duomenimis buvo atliktos laiku. Audito mechanizmai apima:

- Kiekvienos duomenų laikmenos identifikavimą
- Duomenų transakcijų maršrutų valdymą
- Mechanizmus užtikrinančius, kad visa informacija pasiekia adresatą
- Informacijos „eilių“ valdymas
- Mechanizmus, identifikuojančius nutrauktas ar besidubliuojančias informacijos perdavimus bei apie tai informuoja transakcijos savininką

Kai duomenų perdavimas yra nutraukiamas turi egzistuoti mechanizmai informuojantis su transakcija susijusius žmones. Egzistuoja net keli niuansai susiję su šiuo atveju:

- Paprastai informacija apie nutrauktas operacijas yra kaupiama. Kaip ilgai ši informacija yra saugoma ?
- Ar klaidos pranešimas yra lengvai suprantamas ?
- Ar sistemos žingsniai aprašyti ir ar kiekviena klaida dokumentuota ?
- Besidubliuojančių operacijų identifikavimo įrankiai ?
- Pasikartojančių klaidų stebėjimas ?
- Ar klaidų sąrašai analizuojami ir daromos išvados ?
- Procedūros, veiksmų šablonai, tendencijų analizės – kaip elgtis tam tikrais sistemos sutrikimo atvejais?

Saugus komunikavimas(šifravimas)

Šioje dalyje paminėsiu keletą panaudojimo atvejų. Nes jau anksčiau suformuluotose tiriamojo darbo probleminės sritys labiausiai koncentruojasi į duomenų mainų saugumą t.y. komunikavimo saugumą.

Jeigu sistema naudoja viešus tinklus, tokius kaip Internetas, duomenų perdavimui, ar ji pilnai yra pasirengusi užtikrinti paciento duomenų saugumą t.y. ar ji pajėgi yra tai padaryti ? Informacija siunčiama viešu tinklu yra visiems prieinama. Šie tinklai yra prieinami visiems. Sistema turi būti

pasiruošusi, bet kokiam bandymui užvaldyti informaciją, naudodama ugniasienes ar duomenų šifravimo schemas. Pavyzdžiui tam tikrą laboratorija siunčia tyrimų informaciją, ją užsakiusiems pacientams ar organizacijoms. Tam yra naudojamas viešas tinklas. Yra du esminiai pasirinkimai: šifruoti visą informaciją arba šifruoti tik tą informacija kuri yra susijusi su paciento arba gydytojo identifikavimu. „Geležies“ šifravimas taip pat yra viena iš galimybių, kuri kol kas sveiktos apsaugos sistemose nenaudojama.

Kitas saugaus komunikavimo panaudojimo atvejis yra HL7 žinučių mainai tarp dviejų patikimų partnerių. Dvejų sistemų pastovus bendravimas gali būti įvardijamas kaip dažnas scenarijus. Pavyzdžiui, laboratorijos sistemos pastoviai „bendrauja“ su tam tikros sveikatos apsaugos organizacijos sistema. Šis „bendravimas“ buvo numatytas prieš keletą mėnesių. Abi sistemos žino viena kitos ne tik TCP adresus, bet ir bet kurią kitą reikalingą informaciją. Šio panaudojimo atvejo realizavimo technologijos:

- Taip pat gali būti naudojamas ir SSL. Kiekvienos informacijos gavėjas turės informaciją apie informacijos siuntėjo sertifikatą ir galės patikrinti ar siuntėjo sertifikato informacija atitinka pateiktą žinutės MSH segmente.
- EDI gali būti naudojamas lygiai taip pat kaip ir SSL. Abi komunikuojančios pusės turi visą informaciją apie sertifikatus, tad jos gali aptikrinti ar sertifikatai atitinka nurodytuosius HL7 žinutėse[9].

Dar vienas saugaus komunikavimo panaudojimo atvejis yra kai keletas įstaigų siunčia informaciją į vieną sveikatos apsaugos centrą. Šiuo atveju, kiekviena siunčiančioji įstaiga privalo siusti įvairią ataskaitinę informaciją į centrą. Šios ataskaitos bus siunčiamos nereguliariai iš kelių šimtų įstaigų. Nepavykus identifikuoti siuntėjo, gauta informacija nebus atmetama. Informacijos priėmėjas galės pateikti siuntėja identifikuojančią užklausą. Šio panaudojimo atvejo realizavimo technologijos:

- Saugus EDI turėtų šiuo atveju tikti. Kiekvienas informacijos perdavimas bus apsaugotas nuo jos „perėmimo“. Siuntėjo identifikavimas nebus sudėtingas. Kiekvienas siuntėjas galės siųsti elektroninius laiškus, į kuriuos centras neprivalės atsakinėti.
- SSL taip pat turėtų tikti. Kai reikia pasiųsti tam tikrą informaciją į centrą, yra nustatomas SSL ryšys panaudojant iš anksto tam skirtą SSL prievadą ir žinutė išsiunčiama.

Paskutinis saugaus komunikavimo panaudojimo atvejo pavyzdys yra atvejis kai informacijos siuntėjas ar gavėjas nėra tiksliai žinomas t.y. kai nėra pakankamai informacijos apie vieną iš komunikuojančių pusių. Toks atvejis yra ganėtinai dažnas, nes pirminės sveikatos priežiūros įstaigų segmentas turi

tendencijas pastoviai kisti. Dėl to turėti visą reikiamą informaciją kartais yra neįmanoma. Tokiu atveju pagrindinis reikalavimas bus, kad komunikacija būtų „pulsuojanti“. Informacijos apsikeitimą galima būti charakterizuoti kaip vienu „šūviu“ perduodama visą reikalingą informaciją t.y. tam tikru periodu perduodamas tam tikras informacijos kiekis. Šis panaudojimo atvejis apima prieš tai aprašytus du atvejus – patikimi partneriai ir vienas centras. Priešingai nei patikimu partneriu atveju, mes negalėsime naudotis pastovaus ryšio:

Prieinamumas

Duomenų prieinamumo panaudojimo atvejis yra galimybė pasiekti duomenis. Sveikatos apsaugos sistemos turi būti pasiekiamas visą laiką. Gydytojai negali suplanuoti kada jiems prireiks tam tikros informacijos apie pacientą, ypatingai tokios kuri įtakoja tam tikrus jo sprendimus ar gydymo būdus.

Duomenų integravimas

Duomenų integravimo panaudojimo atvejo pavyzdys yra unikali identifikacija. Pacientų ir sveikatos apsaugos darbuotojų identifikacija paklos kelią tolimesnei visų sistemų integracijai bei sinchronizacijai.

Kitas panaudojimo atvejis yra kai sugadinami duomenys. Tą įtakoja neteisingai išsaugotą informaciją, neteisingos nuorodos į ją ar visiškas jos nepasiekiamumas. Tai gali sukelti klaidingų sprendimų priėmimą pacientų atžvilgiu.

Taigi, tinkamai išsprendus unikalios identifikacijos problemą, aukščiau paminėtos problemos irgi išsispręstų. Maišos bei kontrolinių sumų algoritmai turėtų pagelbėti sprendžiant klaidingos informacijos perdavimo problemą. Elektroninio parašo procedūros taip pat gali pagelbėti identifikuojant informacijos „teisingumą“ prieš atliekant transakcijas su ja.

Čia pateikiami tik keli panaudojimo atvejų modeliai kurie tiesiogiai siejasi su sveikatos apsaugos aplinka. Šiuos panaudojimo atvejus naudosime išsiaiškinimui kur turėtų būti naudojami saugumo mechanizmai norint užtikrinti saugius informacijos, palaikomos HL7 standarto, mainus.

Be to panaudojimo atveju pagalba išryškinamos su sveiktos apsaugos informaciją susijusios problemos. Tai yra informacijos saugos ilgaamžiškumas, jos prieinamumas po daugelio metų ir jos saugumas bėgant metams iš metų.

HL7 apsaugos procesų visuma

Panaudojimo atveju pateikiamas detalesnis procesų, atliekamų su duomenimis, vaizdas bei suformuota duomenų apsaugos struktūra padėjo man apibrėžti pagrindinius HL7 standarto saugumo servisus bei įvardinti procesus kurie užtikrins šių servisų saugumą.

Apsaugos servisai	Apsaugos procesai
Autentikavimas	Elektroninis parašas
Autorizacija ir prisijungimo kontrolė	Elektroninis parašas, prisijungimo kontrolės sąrašas
Vientisumas	Šifravimas, elektroninis parašas, reikšmių kontrolė
Konfidencialumas	Šifravimas, raktinis įsipareigojimas
Atsakomybė	Auditas, registrai, pažymos
Veiksmų kontrolė	Šifravimas, elektroninis parašas

HL7 komunikavimo apsaugos servisai

Norint pagerinti HL7 žinučių saugumą, reikalingi baziniai saugumo servisų rinkiniai. Tam tikri šių servisų rinkiniai padeda apsaugoti sveikatos apsaugos sistemas. Įvardinsiu keletą šių servisų rinkinių.

Apsaugos servisai ir mechanizmai

Apsaugos servisai, reaguodami į pavojus ar silpnąsias sistemos vietas, siūlo sąsaja tarp saugumo strategijoje užsibrėžtų saugumo reikalavimų ir saugumo mechanizmų bei reikalavimų valdymo. Kiekvienas saugumo servisas gali būti realizuojamas viena ar keletu apsaugos mechanizmu, priklausomai nuo apsaugos strategijos ar programinės įrangos.

Sveikatos apsaugos sistemoms, išoriniai ir vidiniai saugos servisai gali būti skirtingi. Vidiniai apsaugos servisai apibrėžia komunikuojančių sistemų funkcijas, užtikrinančias komunikavimo saugumą. Išoriniai apsaugos servisai yra servisai kuriuos palaiko „Patikimos Trečiosios Šalys“(Trusted Third Parties - TTP). Jie skirti užtikrinti subjektų, įtrauktų į komunikavimą ir

bendradarbiavimą, patikimumą. Apsistosime ties vidiniais saugumo servisais, nes išoriniai neįeina į apsibrėžtą apimtį.

Sekančioje lentelė pateikiami vidiniai apsaugos servisai, kurie rekomenduotini užtikrinant saugų HL7 žinučių komunikavimą.

Apsaugos servisai	**Apsaugos mechanizmai**	
	Asimetrinės technologijos	Simetrinės technologijos
Pagrindinis identifikavimas ir autentifikavimas	elektroninis parašas, TVPs	Šifravimas, kriptografinė reikšmių kontrolė (MAC), TVPs
Duomenų kilmės autentifikavimas	elektroninis parašas, kriptografinė reikšmių kontrolė, DN	Šifravimas, kriptografinė reikšmių kontrolė (MAC), DN
Vientisumas	elektroninis parašas, kriptografinė reikšmių kontrolė	Šifravimas, kriptografinė reikšmių kontrolė (MAC)
Konfidencialumas	Šifravimas	
Atskaitingumas	Apsaugos auditas (ataskaitos, veiksmų laikmenos, laiko žymės)	
Veiksmų vykdymo užtikrinimo kontrolė	elektroninis parašas, kriptografinė reikšmių kontrolė, DN, laiko žymės	Šifravimas, kriptografinė reikšmių kontrolė (MAC), laiko žymės, DN

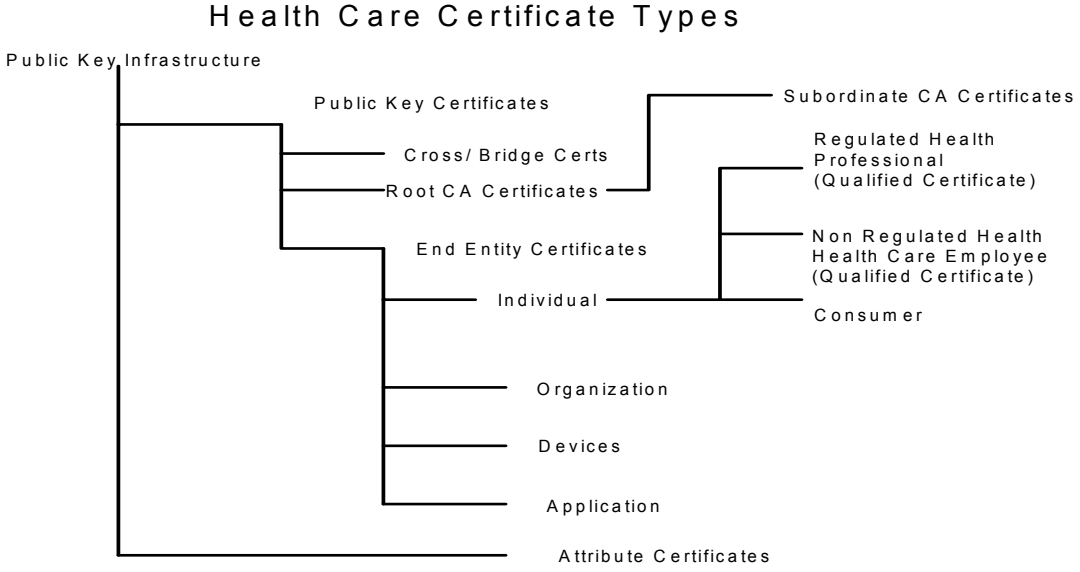
Apsaugos mechanizmų diegimas yra dinaminis procesas, ypatingai priklausantis aplinkos, jos pavojų ir pan.

Priklausomai nuo apsaugos servisų klasės(pakopos), jų realizavimai galima naudoti skirtingas technologijas.

Apsaugos servisų pakopos	Relizavimas
Programinė įranga	SFTP, PEM, PGP, SHTTP, ...
Servisai	Identifikacija, autentifikavimas, vientisumas
Mechnaizmai	elektroninis parašas, šifravimas, reikšmių kontrolė, ...
Procedūros	Apsaugos tarpinis serveris ar apsaugos priemonės su bibliotekomis
Kriptografinė sintaksė	PKCS#7, S/MIME, PGP/MIME, CMS, ...
Algoritmai	DES, RSA, IDEA, MD5, RIPEMD, SHA-1, ...
Techninės priemonės	Atpažinimo priemonės (intelektualios kortelės, raktiniai diskai)…..
Aparatūra ir programinė įranga	Katalogų serveriai, sertifikavimo serveriai…

Veiksmų vykdymo užtikrinimo kontrolė ir vientisumas HL7 standarte

Elektroninis parašas yra kriptografinė technologija, kuri susieja vartotojus kriptografinių raktų poromis. Vienas iš šių raktų yra saugomas „garantuotų būdų“ t.y. intelektualiose kortelėse, ir jis visada išlaikomas paslaptyje. Kitas raktas(viešas raktas) yra išplatinamas visiems vartotojo elektroninio parašo tikrintojams. Todėl sertifikatas yra saugomas viešuose katalogų servisuose(X.500) įskaitant viešuosius parašo raktus. Tokie sertifikatai yra aprašomi naudojantis įvairiomis taisyklėmis(Abstract Syntax Notation One - ASN.1) ir standartais (ISO ir ANSI). Informacijos siuntėjas ir priėmėjas turi susitarti dėl naudojamų taisyklių šifruojant informaciją. Tai yra vienas iš aukščiau aprašytos apsaugos strategijos reikalavimų.



Paveikslas nr. 6. Sveikatos apsaugos sertifikatų tipai

Elektroniniai parašai yra naudojami skirtingais būdais ir skirtingiems tikslams. Vienas iš panaudojimo sričių – žinutės autentifikavimas ir duomenų kilmės identifikavimas bei duomenų vientisumo kontrolė.

Veiksmų vykdymo užtikrinimo kontrolė ir vientisumas

Pasirašinėjant dokumentą, šis dokumentas ir vartotojo slaptas raktas yra pradinės kriptografinio proceso reikšmės. Tikrinant parašą, parašas, dokumentas ir vartotojo viešas raktas yra kriptografinio proceso dalis, kuris gražina parašo patvirtinimo ar atmetimo reikšmę. Bet kokie dokumento pakeitimai atlikti po jo pasirašymo inicijuos parašo patikros atmetimą(autentifikavimo nesėkmę). Tad, elektroninis parašas yra

kaip garantas, kad duomenis yra nesuklastoti bei jų kilmė yra patikima. Elektroniniai parašai yra formuojami naudojantis šifravimo algoritmais tokiais kaip RSA.

Mechanizmai ir technologijos

Pasirašant HL7 žinutę, pirmiausiai parašas yra sumaišomas į viena bloką pasinaudojant vienapuse funkcija. Vienapuses funkcijos pagrindinė savybė, kad ji „sumaišo“ simbolius į tokį simbolių kratinį, kurio analogišką reikšmė neegzistuoja. Šis procesas yra vykdomas pasinaudojant vartotojo slaptu raktu. Gavus „simbolių kratinį“ jis pridedamas prie žinutės.
Parašo šifravimas atskirai nuo žinutės, sumažina šifruojamos informacijos kiekį. Tai yra labai svarbu, kadangi viešų raktų algoritmai yra labiau lėtesnį nei tradiciniai algoritmai. Pasirašymo procesas taip pat prie žinutės prideda papildomos informacijos. Ši informacija žinutės adresatui padeda identifikuoti ar buvo koreguotas žinutės turinys.
Tikrinant parašą, jis yra apdorojamas su tikruoju viešuoju raktu ir gautas rezultatas yra palyginamas su žinute. Palyginimo rezultatas ir identifikuoja ar parašas tikras ar ne.

Parašas ant duomenų elemento

Nuo pat duomenų sukūrimo pradžios, duomenų vientisumas turi būti paremtas elektroninių parašų. Tai reiškia, kad duomenų objektas ar patys duomenis negali būti keičiami komunikavimo proceso metu. HL7 taikomoji programa „A“, kartu su siunčiamais duomenų elementais turi perduoti(persiųsti, apdoroti) ir parašą, nepriklausomai nuo komunikavimo saugumo mechanizmų. Priimančioji taikomoji programa „B“, apdoroja duomenų elementus kartu su parašu ir perduoda visą informaciją galutiniam adresatui.
Paprastai HL7 žinutė struktūra susideda iš kelių segmentų. Kiekvienas segmentas susideda iš vieno ar daugiau laukų. Kiekvienas laukas susideda iš vieno ar daugiau komponentų. Teoriškai įmanoma uždėti elektroninį parašą ant kiekvieno anksčiau paminėto lygmens. Tai reiškia papildomų HL7 duomenų struktūros pakeitimų atsiradimą.
Atskirų komponentų žymėjimas elektroninių parašų naudojamas kai vartotojas nėra atsakingas už kiekvieno informacijos lauko užpildymą t.y. kai jis užpildo ar koreguoja tik dalį informacijos. Kaip praktika rodo, vartotojas dažniausiai keičia arba papildo tik dali informacijos. Dėl to griežtai rekomenduojama, kad būtų parašu būtų žymimi atskiri komponentai.
HL7 žinutės saugumo funkcionalumo išplėtimas elektroniniu parašu, įtakoja žinutės duomenų struktūros pakeitimus ar papildymus. Tam kad būtų galima atskirti parašą nuo komponento ar duomenų lauko, naudojamas naujas skyriklis.

Šis metodas reikalauja iš HL7 aplinkos „sumanumo“. Aplinka paeiliui skaičiuodama skyriklius, turi nustatyti parašo reikšmę.

Ar papildomo skyriklio įvedimas „nesugriaus“ HL7 žinutės struktūros ? Remiantis HL7 standartais, galima naudotis naujais skyrikliais – tik jie neturi persidengti su skyriklių/kontrolės informacija ir žinutės informacija. Be to, nauji skyrikliai turi būti pasirenkami iš ASCII rašmenų rinkinio.

HL7 komunikacijų saugumo užtikrinimo technologiniai sprendimo būdai

HL7 žinučių mainų saugumą užtikrinančių technologijų diegimas komunikuojančiose įrenginiuose, kaip reikalavimą iškelia, kad programinė įranga „palaikytų“ vartotojų autentifikavimą ir informacijos apsaugą(konfidencialumas, vientisumas ir siuntėjo bei priėmėjo veiksmų kontrolės užtikrinimas)[4]. HL7 komunikavimo serveris turi „palaikyti“ sistemos autentifikavimą ar duomenų perdavimo saugumą. Remiantis HL7 paradigma, aplikacijos „susitinka“ tam tikroje vietoje ir apsikeičia žinutėmis naudodamos MLLP ar HLLP. Kriptografiškai užšifruotos(naudojantis S/MIME ar PGP/MIME) informacijos išnešiojimas nepriklauso nuo komunikavimo protokolo tokio kaip elektroninis paštas ar FTP protokolas. v galima papildyti kriptografiniais apsaugos servisais naudojančiais S/MIME ar PGP/MIME technologijas. Tai galima padaryti tradiciniais vartotojo elektroninio pašto agentais(MUAs). Bet nėra griežtai ribojamas jų naudojimas. Šie apsaugos servisai gali būti naudojami su bet kuriuo informacijos transportavimo mechanizmų, kuris perduoda MIME duomenis(http ar ftp).

Užtikrinant EDI transakcijų saugumą, dėmesys turi būti kreipiamas ne vien tik žinučių pasiuntimui ar gavimui. Būtina stebėti ir pačius veiksmus t.y. siuntimą ir priėmimą. HL7 paprastai reikalauja atsakymo apie įvykdytą veiksmą. Taip pat yra reikalauja, kad atsakymo žinutės būtų poruojamos kartu su užklausimo žinute. Tai galima padaryti naudojantis turiniu paremta, MIME daugialype technologija.

Kriptografinė žinučių apsauga

PKCS#7

Viešųjų raktų kriptografinis standartas nr. 7 (PKCS#7 versija 1.5) aprašo bendrąją sintaksę duomenims(elektroninis parašas, elektroninis vokas) kuriems gali būti taikoma kriptografija. Sintaksė palaiko rekursiją, kas leidžia vieną duomenų voką įdėti į kitą voką. Ši sintaksė aprašo tokius požymius kaip turinio tipas, žinutės santrauka, pasirašymo laikas, parašo patvirtinimas.

CMS

Kriptografinė žinutės sintaksė (Cryptographic Message Syntax) yra viena iš S/MIME versijos 3 dalių ir kilusi iš PKCS#7 versija 1.5. taigi ši sintaksė taip pat yra skirta naudojantis elektroniniais parašais, parašų patvirtinimu, autentifikavimu ar šifruojant žinutes.

Schemų saugojimas ir persiuntimas (S/MIME ir PGP/MIME)

Schemų saugojimo ir persiuntimo technologija – tai S/MIME ir PGP/MIME sprendimų apjungimas. Tiek S/MIME, tiek PGP/MIME yra prieinamos kaip programinė įranga naudojant elektroninį paštą. Tie patys sprendimai yra prieinami ir naudojantis SHTTP protokolu. Nenaudojant schemų saugojimo ir persiuntimo technologijos, nerekomenduojama naudotis tiesioginio ryšio sprendimais, tokiais kaip du, tarpusavyje komunikuojantis SMTP serveriai.

PGP-Servisai

PGP servisai apima elektroninius parašus, elektroninius vokus, duomenų suspaudimą, ir sertifikatus. Duomų suspaudimas yra artimas saugumui. Įvairius simbolių junginių pasikartojimų sumažinimas duomenyse, juos suspaudžiant, mažina galimybę jog duomenis bus pažeisti. Paprastai PGP šifruoja ir žymi duomenis elektroniniu parašu per vieną žingsnį. Bet tai nerekomenduojama HL7 atveju.

S/MIME

Apsauga/MIME numato nuoseklų MIME žinučių siuntimo ir priėmimo kelią. Paremta Internetiniu MIME standartu, ši technologija siūlo kriptografinius saugumo servisus skirtus elektroninių žinučių perdavimo technologijoms: žinučių konfidencialumas, žinučių vientisumas ir elektroninis parašas.
S/MIME V2 aprašo kaip turi būti formuojamos MIME turinio dalys, kurios buvo kriptografiškai apdorotos naudojant PKCS#7[9].

MIME technologijos panaudojimas HL7 žinutėms

Prieš išsiunčiant HL7 žinutę naudojantis MIME technologijomis(S/MIME ar PGP/MIME), žinutė privalo būti sukoduota į Base64 koduotę. Tas yra reikalinga norint apsaugoti nuo praradimo tam tikrus HL7 simbolius(kas vėliau įtakoja elektroninio parašo sugadinimą). Be to dar žinutė yra „įvelkama“ į MIME „kūną“. Elektroninis parašas yra įterpiamas ir pirmąsias MIME žinutės dalis.
Po HL7 žinutės transportavimo, ji yra iššifruojama ir patikrinama. Patikrinimui, MIME „kūnas“ kuriame yra HL7 žinutė, turi būti dekoduotas iš Base64 koduotės ir iššifruotas.
Žinutės “priėmėja” privalo mokėti atpažinti gautų duomenų tipą. Dėl tos priežasties, HL7 „įvilkta“ į MIME „kūną“, privalo turėti identifikacijos atributus(„content-type”, turinio aprašymas –

„application/x-EDI-HL7“).Tarp identifikuojančių atributų būtinai turi būti informacija apie sintaksę ir versijas. Šių atributų panaudojimas kaip pavyzdys galėtų būti šifravimas.

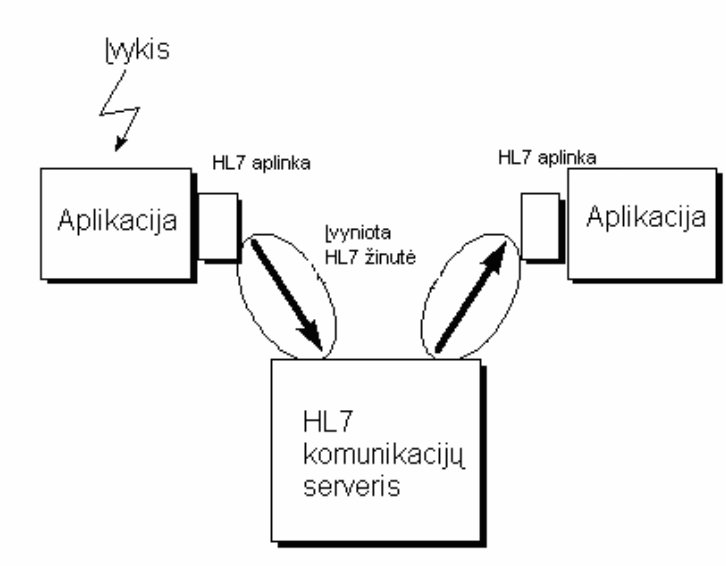
Kitas galimas sprendimas yra HL7 žinutės prijungimas prie X12 žinutės naudojantis standartinėmis prijungimo taisyklėmis(turinio aprašymas – „application/EDI-X12“).

Apdorojant stambias laikmenas, jų „suspaudimui“, prieš jas šifruojant, galima panaudoti EDI žinučių „suspaudimo“ technologiją(jei reikalinga, elektroninis parašas priskiriamas prieš duomenų apdorojimo procesą). „Suspaudimo“ procesas veikia efektyviai nes didžioji dalis informacijos pasikartoja. Be to duomenų suspaudimas prieš juos šifruojant, sustiprina kriptografinę apsaugą – pasikartojančių eilučių skaičius yra sumažinamas iki minimumo. MIME standartas nereikalauja nurodyti informacijos „suspaudimo“ tipo, bet palaiko tokios informacijos aprašymą(„

Content-Encoding: gzip”)

Komunikacijos protokolai

HL7 žinutės, informacijos apsikeitimo metu, yra „įvyniojamos“ į apsauginį voką. Tam yra naudojami išoriniai HL7 komunikacijų protokolai su integruotomis apsaugos priemonėmis(SHTTP ar SFTP).



Paveikslas nr. 7. Žinutės apdorojimo schema

SSL ir TLS

SSL yra naudojamas kaip TCP programinės sąsajos praplėtimas arba papildoma programinė sąsaja einanti ant TCP programinės sąsajos. Galima teigti, kad SSL yra tarpinė grandis tarp programinės įrangos ir TCP. SSL privalumai:

- Užkerta kelia slaptiems informacijos nuskaitymams

- Komunikuojant dviem sistemoms, viena pusė patikrinti kitos pusės identifikacijos informaciją. Viena pusė pateikia „sertifikatą“ kitai pusei įrodanti jos tapatybę.
- Duomenų vientisumas yra garantuotas. Bet koks informacijos baito pakeitimas pripažins kontrolinę sumą ir tuo pačiu didelę informacijos porciją kaip negaliojančia.

SSL yra naudingas standartinėms, šiuo metu naudojamoms HL7 sąsajoms kurios naudoja TCP. Taip pat jis yra naudingas “HL7 informacijos manai naudojant HTTP”. Šios technologijos varomoji jėga yra elektroninis sertifikatas. Elektronines sertifikatas patvirtina, kad jus žinote apie kitos „pusės“ slaptą raktą. Kadangi šis slaptas rakta niekada nėra perduodamas, operaciškai yra lengviau išlaikyti slaptą raktą paslaptyje.

IPv6

Naujo protokolo IPv6 architektūra labai daug dėmesio skiria informacijos saugumo servisams. Jis taip pat pagerina visų tinklų našumą bei funkcionalumą.

Nepriklausomai nuo jau egzistuojančių saugumo užtikrinimo sprendimų, naujame protokole yra įdiegta daug naujų saugumo galimybių: IP duomenų apsaugos servisai aptarnauja netgi tą programinę įrangą kuri ignoruoja duomenų apsaugą. IPv6 palaiko du saugumo funkcionalumus : autentifikavimą ir privatumas. Autentifikavimo mechanizmas užtikrina, kad priimtas duomenų paketas buvo siuntėjo, kurio duomenys nurodyti paketo antraštėje. Taip pat autentifikavimas užtikrina, kad žinutės turinys nebuvo sugadintas perdavimo metu. Privatumas, garantija, kad žinutė gali būti perskaityta tik autorizuotų subjektų, realizuojamas pasitelkiant sudėtingas šifravimo technologijas.

3. Projektinė dalis

HL7 žinučių saugumo realizavimas

Suformulavęs medicininių dokumentų saugumo struktūrą, iškėliau sau tris pagrindines problemines sritis: identifikavimas, vientisumas ir veiksmų kontrolė. Išanalizavau duomenų apsaugos technologijas ir jų integraciją kartu su HL7 standartų. Probleminių sričių sprendimui pasirinkau duomenų mainų technologiją MIME ir elektroninį parašą. Šių technologijų integravimą kartu su HL7 pateikiu praktinio pavyzdžio pavidalu[5].

Pirmas žingsnis, tai HL7 užklausos, gauti tam tikrą informaciją, generavimas.

Pavyzdyje pateikti duomenis yra išgalvoti. Jie reikalingi, kad būtų galima lengviau įsivaizduoti visą HL7 duomenų mainų procesą.

```
+-------------------------------------------------------------------------+
|MSH|^~\&|OE|GYD.JONAITIS|LAB|LIGONINE-Y|...||ORM|RQ-O01-01|P|2.2|      |
|PID|||08157411||PETRAS^PETRAITIS||19800313|M|                            |
|PV1||O|||||0123^JONAITIS^JONAS|||||||||||12|                             |
|ORC|NW|12345|||F|                                                        |
|OBR||12345||||||20040511175948||7^ML||||||BLDV                          |
|ORC|CH|12345-1|||F||12345|                                              |
|OBR||12345-1|||5383-5^LIGA X^LN|                                        |
|ORC|CH|12345-2|||F||12345|                                              |
|OBR||12345-2|||5381-9^LIGA X^LN|                                        |
|ORC|CH|12345-3|||F||12345|                                              |
|OBR||12345-3|||5385-0^KRAUJO TYRIMAI Z^LN|                              |
+-------------------------------------------------------------------------+
```

Ši užklausa yra „įvyniojama“ į MIME-EDI esybę t.y. „prikabinama“ MIME antraštė identifikuojanti. Tai reikalinga tam, kad kita komunikuojanti pusė lengviau galėtų identifikuoti kokia technologija buvo panaudota formuojant žinutę.

```
+-------------------------------------------------------------------------+
|Content-Type: application/edi-hl7                                        |
|Content-Transfer-Encoding: quoted-printable                              |
|                                                                         |
|MSH|^~\&|OE|GYD.JONAITIS|LAB| LIGONINE-Y |20040511175948||ORM=          |
||RQ-O01-001|P|2.2=0DPID|||08157411||PETRAS^PETRAITIS||19800313|M|=0DP=|
|ID|||08157411|| PETRAS^PETRAITIS||19800313|M|=0DPV1||O||||0123^JONAIT=|
|IS^JONAS|||||||||||12|=0DORC|NW|12345|||F|=0DOBR||12345||||=           |
|||20040511175948||7^ML||||||KRAUJ=0DORC|CH|12345-1|||F||12345|=         |
|=0DOBR||12345-1|||5383-5^KRAUJO TYRIMAI Z^LN|=0DORC|CH|1=              |
|2345-2|||F||12345|=0DOBR||12345-2|||5381-9^KRAUJO TYRIMAI Z^=          |
|LN|=0DORC|CH|12345-3|||F||12345|=0DOBR||12345-3|||5385-0^KRAUJ=         |
|O TYRIMAI Z ^LN|=0D                                                     |
+-------------------------------------------------------------------------+
```

Kitas žingsnis tai žinutės pažymėjimas ar parašo padėjimas. Parašas generuojamas virš MIME-EDI antraštės. PGP išvestis yra prijungiama kaip antroji daugialypės/pažymėtos MIME esybės dalis. Šis pavyzdys yra mano anksčiau įvardintos identifikavimo problemos sprendinys. Prie žinutės pridėjus

parašo identifikatorių, komunikuojančios t.y. šią žinutė priimančios, pusės galės lengviau nustatyti kas yra užklausos siuntėjas.

```
+-----------------------------------------------------------------------+
|Content-Type: multipart/signed;                                        |
|   protocol="application/pgp-signature"                                |
|   micalg="pgp-md5"; boundary="sigbound"                               |
|                                                                       |
|--sigbound                                                             |
|Content-Type: application/edi-hl7                                      |
|Content-Transfer-Encoding: quoted-printable                            |
|                                                                       |
|MSH|^~\&|OE|GYD.JONAITIS|LAB| LIGONINE-Y |20040511175948||ORM=        |
||RQ-O01-001|P|2.2=0DPID|||08157411||PETRAS^PETRAITIS||19800313|M|=0DP=|
|ID|||08157411|| PETRAS^PETRAITIS||19800313|M|=0DPV1||O||||0123^JONAIT=|
|IS^JONAS|||||||||||12|=0DORC|NW|12345|||F|=0DOBR||12345||||=          |
|||20040511175948||7^ML||||||KRAUJ=0DORC|CH|12345-1|||F||12345|=       |
|=0DOBR||12345-1|||5383-5^KRAUJO TYRIMAI Z^LN|=0DORC|CH|1=              |
|2345-2|||F||12345|=0DOBR||12345-2|||5381-9^KRAUJO TYRIMAI Z^=         |
|LN|=0DORC|CH|12345-3|||F||12345|=0DOBR||12345-3|||5385-0^KRAUJ=       |
|O TYRIMAI Z ^LN|=0D                                                    |
|--sigbound                                                             |
|Content-Type: application/pgp-signature                                |
|                                                                       |
|-----BEGIN PGP MESSAGE-----                                            |
|Version: 2.6.3ia                                                       |
|                                                                       |
|iQBVAwUANKPor3g+w2PflLsNAQH/iwIAnqYzaL0qs2hqItqniL1D3jpf3+9ku         |
|u6w5URl9G3KM9s6GzgtY0VgUCpO/gkToG3iRYLjhuKjmI2mJV76ItZMA==             |
|=52tL                                                                  |
|                                                                       |
|-----END PGP MESSAGE-----                                              |
|                                                                       |
|--sigbound--                                                           |
+-----------------------------------------------------------------------+
```

“Prikabinus” prie žinutės parašą, žinutė yra “įdedama” į voką. Žinutė iš voko gali būti ištraukta tik dedikuoto adresato t.y. to kuriam ji yra siunčiama.

```
+-----------------------------------------------------------------------+
|Content-Type: multipart/encrypted;                                     |
|   boundary="encbound"; protocol="application/pgp-encrypted"           |
|                                                                       |
|--encbound                                                             |
|Content-Type: application/pgp-encrypted                                |
|                                                                       |
|Version: 1                                                             |
|                                                                       |
|                                                                       |
|--encbound                                                             |
|Content-Type: application/octet-stream                                 |
|                                                                       |
|-----BEGIN PGP MESSAGE-----                                            |
|Version: 2.6.3ia                                                       |
|                                                                       |
|hEwDp7HUcMTu8A0BAf47c+gxPvgY90sbNmXK67p5AC0OjJ8ZYrSMJLmo6UTUU          |
|SyjikhDVjXSlaRK5L+rW8AzAbTcuJ3wA3y3wFrF+pgAAA/FHZhtIG/bSb0I8F          |
|YHK+rXFVL6zMGiVnJlrqcyHnaqQyxgAAhXwFNZODjEfuAxX5R6QzYPLZJiCAf          |
```

```
|9yGgHyW43qd0OqSZ1yjIazgS4JYXreRkkGvnKKI+gAHG9l9AuTqI384aKYZOX          |
|eIoDAOEJCVVeXiTAW4/AxZhinQDYmaLPSCExKZRx0qvFv8L5kX5VlgJ6e0MCc          |
|2b/K9guTM9dL0O7xyoQd5FDDwZja6mauhboGEsRzKHrpcyrgxNFL80/vLTnP5          |
|TtBMc7vW6xRpW2l7NDVwpXQGi3zJU+zybRekOVg34xNcMjO/yZwfopmiCax41          |
|KZu9ZW4Y2T3vkAKR6njbqvx7Y6ME6u+G+fd2wYVeCi3oI8t913ZAxn6MkO+dg          |
|oA4ehfdFrpSLNgSVQsgdxaS28Ew6Xuc6S4c9IVjI4xBYlo0XKzU8i5yZardXJ          |
|hvD3o2Tm6BNCC8o3ODKTyfzbt0XamBr7oM4UfCTb29m90paxUuIonD8NWSl9H          |
|RCtS8ZWjlWYjMoDyDZ2ssFG0X46LVhHBSp3HR5gmhtaamTqhEG+0b/HRkc98A          |
|QysGFMIeZdw6SUilMHl0Vx7yZ+qimFRHVVYJVxKOCZ6weEzORdukB4rLOZNVL          |
|AO4lrDm6gMewehQ7nCTpaJuG1LrifeagcKAZqdQe5DkwnQRuEbh0ed1ivbVd5          |
|cFTQiT5LG2i4G5Bu676WhIHoQXmBaMBlX1FaJddxdfIHoFL2J9RcfNwCka7YW          |
|hTGNM8PT5VSoW1Wd56BCQaOmySSaJ6C/HhGVoEQbcIElwWLiHqlGAMITlHwk8          |
|UwI7mLBNugG5Z8QPfQAYlG5cSw3rwFQkfMo1GAYSQAcWK4vLZxhk84ar2jZc1          |
|gdr0reXxZaso3PCchJMJ8CIPN771J64JtBRi4N2sbD5V8saPoyzTgvPVYkESs          |
|n+hPovIK8d/rgGNJ/WH0EXOALzmrdqmt+M2BD5einlgG9o43                        |
|=q5P+                                                                   |
|                                                                        |
|-----END PGP MESSAGE-----                                               |
|                                                                        |
|--encbound--                                                            |
+------------------------------------------------------------------------+
```

Sistema kuriai buvo adresuota ši žinutė, „išima“ jai adresuota informaciją iš elektroninio voko.

```
+------------------------------------------------------------------------+
|Content-Type: multipart/signed;                                         |
|   protocol="application/pgp-signature"                                 |
|   micalg="pgp-md5"; boundary="sigbound"                                |
|                                                                        |
|--sigbound                                                              |
|Content-Type: application/edi-hl7                                       |
|Content-Transfer-Encoding: quoted-printable                             |
|                                                                        |
|MSH|^~\&|OE|GYD.JONAITIS|LAB|LIGONINE-Y|20040511175948||ORM=           |
||RQ-O01-001|P|2.2=0DPID|||08157411||PETRAS^PETRAITIS||19800313|M|=0DP=|
|ID|||08157411|| PETRAS^PETRAITIS||19800313|M|=0DPV1||O||||0123^JONAIT=|
|IS^JONAS|||||||||||12|=0DORC|NW|12345|||F|=0DOBR||12345||||=           |
|||20040511175948||7^ML||||||KRAUJ=0DORC|CH|12345-1|||F||12345|=        |
|=0DOBR||12345-1|||5383-5^KRAUJO TYRIMAI Z^LN|=0DORC|CH|1=              |
|2345-2|||F||12345|=0DOBR||12345-2|||5381-9^KRAUJO TYRIMAI Z^=          |
|LN|=0DORC|CH|12345-3|||F||12345|=0DOBR||12345-3|||5385-0^KRAUJ=        |
|O TYRIMAI Z ^LN|=0D                                                     |
|--sigbound                                                              |
|Content-Type: application/pgp-signature                                 |
|                                                                        |
|-----BEGIN PGP MESSAGE-----                                             |
|Version: 2.6.3ia                                                        |
|                                                                        |
|iQBVAwUANKPor3g+w2PflLsNAQH/iwIAnqYzaL0qs2hqItqniL1D3jpf3+9ku          |
|u6w5URl9G3KM9s6GzgtY0VgUCpO/gkToG3iRYLjhuKjmI2mJV76ItZMA==              |
|=52tL                                                                   |
|                                                                        |
|-----END PGP MESSAGE-----                                               |
|                                                                        |
|--sigbound--                                                            |
+------------------------------------------------------------------------+
```

Parašas “prikabintas” prie žinutės, yra tikrinamas sistemos(vykdomo identifikavimo kontrolė), tam

kad autentifikuoti žinutę. Autentifikavus žinutę, yra „išgryninama“ informacijos užklausą.

```
+--------------------------------------------------------------------+
|Content-Type: application/edi-hl7                                   |
|Content-Transfer-Encoding: quoted-printable                         |
|                                                                    |
|MSH|^~\&|OE|GYD.JONAITIS|LAB|LIGONINE-Y|20040511175948||ORM=         |
||RQ-O01-001|P|2.2=0DPID|||08157411||PETRAS^PETRAITIS||19800313|M|=0DP=|
|ID|||08157411|| PETRAS^PETRAITIS||19800313|M|=0DPV1||O||||0123^JONAIT=|
|IS^JONAS|||||||||||12|=0DORC|NW|12345|||F|=0DOBR||12345||||=        |
|||20040511175948||7^ML||||||KRAUJ=0DORC|CH|12345-1|||F||12345|=      |
|=0DOBR||12345-1|||5383-5^KRAUJO TYRIMAI Z^LN|=0DORC|CH|1=           |
|2345-2|||F||12345|=0DOBR||12345-2|||5381-9^KRAUJO TYRIMAI Z^=       |
|LN|=0DORC|CH|12345-3|||F||12345|=0DOBR||12345-3|||5385-0^KRAUJ=      |
|O TYRIMAI Z ^LN|=0D                                                 |
+--------------------------------------------------------------------+
```

Po to kai žinutė yra “ištraukiama” iš MIME-EDI konteinerio, ji perduodama į informacinės sistemos duomenų bazę. Ji savo ruožtu generuoja atsakymą į gautą užklausą:

```
+--------------------------------------------------------------------+
|MSH|^~\&|LAB|LIGONINE-Y|OE|GYD.JONAITIS|...|ORR|RP-O01-831|P|2.2     |
|MSA|AA|RQ-O01-001|UZKLAUSA PRIIMTA|                                 |
|PID||47110815|08157411||PETRAS^PETRAITIS||||                        |
|PV1||O|||||0123^JONAITIS^JONAS|||||||||||12|                       |
|ORC|OK|12345|54321||SC                                             |
+--------------------------------------------------------------------+
```

Užklausą priėmusi informacinė sistema signalizuoja užklausėjo informacinei sistemai, kad užklausa buvo sėkmingai priimta. Sekančiu žingsniu yra tikrinamas žinutės duomenų vientisumas – kitos duomenų apsaugos probleminės srities – vientisumas, sprendimas. Tai yra daroma lyginant turinio informaciją su žinutės paraše esančia informacija(nurodyti parametrai, apibrėžimai, taisyklės):

```
+--------------------------------------------------------------------+
|Content-Type: multipart/related;                                    |
|   type="application/x-edi-response";                               |
|   boundary="relbound"                                              |
|                                                                    |
|--relbound                                                          |
|Content-Type: application/edi-hl7                                   |
|Content-Transfer-Encoding: quoted-printable                         |
|                                                                    |
|MSH|^~\&|LAB|LIGONINE-Y|OE|GYD.JONAITIS|20040511182611||O=          |
|RR|RP-O01-883157170|P|2.2=0DMSA|AA|RQ-O01-001|UZKLAUSA PRIIMTA=     |
|D|=0DPID||47110815|08157411||PETRAS^PETRAITIS||||=0DPV1||O|||||0123=  |
|^JONAITIS^JONAS|||||||||||12|=0DORC|OK|12345|54321||SC=0D=           |
|                                                                    |
|--relbound                                                          |
|Content-Type: multipart/report;                                     |
|   report-type="disposition-notification";                          |
|   boundary="repbound"                                              |
|                                                                    |
|--repbound                                                          |
|Content-Type: text/plain                                            |
|                                                                    |
```

```
|your message has been processed                                          |
|                                                                         |
|--repbound                                                               |
|Content-Type: message/disposition-notification                           |
|Content-Transfer-Encoding: 7bit                                          |
|                                                                         |
|Received-content-MIC: 54ee0a959b7a92fdbe766538c948dbfeccdeb2,sha1        |
|                                                                         |
|--repbound--                                                             |
+-------------------------------------------------------------------------+
```

Atsakymas ir parašas yra supakuojamas į daugialypės/pažymėtos MIME esybę.

```
+-------------------------------------------------------------------------+
|Content-Type: multipart/signed;                                          |
|   protocol="application/pgp-signature";                                 |
|   micalg="pgp-md5"; boundary="sigbound"                                 |
|                                                                         |
|--sigbound                                                               |
|Content-Type: multipart/related;                                         |
|   type="application/x-edi-response";                                    |
|   boundary="relbound"                                                   |
|                                                                         |
|--relbound                                                               |
|Content-Type: application/edi-hl7                                        |
|Content-Transfer-Encoding: quoted-printable                              |
|                                                                         |
|MSH|^~\&|LAB| LIGONINE-Y |OE| GYD.JONAITIS |20040511182611||O=          |
|RR|RP-O01-883157170|P|2.2=0DMSA|AA|RQ-O01-001| UZKLAUSA PRIIMTA =       |
|D|=0DPID||47110815|08157411|| PETRAS^PETRAITIS ||||=0DPV1||O|||||0123=|
|^JONAITIS^JONAS ||||||||||||12|=0DORC|OK|12345|54321||SC=0D=             |
|                                                                         |
|--relbound                                                               |
|Content-Type: multipart/report;<LF>                                      |
|   report-type="disposition-notification";                               |
|   boundary="repbound"                                                   |
|                                                                         |
|--repbound                                                               |
|Content-Type: text/plain                                                 |
|                                                                         |
|your message has been processed                                          |
|                                                                         |
|--repbound                                                               |
|Content-Type: message/disposition-notification                           |
|Content-Transfer-Encoding: 7bit                                          |
|Received-content-MIC: 54ee0a959b7a92fdbe766538c948dbfeccdeb2,sha1        |
|                                                                         |
|--repbound--                                                             |
|                                                                         |
|--relbound--                                                             |
|                                                                         |
|--sigbound                                                               |
|Content-Type: application/pgp-signature                                  |
|                                                                         |
|-----BEGIN PGP MESSAGE-----                                              |
|Version: 2.6.3ia                                                         |
|                                                                         |
|iQBVAwUANKPotKex1HDE7vANAQFYtgH9EZA4gWleqqZYUhTVsoLcYtykALNKCkqW         |
|nCYsPbnL43YSnuL0dWEavfoWT9i08QtzAVM+73Lhxm4bqJNjY+F/oA==                 |
|=ldjq                                                                    |
|                                                                         |
```

```
|-----END PGP MESSAGE-----                                                |
|<LF>                                                                     |
|--sigbound--                                                             |
+-------------------------------------------------------------------------+
```

Galiausiai pasirašytas atsakymas yra šifruojamas ir siunčiamas autentifikuotui užklausimo siuntėjui.

```
+-------------------------------------------------------------------------+
|Content-Type: multipart/encrypted; boundary="encbound";                  |
|   protocol="application/pgp-encrypted"                                  |
|                                                                         |
|--encbound                                                               |
|Content-Type: application/pgp-encrypted                                  |
|                                                                         |
|Version: 1                                                               |
|                                                                         |
|--encbound                                                               |
|Content-Type: application/octet-stream                                   |
|                                                                         |
|-----BEGIN PGP MESSAGE-----                                              |
|Version: 2.6.3ia                                                         |
|hEwDeD7DY9+Uuw0BAf0eLhV0xFGF9EQbe1OtcqnZQGWXhOEw+/8ibnHQ2BGHa           |
|zEsazOmBOiyf+gGm79ISQY83rZkZ0McHn4Yne72cpgAABdnTCq9qY6XrA1vmt           |
|HQT3WS5qU7aMSFcKusfVUmkW2Cy/RZrJBqV9bKuH2n3i01OcIBQVbHdUC01uH           |
|nvmn/J7tktA9b0W5yAWLaGbCufsyaZxJyS7e7JooAzrYx5Y229Lhgtykb9r2V           |
|GAqvd/qgN2ZPvDhkyfh0p58bHv+ePQqVB979GMLblagOUdp6XtBtl3uDD8h73           |
|FgHpnP88M+U6AJReTgQAe01DKmUD4NaKxkZyPuHi9V/GCZdkCBZGOzBae2g3a           |
|fSo2aNqgjHGieF8CfJCHcMZKFgq8XNURQhAl+zcU02DpdH/aOnqWO3fPo5gCf           |
|cb3Nthm9vLIsQRA78TJAsxbKv8TVBQChutzDm19qdWemR5lmUIjheKEINd9nn           |
|HQ3oP0PC1PCNxJ7FWgUMxE3xZ6AaAC12YVSg14br6CFdCaDOA55flnNiLvdoC           |
|Llxi3UBsBGtaSfTsF5gtgumlV3xPpaS02c3sl7Mc7xcQkrg33smTkx3nhQDXs           |
|u4Ed1X67OOMTGVSbI5cGC1CYOI867ogI2B7Z0U274oQNH71xWchSHfbLwu7z9           |
|wYnVZQLbb2ncmBArcPoCnIznfQ7COnmPwkFHNTNV55Cif12JxZXdQyEnDbMnK           |
|Deyq6pHzaguq3PKxKt37aQtK1QSvhwBvcO4SMH5zJU/OR1R2Z+9ZpIeFoh79e           |
|LJZ60VAOuQ/lzejE8EI8R2Bcm9/GPRtCH6+CIEC2xgW/JfvyOtGcWUhVHrwGz           |
|jatqBGdqxyampHcGgnB1hPQVfhRzoI0jPdeEC5MBzD2feoTOj97MhGbx2oT8s           |
|FArMifectOLqayU3ELjGOdG6KvEc2sv68xeCv481yj3AoK6V3tvRJyukSaUXD           |
|yHUusUPyoZ4FTNjaXvHwEUmDkphT5XwithhKtr38id6eG+XubJMd1vKRbbsu5           |
|90y+kGINWpAozwJY79Hf4v5dIMkTVYJdTRvTQgeMhkytSmbc4ONr40FLfcyCV           |
|tAYpLqVTsnLMblwPnS0qVNSZi72UD7G/1Lf2dpXzUh8PrNTbAWbMCeB/xrifC           |
|wAGjAEqRxFJKFwl2IHgoewEM/Yxt9L0DuPdB/ow8kF301p80iHZ1NL0V4lM=           |
|=wyMm                                                                    |
|                                                                         |
|-----END PGP MESSAGE-----                                                |
|                                                                         |
|--encbound--                                                             |
+-------------------------------------------------------------------------+
```

Užklausą suformavusį informacinė sistema priima atsakymą. Po to jis yra iššifruojamas ir patikrininama jo autentifikacija.

Šis pavyzdys padeda susidaryti bendrą vaizdą kaip yra panaudojamos pasirinktos apsaugos technologijos HL7 žinučių formavime. Be to tai yra įrodymas, kad buvo rastas visų mano iškeltų probleminių sričių sprendimai.

4. Tyrimo dalis

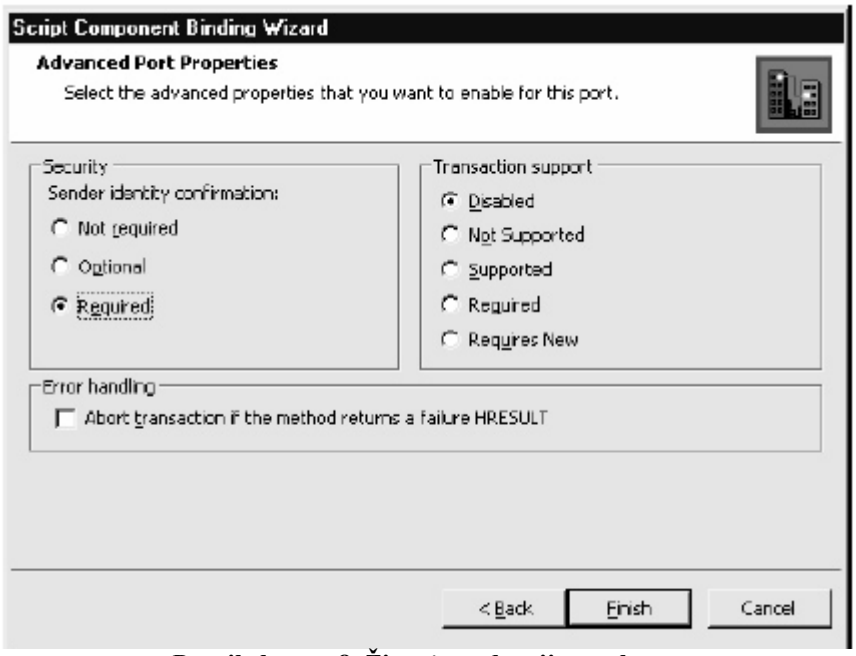
Kaip minėjau šio dokumento santraukoje, kad neapsiribosiu vien informacijos saugumo sprendimų suradimu ir jų realizavimu.

Vienas iš šio tiriamojo darbo uždaviniu yra apsaugos sprendimų integravimas su jau egzistuojančia medicininių dokumentų mainų sistema. Ją galima įvardinti kaip medicininių dokumentų mainų prototipine programine įranga. Jos architektūra yra paremta B2B architektūra. Šiame informacijos mainų sprendime panaudotas BizTalk serveris, kuris realizuoja B2B architektūrą.

Tad šioje dalyje aptarsime HL7 žinučių saugumo sprendimo integravimą su BizTalk serveriu. Šis serveris atlieka informacijos mainų užtikrinimą tarp kelių komunikuojančių subjektų.

Elektroninių dokumentų apsauga

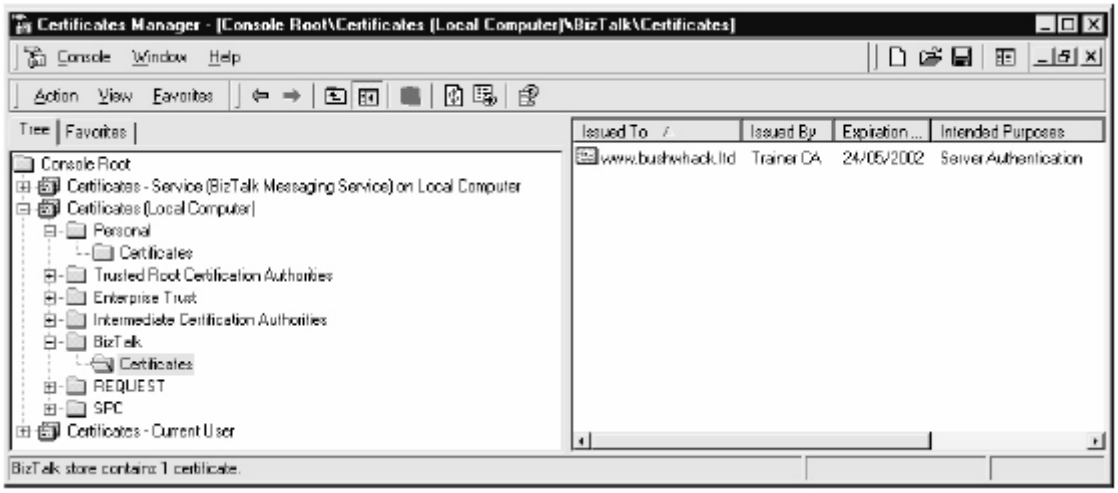
Saugumo sprendimo integravimas koncentruojasi ties duomenų identifikavimu, vientisumu ir veiksmų kontrolės realizavimu, pasitelkiant analitinėje dalyje įvardintas technologijas.



Paveikslas nr. 8. Žinutės apdorojimo schema

Informacijos identifikavimas

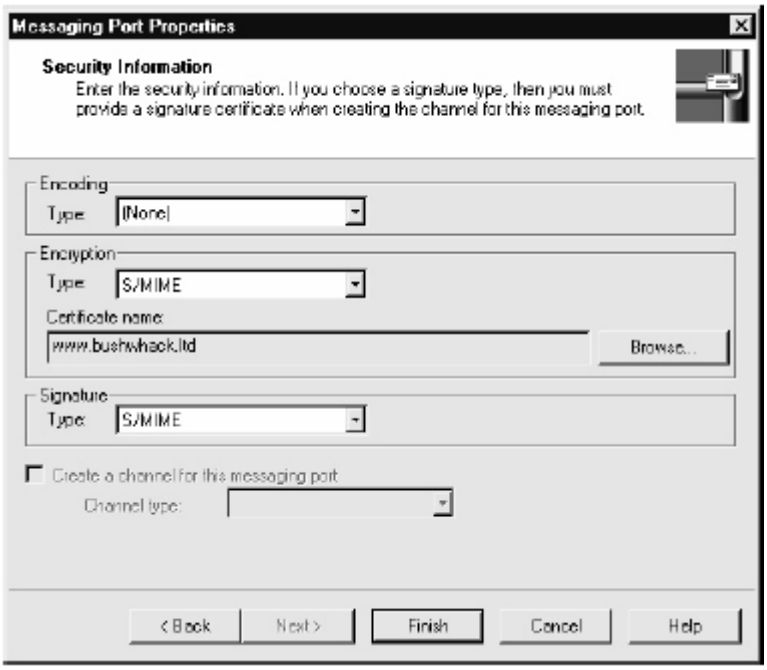
Vienai iš komunikuojančių pusių, siunčiant S/MIME šifruotą informaciją, BizTalk serveris atlieka šio informacijos identifikavimą. Prieš tai būtina išsaugoti elektroninį siunčiančiosios pusės sertifikatą(paveikslas nr. 9) tam, kad serveris galėtų palyginti gautą informaciją su turimu sertifikatu



Paveikslas nr. 9. Elektroninio sertifikato saugojimo vieta

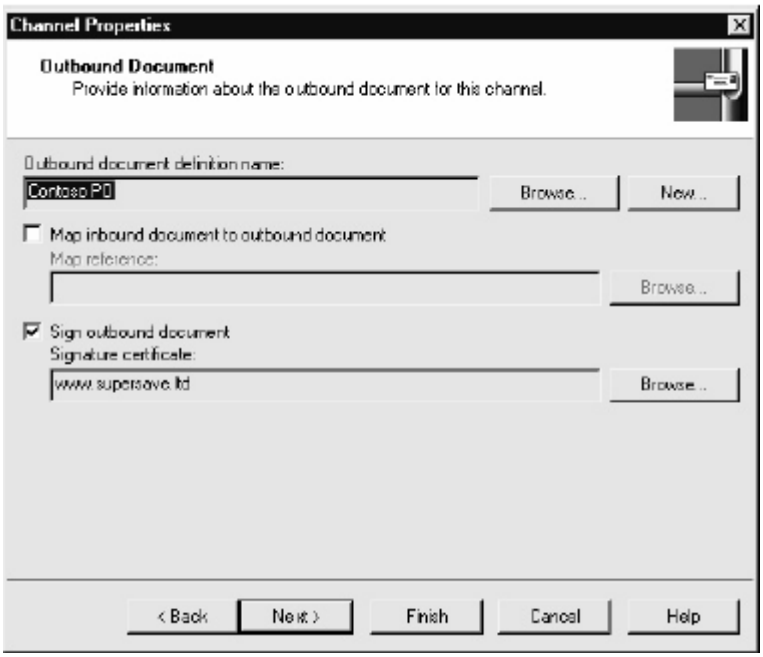
Išeinančios informacijos žymėjimas ir šifravimas

BizTalk serveris užtikrina išeinančios informacijos žymėjimą bei jos šifravimą. Tai yra daroma pasitelkiant S/MIME apsaugos ir šifravimo technologijas.



Paveikslas nr. 10. Informacijos mainų kanalo apsaugos nustatymas

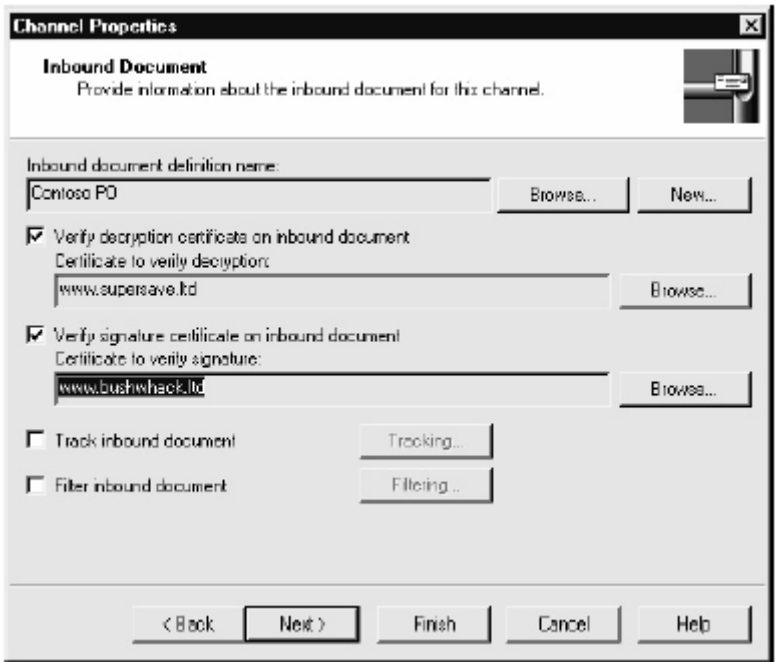
Iš serverio išeinanti informacija yra žymima elektroniniu parašu. Apsirašant atskirus komunikavimo informacijos kanalus jiems galima priskirti skirtingus elektroninius parašus(paveikslas nr. 11). Norėdami šifruoti išeinančią informaciją, nustatymuose (paveikslas nr. 10) pasirenkame šifravimo tipą.



Paveikslas nr. 11. Informacijos mainų kanalo apsaugos nustatymas

Įeinančios informacijos identifikavimas ir dešifravimas

Jeigu įeinanti informacija yra pažymėta elektroniniu parašu, serveris atlieka jo autentifikavimo procedūra. Šis funkcionalumas yra užtikrinamas, apsirašius, informaciją priimančio, komunikacijos kanalo, elektroninio parašo tikrinimo funkcijas.



Paveikslas nr. 12. Įeinančios informacijos elektroninio parašo priskyrimas

Norint iššifruoti gautą informaciją, nustatymuose(paveikslas nr. 12) pasirenkame dešifravimo sertifikatą.

Informacijos transportavimo apsauga

Projektinėje dalyje realizuotame duomenų apsaugos sprendime, duomenų transportavimui naudoju SMTP transportavimą. BizTalk serveris taip pat leidžia duomenis perdavinėti pasinaudojant SMTP. Pasitelkus S/MIME technologijas, galima pareikalauti autentifikavimo atliekant informacijos mainus.

5. Eksperimentinė dalis

Šioje dalyje atlieku eksperimentinę, duomenų apsaugos integracijos su BizTalk serveriu, analizę. Specialios analizės metodikos nenaudosiu. Pagrindiniais analizės aspektais pasirinksiu trijų dimensijų kontrolinį funkcionalumo patikrinimą. Pirmos dimensijos tyrimas apima tiriamojo darbo metu suformuluotų probleminių sričių realizavimą su BizTalk. Šios probleminės sritys, tai identifikavimas, duomenų vientisumas ir veiksmų kontrolė. Eksperimento rezultatai yra pateikiami šio dokumento priede nr. 4. Apibendrinant šiuos rezultatus, matome, kad identifikavimo ir vientisumo problemines sritis pavyko realizuoti su BizTalk. Veiksmų kontrolės nerealizavau nes tai reikalauja papildomų programinių pakeitimų, susijusių su jau egzistuojančios programinės įrangos pakeitimais. Tam reikalinga parašyti „skriptus“ kurie fiksuotų atliekamas su informaciją operacijas, bei atlikinėtų patvirtinimus informuojančius visas komunikuojančias puses, susijusias su užklausomis.
Antroji BizTalk integracijos analizės dimensiją – pagrindinio apsaugos funkcionalumo realizavimas. Ši analizė parodo kokį apsaugos funkcionalumo rinkinį man pavyko realizuoti su BizTalk serveriu. Pagrindines apsaugos funkcijas apsibrėžiau analitinėje ir projektinėje dalyse. Prie pagrindinio apsaugos funkcionalumo priskyriau elektroninius vokus, elektroninius sertifikatus, išeinančių dokumentų šifravimą bei žymėjimą, įeinančių dokumentų dešifravimą, informacijos siuntėjo identifikavimą, informacijos transportavimo apsaugą. Šio eksperimento rezultatai pateikiami priede nr. 5. Iš jų matome, kad integracijos metu pavyko realizuoti visas pagrindines duomenų apsaugos funkcijas. Paskutiniu analizės tašku(dimensija) pasirinkau buvusio duomenų mainų programinio sprendimo, pagrindinio funkcionalumo pasikeitimų kontrolinį sąrašą. Kontroliniame sąraše pateikiu pagrindines funkcijas kurias atlieka HL7 informacijos mainų sistema. Ši sąrašą galima rasti priede nr. 6. Prie kiekvienos funkcijos yra įvardinama ar pasikeitė šis funkcionalumas, bei ar buvo reikalingi programiniai sistemos pakeitimai. Iš šio tyrimo rezultatų galima daryti išvada, kad labiausiai buvo paliestos užklausų formavimo bei jų priėmimo funkcijos. Pasikeitimus įtakoja elektroninio sertifikato prijungimas prie žinutės, taip pat jos šifravimas. Jei yra gaunama šifruota informacija, yra reikalingi pakeitimai susiję su priimtos informacijos apdorojimu. Šie pakeitimai buvo realizuoti naudojantis standartinius BizTalk serverio nustatymus. Taip pat buvo atlikta dalis pakeitimų kuriems yra būtinas programinis kodas. Šie pakeitimai susiję su informacijos šifravimo algoritmų nustatymais.

6. Išvados

Medicininių dokumentų HL7 standarte saugumo sprendimų vystymasis yra dar tik pradinėje stadijoje. Dėl to konkrečių sprendimų apimančių HL7 informacijos saugumą nėra. Šiame tiriamajame darbe suformuodamas duomenų apsaugos struktūrą ir įvardindamas technologijas, kuriomis realizuojama ši struktūra, iš dalies išsprendžiau medicininių dokumentų saugumo problemą.

Suformuluota duomenų apsaugos struktūra buvo pritaikyta HL7 standartui. Toks apsaugos struktūros pritaikymas HL7 standartui yra naujas dalykas. Tai padėjo apibrėžti konkrečius HL7 standarto saugumo servisus bei aprašyti panaudojimo atvejų modelius. Detali panaudojimo atvejų analizė padėjo nustatyti duomenų mainų pagrindines operacijas, kurių saugumui reikalinga panaudoti informacijos apsaugos technologijas. Atlikus šią iteraciją pereinama prie duomenų saugumui reikalingų technologijų analizės.

Analizuojant informacijos saugumo technologijas ir jas integruojant su aprašytais HL7 standarto saugumo reikalavimais, kaip sprendimas duomenų mainų saugumo realizavimui pasirinktas elektroninis paštas su MIME technologijomis.

Projektinėje dalyje pateikdamas detalesnį žinutės formavimą su pasirinktomis saugumo technologijomis, įrodau, kad šios technologijos yra suderinamos su HL7 standartu.

Tiriamojoje šio dokumento dalyje buvo atlikta aprašyto duomenų apsaugos sprendimo integravimas su jau egzistuojančia HL7 duomenų mainų programine įranga. Sėkmingas saugumo sprendimų integravimas, pabrėžia kad HL7 medicininių dokumentų saugumo sprendimai yra lankstūs ir lengvai pritaikomi egzistuojančioms HL7 informacijos mainų sistemoms.

7. Literatūra

Straipsniai iš elektroninių žurnalų:

1. Requirements for Inter-operable Internet EDI (draft-ietf-ediint-req), Internet Draft (EDIINT Working Group), C.Shih, M.Jansson, R.Drummond, July 8, 1997. [žiūrėta 2004.02.04] http://www.ietf.org/html.charters/ediint-charter.html

2. Canadian Institute for Health Information. National Electronic Claims Standart Initiative. Prieiga per internetą. 2004.01.14 [žiūrėta 2004.02.25] Prieiga per internetą: http://secure.cihi.ca/cihiweb/dispPage.jsp?cw_page=infostand_eclaims_e

3. HL7 Organization. HL7 Standardart Documentation. 2002.01 [žiūrėta 2004.03.05]. Prieiga per internetą: http://www.hl7.org

4. Secure HL7 Transactions Using Internet Mail (draft-ietf-ediint-hl7), Internet Draft (EDIINT Working Group), G.Schadow, M.Tucker, W.Rishel, June, 1998. [žiūrėta 2004.04.09] http://www.ietf.org/internet-drafts/draft-ietf-ediint-hl7-00.txt

5. HTTP Transport for Secure EDI (draft-ietf-ediint-as2), Internet Draft (EDIINT Working Group), C.Shih, D.Moberg, R.Drummond, November 14, 1997. [žiūrėta 2004.04.14] http://www.ietf.org/html.charters/ediint-charter.html

6. German legal regulations concerning "The German Digital Signature Law" (SigG) as part of the German "Information and Communication Services Law" (IuKDG). [žiūrėta 2004.05.04] http:/www.iid.de/rahmen/iukdg.html

Kita naudota literatūra:

7. Ford, W.: Computer Communications Security. PTR Prentice Hall, 1994.

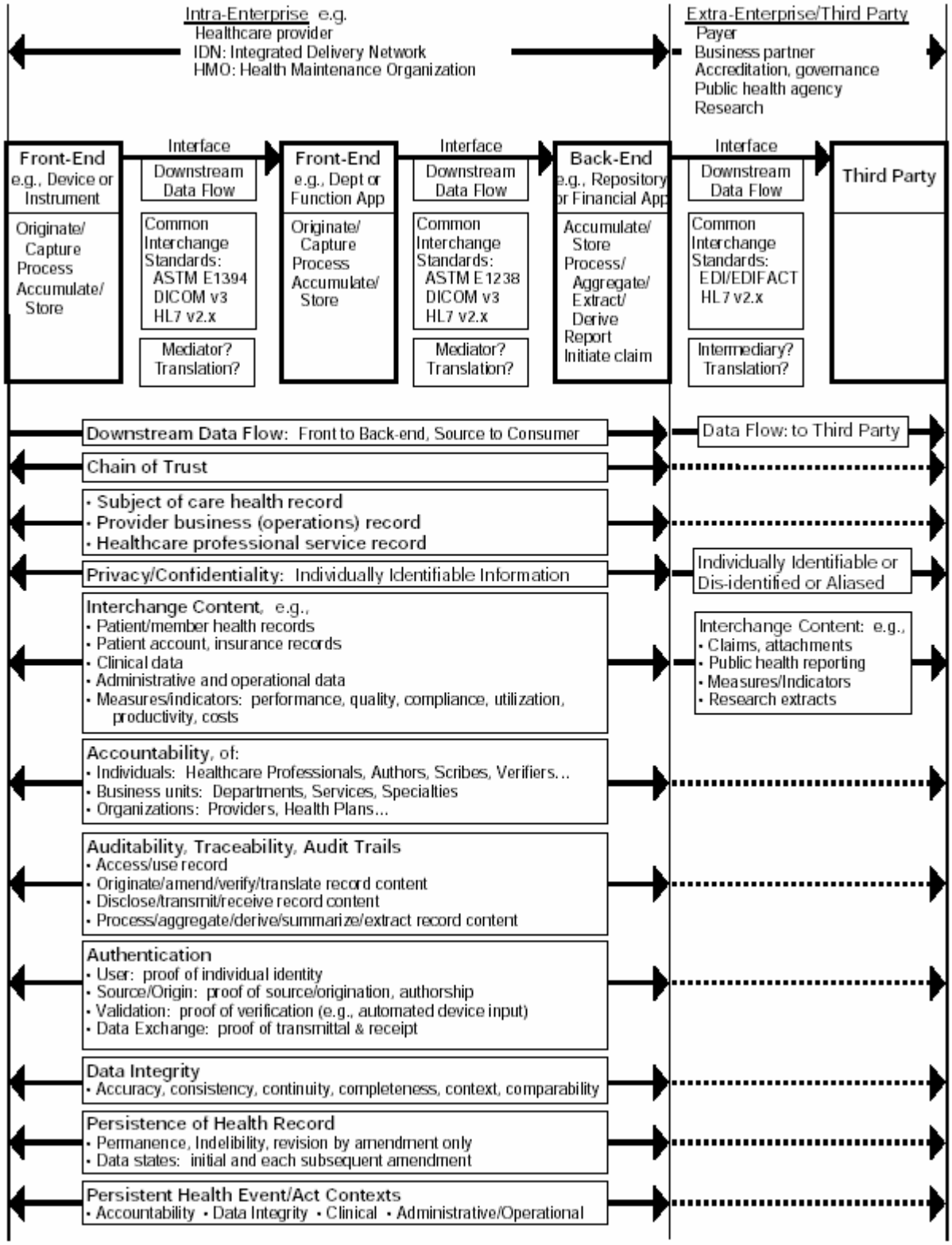
8. Glossary Of Terms Related To Information Security In Healthcare Information Systems. HL7 Secure Transaction Special Interest Group, Draft, June 1998.

9. Standard Guide for EDI (HL7) Communication Security. Draft Version 0.55.Multipurpose Internet Mail Extensions (MIME) Part One-Five, Request for Comments: 2045, 2046, 2047, 2048, 2049 (Network Working Group), N.Freed, N.Borenstein (2045, 2046, 2049); K.Moore (2047); N.Freed, J.Klensin, J.Postel (2048), November 1996.

8. Terminų ir santraukų žodynai

Santrauka	Aprašymas
HL7	Health Level Seven – medicininių dokumentų standartas
IEEE	The Institute of electrical and Electronics Engineers
SIG	Secure Transactions Special Interest Group – HL7 standarto saugumu besirūpinanti darbo grupė
MIME	The Multipurpose Internet Mail Extension – elektroninio pašto turinio papildymas
ISO	International Organization for Standardization – tarptautinė standartizavimo organizacija.
EDI	Electronic Data Interchange – elektroniniai duomenų apsikeitimai

9. Priedai

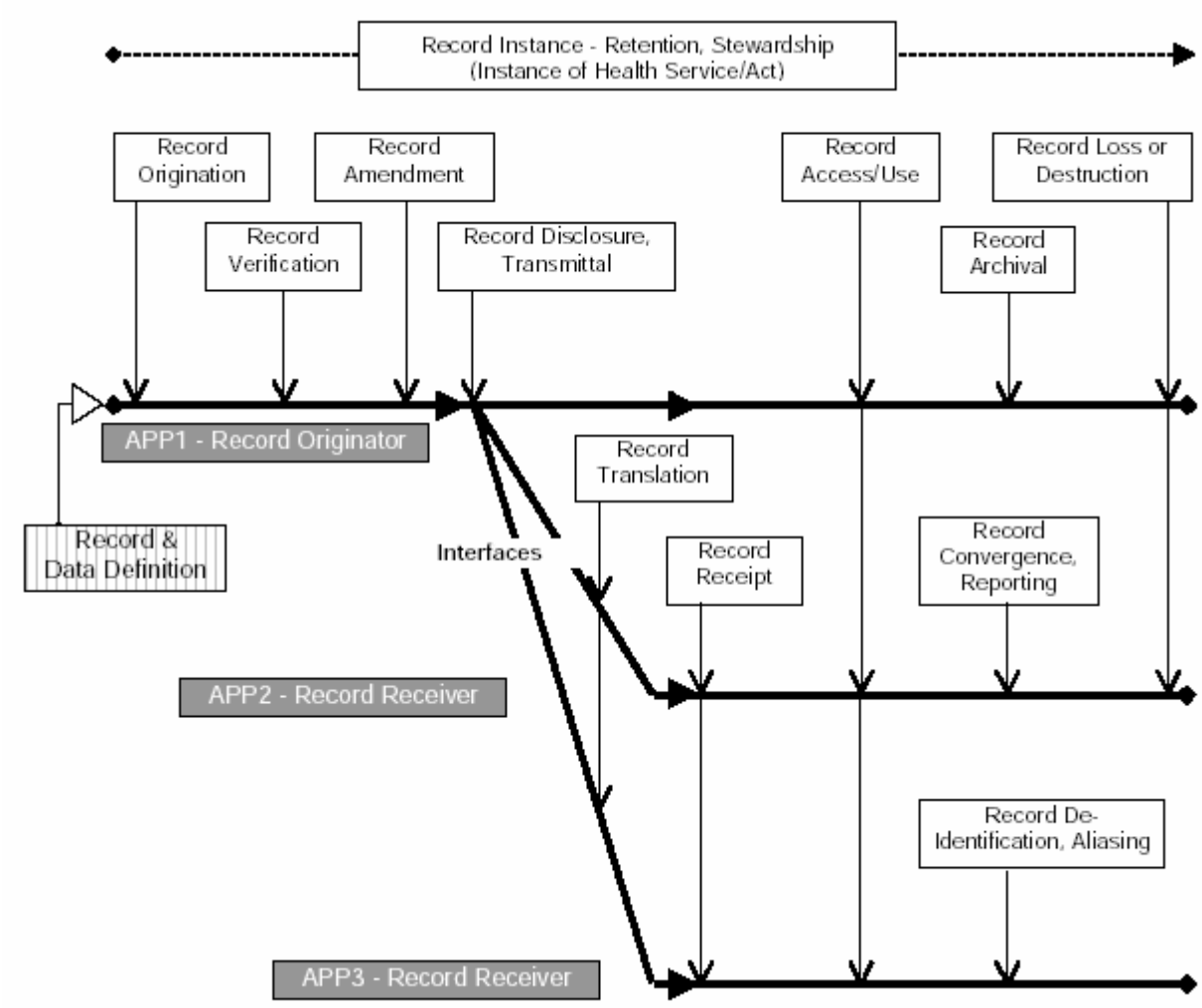


Priedas nr. 1. Tiesioginis informacijos judėjimas

Trust Constituency: for health record content, including individually identifiable information Constituent Party	Individual	Organization	Business Unit	Subject of Record	Accountable Source, Author of Record Content	Accountable Verifier of Record Content	Accountable Scribe/Proxy of Record Content	Accountable User of Record Content	Accountable Record Steward	Accountable Provider of Health Services as Ascribed in Record
Subject of Care, Health Plan Member	X			Yes	Yes	A/A	N/A	A/A	No	No
Next of Kin, Emergency Contact	X			Yes	No	No	No	No	No	No
Healthcare Professional, Caregiver	X			Yes	Yes	Yes	Yes	Yes	Yes	Yes
Care Assistant	X			Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transcriptionist	X			Yes	No	A/A	Yes	A/A	Yes	No
Department, Service, Specialty			X	Yes	N/A	N/A	N/A	Yes	Yes	Yes
Healthcare Provider	X	X		Yes	N/A	N/A	N/A	Yes	Yes	Yes
Integrated Delivery Network (IDN)		X		Yes	N/A	N/A	N/A	Yes	Yes	Yes
Payment Guarantor, Health Plan, HMO	X	X		A/A	No	No	No	Yes	Yes	No
Value Added Network, Claims Clearinghouse		X		No	No	No	No	Yes	Yes	No
Employer	X	X		A/A	No	No	No	Yes	A/A	No
Public Health Agency		X		No	No	No	No	Yes	A/A	No
Regulatory Agency		X		No	No	No	No	Yes	A/A	No
Accreditation Agency		X		No	No	No	No	Yes	A/A	No
Research	X	X		No	No	No	No	Yes	A/A	No
Professional Education	X	X		No	No	No	No	Yes	A/A	No
Others										

N/A = Not applicable A/A = As applicable

Priedas nr. 2. Informacijos prieinamumas tam tikriems subjektams



Priedas nr. 3. Esminiai faktoriai tiesioginiame informacijos judėjime

Probleminės sritys	**HL7 duomenų apsaugos sprendimas**	**BizTalk**
Identifikavimas	Taip	Taip
Vientisumas	Taip	Taip
Veiksmų kontrolė	Taip	Ne*

Priedas nr. 4. Probleminių sričių realizavimas

Pagrindinės duomenų apsaugos užtikrinimo funkcijos	HL7 duomenų apsaugos sprendimas	BizTalk
Elektroniniai vokai	Taip	Taip
Elektroniniai sertifikatai	Taip	Taip
Išeinančios informacijos žymėjimas	Taip	Taip
Išeinančios informacijos šifravimas	Taip	Taip
Informacijos siuntėjo identifikavimas	Taip	Taip
Įeinančios informacijos dešifravimas	Taip	Taip
Informacijos transportavimo apsauga	Taip	Taip

Priedas nr. 5. Pagrindinio duomenų apsaugos funkcionalumo išpildymas

s

Pagrindinis funkcionalumas	Funkcionalumo pasikeitimas	Reikalingi programiniai pakeitimai
Funkcijų reaguojančios į užklausimų įvykius	Taip	Taip
Duomenų atvaizdavimas	Ne	Ne
Informacijos transformaciją į HL7 formatą	Ne	Ne
Informacijos užklausų formavimas	Taip	Taip
Duomenų bazėje esančios informacijos apdorojimas	Ne	Ne

Priedas nr. 6. Buvusios sistemos funkcijų pakeitimai