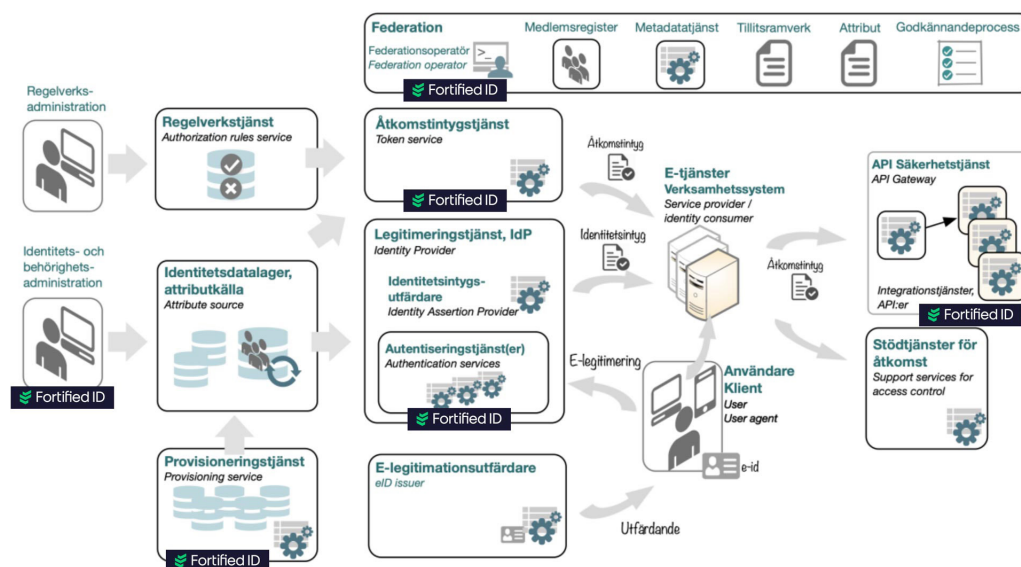


Fortified ID och Ineras Referensarkitektur

Fortified ID integrerar robusta identitets- och åtkomsthanteringslösningar med referensarkitekturs krav och tekniska regelverk. Plattformen erbjuder stöd som Regioner påverkas av gällande standardiserade protokoll, vilket möjliggör interoperabilitet, säker autentisering och delegerad åtkomst. Genom att följa etablerade ramverk samt implementera effektiva provisioneringsmetoder säkerställer Fortified ID en enhetlig och tillförlitlig identitetsinfrastruktur som uppfyller kraven på både säkerhet och flexibilitet.



Koppling mellan Fortified ID och Referensarkitekturs samverkan och funktion

Legitimeringstjänst (IdP)

Fortified ID erbjuder robusta IdP-tjänster som möjliggör användarautentisering och generering av säkra identitetsintyg. Lösningarna stöder flera autentiseringsmetoder och protokoll, vilket säkerställer interoperabilitet och användarvänlighet. Detta inkluderar stöd för singelinloggning (SSO) och hantering av autentiseringskontext, vilket är i linje med krav i referensarkitekturen.

Utfärdande och förmedling av intyg

Fortified ID:s plattform möjliggör utfärdande av både identitets- och åtkomstintyg, med stöd för både front-channel och back-channel kommunikation. Intyg signeras digitalt och kan skräddarsys för specifika attribut enligt principen om uppgiftsminimering, vilket uppfyller arkitekturs säkerhetskrav.

Identitetsdatalager

Fortified ID tillhandahåller en konsoliderad datalagerlösning, enligt mönstret "identity fabric" som säkerställer kvalitetssäkrad identitetsinformation. Lösningen stöder attributbaserad behörighetsutvärdering och kan integrera data från flera källor, inklusive personaladministrativa system och register över legitimationer, vilket är centralt för att skapa en enhetlig användarprofil.

Provisioneringstjänst

Genom att automatisera provisionering av identitetsdata hjälper Fortified ID organisationer att hantera livscykeln för identiteter effektivt. Lösningen stöder både push- och pull-mönster för provisionering och är kompatibel med standardprotokoll som SCIM.

E-legitimationsutfärdare

Fortified ID är endast involverat i utfärdandet av Fortified ID Mobile. I övriga fall används redan befintliga e-legitimationer, såsom SITHS eller BankID. Lösningen uppfyller höga krav på tillit och erbjuder stöd för multifaktorsautentisering.

Åtkomstintygstjänst

Fortified ID utfärdar och hanterar åtkomstintyg som möjliggör finjusterad åtkomstkontroll baserad på regelverk och attribut. Åtkomstintygen integreras sömlöst i e-tjänster för att uppfylla säkerhets- och auktorisationskrav.

API Säkerhetstjänst

Fortified ID:s API-säkerhetslösningar erbjuder autentisering och auktorisation på systemnivå, vilket underlättar säker kommunikation mellan system. Lösningen inkluderar stöd för tokens och krypterade anslutningar enligt moderna standarder.

Autentisering och auktorisation av system

Plattformen möjliggör säker autentisering och auktorisation mellan system genom standardiserade protokoll och token-hantering. Detta inkluderar stöd för delegation och verifiering av åtkomstbehörigheter.

Delegerad åtkomst från användare

Fortified ID implementerar lösningar för delegerad åtkomst, som gör det möjligt för användare att överföra åtkomsträttigheter säkert och effektivt, inklusive över organisationsgränser. Detta stödjer flera interaktionsmönster såsom intygsväxling och förnyad autentisering.

Identitets- och behörighetsfederation

Fortified ID:s federationslösningar säkerställer interoperabilitet mellan olika organisationer och tjänster genom standardiserade tillitsramverk och attribututbyte. De möjliggör effektivt samarbete genom säkra och tillförlitliga processer.

Regelverkstjänst

Regelhantering i Fortified ID är flexibel och skalbar, vilket gör det möjligt att implementera och tolka regler på ett maskinläsbart sätt. Tjänsterna stöder granulära och dynamiska regler för åtkomststyrning.

Stödtjänster för reglering och uppföljning av åtkomst

Fortified ID erbjuder omfattande stödtjänster för uppföljning och efterlevnad (governance), inklusive loggning och rapportering för att säkerställa att regelverket följs och att åtkomst är korrekt reglerad.

Provisioneringstjänst

Genom att automatisera provisionering av identitetsdata hjälper Fortified ID organisationer att hantera livscykeln för identiteter effektivt. Lösningen stöder både push- och pull-mönster för provisionering och är kompatibel med standardprotokoll som SCIM.

Koppling mellan Fortified ID och Referensarkitekturs Tekniska Regelverk

Indelning av tekniska protokoll och format

Fortified ID tillhandahåller stöd för moderna tekniska protokoll och format som krävs för autentisering, federerad inloggning och delegerad åtkomst. Plattformen använder JSON Web Tokens (JWT) och andra standardiserade intygstyper, vilket säkerställer interoperabilitet och säker hantering av identitets- och åtkomstdata enligt rekommendationerna i referensarkitekturen.

Rekommenderade protokoll per förmåga

Fortified ID implementerar de rekommenderade protokollen för federerad inloggning, SSO och delegerad åtkomst, såsom SAML2, OpenID Connect och OAuth 2.0. Denna anpassning möjliggör interoperabilitet med e-tjänster och stödjer parallellt olika tekniska plattformar. Fortified ID fokuserar även på att erbjuda stöd för både nya och befintliga protokoll, såsom SAML2, vilket underlättar integration med existerande system.

Protokoll för federerad inloggning och SSO

Fortified ID:s lösningar implementerar både OpenID Connect och SAML 2.0 för federerad inloggning och SSO. Tjänsterna stödjer autentiseringskontext och säker hantering av autentiseringsbegäran, vilket följer de specifika krav som listas i referensarkitekturen. Lösningarna erbjuder också funktioner för utloggningshantering på ett sätt som harmonierar med rekommenderade standarder.

Protokoll för delegerad åtkomst

Fortified ID använder OAuth 2.0 som det primära protokollet för delegerad åtkomst, inklusive flöden som Authorization Code. Detta möjliggör säker åtkomsthantering mellan användare och system, samt mellan olika system, vilket adresserar de behov som lyfts fram i arkitekturen.

Protokoll för autentisering

Lösningarna från Fortified ID stödjer moderna autentiseringsprotokoll, inklusive Mutual-TLS med x.509-certifikat och FIDO2. Dessa protokoll erbjuder stark säkerhet genom asymmetrisk kryptering och stöd för multifaktorsautentisering, vilket uppfyller kraven på robust autentisering för både användare och system.

Tekniska ramverk för federation

Fortified ID följer ramverk som exempelvis SAMBI, Sweden Connect, Verifiable credentials och OpenID Connect Federation för att säkerställa interoperabilitet och säker hantering av metadata mellan olika identitetsleverantörer och tjänster. Detta stöder tillitsramverk och standarder för federation, vilket är en nyckelkomponent i referensarkitekturen.

Tekniska regelverk för provisionering

Plattformen inkluderar stöd för SCIM-protokollet för effektiv provisionering av identitetsdata. Detta säkerställer att användarinformation kan tillhandahållas till system och e-tjänster på ett standardiserat och kvalitetssäkrat sätt, vilket uppfyller rekommendationerna i arkitekturen.