Autentiseringsmetoder – användning

När du loggar in 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 autentisering mer säker används Flerfaktorautentisering/ Multifaktorautentisering. När man loggar in behövs mer än bara användarnamn och lösenord anges – dvs ytterligare en faktor – för att bevisa vem du är och komma åt VGR:s information och resurser. Val av metoder skiljer sig beroende på vilket system man loggar in mot.

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

När man anger sitt lösenord behöver man alltid komplettera det med ytterligare en av metoderna nedan.

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

För att VGR ska ha en hög tillgänglighet och redundans erbjuder vi flera autentiseringsmetoder.

Nedan visas olika inloggningsrutor som ser lite olika ut utseendemässigt men innehåller delar av samma metoder beskrivet ovan.