

Avtalshantering – Säkerhetsdokument

Secure Socket Layer (SSL)

All kommunikation med avtalshanteringens servrar är säker. Vi använder krypteringsteknologin, Secure Socket Layer (SSL), på avtalshantering.

Med Secure Socket Layer (SSL)-protokollet garanteras äktheten på servern genom ett Digitalt certifikat som skickas till klienten.

Efter det genereras en unik sessionsnyckel som används för att kryptera allt data som skickas mellan servern och klienten. Endast den klienten kan dekryptera informationen och känner även av om informationen förändrats på vägen. Ett giltigt SSL-certifikat kan endast utfärdas av ett fåtal företag runt om i världen.

Avtalshantering har ett så kallat "**Extended Validation Certificate**" (EV) där företaget som utfärdat certifikatet har på egen hand gjort en undersökning som säkerhetsställer att vi driver en seriös verksamhet.

För mer information om Secure Socket Layer och Extended Validation Certificate, besök [verisign.se](https://www.verisign.se)

DigiPass-login

Nu finns även möjligheten att använda **DigiPass**, en koddosa som används utav t.ex. banker, där man får skriva in sin personliga PIN-kod och sedan fylla i den koden som presenteras på skärmen när man loggar in, för att få sitt **OTP (One-Time Password)**. Varje användare kommer få en egen koddosa som vi konfigurerar lokalt och skickar ut till användaren.

För att få tillgång till DigiPass-login, så kommer administratören att få ett mail med en länk, där han/hon får fylla i information om vart koddosorna ska skickas. Vill man ha säker inloggning är det krav på att alla användare ska få en egen dosa. Dosorna kommer vara bundna till ett användarkonto, så ifall någon slutar och någon ny börjar, så måste detta meddelas, så att vi kan binda om dosan till den nya personens användare.

DigiPass-login - Inloggningsförfarande

När man loggar in med dosan så går inloggningen till på följande vis:

1. Användaren loggar in som vanligt på Avtalshantering
2. Användaren får upp en extra ruta med en **Challenge** som man fyller in i dosan.
3. Svaret fyller man sedan in i textboxen på skärmen
4. Användaren blir verifierad mot servern och kan fortsätta logga in



Bild: Bilden representerar själva inloggningsförfarandet i Avtalshantering

Mer information om dosorna/tekniken finns på: vasco.com

Behörighetsnivåer i Avtalshantering

I Avtalshantering har vi 6 användarnivåer för att enkelt kunna ställa in vilka användare som ska komma åt vad.

De nivåer som finns är

- Administratör
- Avdelningsadministratör
- Personligt konto
- Läs/Skriv/Ta bort
- Läs/Skriv
- Läs

Administratör

En administratör ser alla avtal och kan redigera dom. Administratören kan även ställa in vissa inställningar som är företagsspecifika, samt editera användare.

Avdelningsadministratör

Avdelningsadministratören ser alla avtal som ligger i den avdelningen, samt de underavdelningar som han/hon är medlem i. Kan redigera alla dessa avtal.

Personligt konto

Någon med personligt konto kommer endast att kunna se och redigera sina egna avtal.

Läs/Skriv/Ta bort

Rättighet för att tillåta läsning, skrivning/redigering samt borttagning.

Läs/Skriv

Rättighet för att tillåta läsning och skrivning/redigering.

Läs

Rättighet för att tillåta läsning.

IP-Access

I Avtalshantering har vi hantering för att kunna tillåta/blockera IP-adresser. Man kan enkelt välja vilka IP-adresser som är tillåtna att komma åt systemet, på samma sätt kan man enkelt bestämma vilka IP-adresser som inte får logga in.

Det går även att ställa in så att man anger en IP-adress som man måste surfa ifrån för att få komma åt Avtalshantering. T.ex. ifall någon är hemma och sjuk, så kommer den personen inte att kunna logga in hemifrån och ta ut vital data ur systemet.

Säkerhet

Fördelen med att vi har en webbaserad tjänst är att kunderna behöver inte oroa sig för säkerhetsbrister i deras nätverk, tjänsten ligger helt och hållet på våra servrar.

Vi ansvarar för tjänstens säkerhet, bland annat med brandväggar och antivirus-skydd. Vi tar backup på all data dagligen och lagrar detta på band. Vi använder oss också utav UPS för att säkerställa en säker avstängning vid eventuella strömavbrott, så att ingen viktig data förloras.

Databasen ligger skyddad bakom vår brandvägg och tillåter ingen extern åtkomst. Även om någon skulle få tag på databasen så skulle de inte vara hjälpta utav det som står i den, då den är lagrad binärt, vilket omöjliggör läsning utan rätt verktyg och nycklar för att ansluta och hämta ut data.