

CSI MOBILE - DATASÄKERHET



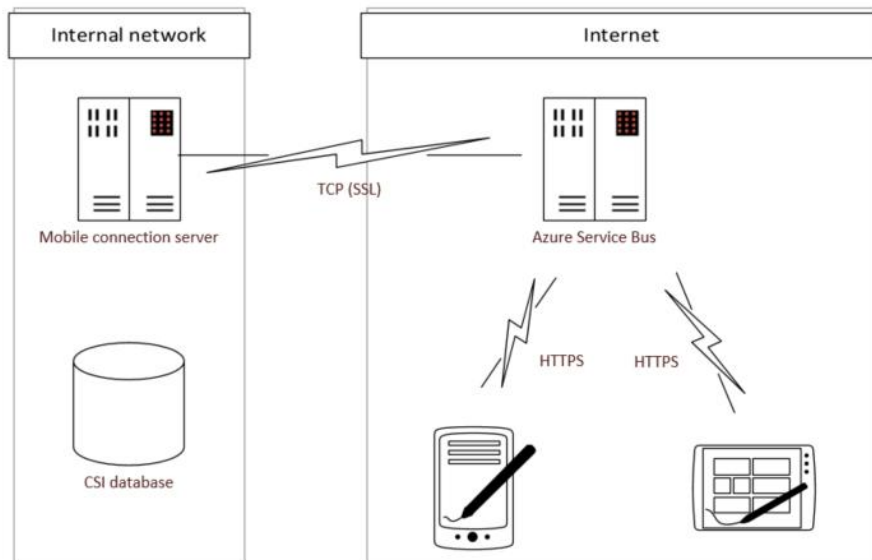
CSI Mobile erbjuder ett säkert sätt att registrera åtgärder i CSI-programmet via mobila enheter. Tekniken är densamma som nätbanker använder.

Lösningen baserar sig på molntjänsten Microsoft Azure Service Bus Relay, som fungerar som en länk mellan CSI-programmets server och mobilenheten. Kontakten från mobilenheten till CSI-programmets server sker via s.k. delad nyckel-metod (Shared Key). När man tar kontakt med Service Bus -tjänsten från en mobilenhet vars nyckel motsvarar den nyckel som har sparats i CSI-programmet, skapar Service Bus en säker kontakt mellan mobilenheten och CSI-servern. All dataöverföring mellan servern, molnet och telefonen är krypterad.

I mobilenheten sparas enbart användarens inloggningsuppgifter så att kontakt ska kunna skapas, samt ID för de åtgärdstyper som användaren har angivit som favoriter. Andra uppgifter som syns i programmet försvinner från telefonens minne när mobilapplikationen stängs.

TEKNISK BESKRIVNING

CSI Mobiles datasäkerhetslösning använder sig av Microsofts Azure Service Bus Relay -tekniken. Både från det interna nätverkets server (CSI-programmets server) och från mobilenheten skapas utgående förbindelser som sammanförs med varandra i Azure Service Bus -servern. Man kan bekanta sig närmare med hur Service Bus fungerar här: <http://azure.microsoft.com/en-gb/services/service-bus/>.



UPPRÄTTA EN SERVICE BUS - FÖRBINDELSE

Så att Service Bus på ett säkert sätt ska kunna förmedla trafiken mellan mobilenheten och servern måste båda vara autentiserade till Service Bus-tjänsten. Här används delad nyckel-metoden (Shared Key) i båda ändarna. Den delade nyckeln skapas i Azure-tjänsten och flyttas till kunden i samband med installationen. Nyckeln är så lång att det inte går att mata in den i mobilenheten manuellt, utan den sparas istället tillfälligt i registreringsskedet i en tjänst som finns i Azure. Tjänsten förmedlar nyckeln till mobilenheten med hjälp av en engångs-login.

REGISTRERA ENHETEN

När man påbörjar registreringen av mobilsystemet hämtar mobilenheten en ID-kod från registreringstjänsten och ber användare mata in de på datorn i CSI-programmets registreringsfönster. När det är gjort hämtar CSI-programmet i sin tur registreringskoden från registreringstjänsten och ber användaren att mata in den på mobilenheten. Den delade nyckeln sparas på mobilenheten när registreringsprocessen har lyckats.

AUTENTISERING AV CSI-PRODUKTEN

I samband med registreringen ber enheten om de identifieringsuppgifter som användaren loggar in i CSI-programmet med. Dessa fungerar också som CSI Mobiles identifieringsuppgifter, och de sparas i telefonen för fortsatt användning. Om användaren loggar in i CSI-programmet med domainuppgifter måste hen ange ett eget användarnamn och lösenord för att använda CSI Mobile.

SERVERFÖRFRÅGNINGARNAS STRUKTUR

För autentiseringen använder serverförfrågningarna tre autentiseringskoder (Authorization Headers). En standardenlig autentiseringskod täcker för Service Bus-tjänstens del en Shared Access Signature som är skapad med hjälp av en delad nyckel. "AuthCSI"-koden täcker autentiseringsuppgifterna för CSI-produkten och "DeviceID"-koden enhetens identifieringsuppgift. I samband med varje förfrågan skickas alla dessa identifieringskoder som säkerställer att a) enheten är registreras i Service Bus, b) att kunden är bekant i CSI-produkten och c) att enheten är registrerad i CSI-programmet för ifrågavarande användare.

TA BORT REGISTRERING AV ENHET

CSI Mobile-applikationen kan raderas från mobilenheten i Inställningarna. Om mobilenheten försvinner kan dess registrering också raderas från användarens uppgifter via CSI-programmet på datorn. Enheten i fråga har då inte längre tillgång till CSI-programmets information innan mobilenheten registreras på nytt.

