Beskæftigelses-
ministeriet

Peter Anton Sørensen
Chefkonsulent
27. September 2022.

mTime som "betalingsafledende system"

Oplæg på erfa-dag 28. september

Peter Anton Sørensen
Helle Randholm
Connie Christiansen
Kristian Malte Andersen

Baggrund -

Britta sagen -> nye fællestatslige krav for at undgå svig

- Marts 2021 – nye retningslinjer – 17 krav
- Alle statslige ”betalingsafledende” systemer
- Kravene vil primært ”vil gøre sig gældende ved videreudvikling af eksisterende systemer eller ved anskaffelse af nye systemer”.
- ”Minimumskravene vil forventeligt finde anvendelse ved IT-revision af betalingsafledende systemer og bør endvidere danne udgangspunkt for dialog mellem myndighed og leverandør om nye og eksisterende systemer.”
- Fire typer krav: Lovkrav, systemkrav, applikationskrav, tekniske krav.
- Krav operationaliseret i ”referenceimplementering”

Hvad er et betalingsafledende system?

Et system:

- Der afleder udbetalinger, enten direkte eller ved understøttelse af en eller flere delprocesser, herunder håndtering af stamdata,
- Der sikrer, at der effektueres en udbetaling fra et andet system længere fremme i den samlede udbetalingsproces.
- Omfatter tidsregistreringssystemer, der danner grundlag for en udbetaling af løn eller over/merarbejde.

- mTime i BM:
  - Ingen direkte udbetalinger eller direkte overførsel af eventuelle udbetalinger fra mTime til lønsystemet (SLS).
  - På baggrund af chef-godkendte registreringer i systemet trækkes data, der danner grundlag for eventuelle udbetalinger via SLS.
  - Fx timeløn til studentermedhjælpere, over-/merarbejdsudbetalinger, ulempegodtgørelse, ferietilgodehavender.
  - Data, der danner grundlag for løntræk, fx ifm. afholdelse af ferie uden ret til ferie med løn og tjenestefrihed uden løn af kortere varighed.

Arbejdet med minimumskravene

Proces:

- Arbejdsgruppe med TMS, Økonomistyrelsen (ØS), Erhvervsministeriet, Udlændinge- og Integrationsministeriet
- De fleste ministerier repræsenteret ved HR-afdeling
- Første halvår 2022
- Udfyldelse af tilsynsskema fra ØS med BM som case – de tre øvrige ministerier laver selv lokale tilpasninger
- Opdeling i ministeriets bemærkninger og leverandørens
- 17 minimumskrav – men risikobaseret tilgang?

Formål med oplæg i dag:

- Genvej for andre ministerier
- Mulighed for at validere resultat
- -> Slavisk gennemgang af resultat for de 17 punkter

Lovkrav

Regnskab og databeskyttelse

1. Regnskabslovgivning

- Rigsrevisorloven - opfyldt
  - RR er bekendt med mTime og har tidligere revideret det - opfyldt.
- Regnskabsbekendtgørelsen – opfyldt – NB: Ikke udbetalingssystem)
  - §21.2 Instruks
  - §24 Funktionsadskillelse
  - §25 Registreringens omfang
  - §27 Dokumentation
  - §28.2 Kontrol
  - §44 Opbevaring – tid
  - §45 Opbevaring - lokalitet

2. Databeskyttelseslovgivning

- Fokus på registreredes rettigheder (art. 12-22) og og sikkerhed (art. 32).
- Oplysningspligt håndteres ved siden af systemet - opfyldt.
- Data kan rettes og slettes - opfyldt.
- Videregivelse: Data videregives kun til SAM og BM - styrelser indenfor det oprindelige formål - opfyldt.
- Ingen registrering udover til det oprindelige formål – opfyldt.
- Systemsikkerhed håndteres gennem DB-aftaler, tilsyn med leverandører, ISAE 3000 erklæring. Der er lavet cpr-sløring - opfyldt.
- Test og udvikling skal indgå i DB-aftale og risikovurdering.

Systemkrav

Påvirker ikke funktionalitet, men bidrager til sikkerhed omkring adgangen

- 3. Restriktiv adgangsstyring
  - *Passwords* opfyldt - håndteres gennem Statens It's single sign on løsning – ØS har vurderet, at det er tilstrækkeligt.
  - *Autorisationskrav* - ikke opfyldt.
  - BM har politik for adgangsstyring og opdelte rettigheder – fx i forhold til at tildele rettigheder.
  - Men: Administratorer kan godkende egne og andres timer uden yderligere godkendelser ->
  - Enten løsning gennem integration til SLS med mulighed for kontrol eller udvikling af særskilt funktionalitet.
- 4. Pålidelig backup opfyldt gennem Statens It's (som Navision Stat).
- 5. Sikring af adgang til kildekode opfyldt. Ingen kunder har adgang. TMS: Udviklingsmetodikker (GIT og JIRA) sikrer begrænsning og versionsstyring.
- 6. Sammenhængende systemdokumentation opfyldt. ISAE 3000 erklæring dækker ændringsstyring. TMS: Kunder kan følge egne udviklingssager, ændringer og kendte fejl i release notes, brugervejledninger opdateres løbende.
- 7. Robust RPA (robotprocesautomatisering) implementering: Ikke relevant.

Applikationskrav

Design af system i forhold til transaktionssporbarhed, funktionsadskillelse og kontrol

- 8. Påkrævet logning - opfyldt. Dækket af ISAE 3000 erklæring. Alle logningskrav er relevante. ”Udbetalingsdata” = tidsregistreringer.
- 9. Transaktionsspor - opfyldt. ”Stempling” af alle transaktioner med id. TMS: Opfyldt i systemet og i SLS-integration, hvis tilkøbt.
- 10. Datakonsistens og låsning, fx godkendte data skal ikke kunne ændres – opfyldt. TMS: Opfyldt i systemet og i SLS-integration, hvis tilkøbt.
- 11. Ingen undtagelser fra produktstrategien. Uafklaret/ikke opfyldt. Dialog med ØS udestår. TMS vil overveje at ændre i change request.
- 12. Tvungen funktionsadskillelse. Ikke opfyldt, jf. punkt 3.
- 13. End to end udbetalingskontrol. Opfyldt. BM udfører kontroller på baggrund af lønkontrolplan ud fra systemets rapporter.
- 14. Sikker udbetaling via Nemkonto. Ikke relevant.

Tekniske krav

Beskyttelse mod cyberangreb og lignende

- 15. Overholdelse af 20 tekniske minimumskrav - nuværende. Opfyldt. Patchning af operativsystem håndteres af Statens It, applikation af TMS.
- 16. Kryptering af betalingsdata ved udveksling. Opfyldt. Integration til SLS opfylder ØS standarder.
- 17. Blokering for SQL-injektion. Opfyldt. TMS laver screeninger for SQL injections.

Spørgsmål?