Integrity

EFOS
IDP / SP
E-TJÄNSTER
BANK ID / FREJA
SWEDEN CONNECT

Autentisering, SSO och behörigheter för myndighetssverige

Hantering av digitala identiteter och autentisering inom offentlig sektor styrs i stor utsträckning av regulatoriska krav. Sveriges myndigheter befinner sig i en digitaliseringsprocess och det finns rikligt med såväl strategiska som operativa beslut att ta ställning till.

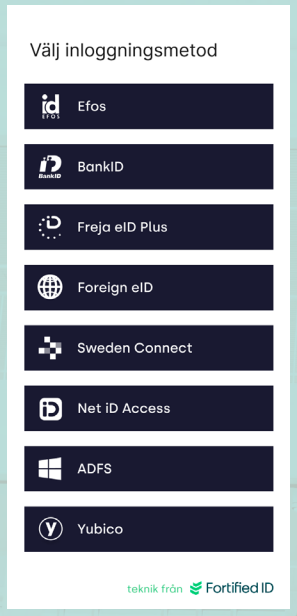
I rapporten Cybersäkerhet i Sverige 2022 , belyses två "Vanligt förekommande sårbarheter"

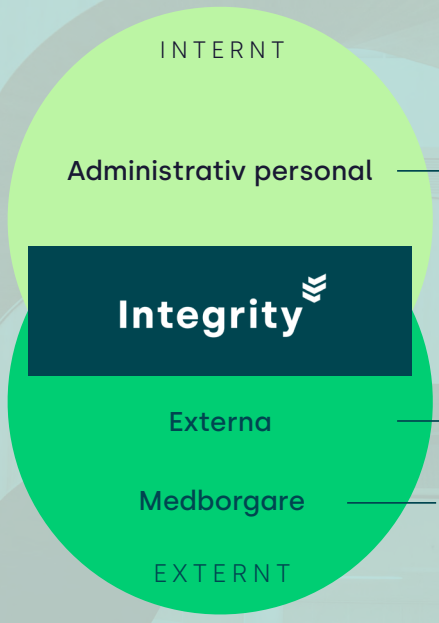
- Brister i autentiseringsfunktioner
- Brister i konto och behörighetshantering

Identitetshantering och stark autentisering är grundpelare inom IT-säkerhet som varje organisation behöver ta i beaktning.

Stark autentisering

Myndigheter har flertalet olika grupperingar av användare som ska erbjudas adekvat autentiseringsmetod.





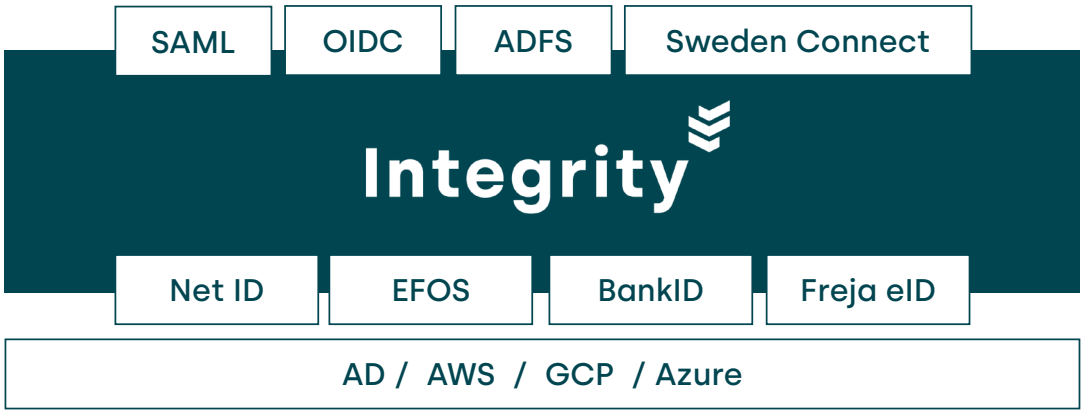
Administrativ personal använder oftast kort eller mobil för att autentisera sig. Användningen av EFOS (E-identitet för offentliga sektor), som Försäkringskassan ansvarar för, utnyttjas av flertal myndigheter. Förutom att EFOS är godkänd som svensk e-legitimation så förenklar den samverkan mellan offentliga aktörer.

Externa användare som konsulter behöver snabbt kunna få access till IT-resurser som ordinarie personal med krav på stark autentisering.
Vilken metod som kan/bör användas påverkas av om det nås via mobil enhet eller dator, gällande LOA nivå, externt exponerade tjänster osv.

Medborgare behöver erbjudas flertalet inloggningsmetoder (BankID, Freja eID, eIDAS) för att kunna nå myndighetens alla e-tjänster.

Single sign-on

Efter stark autentisering bör användaren inte behöva logga in fler gånger under samma session. Detta kräver ibland att applikationerna behöver annan eller ytterligare information än det som initialt skapades på sessions-biljetten vid autentisering.
Denna information hämtas och uppdaterar informationen så att användaren upplever single sign-on.
För att uppnå detta så har Integrity från Fortified ID stöd för befintliga standarder som **SAML**, **OpenID Connect** och **ADFS**.
Med integration med dessa standarder kan Fortified ID även hjälpa myndigheten med **ID-mappning** (en sessions-biljett anpassas till målapplikationens kravbild på användarattribut) och **ticket translation** (att t.ex. göra om en OIDC-biljett till en SAML-biljett).



Rätt behörigheter

Behörighetsstyrning skiljer sig ofta åt mellan myndighetens olika tjänster och applikationer. Därför bör en **IdP** (Identity Provider) vara flexibel och kunna anpassa sig till både lokal respektive central behörighetsstyrning. Vidare kan även en identitet agera i olika roller inom en verksamhet. Identitetens egenskaper är en grundpelare för att få rätt access och behörighet.

Integration

Vi har de senaste 20 åren hjälpt svenska myndigheter med integration av digitala identiteter.
Som identitetsexperter kan vi bistå med att:

- Integrera alla applikationer som redan har stöd för OIDC eller SAML.
- Hantera EFOS med de olika val för medie samt klienter som erbjuds
- Upprätta koppling mot alla interna datakällor för uppslag
- API erbjuds för appar som inte kan hanteras via t.ex. SAML/OpenID Connect.
- ID-mappning och ticket translation
- Fortified ID IdP kan agera som olika logiska IdP'er för att få en logisk separation för olika scenarios.