

CSI MOBILE - TIETOTURVA



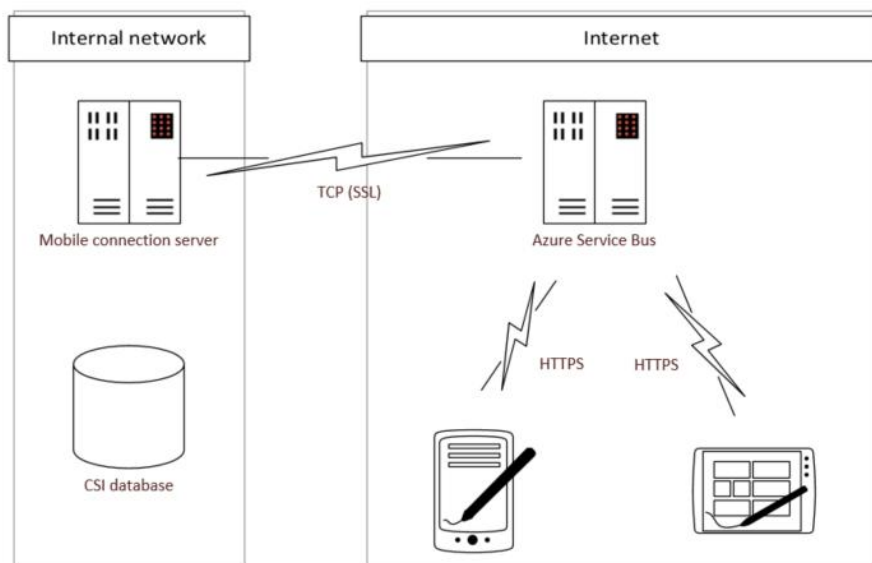
CSI Mobile tarjoaa tietoturvallisen tavan kirjata toimenpiteitä CSI-ohjelmistoon mobiililaitteilla. Siinä käytetään samaa salaustekniikkaa kuin verkkopankeissa.

Ratkaisu pohjautuu pilvessä sijaitsevaan Microsoft Azure Service Bus Relay -palveluun, joka toimii linkkinä CSI-ohjelmiston palvelimen ja mobiililaitteen välillä. Yhteys mobiililaitteelta CSI-ohjelmiston palvelimelle syntyy ns. jaetun avaimen (Shared Key) menetelmällä. Kun Service Bus -palveluun otetaan yhteys mobiililaitteella, jonka avain vastaa CSI-ohjelmiston palvelimelle tallennettua avainta, Service Bus muodostaa tietoturvallisen yhteyden mobiililaitteen ja CSI-palvelimen välille. Kaikki tietoliikenne palvelimen, pilven ja puhelimen välillä tapahtuu salattuna.

Mobiililaitteeseen tallentuvat ainoastaan käyttäjän kirjautumistiedot yhteyden muodostamista varten sekä käyttäjän itselleen kiinnittämien toimeksiantojen ja toimenpidetyyppien tunnisteet. Muut ohjelmassa näkyvät tiedot poistuvat puhelimen muistista, kun mobiilisovellus suljetaan.

TEKNINEN KUVAUS

CSI Mobilen tietoturvaratkaisu hyödyntää Microsoftin Azure Service Bus Relay -tekniikkaa. Sekä sisäverkon palvelimelta (CSI-ohjelmiston palvelin) että mobiililaitteesta muodostetaan ulospäin menevät yhteydet, jotka yhdistyvät toisiinsa Azure Service Bus -palvelimella. Tarkemmin service busin toimintaan voi tutustua <http://azure.microsoft.com/en-gb/services/service-bus/>.



SERVICE BUS -YHTEYDEN MUODOSTAMINEN

Jotta Service Bus voi välittää tietoturvallisesti liikenteen mobiililaitteen ja palvelimen välillä, molempien täytyy olla autentikoituneena Service Bus -palveluun. Tässä käytetään molemmissa päissä jaetun avaimen menetelmää (Shared key). Jaettu avain muodostetaan Azure servicen päässä ja siirretään asiakkaalle asennuksen yhteydessä. Avain on niin pitkä, ettei sitä ole järkevää syöttää mobiililaitteelle käsin, vaan laitteen rekisteröintivaiheessa se tallennetaan tilapäisesti Azuressa sijaitsevaan palveluun. Palvelu välittää avaimen mobiililaitteelle kertakäyttötunnusten avulla.

LAITTEEN REKISTERÖINTI

Kun mobiiliohjelmiston rekisteröinti aloitetaan, mobiililaitte hakee rekisteröintipalvelulta tunnistekoodin ja pyytää käyttäjää syöttämään sen tietokoneella CSI-ohjelmiston rekisteröintikkunaan. Kun tämä on tehty, CSI-ohjelmisto hakee vuorostaan rekisteröintikoodin rekisteröintipalvelulta ja pyytää käyttäjää syöttämään sen mobiililaitteeseen. Jaettu avain tallentuu mobiililaitteeseen, kun rekisteröintiprosessi on onnistuneesti suoritettu.

CSI-TUOTTEEN AUTENTIKOINTI

Rekisteröitymisen yhteydessä laite kysyy tunnistetietoja, joilla käyttäjä kirjautuu CSI-ohjelmistoon. Nämä toimivat myös CSI Mobilen tunnistetietoina, ja ne tallennetaan puhelimeen jatkokäyttöä varten. Mikäli käyttäjä kirjautuu CSI-ohjelmistoon domain-tunnuksilla, hänen on asetettava itselleen erillinen tunnus ja salasana CSI Mobilen käyttöä varten.

PALVELINPYYNTÖJEN RAKENNE

Autorisointia varten palvelinpyynnöissä on kolme autorisointitunnistetta (Authorization headers). Standardin mukainen autorisointitunniste kattaa Service Busia varten Shared Access Signaturen, joka on luotu jaettua avainta käyttäen. "AuthCSI"-tunniste kattaa autorisointitiedot CSI-tuotetta varten ja "DeviceID"-tunniste laitteen tunnistetiedon. Jokaisen pyynnön yhteydessä lähtevät kaikki nämä tunnisteet, joilla varmistetaan, että a) laite on rekisteröity Service Busiin, b) käyttäjä on tunnistettu CSI-tuotteessa ja c) laite on rekisteröity CSI-tuotteeseen kyseiselle käyttäjälle.

LAITTEEN REKISTERÖINNIN POISTAMINEN

CSI Mobile -sovellus voidaan poistaa mobiililaitteelta Asetuksista. Mikäli mobiililaitte katoaa, sen rekisteröinti voidaan poistaa käyttäjän tiedoista myös työasemalla CSI-ohjelmistosta. Kyseisellä laitteella ei silloin ole pääsyä CSI-ohjelmiston tietoihin ennen mobiililaitteen uudelleen rekisteröintiä.

