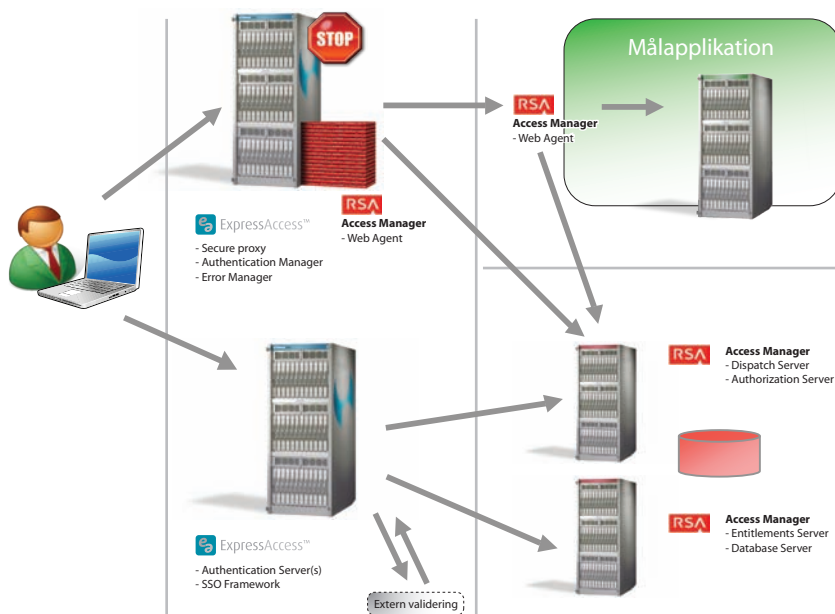


Skolväsendets access lösning för 1,3 miljoner användare



Robert och Hans på Skolverket framför interaktionssekvensen för sitt ExpressAccess system.

ExpressAccess består av en rad olika komponenter, var och en med en dedikerad arkitekturell uppgift. Den komponent som är användarens främsta kontaktpunkt är ExpressAccess Reverse Proxy placerad i DMZ som ökar säkerheten för målapplikationer genom att separera dem från direkt exponering på Internet. ExpressAccess Reverse Proxy innehåller en agent för RSA Access Manager som kontrollerar att användaren är autentiserad och att denna överhuvudtaget tillåts komma åt målapplikationen. I fall användaren inte är autentiserad presenterar komponenten ExpressAccess Authentication Manager ett val av autentiseringsmetod för användaren. Presentationen av detta val genereras dynamiskt baserat på målapplikationens säkerhetsklass, som styr vilka autentiseringsmetoder som är godkända för åtkomst av målapplikationen.

När användaren valt sin autentiseringsmetod, dirigeras användaren till en av ExpressAccess autentiseringsserver. Varje autentiseringsserver bygger på ExpressAccess SSO Framework som genom adapterteknologi kommunicerar med RSA Access Manager för att skapa användarens SSO-token. Efter detta är användaren autentiserad och dirigeras tillbaka till ExpressAccess Reverse Proxy.

Användarens SSO-token talar om för ExpressAccess Reverse Proxy att användaren autentiserats och då återstår kontroll att SSO-token är giltig och att användaren har tillåtelse att komma åt målapplikationen, vilket utförs av agenten för RSA Access Manager. [Läs vidare på andrasidan >>](#)

Teknisk leverans komponenter:

- ExpressAccess Reverse Proxy
- ExpressAccess Authentication Manager
- ExpressAccess Autentiseringsmetod ActiveDirectory
- ExpressAccess Autentiseringsmetod RSA SecurID
- ExpressAccess SSO Framework
- ExpressAccess Error Manager
- RSA Access Manager och agenter
- RSA Authentication Manager (SecurID)

Teknisk leverans servrar:

- Virtualiserad RHEL 4.0
- Virtualiserad Windows 2003 Server R2

ExpressAccess

Ett kostnadseffektivt sätt att implementera en central säkerhetsfunktion för hantering av inloggning och behörighetskontroll. Kan användas för såväl interna som externa användare. Funktionaliteten omfattar bland annat identifiering med e-legitimation, validering av identiteten mot Infracentral, single sign-on och anpassad behörighet för varje tjänst.

ExpressAccess Reverse Proxy slussar därefter användaren vidare till målapplikationen. På målapplikationsservern finns ännu en agent för RSA Access Manager som dels skyddar mot försök att kortsluta ExpressAccess och dels utför mer granulära behörighetskontroller innan användaren släpps igenom för att komma åt målapplikationens resurser. Denna agent möjliggör även mappning av användarens identitet, försörjning av behörighetsunderlag till målapplikationen till exempel roller kopplat till verksamhetsdata samt personalisering.

I och med detta är användaren inloggad i målapplikationen! All trafik skyddas av SSL/TLS och skulle något fel inträffa i flödet dirigeras användaren till ExpressAccess Error Manager som hanterar alla felflöden i systemet.

ExpressAccess-arkitekturen är tydligt uppdelad i autentiseringskontroll och auktoriseringskontroll för att lösningen ska kunna skala efter behov i såväl prestanda som funktionalitet. Uppdelningen bygger på en solid interaktionsmodell för inloggning och på att agenter och ramverk med dedikerad funktionalitet placeras på rätt ställen i arkitekturen, t ex agenterna för ExpressAccess Reverse Proxy respektive målapplikationen och ExpressAccess SSO Framework. Detta ger också en fullgod spårbarhet i systemet.

Ett bevis för arkitekturens kvalitet är till exempel möjligheten att plugga in nya autentiseringsmetoder med minimal insats, ofta handlar det om konfiguration snarare än utveckling. ExpressAccess stöder idag autentiseringsmetoder för ActiveDirectory, LDAP, RSA SecurID, e-legitimationer (Telia, Nordea, BankID), egna tjänstekort och digitala certifikat.