Ajas-palvelun tietoturvaseloste

Dokumentti päivitetty 13.3.2024

Sisällysluettelo

Sisällysluettelo 2
Yleistä Ajas-järjestelmästä 2
Ajas-palvelun tekninen toteutus 2
Ajas-palvelun arkkitehtuuri 3
Palvelun suorituskyky 3
Kirjautuminen palveluihin 3
Tietoturva 4
Päivitykset 5
Palvelun valvonta 5
Varmuuskopiointi ja palauttaminen 5
Tietosuoja 6
Lokikäytännöt 6
Usein kysyttyjä kysymyksiä 7

Yleistä Ajas-järjestelmästä

Ajas on asiakkuuksien hallintaan tarkoitettu järjestelmä, jota tuotetaan SaaS-mallilla (Software as a Service). Ajas Oy vastaa palvelun markkinoinnista ja tuottamisesta. Ajas Oy on osa Eneroc Oy -konsernia. Eneroc vastaa ohjelmiston kehittämisestä ja ylläpidosta.

Tässä dokumentissa kuvataan Ajas-palvelun tekninen toteutus ja tietoturvaratkaisuja olennaisilta osin.

Ajas-palvelun tekninen toteutus

Ajas-palvelu on lähtökohtaisesti tavoitettavissa 100% ajasta ympäri vuorokauden, pois lukien ennalta ilmoitettavat huoltokatkokset, joista ilmoitetaan ajas.fi-sivuston teknisissä tiedotteissa sekä Ajas Touch -järjestelmän etusivulla.

Ajas Oy käyttää palvelun tuottamiseen seuraavia alihankkijoita:

- Atostek Oy on A3-luokan järjestelmä, joka toimittaa Kanta-liitynnät
- Upcloud Oy on Ajas-palvelun pääasiallinen konesalitoimittaja.
    - Palvelimet ja asiakastiedot sijaitsevat Suomessa
    - Palvelinsali täyttää seuraavat standardit: VAHTI T3, KATAKRI, ISO 27001, ISO 9001, ISO 14001, OHSAS 18001.

Dokumentti päivitetty 13.3.2024

- Amazon Web Services EMEA SARL
    - Amazon S3 tiedonsiirtopalvelu. Sijainti: Tukholma, Ruotsi.
    - Alihankkijan palvelimelle ladataan tiedostojen binääridata anonymisoituna ja kryptattuna. Kryptausavaimet sekä tiedosto-indeksi (tiedostonimet) säilytetään Upcloud Oy:n palvelimella Suomessa.

Ajas-palvelu on auditoitu KPMG IT:n toimesta ja se on saanut Valviran A1 sertifikaatin.

Ajas-palvelun arkkitehtuuri

Ajas-palvelu on toteutettu pilvipalveluksi. Palvelu on toteutettu pääosin yleisesti tunnettuihin ja käytettyihin Linux-palvelinteknologioihin perustuen, käyttäen voimassa olevia alan suositeltuja toimintatapoja.

Ajas-palvelinarkkitehtuuri on rakennettu skaalatuvaksi ja vikasietoiseksi. Jokainen tuotantoympäristön järjestelmä on fyysisesti vähintään kahdennettu, eli tallennustila, suorittimet, muisti ja verkkoyhteydet ovat useista rinnakkaisista komponenteista koostuvia ja niitä pystytään vaihtamaan katkotta.

Tuotantoympäristö on suojattu monitasoisesti ja tietokantapalvelin on erotettu julkisesta verkosta kokonaan.

Kanta-liityntään Ajas käyttää Atostekin ERA-järjestelmää, joka toimii välittäjänä kansallisten Kanta-palveluiden ja Ajas-järjestelmän välissä.

Palvelun suorituskyky

Käyttäjälle näkyvä suorituskyky riippuu useista eri tekijöistä. Nopeuteen vaikuttaa mm. käyttäjän verkkoyhteyden nopeus, laitteiston suorituskyky, selainmalli, sekä palvelimen suorituskyky. Asiakkaan käyttötapa vaikuttaa järjestelmän nopeuteen. Esimerkiksi raporttien hakeminen pitkältä ajalta kestää kauemmin kuin lyhyeltä ajalta haettava raportti.

Pääsääntöisesti kaikki sivut latautuvat tavallisella tietokoneella ja verkkoyhteydellä 2 sekunnin kuluessa. Mikäli sivunlataus on jatkuvasti tätä hitaampaa ja yhteydet sekä tietokoneen suorituskyky on tarkistettu, käyttäjän kannattaa ottaa yhteyttä asiakaspalveluun ongelman juurisyyn ratkaisemiseksi.

Kirjautuminen palveluihin

Ajas-palveluihin käytettävät kirjautumistunnukset ovat henkilökohtaiset ja käyttäjä on vastuussa omilla tunnuksillaan palvelussa tehdyistä toimenpiteistä. Ajas-palveluihin vakiona saatavilla olevat kirjautumistavat ovat

- Käyttäjätunnus ja salasana (estettävissä asetuksista vaatimalla 2FA)

Dokumentti päivitetty 13.3.2024

- 2-vaiheinen tunnistautuminen
- Kirjautuminen SOTE-ammattikortilla
- Vahva tunnistautuminen

Kaikissa kirjautumisissa täytyy olla lisäksi validi yritystunniste.

Kirjautuminen on suojattu Brute force -hyökkäyksiltä. Jos salasanaa yritetään väärin monta kertaa, tunnuksen kirjautumiseen tulee käyttötauko. Jos samasta IP-osoitteesta tulee paljon kirjautumisyrityksiä, niin IP-osoite estetään määräajaksi.

Käyttöoikeudet

Järjestelmiin kirjaudutaan omalle käyttäjätilille. Järjestelmä tukee eri tasoisia käyttäjärooleja. Käyttöoikeudet ja pääsy tiettyihin tietoihin voidaan rajata yksityiskohtaisesti käyttäjätasolla.

Tietoturva

Ajas-järjestelmän tietoturva perustuu sekä tekniseen että hallinnolliseen tietoturvaan, jota kehitetään ja valvotaan säännöllisesti.

Hallinnollinen tietoturva
Yrityksessä on tietoturvamääräykset, joita kaikkien tulee noudattaa. Ajas-tietoturvaan liittyviin tehtäviin palkataan vain korkeasti koulutettuja henkilöitä. Henkilöstöä ohjataan aktiivisesti päivittämään tietojaan.

Järjestelmän tietoturvaratkaisut on auditoitu käyttämällä ulkoista tahoa. Auditointi on todistettu A1-sertifikaatilla. Yrityksessä järjestetään säännöllisesti sisäisiä tietoturvakatselmuksia ja sisäisiä auditointeja, joissa pohditaan parannettavia kohtia. Näissä havaitut puutteet organisoidaan henkilöstölle tehtäviksi. Toimitilat on suojattu murtosuojauksella ja vartiointipalvelulla. Tilojen ulko-ovet ovat lukittu, eikä tuntemattomia päästetä tiloihin. Ylläpitäjien toimintaperiaatteisiin on kirjattu tietoturvan perustaksi se, että yhden suojauksen pettäminen ei voi avata rajoittamatonta käyttöoikeutta kaikkeen mahdolliseen tietoon.

Yrityksen palveluksessa on tietoturva-asiantuntija joka vastaa yrityksen tietoturvatiimin toiminnasta. Tietojen käyttöoikeus on vain niillä käyttäjillä, jotka tarvitsevat tietoja tehtävissään ja oikeus on ajallisesti rajattu vain niihin tilanteisiin, joissa tietoihin pääsyä edellytetään esimerkiksi ongelman selvittämistä varten. Tietojen katselusta jää merkintä järjestelmään.

Tekninen tietoturva

Palvelimilla on palomuurit, jotka estävät yhteydet asiattomiin portteihin ja asiattomista IP-osoitteista. Tiedonsiirto tapahtuu salattujen yhteyksien yli. Tiedonsiirtoprotokolla verkossa on https. Järjestelmässä on monikerroksinen pääsynhallinta. Mm. palvelinyhteydet vain VPN-verkon kautta.

Dokumentti päivitetty 13.3.2024

Niissä järjestelmissä, jotka tallentavat tietoa käyttäjän oman koneen kiintolevylle, tieto tallentuu salattuna. Palvelimille asennetaan uusimmat tietoturvapäivitykset ja niiden tilaa valvotaan jatkuvasti. Verkkoon yhteydessä olevilla palvelimilla on tietoturvaohjelmisto, joka pyrkii eliminoimaan jo ennalta mahdolliset hyökkäysyritykset. Tietoturvalokit kerätään keskitettyyn valvontajärjestelmään, jossa automatiikka etsii mahdollisia tietoturvapoikkeamia ja hälyttää niistä.

Päivitykset

Käyttäjien ei tarvitse huolehtia ohjelmiston päivittämisestä uuteen versioon. Uudet versiot ja tietoturvapäivitykset tulevat käyttöön automaattisesti. Kehittäjillä on valmius julkaista kriittisiä tietoturvaan liittyviä päivityksiä päivittäin.

Palvelun valvonta

Palvelun valvontaa hoitaa Enerocin palvelusta ja palvelimista vastaavat henkilöstöt, omien toimenkuviensa mukaisesti. Henkilöstö huolehtii palvelun tavoitettavuudesta, turvallisuudesta ja skaalautuvuudesta.

Varmuuskopiointi ja palauttaminen

Data varmuuskopioidaan monitasoisesti

Tietokannat ovat kahdennettu binäärilokin avulla. Jokainen muutos tallentuu kahteen paikkaan. Tietokannoista otetaan päivittäin automaattiset varmuuskopiot ensisijaiseen varmistusjärjestelmään, jossa niitä säilytetään 7 päivää. Varmuuskopiot siirretään päivittäin myös toissijaiseen varmistusjärjestelmään, jossa niitä säilytetään salattuna 2 vuoden ajan, poissa julkisesta verkosta.

Tiedon korruptoituessa lähtökohtaisesti kaikki tieto saadaan palautettua takaisin replikointipalvelimelta, eikä dataa jää puuttumaan lainkaan.

Mikäli kloonista palautus ei jostain syystä onnistuisi, toissijaisesti palautus tapahtuu varmuuskopiosta, jotka ovat korkeintaan 24 tuntia vanhoja. Varmuuskopioista palauttamista testataan säännöllisesti, sisäisen ohjeistuksen mukaan.

Varmuuskopiosta palauttaminen sisältyy kuukausimaksuihin vain siinä tapauksessa, että ongelma on aiheutunut Ajas-järjestelmän päässä. Asiakkaan pyynnöstä tehtävä palautus varmuuskopiosta on mahdollinen erillisenä tilaustyönä, kulloinkin voimassa olevan tuntihinnaston mukaisesti.

Lisäksi viranomaisen pyynnöstä tai maksua vastaan on mahdollista palauttaa tietyn hetken historiatilanne varmuuskopioista sillä tarkkuudella kuin varmuuskopioita on otettu.

Dokumentti päivitetty 13.3.2024

Tietosuoja

Eneroc Oy -konserni on sitoutunut noudattamaan EU:n yleistä tietosuoja-asetusta sekä voimassaolevaa tietosuojalainsäädäntöä. Keräämme jatkuvasti palautetta asiakkailtamme ja seuraamme viranomaistiedotteita. Olemme laatineet ohjeita sekä valmiita vastauksia tietosuojaa koskeviin kysymyksiin.

Suunnittelemme ja toteutamme jatkuvasti myös tietosuoja-asetuksen noudattamista helpottavia toimintoja. Ajas on liittynyt Kanta-arkistoon, jonka avulla rekisterinpitäjä voi huolehtia myös hoitoalan potilastietoja koskevasta erityislainsäädännöstä.

Kaikki tieto, jonka rekisterinpitäjä ja sen asiakkaat tallentavat järjestelmäämme, käsitellään huomioiden tietojenkäsittelysopimukset ja käyttäjän ohjeet.

Henkilöstön vaitiolovelvollisuus
Vaadimme kaikkia työntekijöitämme hyväksymään allekirjoittamaan vaitiolosopimuksen, jossa henkilöstömme sitoutuvat olemaan kertomatta vaitiolon piiriin kuuluvia asioita kellekään tai millekään taholle.

Tietojen säilytysajoissa ja poistopolitiikassa noudatetaan potilasasiakirjoista ja käyttölokitiedoista asetettuja lakeja ja viranomaisvaatimuksia.

Lokikäytännöt

Järjestelmässä on käyttöloki, johon tallentuu yksityiskohtaiset tiedot kaikista asiakastietoihin tehtävistä muutoksista ja katseluista. Lokin avulla selviää, kuka on katsellut mitäkin tietoja. Käyttöliittymälle on tuotu pääsy yleisimpiin käyttölokeihin, joista pääkäyttäjä näkee esimerkiksi kuka on muokannut tai katsellut ajanvarauksen tai asiakkaan tietoja.

Käyttölokista pystytään selvittämään tapahtuman ajankohta, muutoksen tehnyt käyttäjä sekä tietueet (esim. potilaskirjaus, ajanvaraus, käynti). Asiakkaan GDPR-vientiin tallentuu myös asiakasta koskevat lokitiedot.

Käyttölokin lisäksi järjestelmä tallentaa aiemmin kuvatulla tavalla palvelimen tietoturvalokeja, jotka ovat vain palvelintiimin saatavilla. Niitä on mahdollista hyödyntää tilanteissa, joissa selvitykselle on viranomaistaholta tullut määräys. Tällainen pyyntö toimitetaan Ajas Oy:lle asiakaspalvelun kautta. Sama koskee niitä käyttölokeja, joihin käyttöliittymästä ei ole pääsyä. Sellaiset käyttäjän organisaatiota

koskevat lokit, joita on mahdollista luovuttaa käyttäjälle ilman muiden henkilöiden tietosuojan salassapidon vaarantumista, voidaan etsiä ja toimittaa tuntityön hinnaston mukaisesti.

Usein kysyttyjä kysymyksiä

Kysymys: Kun palvelun käyttö on mahdollista mistä tahansa osoitteesta, niin onko se turvallista?
Vastaus: Palveluun pääsee ainoastaan kirjautumalla ja kaikki tiedonsiirto palvelimen ja selaimen välissä on salattua. Kirjautumisen tietoturvaa voidaan myös tiukentaa useilla eri menetelmillä. Mikäli asiakasorganisaatiossa on tarve rajata pääsyä palveluun vain tietyistä IP-osoitteista, ominaisuus on aktivoitavissa Ajas asiakaspalvelun kautta.

Kysymys: Miten säilytän asiakastiedot ja lokit, jos lopetan palvelun käytön
Vastaus: Ajas tarjoaa mahdollisuutta tilata hinnaston mukaisesti tietojen säilytyspalvelun, jossa tiedot säilytetään vuosimaksua vastaan tietoturvallisesti. Kun käytön lopettaa, asiakastiedot on myös mahdollista ladata kerran zip-pakettina, joka sisältää PDF-muotoiset asiakastiedot. Jos käytät Kanta-arkistoa, niin kaikki potilastietomerinnät säilyvät siellä myös Ajas-palvelun käytön lopettamisen jälkeen.

Kysymys: Voiko järjestelmän vaihtamista aikova käyttäjä saada palveluun tallennetut asiakastiedot siirrettyä toiseen järjestelmään.
Vastaus: Kyllä. Jos asiakas haluaa sellaisen viennin, joka on siirrettävissä toiseen järjestelmään, on toimitettavissa erilaisia “data export” -vientejä erillistä maksua vastaan. Tavanomaisin on CSV-muotoiset listaukset tiedoista, mutta myös json-muotoinen vienti on saatavilla.