Autentisering
2026-04-01

Att använda VGR:s autentiseringsmetoder

När du loggar in i en tjänst med ditt konto – den process som kallas autentisering – bevisar du för tjänsten att du är den du utger dig för att vara. För att göra autentiseringen mer säker används flerfaktorautentisering/ multifaktorautentisering. Det innebär att när du loggar in behöver du ange något mer än bara användarnamn och lösenord – alltså ytterligare en faktor – för att bevisa vem du är och få komma åt VGR:s information och resurser. Vilka metoder du kan välja skiljer sig åt beroende på vilket system du loggar in i.

Tips! Vill du slippa skriva in ditt lösenord? I många inloggningar kan du ange användarnamn och välja ett av SITHS-alternativen för att loggas in direkt.

När du anger ditt lösenord behöver du alltid komplettera det med ytterligare en av metoderna nedan.

- **SITHS eID på annan enhet**: Med SITHS eID app på en mobiltelefon/surfplatta kan du legitimera dig till olika tjänster genom att skanna en QR-kod och ange personlig kod.
- **SITHS eID på denna enhet**: SITHS eID-applikationen i datorn visas och du skriver in din personliga kod för att legitimera dig. Kräver att SITHS-kortet är insatt i kortläsaren.
- **SITHS-kort på denna enhet**: Detta alternativ använder sig av datorns inbyggda program och här väljer du certifikat för SITHS-kortet. Sen legitimerar du dig genom att fylla i din personliga kod. Kräver att SITHS-kortet är insatt i kortläsaren.
- **MFA Microsoft Authenticator på mobil enhet**: Autentisering via mobil-applikationen Microsoft Authenticator. Kräver en säkerhetskod från inloggningssidan.
- **RSA SecurID på fysisk hårdvarunyckel**: Används av externa leverantörer eller användare.

VGR erbjuder flera olika metoder för autentisering för att ha en hög tillgänglighet och redundans.

Nedan visas olika varianter av rutor för att logga in. De ser lite olika ut men båda innehåller metoder för inloggning som beskrivits ovan.