Säker roll- och behörighetsidentifikation

Ulf Palmgren, SKL

Webbseminarium 181114

Bakgrund

- Socialstyrelsens rapport
  - E-hälsa och välfärdsteknik i kommunerna 2018
- Socialtjänsten stack ut gällande
  - Säker roll- och behörighetsidentifikation
- Presentation från 2018-07-09 finns på:
  - https://ehalsa2025.se/2025-podden/e-halsa-och-valfardsteknik-kommunerna-2018/

Socialstyrelsens rapport

E-hälsa och välfärdsteknik i kommunerna 2018

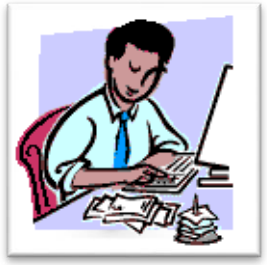
– **Socialtjänstpersonalen har inte** i lika hög utsträckning som hälso- och sjukvårdspersonalen tillgång till **säker roll- och behörighetsidentifikation**.

– När det gäller personal i myndighetsutövningen är det **52 procent** av kommunerna som anger att all personal **använder en säker roll- och behörighetsidentifikation i sitt arbete**

Vad är Säker roll- och behörighetsidentifikation?

Säker roll- och behörighetsidentifikation

– Stark Autentisering (Säker inloggning)
  – Vem du är



– Behörighetsstyrning (Aktiv och behovsprövad)
  – Vad du kan göra

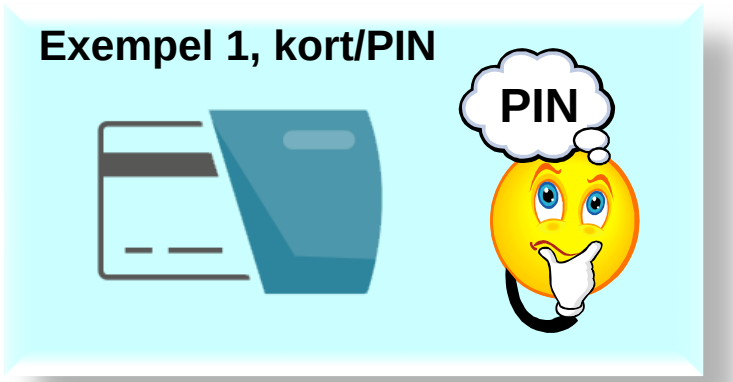
– Åtkomstkontroll (Systematisk loggуppföljning)
  – Uppföljning om du hade behov
  – Även privatpersonen har rätt till loggutdrag

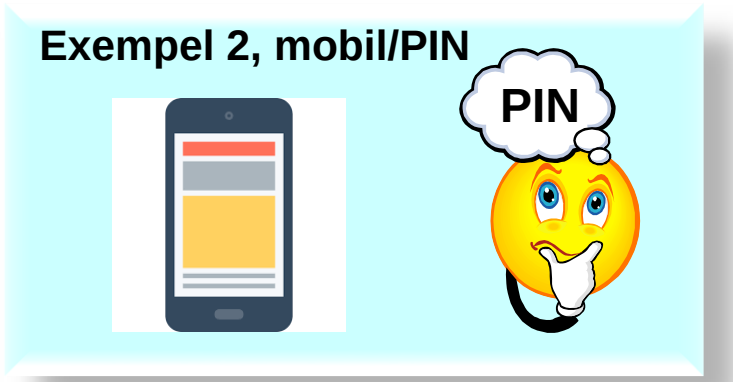
Stark autentisering (Säker inloggning)

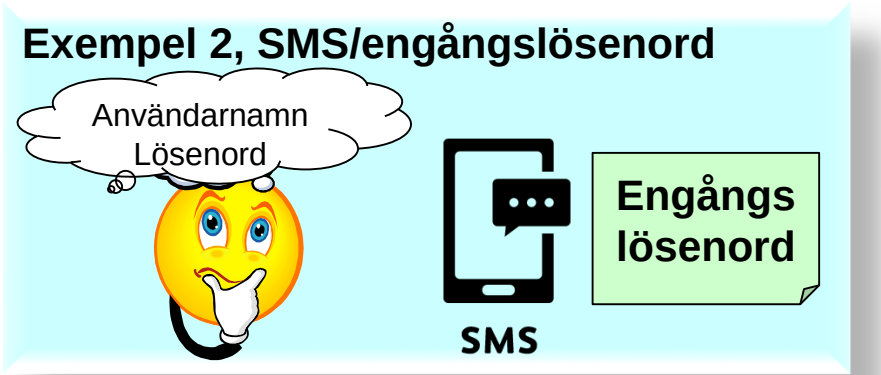
- Om (integritets-) känsliga personuppgifter är åtkomliga över öppet nät, till exempel Internet, **ska användarnas identitet säkerställas med en teknisk funktion som ger en stark autentisering**
- Stark autentisering – ett samlingsnamn för tekniska funktioner som säkerställer en användares identitet genom användarcertifikat, engångslösenord eller motsvarande, det vill säga **mer än enbart användarnamn och lösenord.**
- Om en autentiseringslösning innefattar **fler än en faktor** sägs vanligen att den kan uppnå en **stark autentisering** av användaren.

Stark Autentisering Säker inloggning

- 2-faktors autentisering
  - Två av följande ”faktorer” ska vara uppfyllda:
    - Något du kan (lösenord, PIN-kod)
    - Något du har (eID-kort, dosa, ”skraplott”, telefon/SMS)
    - Något du är (fingeravtryck, röst, retina-scan)







Behörighetsstyrning

– Utgångspunkten är att **behörigheten ska begränsas till vad som behövs** för att användaren ska kunna fullgöra sina arbetsuppgifter.

– Krav på att **organisationen ska ha rutiner** för att tilldela, förändra, ta bort och regelbundet följa upp individuella (tekniska) behörigheter för åtkomst till patientuppgifter.

Artikel 29 Säkerhet i samband med behandling

Sveriges Kommuner och Landsting

– säkerställa att personer som är behöriga att använda ett automatiserat behandlingssystem **endast har tillgång till personuppgifter som omfattas av deras behörighet** (åtkomstkontroll),

– säkerställa att det är möjligt att i efterhand kontrollera och fastställa vilka personuppgifter som förts in i ett automatiserat behandlingssystem, samt **när och av vem personuppgifterna infördes** (indatakontroll),

– förhindra obehörig läsning, kopiering, ändring eller radering av personuppgifter i samband med överföring av sådana uppgifter eller under transport av databärare (*transportkontroll*),

Systematisk logguppföljning

- Informera personalen
  - Informera personalen om att logguppföljning sker, under vilka omständigheter personalen får ta del av uppgifter, att personalen har ett eget ansvar att endast ta del av uppgifter som de behöver i arbetet samt om följderna av att olovligen ta del av uppgifter.
- Kontrollera de tekniska förutsättningarna
- Ta fram rutiner för loggarna genom att bestämma urval och omfattning av loggposterna
  - Fastställ en skriftlig rutin för hur loggposterna följs upp och där urvalet av vilka loggposter som kontrolleras framgår.
- Dokumentera logguppföljningen och följ upp rutinen

Sveriges Kommuner och Landsting

Datainspektionen

Artikel 25 Loggning

Sveriges Kommuner och Landsting

1. Medlemsstaterna ska säkerställa att loggar förs över: insamling, ändring, läsning, utlämning inbegripet överföringar, sammanförande och radering. Loggarna över läsning och utlämning ska göra det möjligt att fastställa motivering, datum och tidpunkt för sådan behandling och i möjligaste mån **vem som har läst eller lämnat ut personuppgifter**, samt **vilka som har fått tillgång till personuppgifterna**.
2. Loggarna bör endast användas för att **kontrollera om behandlingen är tillåten**, för egenkontroll, för att säkerställa personuppgifternas integritet och säkerhet, samt inom ramen för straffrättsliga förfaranden.

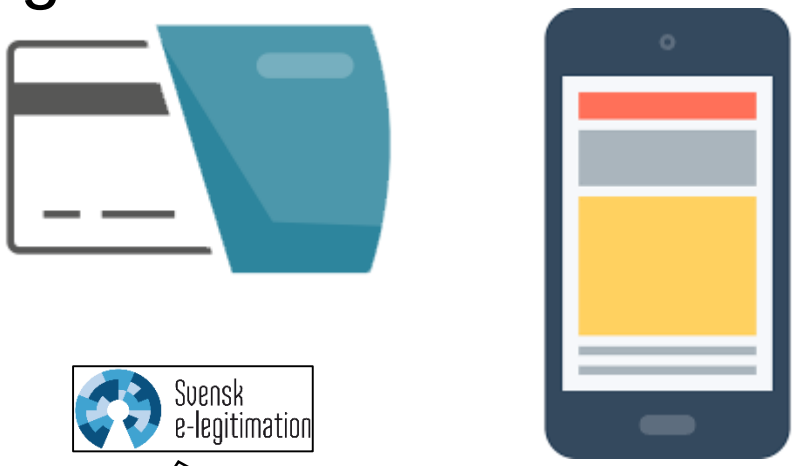
Vilka lösningar finns idag?

Verksamhetens önskemål:
En säkerhetslösning, inte många…

- Användarnamn lösenord
- Sms
- Dosor
- E-tjänstelegitimation
- Privat e-legitimation

Vad kan vi göra idag?

Se till att E-legitimationer i tjänsten uppfyller Svensk e-legitimation



Godkänd av E-legitimationsnämnden som utfärdare av Svensk e-legitimation

Fördelar

– Alla uppfyller ett gemensamt tillitsramverk för e-leg

– Möjliggör att kunna ingå i federationer

– E-legitimationer som uppfyller kraven kan notifieras för eIDAS.

– Komplettera gärna med leverantör av eID-tjänst för privat användning

Inera: Säker inloggning

- SITHS-kort
  - Dagens lösning med ID-Kort försett med e-legitimation
- EFOS (E-identitet för offentlig sektor)
  - Tillsammans med myndigheterna morgondagens gemensamma lösning
    - Ersätter både SITHS-kortet och myndigheternas MCA-kort
- Mobilt EFOS
  - Inera kommer att leverera en mobil lösning som gör det möjligt för en användare att logga in i e-tjänster med mobiltelefoner och surfplattor.