Rekommendation gällande att dela på IT-lösningar t.ex. mjukvara vid anslutning till SDK

Vissa användarorganisationer samarbetar med ett företag eller en annan kommun som driftar IT för flera kommuner samtidigt. Frågan som då uppkommit är om dessa kommuner behöver ha en egen AP/Meddelandetjänst per kommun/organisation eller finns det någon speciallösning för dem?

SDKs regelverk reglerar inte direkt hur en användarorganisation organiserar sin IT-drift, leverantörer eller mjukvara (t.ex. MT och MK). En förutsättning är dock att regelverk och specifikationer följs. Se Regelverk för anslutning till Säker digital kommunikation - Informationssäkerhet v 1.2 (2022), avsnitt 3.1:

"*En användarorganisation som på annan part har lagt ut utförandet av en eller flera av de åtaganden som omfattas av detta regelverk, ska genom avtal ålägga utförande parten (leverantören) och dess eventuella underleverantörer samma skyldigheter som åläggs användarorganisationen i relevanta delar".*

Kortfattat kan man säga att en användarorganisation kan använda en eller flera valfria leverantörer som levererar, tillhandahåller och förvaltar IT-lösningar som t. ex. Accesspunkt (AP), Meddelandetjänst (MT) och Meddelandeklient(er) (MK) under förutsättning att regelverk och specifikationer följs. Det krävs en säker och lagenlig separering av användarorganisationens information för att vara följsam mot SDKs regelverk.

Några exempel:

- Endast behörig användare skall kunna ta del av användarorganisationens information. *(Källa: 4.1 Åtkomst till information som förmedlas via SDK)*
- Användarorganisationen skall kunna kontrollera att endast behörig användare har tillgång till användarorganisationen information. *(Källa: Regelverk för anslutning 4.1 Åtkomst till information som förmedlas via SDK)*
- Säkerställa konfidentialitet och riktighet mellan anslutande system och accesspunkt, s k inre säkerhet. *(Källa: IT-säkerhetsbilaga till regelverk för anslutning till Säker digital kommunikation - Informationssäkerhet v.1.1 (2022), avsnitt 2.4 Inre säkerhet – skydd mellan anslutande system och accesspunkt)*
- Leverantörens IT-system måste separera varje användarorganisations metadata. *(Källa: Regelverk för anslutning 4.2 Hantering av metadata och adressinformation)*
- Varje användarorganisation skall ha sin egen privata nyckel för kryptering, dekryptering, signering och validering av signatur.

- *“*Kryptografiskt nyckelmaterial som används för skydd av överföring av meddelanden via SDK ska skapas på ett säkert och trovärdigt sätt, samt skyddas vid förvaring och användning så att det inte röjs till obehöriga.*” (Källa: Regelverk för anslutning 5.4 Hantering av kryptografiskt nyckelmaterial)*

- Spårbarhet. *“*En användarorganisation ska säkerställa att alla meddelandeöverföringar via dess lokala komponenter som användarorganisationen är deltagande part i loggas”. *(Källa: Regelverk för anslutning 5.1 Spårbarhet)*