Tampereen ammattikorkeakoulu

Korkeakoulupalveluiden Peppi-järjestelmän tietokantayhteyden suojaus

Mona Halonen

OPINNÄYTETYÖ
Marraskuu 2023

Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

HALONEN, MONA:
Korkeakoulupalveluiden Peppi-järjestelmän tietokantayhteyden suojaus

Opinnäytetyö 32 sivua
Marraskuu 2023

Opinnäytetyön tavoitteena oli turvata korkeakoulupalveluiden Peppi-järjestelmään liittyvä tietoliikenne kahden eri palvelimen välillä. Tarkoituksena oli salata tietokantapalvelimen ja sovelluspalvelimen välinen tietokantaliikenne nykyaikaisin tekniikoin.

Opinnäytetyössä keskityttiin tarkastelemaan tietoturvaan, salausteknologioihin ja -protokolliin, sekä erilaisiin menetelmiin, joilla voitiin tehokkaasti suojata tietokantayhteys. Tavoitteena oli tarjota kokonaisvaltainen käsitys tietoturvasta ja sen soveltamisesta käytännön tietokantayhteyksissä.

Opinnäytetyössä hyödynnettiin Stunnel-tekniikkaa vahvistamaan tietokantaliikenteen salausta sovelluspalvelimen ja tietokantapalvelimen välillä. Stunnelin avulla pystyttiin luomaan onnistuneesti turvallinen salattu yhteys tietokannan ja sovelluksen välille. Tämä paransi huomattavasti tietoturvaa, vähensi riskiä tietojen luvattomasta pääsystä ja edisti yksityisyyden suojaa tietokantaliikenteessä. Opinnäytetyössä tarkasteltiin yksityiskohtaisesti Stunnelin toimintaa ja sen käyttöä tietokantayhteyden suojaamisessa, tarjoten siten arvokasta tietoa Peppi-järjestelmän tietoturvan parantamiseksi.

Asiasanat: tietoturva, Stunnel, tietokanta, suojaus, Peppi

ABSTRACT

Tampereen Ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunications and Networks

HALONEN, MONA:
Security of the Database Connection for the Peppi System of Higher Education Services

Bachelor's thesis 32 pages
November 2023

The aim of the thesis was to secure the data communication between two different servers in connection with the Peppi system for higher education services. The objective was to encrypt the database traffic between the database server and the application server using modern techniques.

The thesis focused on information security, encryption techniques and protocols, as well as the effective securing of database connections. Its goal was to provide a comprehensive understanding of the security of practical database connections.

Stunnel technology was used to enhance the database encryption between the application server and the database server, significantly improving the data security, reducing the risk of unauthorized access, and promoting privacy protection. The thesis thoroughly investigated the functionality and the role of Stunnel in securing the database connection, offering valuable insights into improving the information security of the Peppi system.

Key words: information security, Stunnel, database, security, Peppi

SISÄLLYS

1 JOHDANTO 6
2 KORKEAKOULUJEN PEPPI-TIETOJÄRJESTELMÄ 8
2.1 Peppi-järjestelmän palvelut 8
2.2 Arkkitehtuurikuvaus 9
2.2.1 MYSQL-tietokanta 10
2.2.2 Apache ServiceMix -palveluväylä 10
3 TIETOTURVA, SALAUSTEKNOLOGIAT JA - PROTOKOLLAT 12
3.1 Tietoturvan kolme ulottuvuutta 12
3.2 Epäsymmetrinen ja symmetrinen salaus 14
3.3 Digitaalinen sertifikaatti 15
3.4 Transport Layer Security -turvallisuusprotokolla 16
3.5 OpenSSL -tietoturvaohjelmisto 18
3.6 Stunnel -välityspalvelin 18
4 SUOJATUN TIETOKANTAYHTEYDEN TOTEUTTAMINEN 20
4.1 Kahden toteutusvaihtoehdon vertailu 20
4.2 Suojauksen toteutus 22
4.2.1 Stunnel client asetukset 24
4.2.2 Stunnel server asetukset 26
5 POHDINTA 28
LÄHTEET 30

LYHENTEET JA TERMIT

CSR	Certificate Signing Request
ESB	Enterprise Service Bus
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IMAP	Internet Message Access Protocol
MySQL	Relaatiotietokantaohjelmisto
OSGi	Open Service Gateway Initiative
PKI	Public Key Infrastructure
POP3	Post Office Protocol
SOA	Palvelukeskeinen Arkkitehtuurikuvaus
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSO	Single sign on
TLS	Transport Layer Security

1 JOHDANTO

Tässä opinnäytetyössä tarkastellaan korkeakoulujen Peppi-järjestelmän tietokantayhteyden suojausta. Korkeakoulupalveluiden Peppi-järjestelmä on edistyksellinen ja monipuolinen tietojärjestelmäratkaisu, joka on suunniteltu vastaamaan koulutusorganisaatioiden tarpeisiin, erityisesti opetuksen ja koulutuksen hallinnassa. Järjestelmä tarjoaa laajan valikoiman ominaisuuksia, jotka helpottavat korkeakoulujen opintojen, opetuksen ja niihin liittyvien digitaalisten palveluiden hallintaa. Peppi-järjestelmä on suunniteltu tarjoamaan käyttäjäystävällisiä työkaluja opintojen suunnitteluun, hallintaan ja tiedonvaihtoon opiskelijoille ja henkilökunnalle. Se edustaa edistynyttä tietojärjestelmäratkaisua, joka tukee koulutusorganisaatioiden päivittäisiä toimintoja. Tässä opinnäytetyössä keskitytään erityisesti tietokantayhteyden suojaukseen, joka on olennainen osa Peppi-järjestelmän tietoturvaa.

Tämän opinnäytetyön tavoitteena on turvata korkeakoulupalveluiden Peppi-järjestelmään liittyvä tietokantaliikenne kahden eri palvelimen välillä. Tarkoituksena on salata tietokantapalvelimen ja sovelluspalvelimen välinen tietokantaliikenne nykyaikaisin tekniikoin. Tietokantayhteyden suojaamisessa on otettava huomioon palvelimien väliset liikenteet ja konfiguraatiot. Opinnäytetyössä tullaan hyödyntämään Stunnel-tekniikkaa tietokantaliikenteen salaamisessa sovelluspalvelimen ja tietokantapalvelimen välillä. Työssä syvennytään myös tietoturvaan ja tutkitaan erilaisia menetelmiä tietokantayhteyden suojaamiseksi. Lopullisena tarkoituksena on toteuttaa toimiva tietokantayhteyden suojaus Peppi-järjestelmään Netum Oy:lle. Tässä työssä tullaan esittämään yksityiskohtaisesti, miten suojaus toteutetaan Stunnel-tekniikan avulla.

Opinnäytetyö on toteutettu toimeksiantona Netum Oy:lle, joka on suomalainen IT-palvelutalo, jolla on yli 20 vuoden kokemus alalta. Netum tarjoaa laajan valikoiman IT-palveluita mukaan lukien digi-, järjestelmien jatkuvuus-, integraatio-, kyber- sekä johdon konsultointipalveluita (Netum Oy n.d.) Opinnäytetyö on toteutettu järjestelmien jatkuvuuspalveluiden tiimissä Netumilla. Tämä tiimi vastaa monipuolisesti mm. Peppi-järjestelmän käyttöönotosta, ylläpidosta ja kehitykseen

liittyvistä palveluista. Peppi-järjestelmä on merkittävä osa korkeakoulujen hallintoa ja opiskelijatietojärjestelmää ja sen sujuva toiminta on olennaista oppilaitosten päivittäisessä toiminnassa. Opinnäytetyön päämääränä on vahvistaa Peppi-järjestelmän tietoturvaa ja taata sen luotettava toiminta suojatussa ympäristössä.

2 KORKEAKOULUJEN PEPPI-TIETOJÄRJESTELMÄ

Korkeakoulujen Peppi-tietojärjestelmä on suunniteltu tukemaan koulutusorganisaatioiden tarpeita. Tämä edistynyt tietojärjestelmä tarjoaa monipuolisen valikoiman ominaisuuksia, jotka helpottavat korkeakoulujen opintojen, opetuksen ja niihin liittyvien digitaalisten palveluiden hallintaa. Tässä kappaleessa tarkastellaan lähemmin Korkeakoulujen Peppi-järjestelmää ja tämän arkkitehtuurikuvausta, joka muodostaa sen perustan ja mahdollistaa sen monipuolisen toiminnallisuuden. (Peppi-konsortio n.d.)

2.1 Peppi-järjestelmän palvelut

Korkeakoulujen Peppi-tietojärjestelmä on suunniteltu tukemaan koulutusorganisaatioiden opetukseen ja koulutukseen liittyviä toimintoja. Tietojärjestelmä tarjoaa kattavan valikoiman ohjauspalveluja korkeakoulujen opintojen, opetuksen ja niihin liittyvien sähköisten palveluiden tarpeisiin. Peppi on nykyaikainen ratkaisu, joka pyrkii yhdistämään monipuolisen toiminnallisuuden helppokäyttöisyyteen ja saumattomaan käyttökokemukseen. (Peppi-konsortio n.d.)

Tällä hetkellä Peppi on erityisesti suunnattu yliopistoihin ja ammattikorkeakouluihin. Sen tarkoituksena on tehostaa ja helpottaa opetuksen ja opiskelun käytännön järjestelyjä näissä oppilaitoksissa. Järjestelmä mahdollistaa muun muassa opintojen suunnittelun, ilmoittautumisten hallinnan, aikataulutuksen, tenttien järjestämisen ja opintosuoritusten seurannan. Lisäksi Peppi tarjoaa sähköisiä palveluita, jotka tukevat opiskelijoiden ja henkilökunnan arkea, edistäen tehokasta viestintää ja tiedonvaihtoa. (Peppi-konsortio n.d.)

Peppi-järjestelmän avulla korkeakoulut voivat keskittyä oleelliseen eli opetuksen laatuun ja opiskelijoiden tukemiseen, sillä järjestelmä tarjoaa käytännön työkaluja monimutkaisten prosessien helpottamiseen ja virtaviivaistamiseen. (Peppi-konsortio n.d.)

2.2 Arkkitehtuurikuvaus

Peppi-järjestelmän suunnittelussa on otettu huomioon palvelukeskeisen arkkitehtuurin (SOA) periaatteet. Suunnittelussa on huomioitu erityisesti valtiovarainministeriön asettamat vaatimukset järjestelmäarkkitehtuurille. Lisäksi suunnittelussa on hyödynnetty Raketti-hankkeessa määriteltyjä opetussuunnitteluun liittyviä skeemoja ja käsitteitä sekä hyödynnetty Kuali-yhteisön toteuttamia opetussuunnitteluun liittyviä järjestelmämoduuleita. Tällä tavoin Peppi-järjestelmän suunnittelu on vahvasti pohjautunut alan parhaisiin käytäntöihin ja standardoituihin ratkaisuihin, mikä tukee sen toiminnallisuutta ja yhteensopivuutta. (Peppi-konsortio, Arkkitehtuurikuvaus n.d.)

Peppi-arkkitehtuurissa teknologiana on hyödynnetty Javaa ja lisäksi järjestelmässä on käytetty avoimen lähdekoodin palvelinohjelmistoja ja sovelluskehyksiä. Peppi-järjestelmän arkkitehtuuri on rakennettu kolmeen keskeiseen moduuliin: käyttöliittymäkerrokseen, palvelukerrokseen ja tietokantakerrokseen (kuvio 1). Tämä järjestely mahdollistaa selkeän toiminnallisen erottelun eri osien välillä ja auttaa järjestelmän tehokkaassa hallinnassa ja ylläpidossa. (Peppi-konsortio, Arkkitehtuurikuvaus n.d.)

KUVIO 1. Pepin arkkitehtuuri (Peppi-konsortio, Arkkitehtuurikuvaus n.d).

2.2.1 MYSQL-tietokanta

Tietokannat ovat olennainen ja keskeinen osa nykyaikaista tietojenkäsittelyä. Ne tarjoavat tehokkaan väylän tietojen tallentamiseen, hallintaan ja hakemiseen (Ohjelmointiputka 2009). Yksi merkittävimmistä ja suosituimmista avoimen lähdekoodin tietokantahallintajärjestelmistä on MySQL. Se on luotettava ja skaalautuva ratkaisu tietojen tallentamiseen ja käsittelyyn. Se tarjoaa käyttäjilleen monipuolisen valikoiman toiminnallisuuksia (Oracle 2023).

MySQL:n toiminta perustuu SQL-kieleen, joka mahdollistaa monenlaiset tietokantatoiminnot. SQL:n avulla voimme suorittaa tietojen lisäämistä, muokkaamista, poistamista ja monimutkaisia hakuoperaatioita tietokannassa. (Inshal 2023.) MySQL nähdään arvokkaana resurssina monilla eri sovellusalueilla. Se tukee monia sovellusalueita, kuten verkkosivustojen taustatietokantaa, liiketoimintasovelluksia ja analytiikkaa. (Laaksonen 2020.)

MySQL on tunnettu nopeudestaan ja luotettavuudestaan suurissakin dataympäristöissä. Se kykenee käsittelemään suuria määriä tietoa tehokkaasti, mikä tekee siitä suositun valinnan yrityksissä ja organisaatioissa, jotka tarvitsevat vankkaa ja suorituskykyistä tietokantaratkaisua. (Oracle 2023.)

2.2.2 Apache ServiceMix -palveluväylä

Apache ServiceMix on avoimen lähdekoodin palveluväylä (ESB), joka yhdistää palvelukeskeisen arkkitehtuurin (SOA) periaatteet toiminnallisuuden lisäksi mahdollisuuden muuntaa ja sovittaa erilaisia komponentteja yhteen. Tämä tarkoittaa käytännössä sitä, että ServiceMix mahdollistaa tehokkaan tapahtumien ja tietojen liikkumisen eri sovellusten ja järjestelmien välillä samalla kun se tarjoaa kyvyn muokata ja sovittaa tietoja tarvittavaan muotoon. Hyödyntämällä tätä palveluväylää, voidaan saavuttaa tehokas sovellusten integrointi ja vähentää riippuvuuksia eri osien välillä. (ServiceMix n.d.)

Apache ServiceMix perustuu Apache Karaf -alustaan, joka on kompakti OSGi-pohjainen käyttöympäristö. Karaf mahdollistaa erilaisten komponenttien ja sovellusten asentamisen ja hallinnan kevyessä kontissa. Tämä rakennelma tekee ServiceMixistä joustavan ja skaalautuvan alustan palvelukeskeisen arkkitehtuurin toteuttamiseen, sekä erilaisten järjestelmäkomponenttien saumattomaan yhteistoimintaan. (ServiceMix n.d.)

3 TIETOTURVA, SALAUSTEKNOLOGIAT JA - PROTOKOLLAT

Tietoturva on moniulotteinen käsite, joka muodostuu useista tärkeistä komponenteista. Sen ytimessä ovat kolme keskeistä ulottuvuutta: eheys, luottamuksellisuus ja käytettävyys. Tämä tarkoittaa, että tietojen on oltava vain oikeutettujen käyttäjien saatavilla, niitä ei saa muuttaa luvattomasti ja ne tulee olla käytettävissä tarvittaessa. Tietoturvan varmistamiseksi on kehitetty monia teknologioita ja menetelmiä. Näiden teknologioiden ja menetelmien yhteistyö mahdollistaa vahvan tietoturvan varmistamisen, suojaten arkaluontoista tietoa ja edistäen luottamusta digitaalisessa maailmassa.

3.1 Tietoturvan kolme ulottuvuutta

Tietoturva koostuu kolmesta keskeisestä ulottuvuudesta (kuvio 2), jotka yhdessä muodostavat kokonaisvaltaisen lähestymistavan tietojen suojaamiseen.

KUVIO 2. Tietoturvan kolme ulottuvuutta (University Of Toronto n.d).

1. **Eheys (Integrity):** Eheydellä tarkoitetaan sitä, että tietojen tulee säilyä muuttumattomina. Eheyteen liittyy kolme lisäominaisuutta, jotka koskevat tiedon tilaa. Nämä ominaisuudet ovat alkuperäisyys, koskemattomuus ja kiistämättömyys. Yksinkertaisesti sanottuna tämä tarkoittaa, että ensinnäkin on varmistettava, että tieto on lähtöisin oikeasta lähteestä. Toiseksi on taattava, ettei tietoa ole muutettu matkalla ja kolmanneksi on vahvistettava, että tieto vastaa sitä, mitä uskomme sen olevan. Eheyden ylläpitäminen on siis ensiarvoisen tärkeää tiedon luotettavuuden ja aitouden varmistamiseksi. (Rautiainen 2013.)

2. **Luottamuksellisuus (Confidentiality):** Luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat käytettävissä vain niille henkilöille ja organisaatioille, joilla on siihen oikeus, eikä niitä paljasteta ulkopuolisille. Mikäli tieto päätyy vääriin käsiin tai oikeudettomille tahoille, sen luottamuksellisuus on menetetty. Tämä tarkoittaa, että tietojen salaus ja rajoitettu pääsy ovat tärkeitä toimenpiteitä sen varmistamiseksi, että tiedot ovat turvassa ja vain valtuutettujen osapuolten käytettävissä. (Rautiainen 2013.)

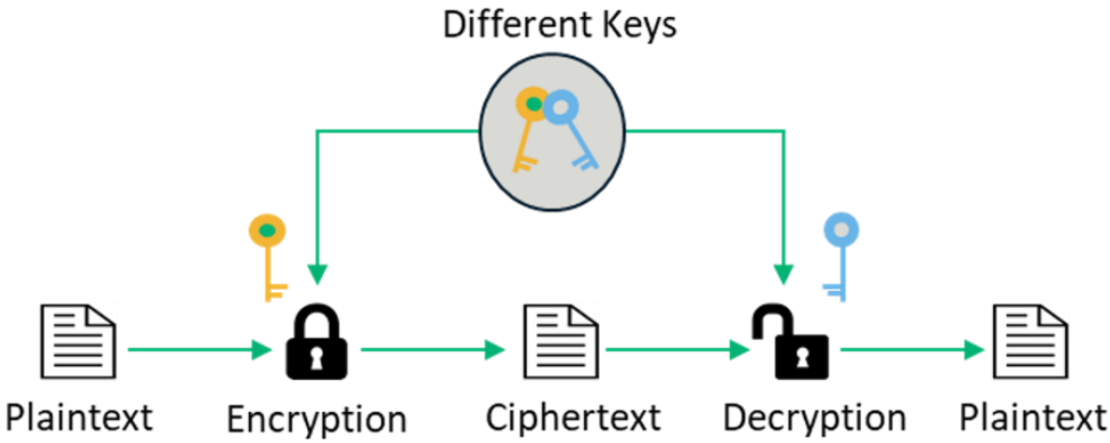
3. **Käytettävyys (Availability):** Käytettävyydellä tarkoitetaan sitä, että tiedot ja niihin liittyvät palvelut ovat käytettävissä niille tahoille, joilla on siihen oikeus ja ne ovat saavutettavissa oikeaan aikaan. Tämä tarkoittaa, että järjestelmien ja palveluiden tulee toimia moitteettomasti ja olla tarvittaessa saatavilla, jotta tietoa voidaan käyttää tehokkaasti ilman keskeytyksiä tai viivytyksiä. (Rautiainen 2013.)

Nämä kolme ulottuvuutta: eheys, luotettavuus ja käytettävyys – muodostavat perustan kokonaisvaltaiselle tietoturvalle. Jokaisen ulottuvuuden vahvistaminen auttaa suojaamaan tietoja ja tietojärjestelmiä laajemmin erilaisilta uhilta ja riskeiltä.

3.2 Epäsymmetrinen ja symmetrinen salaus

Epäsymmetrinen ja symmetrinen salaus ovat tärkeitä käsitteitä kryptografiassa. Salausprosessissa muutetaan selkeä teksti salatuksi viestiksi luottamuksellisuuden varmistamiseksi. Tämä menetelmä on ollut ratkaiseva tekijä Internetin tiedonsiirrossa tietojen suojaamiseksi. (Website Rating n.d.)

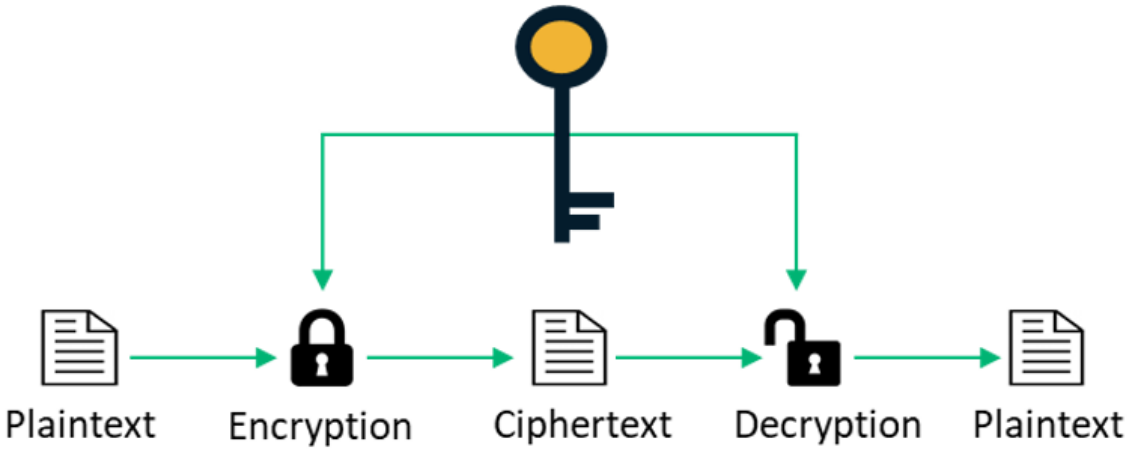
Epäsymmetrinen salaus: tunnetaan myös toisella nimellä julkisen avaimen salaus. Epäsymmetrinen salaus perustuu kahteen avainpariin julkiseen avaimeen ja yksityiseen avaimeen. Viestin salaamiseen käytetään julkista avainta ja salauksen purkamiseen käytetään yksityistä avainta (kuvio 3). Julkista avainta voidaan jakaa avoimesti, mutta yksityinen avain tulee pitää täysin salassa. (Heinonen n.d.) Epäsymmetrisellä salausmenetelmällä voidaan tarjota korkeamman tason turvallisuutta verrattuna symmetriseen salaukseen.



KUVIO 3. Epäsymmetrinen salaus (SectigoStore.com 2020).

Symmetrinen salaus: tunnetaan myös toisella nimellä yksityinen salaus. Symmetrinen salaus on salaustekniikka, jossa on vain yksi avain ja tätä samaa avainta käytetään sekä viestin salaamisessa että sen purkamisessa (kuvio 4). Tämä avain jaetaan lähettäjän ja vastaanottajan kesken. Molemmilla tulee olla identtiset avaimet, joka mahdollistaa viestin salaamisen ja purkamisen. (Website Rating n.d.) Symmetriset salausalgoritmit voivat toimia lohkosalauksella tai virtasalauksella. Lohkosalauksessa käsitellään tietty määrä bittejä yhtenä lohkona salauksen aikana.

Esimerkiksi AES-salauksessa käytetään 128 bitin lohkokokoa ja siinä on mahdollisuus valita avaimen pituudeksi 128, 192 tai 256 bittiä. (SectigoStore.com 2020.)



KUVIO 4. Symmetrinen salaus (SectigoStore.com 2020).

Symmetrinen salaus on nopeampaa ja yksinkertaisempaa kuin epäsymmetrinen, mutta se edellyttää avaimen turvallista jakamista lähettäjän ja vastaanottajan kesken. Epäsymmetrinen salaus puolestaan ratkaisee tämän haasteen sallimalla julkisen avaimen laajan jakamisen, kun samalla yksityinen avain pysyy salassa. Kummallakin salausmenetelmällä on omat etunsa ja rajoituksensa ja valinta riippuu tilanteen erityisvaatimuksista. Symmetristä salausta käytetään usein suurten datamäärien salaamiseen, kun taas epäsymmetristä salausmenetelmää sovelletaan tyypillisesti turvattuun viestintään kahden osapuolen välillä. (Website Rating n.d.)

3.3 Digitaalinen sertifikaatti

Digitaalinen varmenne on tiedostotyyppi, joka toimii salausavainten linkkinä eri kohteiden välillä, kuten verkkosivustojen, yksilöiden ja organisaatioiden. Tällaiset varmenteet ovat tärkeitä erityisesti silloin, kun tarvitaan julkista luottamusta. Luotettavat varmenteen myöntäjät suorittavat varmennusprosessin, jossa ne vahvistavat, tunnistavat ja yhdistävät nämä kohteet oikeisiin salausavaimiin käyttämällä digitaalisia varmenteita. (Wilson 2020.) Tämä prosessi takaa turvallisen ja luotettavan tietoliikenteen verkossa, mikä on erityisen tärkeää verkkoturvallisuuden kannalta.

Mainittu avainpari sisältää kaksi avainta: julkisen ja yksityisen avaimen. Julkinen avain on osa digitaalista varmennetta, kun taas yksityinen avain säilytetään turvassa. Yksityisen avaimen haltija voi käyttää sitä asiakirjojen allekirjoittamiseen, kun taas julkista avainta voidaan käyttää tarkistamaan näiden allekirjoitusten aitous. Lisäksi kolmannet osapuolet voivat käyttää julkista avainta lähettääkseen salattua tietoa, jota vain yksityisen avaimen omistaja voi purkaa. (Wilson 2020.)

Digitaaliset varmenteet noudattavat yleisesti X.509-standardia. X.509-digitaalinen varmenne sisältää julkisen avaimen, digitaalisen allekirjoituksen, identiteettitietoja varmennettavasta kohteesta ja varmentajan tiedot. (Wilson 2020.)

Kun henkilö, verkkosivusto tai organisaatio haluaa hankkia digitaalisen sertifikaatin, he aloittavat prosessin lähettämällä sertifikaatin allekirjoituspyynnön (CSR). Tämä pyyntö sisältää julkisen avaimen ja tärkeät tiedot, joita tarvitaan varmennuksen vahvistamiseen. Julkisesti tunnustettu varmentaja tarkistaa nämä tiedot ja käyttää omaa väliavaintaan vahvistamaan CSR:n, liittäen sen luotettuun juurivarmenteeseen. Tätä varmennettua sertifikaattia voidaan käyttää moniin eri tarkoituksiin, kuten verkkosivustojen käyttäjien tunnistamiseen, asiakkaiden todentamiseen, ohjelmakoodin allekirjoittamiseen, asiakirjojen sähköiseen allekirjoittamiseen ja muihin sovelluksiin, jotka riippuvat myönnetyn varmenteen käyttötarkoituksesta. (Wilson 2020.) Tämä prosessi auttaa varmistamaan, että digitaalisia tietoja käytetään turvallisesti ja luotettavasti.

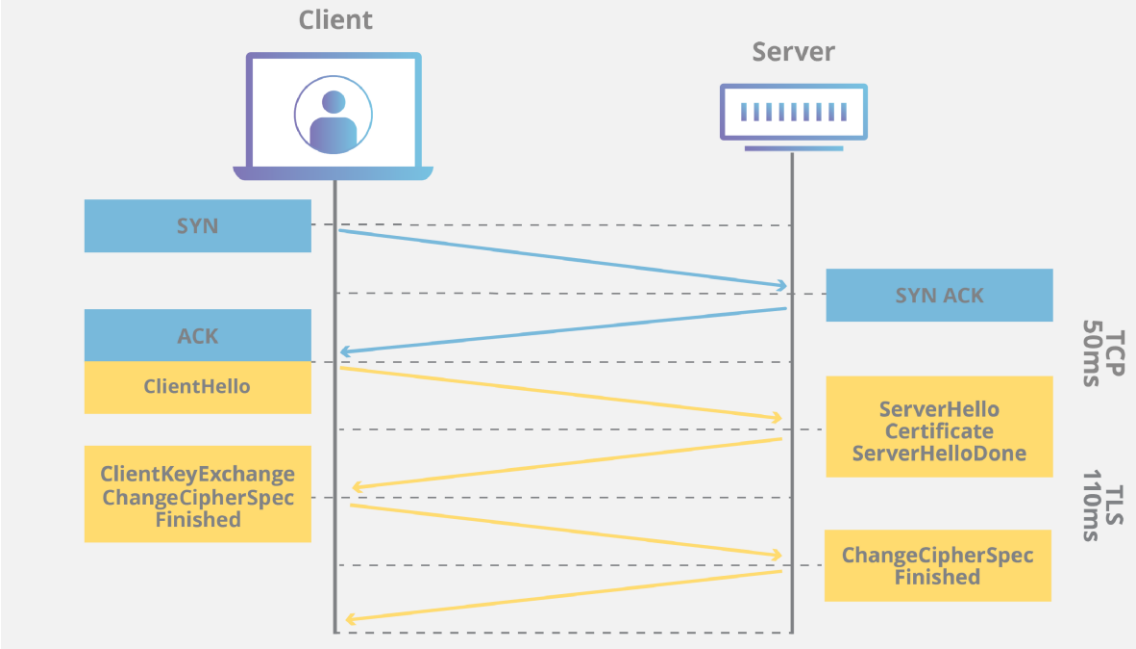
3.4 Transport Layer Security -turvallisuusprotokolla

TLS eli Transport Layer Security on laajasti käytetty turvallisuusprotokolla, jonka tarkoituksena on taata yksityisyys ja tietoturva internetin välityksellä tapahtuvassa viestinnässä. Yksi tärkeimmistä TLS:n käyttötapauksista on viestinnän salaaminen web-sovellusten ja palvelimien välillä esimerkiksi, miten verkkoselaimet lataavat verkkosivuja. (Cloudflare 2023.)

Tietoliikenneturvallisuusprotokolla TLS sisältää kolme keskeistä osaa: salaamisen, autentikoinnin ja eheyden tarkistuksen (Cloudflare 2023). Salaus piilottaa siirrettävän datan kolmansilta osapuolilta, tämä estää ulkopuolisia pääsemästä

käsiksi viestin sisältöön. Autentikointi varmistaa, että viestin lähettäjä ja vastaanottaja ovat todellakin ne henkilöt tai tietokonejärjestelmät, joita he väittävät olevansa. Tämä estää haitallisia hyökkääjiä tekeytymästä toisen osapuolen rooliin ja vähentää identiteettiväärennöksiin liittyviä riskejä. Eheys taas varmistaa, että viestin sisältöä ei ole muutettu tai vahingoitettu siirron aikana. Tällä tavoin voidaan välttää tietojen vääristyminen ja varmistaa, että vastaanotettu tieto on alkuperäisen lähettäjän lähettämää. Yhdessä nämä osat muodostavat TLS-protokollan, joka tarjoaa vahvaa suojaa tietoliikenteelle internetissä. TLS:n avulla verkkoselaimet, palvelimet ja muut tietokonejärjestelmät voivat luottaa siihen, että niiden väliset tiedonsiirrot ovat turvallisia ja luottamuksellisia. (Cloudflare 2023.)

TLS-yhteys aloitetaan sekvenssillä, jota kutsutaan TLS-kädenpuristukseksi. Kun käyttäjä siirtyy TLS-salausta käyttävälle verkkosivustolle, alkaa TLS-yhteys käyttäjän laitteen ja web-palvelimen välillä TLS-kädenpuristuksella (kuvio 5).



KUVIO 5. TLS-kädenpuristus (Cloudflare 2023).

TLS-kädenpuristuksen aikana luodaan jokaiselle viestinnän istunnolle oma salausjoukko. Joukko algoritmeja määrittää yksityiskohdat siitä, mitä jaettuja salausavaimia eli istuntokohteita käytetään kyseisessä istunnossa. TLS pystyy luomaan nämä istuntokohteet salaamattoman kanavan yli käyttämällä julkisen avaimen salaustekniikkaa.

TLS-kädenpuristuksen yksi tärkeimmistä tehtävistä on varmistaa tiedon aitous ja osapuolten todentaminen. Tämä toteutetaan käyttämällä julkisia avaimia. Julkiset avaimet käyttävät yksisuuntaista salakirjoitusta. Tämä tarkoittaa sitä, että kuka tahansa, jolla on pääsy julkiseen avaimen, voi käyttää sitä viestin purkamiseen, joka on salattu palvelimen yksityisellä avaimella. Tämä auttaa varmistamaan viestin alkuperäisyyden. Mutta vain se, joka omistaa yksityisen avaimen, pystyy salaamaan viestin tällä tavalla. Palvelimen julkinen avain, joka on osa sen TLS-varmennetta, toimii olennaisena osana turvallista viestintää verkossa. Kun data on salattu ja sen alkuperä on varmistettu, siihen lisätään viestin todennuskoodi (MAC). Vastaanottaja voi käyttää tätä koodia tarkistaakseen datan eheyden ja varmistaa ettei se ole matkalla muuttunut tai vioittunut. (Cloudflare 2023.)

3.5 OpenSSL -tietoturvaohjelmisto

OpenSSL on avoimen lähdekoodin tietoturvaohjelmisto, joka on suunniteltu tarjoamaan monipuolisia työkaluja ja kirjastoja tietojen salaamiseen, varmenteiden hallintaan ja yleisesti tietoturvan parantamiseen. Se sisältää kattavan valikoiman salausalgoritmeja, tietoturvatoimintoja ja protokollien toteutuksia, kuten SSL ja sen seuraaja TLS, jotka tarjoavat suojatun tiedonsiirron internetissä. (Techradar Pro. 2023.)

OpenSSL:n avulla voidaan luoda ja hallita salattuja yhteyksiä, digitaalisia allekirjoituksia ja varmenteita (SSL Dragon 2023). Lisäksi OpenSSL tarjoaa myös tukea monille erilaisille salaustekniikoille ja protokollille, joiden avulla voit mukauttaa tietoturvan tarpeidesi mukaan.

3.6 Stunnel -välityspalvelin

Tietoturvan kannalta erittäin tärkeä avoimen lähdekoodin Stunnel on monikäyttöinen välityspalvelin, joka tarjoaa TLS-salausominaisuuden asiakas- ja palvelinohjelmille ilman, että niiden koodia tarvitsee muuttaa. Stunnelin käyttämä OpenSSL-kirjasto mahdollistaa kaikkien OpenSSL-kirjastossa saatavilla olevien

salausalgoritmien käytön. Tämä takaa, että SSL-yhteydet ovat turvallisia ja luottamuksellisia. Yhteyden turvaamiseksi käytetään julkisen avaimen kryptografiaa, joka varmennetaan digitaalisilla x509-sertifikaateilla. Myös asiakkaat voidaan todentaa varmenteiden avulla. (Stunnel.org n.d.)

Stunnelin vahva ominaisuus on sen kyky luoda tietoja, joita hyökkääjä ei voi purkaa tai ymmärtää. Tämän ansiosta sillä voidaan luoda salattuja tunneliyhteyksiä tietyille sovelluksille, mikä tekee siitä erinomaisen vaihtoehdon tietoturvan parantamiseksi. Salausavaimet tallennetaan paikallisesti sekä client-palvelimelle että server-palvelimelle. (GeeksforGeeks 2022.)

Kun kahden päätepisteen välille tarvitaan viestintää, Stunnel muodostaa yhteyden palvelimeen, vastaanottaa avaintiedot palvelimelta ja luo sitten salatun tunnelin salatun TCP/IP-yhteyden yli. Kun tunnelin luominen on valmis, Stunnel vapauttaa TCP/IP-tunnistetiedot ja lopettaa toimintansa. (GeeksforGeeks 2022.)

Stunnel on toteutus SSL- ja TLS-protokollista, mikä mahdollistaa loppuun asti salatun viestinnän, tietojen eheyden ja autentikoinnin kahden viestivän sovelluksen tai kahden tietokoneen välillä. Stunnelia voidaan hyödyntää monien eri protokollien, kuten FTP, IMAP, POP3, telnet ja HTTP salauksessa. Lisäksi se tarjoaa joustavat vaihtoehdot asiakkaan todentamiseen palvelimelle asiakasvarmenteiden tai todennusagentin avulla yksittäisen kirjautumisen kautta (SSO). Stunnelia voidaan myös hyödyntää tarjoamalla salattu kerros verkkoliikenteelle, joka ei vaadi palvelimen todentamista. (GeeksforGeeks 2022.)

4 SUOJATUN TIETOKANTAYHTEYDEN TOTEUTTAMINEN

Tässä luvussa keskitymme tietokantasuojauksen kahden toteutusvaihtoehdon vertailuun sekä tietokantayhteyden suojaamiseen. Suojauksen toteutusvaihtoehtojen vertailu on ensisijaisen tärkeä vaihe ja erityisesti Peppi-järjestelmän kaltaisissa ympäristöissä se on kriittinen varmistettaessa, että herkät tiedot ja järjestelmän tietoturva ovat asianmukaisesti suojattuja. Tässä yhteydessä vertailemme kahta erilaista suojauksen lähestymistapaa, TLS ja Stunnel ja arvioimme niiden soveltuvuutta Peppi-järjestelmän tietokantayhteyden suojaamiseen.

4.1 Kahden toteutusvaihtoehdon vertailu

Tietokantasuojauksen valinta on kriittinen askel organisaation tietoturvassa ja tässä yhteydessä on tärkeää vertailla eri toteutusvaihtoehtoja perusteellisesti. Tässä kappaleessa tarkastelemme tietokantasuojauksen kahden päävaihtoehdon TLS:n ja Stunnelin ominaisuuksia ja vertailemme niitä toisiinsa. Alla olevassa taulukossa (taulukko 1) esitämme keskeiset vertailupisteet, jotka auttavat ymmärtämään näiden kahden menetelmän vahvuudet ja heikkoudet tietokantasuojauksessa.

TAULUKKO 1. TLS:n ja Stunnelin ominaisuuksien vertailua.

Ominaisuus	TLS	Stunnel
Tietoturva	TLS on laajasti käytetty tietoturvaprotokolla, joka tarjoaa vahvan salaustason, varmentamisen ja tiedon eheyden tarkistuksen.	Stunnel pystyy tarjoamaan vahvan salaustason. Konfiguraatioiden kanssa tulee olla huolellinen.
Helppokäyttöisyys	TLS on tunnettu, mutta voi vaatia enemmän integraatiota sovelluksiin, sekä käyttöönotto voi olla monimutkaisempaa.	Stunnel toimii välikätenä ja vähentää integraation tarvetta, mikä voi nopeuttaa käyttöönottoa.
Yhteensopivuus	TLS on laajasti tuettu tietoturvaprotokolla, mutta integraatiotarpeet voivat vaihdella eri järjestelmissä.	Stunnel on yhteensopiva monien tietokantaohjelmistojen kanssa ja joustava eri ympäristöissä.

Tietoturva: Molemmat ratkaisut tarjoavat vahvan salaustason tietokantayhteyksille. TLS on laajasti tunnustettu ja hyväksytty tietoturvaprotokolla, joka mahdollistaa tietoliikenteen salaamisen, varmentamisen ja tiedon eheyden tarkistamisen. Stunnel pystyy myös tarjoamaan saman tietoturvatason, kun se on huolellisesti konfiguroitu. Tässä mielessä molemmat vaihtoehdot voivat tarjota korkean tietoturvatason tietokantayhteyksille.

Helppokäyttöisyys: TLS voi vaatia enemmän aikaa ja resursseja integraatioon sovellusten kanssa. Stunnel toimii usein yksinkertaisena välikätenä tietokannan ja sovelluksen välillä, mikä vähentää integraation tarvetta. Tämä voi nopeuttaa käyttöönottoa, erityisesti tilanteissa, joissa nopea tietokantasuojaus on tarpeen.

Yhteensopivuus: Vaikka TLS on laajalti tuettu tietoturvaprotokolla, sen integraatiotarpeet voivat vaihdella eri tietokantajärjestelmissä. Stunnel on joustava ja yh-

teensopiva monien erilaisten tietokantaohjelmistojen kanssa. Tämä tekee Stunnelista varteenotettavan vaihtoehdon organisaatioille, joilla on monenlaisia tietokantajärjestelmiä.

Kun vertailimme TLS:ää ja Stunnelia tietokantasuojauksen näkökulmasta huomasimme, että kummallakin näistä tietoturvaratkaisuista on omat vahvuutensa. Aluksi päätimme suosia TLS-tekniikkaa sen laajan tunnettavuuden ja sen tarjoaman vahva tietoturvatason takia. Kuitenkin, kun ryhdyimme toteuttamaan TLS:ää, aloimme ymmärtää sen haasteellisuuden ja monimutkaisuuden paremmin. Tarkemman perehtymisen myötä huomasimme, että sen käyttöönotto oli odotettua vaativampaa. TLS:n toteuttamiseen liittyi monia Peppi-järjestelmän konfiguraatioihin ja asetuksiin liittyviä haasteita. Lisäksi sen integroiminen tietokannan ja sovelluksen väliin osoittautui teknisesti haastavaksi tehtäväksi, joka olisi vaatinut syvää osaamista ja resursseja. Useista yrityksistä huolimatta, emme onnistunut saamaan TLS:ää toimimaan haluamallamme tavalla, joten tämä johti päätökseen vaihtaa toteutustapa Stunneliin.

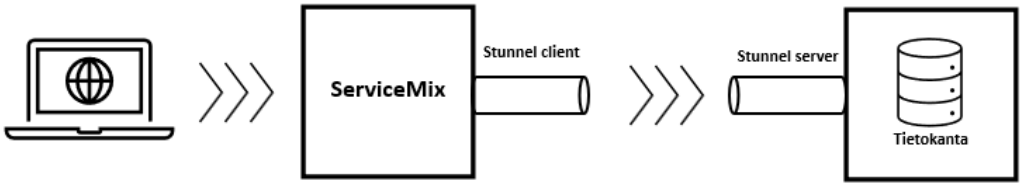
Stunnelin valintaan vaikutti myös ensisijaisesti sen kyky tarjota vahva tietoturvataso. Mikä tarkoittaa, että voimme varmistaa tietokantayhteyksiemme suojauksen ja luottamuksellisuuden Stunnelin avulla myös ilman, että joudumme tekemään kompromisseja tietoturvan suhteen. Lisäksi Stunnelin helppokäyttöisyys oli merkittävä tekijä päätöksessämme tässä kohtaa. Stunnel toimii usein yksinkertaisena välikätenä tietokannan ja sovelluksen välillä, mikä vähentää tarvetta monimutkaisille integraatioille ja mahdollistaa nopeamman käyttöönoton.

Kun tarkastelemme koko prosessia ja siihen liittyvää päätöstä vaihtaa toteutustapaa kesken kaiken Stunneliksi koimme tämän kuitenkin oikeaksi ratkaisuksi. Se vastasi tässä tapauksessa parhaiten tarpeisiin, osoittautui tehokkaaksi ja auttoi varmistamaan vahvan tietoturvan tietokantasuojauksessa.

4.2 Suojauksen toteutus

Alla oleva kuvio (kuvio 6) havainnollistaa Stunnelin roolia tietokantasuojauksessa ja sen käyttöä tietoturvakerroksen luomiseen tietokannan ja sovelluksen välille.

Kuviosta voidaan nähdä, miten Stunnel toimii välikätenä, joka luo salatun yhteyden tietokantapalvelimen ja sovelluspalvelimen välille. Tämä lisää tietoturvaa, estäen mahdollisia tietoturvaongelmia ja suojaamalla tietokantatietoja.



KUVIO 6. Suunnitelma Stunnelin toteutuksesta.

Tässä on yksityiskohtainen kuvaus Stunnelin toteuttamisesta tietokantasuojauksessa:

1. **Asennus ja konfigurointi:** Ensimmäinen vaihe on asentaa Stunnel-palvelin molempiin päätepisteisiin, joita halutaan suojata, eli tietokantapalvelimeen ja sovelluspalvelimeen. Tämä voidaan tehdä useilla eri käyttöjärjestelmillä, kuten Linuxilla tai Windowsilla, käyttäen yleensä paketinhallintaa tai suoraan lähdekoodista.

2. **Sertifikaattien ja avainten luominen:** SSL/TLS-salausta varten tarvitaan yleensä julkisia ja yksityisiä avaimia sekä sertifikaatteja. Nämä voidaan joko hankkia luotettavalta sertifikaattiviranomaiselta tai luoda itse allekirjoitetut sertifikaatit testiympäristöä varten. Avainten ja sertifikaattien tulee olla huolellisesti suojattuja, koska ne ovat kriittisiä tietoturvan kannalta.

3. **Stunnelin asetuksien määrittely:** Stunnelin käyttöönoton jälkeen sinun on määritettävä Stunnelin asetustiedosto, joka kertoo sille, miten se toimii. Stunnelin asetustiedostoon lisätään tarvittavat tiedot, kuten tietokantapalvelimen ja sovelluspalvelimen IP-osoitteet, porttinumerot, sekä polut avaimiin ja sertifikaatteihin. Asetuksissa määritellään myös käytettävä salaustaso ja muita salausta koskevia parametreja.

4. **Stunnelin käynnistäminen:** Kun asetustiedosto on määritelty oikein, voit käynnistää Stunnel-palvelimen kummallakin päätepisteellä. Stunnel luo salatun yhteyden tietokantapalvelimen ja sovelluspalvelimen välille, toimien niiden välikätenä.

5. **Testaus ja valvonta:** Kun Stunnel on käynnissä, on tärkeää testata yhteyden toimivuus huolellisesti.

6. **Valvonta ja ylläpito:** Stunnelin tulee olla jatkuvassa valvonnassa ja ylläpidossa. On tärkeää päivittää Stunnel ja siihen liittyvät komponentit säännöllisesti ja seurata lokitietoja mahdollisten ongelmien tai epäilyttävien tapahtumien varalta.

Stunnelin käyttö tietokantasuojaustarkoituksessa on tehokas ja luotettava tapa suojata tietokantayhteyksiä salauksen avulla. Se tarjoaa vahvan tietoturvaratkaisun, joka voidaan helposti integroida olemassa oleviin järjestelmiin ilman merkittäviä muutoksia. Tietokantasuojausta varten Stunnel luo salatun yhteyden ja toimii välikätenä tietokannan ja sovelluksen välillä, mikä parantaa tietoturvaa ilman monimutkaista konfigurointia.

4.2.1 Stunnel client asetukset

Stunnel client konfiguraatioissa (taulukko 2) on kyse PKI-asiakkaalle (Public Key Infrastructure) suunnatusta asetuksesta, joka on tarkoitettu turvallisen tiedonsiirron mahdollistamiseen. PKI on yleinen menetelmä julkisten ja yksityisten avainten hallintaan ja sitä käytetään laajalti SSL/TLS-salaustekniikan kanssa.

TAULUKKO 2. Stunnel client konfiguraatiot (Stunnel.org n.d.)

[PKI client]
client = yes
accept = 0.0.0.0:<src_port>
connect = <server_host>:<server_port>
verifyChain = yes
CAfile = ca-certs.pem
cert = cert.pem
key = key.pem
checkHost = <server_host>

Stunnel client -asetukset:

- **Client:** Stunnel toimii tässä konfiguraatiossa client -roolissa, kun konfiguraatioissa on määritetty client = yes. Tämä tarkoittaa, että se yrittää muodostaa yhteyden palvelimeen.
- **Accept:** Tämä asetus määrittelee Stunnelille hyväksyttävän lähtöportin <src_post> ja IP-osoitteen yhdistelmän, jolta Stunnel hyväksyy saapuvan liikenteen. Tämä tarkoittaa, että stunnel hyväksyy liikenteen vain tietyltä IP-osoitteelta ja tietystä lähtöportista.
- **Connect:** Tämä asetus määrittelee kohdepalvelimen tiedot, johon Stunnel muodostaa salatun yhteyden. <Server_host> korvataan kohdepalvelimen osoitteella ja <server_port> kohdepalvelimen portilla.
- **VerifyChain:** Kun tämä määritys on määritetty ”yes”. Stunnelille tarkistaa, että palvelimen käyttämä sertifikaatti on oikeutettu ja voimassa oleva, koska se voidaan jäljittää takaisin luotettavaan Certificate Authority (CA) -tahoon.
- **CAfile:** Tämä määrittää tiedoston, joka sisältää CA-sertifikaatit. Stunnel käyttää näitä sertifikaatteja tarkistamaan kohdepalvelimen sertifikaatin aitouden.
- **Cert:** Tämä asetus määrittää asiakkaan omaan sertifikaattiin liittyvän tiedoston, joka on tarpeen SSL/TLS-yhteyden muodostamiseksi kohdepalvelimen kanssa.

- **Key:** Tämä määritys kertoo, mistä se löytää asiakkaan yksityisen avaimen tiedoston. Tämä avain liittyy asiakkaan sertifikaattiin ja on välttämätön salatun yhteyden muodostamiseksi.
- **CheckHost:** Tämä asetus määrittää tarkistettavan kohdepalvelimen nimen. Stunnel käyttää tätä asetusta varmistaakseen, että kohdepalvelimen nimi vastaa odotettua nimeä.

4.2.2 Stunnel server asetukset

Stunnel server (taulukko 3) konfiguraatio on suunniteltu palvelimelle, joka perustuu sertifikaattipohjaiseen varmennukseen ja käyttää asiakassertifikaatteja tunnistamiseen.

TAULUKKO 3. Stunnel server konfiguraatiot (Stunnel.org n.d.)

[certificate-based server]
accept = <server_port> connect = <dst_port> cert = cert.pem key = key.pem CAfile = ca.pem verify = 2

Stunnel Server -asetukset:

- **Accept:** Tämä asetus määrittää palvelimen portin, jota käytetään kuuntelemaan saapuvia yhteyksiä.
- **Connect:** Tämä asetus määrittelee kohteen portin, johon Stunnel ohjaa saapuvat yhteydet. <dst_port> korvataan kohdeportin numerolla.
- **Cert:** Tämä asetus määrittää palvelimen käyttämän sertifikaattiin liittyvän tiedoston.
- **Key:** Tämä asetus määrittää palvelimen yksityisen avaimen sertifikaatin.
- **CAfile:** Tämä määrittää tiedoston, joka sisältää luotettavien Certificate Authority (CA) -sertifikaattien tiedot. Stunnel käyttää tätä tiedostoa tarkistaakseen saapuvien asiakkaiden sertifikaattien aitouden.

- **Verify:** Tämä asetus määrittää varmistustason. Arvo 2 tarkoittaa, että Stunnel vaatii asiakkaan sertifikaatin ja tarkistaa sen CA:n avulla. Tämä vahvistaa, että asiakkaalla on kelvollinen sertifikaatti ja että se on allekirjoitettu luotettavan CA:n toimesta ennen yhteyden hyväksymistä.

5 POHDINTA

Tässä projektissa tavoitteeseen pääseminen oli matka täynnä oppimista ja haasteita. Alkuperäinen suunnitelma toteuttaa Peppi-järjestelmän tietokannan suojaus TLS-tekniikalla vaikutti aluksi houkuttelevalta, mutta käytännön toteutuksessa ilmenneet haasteet muuttivat suuntaa. Toteutuksen alkuvaiheessa huomasimme, että TLS-tekniikan käyttö tietokantasuojauksessa oli odotettua monimutkaisempaa. Vaikka TLS tarjoaa vahvan tietoturvakerroksen, sen integroiminen tietokannan ja sovelluksen välille osoittautui teknisesti vaativaksi tehtäväksi. Tämä herätti epäilyksiä siitä, voisimmeko saavuttaa alkuperäisen tavoitteemme ilman, että jouduimme käyttämään kohtuuttomasti aikaa ja resursseja tekniseen konfigurointiin.

Seuraavassa vaiheessa päätimme tarkastella vaihtoehtoja ja Stunnel nousi esiin kiinnostavana vaihtoehtona. Ratkaisevat tekijät päätökseemme olivat Stunnelin helppokäyttöisyys ja se, kuinka se toimii käytännössä näkymättömänä välikätenä tietokannan ja sovelluksen välillä. Tämä vaihtoehto tarjosi meille selkeän polun tietokantasuojauksen toteuttamiseen ilman, että jouduimme käsittelemään TLS:n monimutkaisempia teknisiä yksityiskohtia. Lopulta Stunnel osoittautui hyväksi valinnaksi, jonka avulla saimme saavutettua tavoitteemme sujuvasti ja tehokkaasti. Se tarjosi turvallisen tavan suojata tietokantayhteyden ilman, että jouduimme taistelemaan monimutkaisten teknisten konfiguraatioiden kanssa. Tämä kokemus opetti, että tavoitteiden saavuttamiseen ei aina tarvita alkuperäistä suunnitelmaa, vaan joustavuus ja kyky sopeutua muuttuviin olosuhteisiin voivat olla avaimia onnistumiseen.

Kun tietokantasuojaus Stunnelin avulla on nyt onnistuneesti toteutettu, on tärkeää harkita, miten voimme parantaa ja vahvistaa tätä järjestelmää tulevaisuudessa. Yksi keskeinen näkökulma on pitää suojausmekanismit ajan tasalla säännöllisillä päivityksillä ja seuraamalla aktiivisesti Stunnelin kehitystä mahdollisten haavoittuvuuksien ja päivitysten suhteen. Tietoturva-uhkat muuttuvat jatkuvasti, siksi päivitysten ja parannusten seuraaminen on ensisijaisen tärkeää. Lisäksi voimme harkita tarkempaa tietokantasuojausten valvontaa ja seurantaa. Jatkuva

valvonta voi auttaa havaitsemaan epäilyttäviä toimintoja tai turvallisuus-poikkeamia ajoissa, mikä puolestaan voi auttaa ennaltaehkäisemään mahdollisia tietoturvaongelmia. Toinen askel voisi olla tietoturva-auditointi, joka arvioi koko järjestelmän haavoittuvuudet ja heikkoudet. Tällainen auditointi voi tarjota syvällisen katsauksen tietoturvakäytäntöihin ja auttaa tunnistamaan alueet, joilla voidaan tehdä parannuksia.

Kokonaisuudessaan tietoturvasta huolehtiminen on jatkuva prosessi, vaikka Stunnel tietokantasuojaus on nyt paikallaan, tulee jatkuvasti arvioida, miten voimme parantaa ja vahvistaa järjestelmän tietoturvaa tulevaisuudessa.

LÄHTEET

Cloudflare. 2023. What is TLS (Transport Layer Security)? Verkkosivu. Viitattu 17.7.2023
https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

GeeksforGeeks.2022.What is stunnel? Verkkosivu. Viitatettu 17.7.2023
https://www.geeksforgeeks.org/what-is-stunnel-tool/

Heinonen, P. n.d. Tiedonsalaaminen. Verkkosivu. Viitattu 16.8.2023.
https://appro.mit.jyu.fi/doc/tiedonsalaus/

Inshal Ali 2023. Ultimate Guide to MySQL Performance Tuning for Optimal Database Efficiency. Verkkosivu. Viitattu 18.8.2023
https://www.cloudways.com/blog/mysql-performance-tuning/

Laaksonen A. 2020. Tietokantojen perusteet syksy 2020. Verkkokurssi. Viitattu 16.8.2023.
https://tikape.mooc.fi/syksy-2020/content/osa-1/index.html#mik%C3%A4-on-tietokanta?

Netum Oy n.d. Yritys. Verkkosivu. Viitattu 12.7.2023.
https://www.netum.fi/yritys/

Ohjelmointiputka. 2009. MySQL ja PHP: Osa 1 – Johdanto. Verkkosivu. Viitattu 16.8.2023.
https://www.ohjelmointiputka.net/oppaat/opas.php?tunnus=mysqlphp01

Oracle 2023. What is MySQL? Verkkosivu. Viitattu 12.7.2023
https://www.oracle.com/mysql/what-is-mysql/#what-is-mysql

Peppi-konsortio. n.d. Peppi. Verkkosivu. Viitattu 25.05.2023.
https://www.peppi-konsortio.fi/elementor-617/

Peppi-konsortio. n.d. Arkkitehtuurikuvaus. Verkkosivu. Viitattu 12.7.2023. https://www.peppi-konsortio.fi/arkkitehtuurikuvaus/

Rautiainen, J. 2013. Tietoturvan kolme kovaa: Luottamuksellisuus, eheys ja saatavuus. Blogi. Viitattu 11.8.2023 https://juhanit.wordpress.com/2013/08/25/tietoturvallisuuden-kolme-kovaa-luottamuksellisuus-eheys-ja-saatavuus/

SectigoStore.com. 2020. 5 Differences Between Symmetric vs Asymmetric Encryption. Verkosivu. Viitattu 16.8.2023. https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/

ServiceMix. n.d. What is Servicemix 4? Verkkosivu. Viitattu 27.7.2023 https://servicemix.apache.org/docs/6.x/user/what-is-smx4.html

SSL Dragon. 2023. What Is OpenSSL? How Does OpenSSL Work? Verkkosivu. Viitattu 17.7.2023 https://www.ssldragon.com/blog/what-is-openssl/

Stunnel.org. n.d. Verkkosivu. Viitattu 17.7.2023 https://www.stunnel.org/

Techradar Pro. 2023. What is OpenSSL? Verkkosivu. Viitattu 18.8.2023 https://www.techradar.com/vpn/what-is-openssl/

University Of Toronto n.d, IT Professionals. Verkkosivu. Viitattu 11.8.2023 https://securitymatters.utoronto.ca/resources/it-professionals/

Website Rating. n.d. Mikä on epäsymmetrinen ja symmetrinen salaus? Verkkosivu. Viitattu. 16.8.2023 https://www.websiterating.com/fi/vpn/glossary/what-is-asymmetric-symmetric-encryption/

Wilson C. 2020. Mikä on digitaalinen sertifikaatti? Verkkosivu. Viitattu 26.10.2023
https://www.ssl.com/fi/FAQ/mik%C3%A4-on-digitaalinen-sertifikaatti/