

BankID för tjänstemän

Hur Fortified ID löser användning av
BankID i tjänsteutövning

BankID är en mycket populär metod för inloggning till olika typer av tjänster för privatpersoner. Man kan enkelt logga in till sin Bank, ICA, Coop, Skatteverket osv för att se saker som tillhör mig som privatperson.

Hur funkar det om den organisation där jag är anställd vill tillåta att jag ska kunna använda mitt privata BankID för att komma åt mina saker som anställd?

Hur kan jag känna mig säker på att mitt personnummer inte missbrukas?

Fördelar:

- ✓ Säkerhet. Hög tillitsnivå. Kontinuerliga förbättringar av säkerheten.
- ✓ Slippa lösenord. Enbart en PIN att komma ihåg, eller biometri.
- ✓ Väl utbrett, >8 miljoner svenskar har BankID. Tusentals organisationer har stöd för användning av BankID
- ✓ Kunskap. Folk vet vad BankID är och hur man använder det.
- ✓ Tillit och arv. BankID utfärdas av banken och anses därför "tryggt"

Nackdelar:

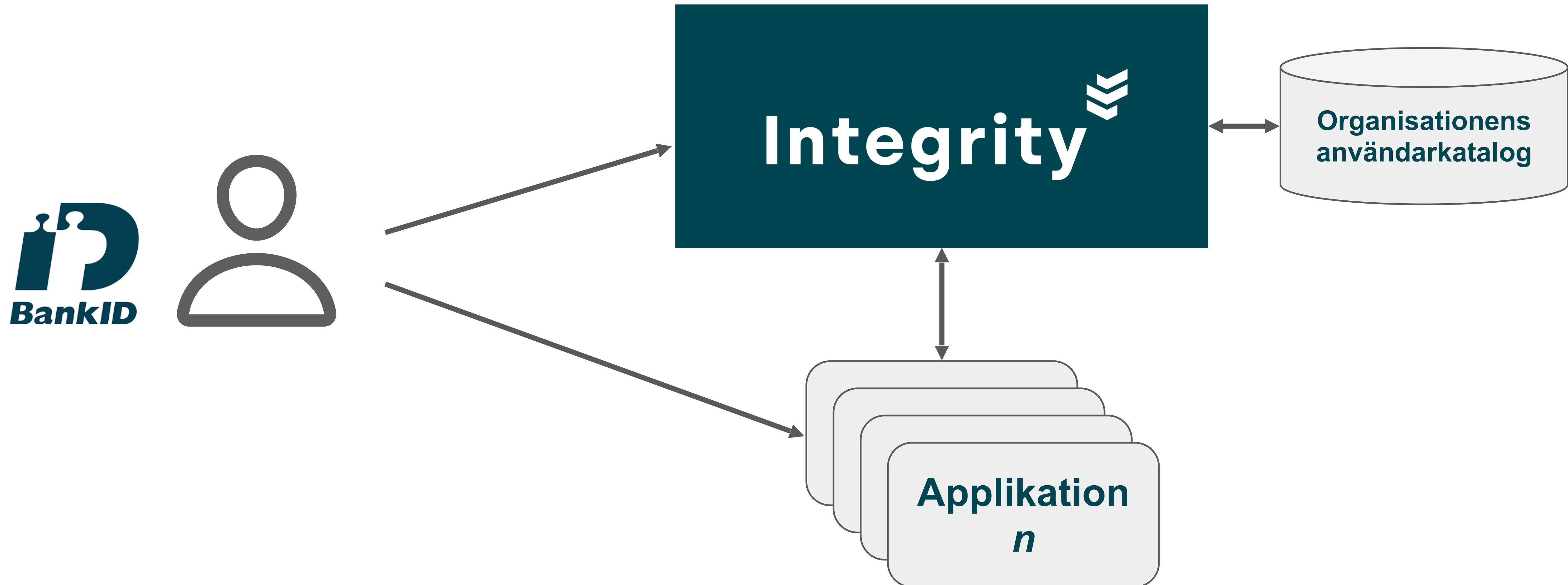
- Använda på jobbet. BankID anses av många, både organisationer och användare, vara för "privat" bruk, och ska därför inte användas på jobbet
 - Risk för att personnummer lagras i organisationens infrastruktur och tjänster

Många organisationer använder multifaktor-inloggning (MFA) för att säkra åtkomst till känsliga resurser och data, samt för att elektroniskt kunna skriva under dokument, tex avtal.

Det finns många olika typer av inloggningsmetoder för MFA, tex:

- ✓ Engångskoder via tex SMS eller en mobilapp
- ✓ Smarta kort
- ✓ Hårdvarunycklar, tex Yubikey
- ✓ e-Legitimation, tex BankID, Freja, SITHS

- ✓ MFA-metoderna, BankID, är något många organisationer önskar använda i större utsträckning, även för sina anställda:
- ✓ Många användare redan har ett BankID och vet hur det fungerar
- ✓ Utfärdandet av BankID hanteras av annan part. Kostnadsbesparande.
- ✓ Många organisationer är dock tveksamma till införande, då många användare är ovilliga till att använda sin "privata" e-Legitimation i tjänsten.
- ✓ **Fortified IDs lösning "BankID för tjänstemän" kan hjälpa er!**



- ✓ Fortified ID har skapat en lösning för BankID för tjänstemän.
- ✓ Fortified ID anser att legitimeringen, dvs identifieringen av en person, avser att legitimera den *fysiska* personen.
- ✓ Huruvida den fysiska personen agerar *privat* eller i sin roll som *tjänsteman* bestäms *efter* legitimeringen.
- ✓ Att den fysiska personen agerar som en tjänsteman, bestäms av de behörigheter som samlas ihop efter legitimeringen.

Med BankID för tjänstemän använder du ditt privata BankID (jämför Freja där det finns en privat Freja och en tjänste-Freja (OrgID)).

Med BankID för tjänstemän behöver du alltså *inte* aktivera ytterligare ett BankID.

BankID för tjänstemän använder alltid organisationens användarkatalog för att kontrollera att användaren tillhör organisationen, samt hämta behörigheter

Mappning mellan BankID och organisationens användarkatalog utförs via ett omvandlat personnummervärde, för att undvika lagring av personnummer i klartext

Aktivering (Fortified ID aktiveringsportal)

1. Logga in i Fortified ID aktiveringsportal för att mappa BankID till tjänstekonto
 - 1.1. Självaktivering
 - 1.2. Aktivering av delegerad administratör

Användande (Fortified ID IdP)

1. Användare loggar in mot organisationens tjänster med sitt personliga BankID
2. Personnumret är skyddat med Fortified IDs IdP

Deaktivering (Fortified ID aktiveringsportal)

1. Självdeaktivering
2. Deaktivering av delegerad administratör

Aktivering av BankID för tjänstemän krävs för att lagra den data som krävs för att mappa mellan BankID och användarkontot i organisationens användarkatalog. Aktiveringen kan utföras av användaren själv eller av en administratör i organisationen.

Användaren

1. Användaren öppnar webbsida
2. Användaren loggar in med sitt användarkonto i organisationen (inloggningsmetod kan variera. Till exempel användarnamn / lösenord)
3. Väl inloggad klickar användaren på "Koppla mitt BankID"
4. Användaren legitimerar sig med BankID
5. Fortified ID tar personnumret från BankID, omvandlar personnumret till ett annat värde och lagrar värdet på användarkontot i organisationens användarkatalog.

Administratör

1. Behörig administratör öppnar websida
2. Behörig administratör loggar (inloggningsmetod kan variera. Till exempel användarnamn / lösenord)
3. Behörig administratör söker upp användaren
4. Behörig administratör redigerar användaren
5. Behörig administratör klickar på "Koppla BankID"
6. Behörig administratör anger användarens personnummer
7. Fortified ID tar personnumret från BankID, omvandlar personnumret till ett annat värde och lagrar värdet på användarkontot i organisationens användarkatalog.

Användaren

1. En tjänsteman behöver komma åt en tjänst i organisationen (tex VPN, Intranät mm)
2. Tjänstemannen identifierar sig med BankID via Fortified ID
3. Fortified ID tar personnumret från BankID och omvandlar personnumret till ett annat värde
4. Fortified ID verifierar att den identifierade tjänstemannen tillhör organisationen genom kontroll i organisationens användarkatalog, via uppslag där värdet från punkt 3 används som nyckel
5. Fortified ID hämtar tjänstemannens organisationsidentifierare.
6. Fortified ID hämtar behörighetsstyrande egenskaper från organisationens användarkatalog [OPTIONAL]
7. Fortified ID skickar organisationsidentifierare och eventuella behörighetsstyrande egenskaper till tjänsten som släpper in användaren.

Deaktivering av BankID för tjänstemän kan utföras av användaren själv eller av en administratör i organisationen.

Användaren

1. Användaren öppnar websida
2. Användaren loggar in med sitt användarkonto i organisationen (inloggningsmetod kan variera. Till exempel användarnamn / lösenord)
3. Väl inloggad klickar användaren på "Deaktivera BankID från organisationen"
4. Fortified ID tar bort kopplingen genom att ta bort värdet på kontot i användarkatalogen

Administratör

Alternativ 1 - användares tjänst upphör

1. Behörig administratör tar bort användarkontot från organisationens användarkatalog.

Alternativ 2 - användare jobbar kvar

1. Behörig administratör öppnar websida
2. Behörig administratör loggar in (inloggningsmetod kan variera. Till exempel användarnamn / lösenord)
3. Behörig administratör söker upp användaren
4. Behörig administratör redigerar användaren
5. Behörig administratör klickar på "Deaktivera BankID från organisationen"
6. Fortified ID tar bort kopplingen genom att ta bort värdet på kontot i användarkatalogen

- ✓ Personnummeruppgifter sprids inte till några tjänster i organisationen.
- ✓ En tjänsteman som slutar i organisationen kommer tas bort från katalogen vilket automatiskt tar bort all åtkomst till organisationens alla tjänster
- ✓ Aktivering, dvs att koppla BankID med användarkontot i organisationens användarkatalog, kan genomföras av:
 - Personen själv (self-service) [OPTIONAL]
 - Administratör (delegerad)
- ✓ Vid aktiveringen omvandlas personnumret till ett så kallat hashat värde som sparas i katalogen. Personnummer lagras alltså inte i klartext i användarkatalogen, istället används ett omvandlat värde (hash)
 - GDPR, privacy
- ✓ Stöd för legitimering med mobilt bankid, bankid på kort, bankid på fil
- ✓ Konfigurerbart attribut i användarkatalog för koppling mellan BankID<->användarkonto
- ✓ Även andra e-Legitimationer, tex för de användare som inte har BankID, kan adderas till lösningen

Referenser

- ✓ Fortified ID jobbar idag med flera kunder som använder BankID för tjänstemän.
- ✓ Referenser kan delas på begäran.