Hur AMS ersatte lösenord med smarta kort

eller

Den vilda jakten på lösenorden

Om AMS/AMV

- Arbetsmarknadsstyrelsen är huvudmyndighet i Arbetsmarknadsverket som förutom AMS består av 21 stycken länsarbetsnämnder
  - Totalt ca. 10500 anställda
  - 350 kontor från Karesuando i norr till Ystad i söder
- AMS IT-enhet är ansvarig för all IT-verksamhet inkl. utveckling och drift
  - 315 anställda plus 65 konsulter
  - 15000 klientdatorer (Windows)
  - 5000 servrar (Solaris, Linux, Windows)
- Från årsskiftet en myndighet - Arbetsförmedlingen

Om mig

- Ansvarig för IT-enhetens Säkerhetsstab
  - Säkerhetsstaben är ansvarig för IT-säkerheten på IT-enhet och deltar också i övergripande IT-säkerhetsarbete inom AMV
- Arbetat med smarta kort sedan 1985 och PKI sedan 1991
- Deltagit i flera standardiseringsarbete runt säkerhet och smarta kort, både nationellt och internationellt
- Just nu bl.a. medlem i ett EU-projekt som syftar till att skapa en gemensam syn på och teknisk lösning för elektronisk identifiering av EU-medborgare

Våra lösenord

- En normal AMV-användare har 5-10 lösenord som skall memoreras och bytas med jämna mellanrum
- Administrativ personal har ännu fler och personalen på IT-enheten har massor
- Vi byter (bytte!) minst ett hundratal bortglömda lösenord varje dag med mer eller mindre säkra rutiner
- Många användare uppfattar inte lösenorden som speciellt känsliga och delar gärna med sig av dem
- Våra lösenorden är med andra ord jobbiga, dyra och mycket osäkra

Tjänstekortsprojektet

- 2003 tog vår dåvarande generaldirektör beslut om införande av Tjänstekort
- Korten skulle användas för inloggning och visuell identifiering
- Efter en del initiala tester tog det hela fart våren 2005
- Sommaren 2007 hade 11000 kort delats ut och används nu dagligen för inloggning
- Huvudsakliga drivkrafter har varit (i nämnd ordning)
  1. GD-beslutet
  2. Säkerhet
  3. Enkelhet för användarna
  4. Kostnadsbesparingar

Nuläge

- Alla våra (interna) användare har ett Tjänstekort
- Det är obligatoriskt att använda kort vid inloggning i vår Windowsproduktionsdomän
- Ett par hundra användare som använder fem trasslande applikationer är fn. undantagna
  - Alla undantag skall vara rensade senast vid årsskiftet
- Ett tjugotal webbbaserade applikationer får sin identifiering via tjänstekortet och en SSO-lösning
- Det mesta fungerar rent tekniskt och det är få supportärenden

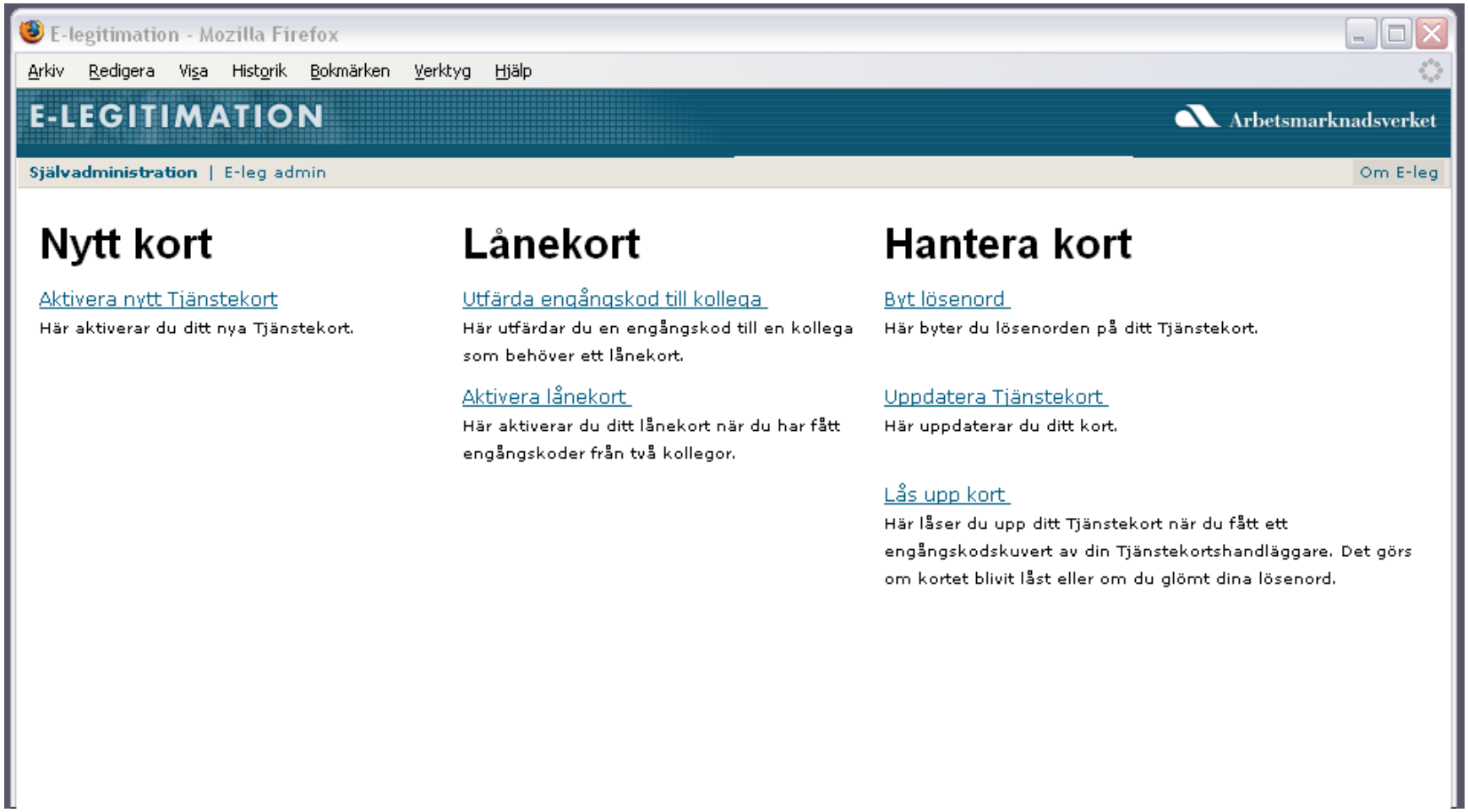
Kortutgivningsprocessen

- SIS-kortsprocessen (SBC 151) är grunden för vår utgivningsprocess och all korthantering sker enligt denna
- Vi har 72 Tjänstekortshandläggare utspridda i landet och som oftast är knutna till personalavdelningen
- De flesta beställningar sker helt elektroniskt direkt till Setec
- Kort levereras till handläggaren senast en vecka efter beställning
- Korten levereras med enbart förgenererade RSA-nycklar och en grundläggande PKCS-15 struktur
- Kortens PUK-koder levereras till oss centralt och användarna får inga PIN- eller PUK-koder

Kortutgivningsprocessen, forts.

- Tillsammans med kortet knyts och delas ett engångskod-kuvert ut till användaren av en Tjänstekortshandläggare
- På godtycklig klientdator loggar användaren in som Gäst och går in på http://eleg.ams.se
- Användaren anger sitt personnummer, engångskod (från kuvertet) och väljer själv PIN-koder till kortet
- Kortet laddas med certifikat och är sedan klart att använda
- Låsta kort följer samma strikta process, dvs. användaren måste besöka en Tjänstekortshandläggare och få ett engångskodkuvert
  - Kan även skickas ut med rekommenderat brev
- Lånekort kan utfärdas tillfälligt och med lägre krav på identifiering

Mycket självadministration



Nästa steg

- Vi håller på att testa en lösning för applikationer som inte klarar vår webb-SSO
  - Varje klientdator har en agent som hanterar användarens id/lösen
  - Agenten krypterar id/lösen med användarens Tjänstekort
  - Id/lösen skickas ut centralt och hanteras aldrig av användaren själv
  - Lösenorden är långa och slumpmässiga och behöver inte bytas
- All konto- och behörighetshantering centraliseras i en gemensam IdM-lösning
  - Lösenord ”skjuts” ut till applikationer och användarna
- Kerberosbiljetter baserade på identifiering med Tjänstekortet
  - Kan användas för inloggning av administratörer i Solaris och Linux
- Federerade identiteter
  - Samarbete med andra svenska myndigheter och inom EU

Erfarenheter från vårt Tjänstekortsprojekt

- Genom att kräva kortinloggning i Windows har vi skapat en naturlig daglig användning av Tjänstekortet
- SIS-stämpeln gör att användarna håller i sina kort
- Anpassade administrativa rutiner har väsentligt förenklat införandet och acceptansen
- Vi har nu lagt ribban för nya applikationer, dvs. de måste fortsättningsvis anpassa sig till Tjänstekorten
- GD-beslutet var vårt ”carte blanche”
- Vi skulle slagit på kortkravet i takt med att användarna fick kort
- Allt har tagit längre tid än planerat men det har nödvändigtvis inte varit en nackdel
- Till synes enkla tekniska koncept kan ändå upplevas svåra för en vanlig användare
- Man kan aldrig informera för mycket!!!

AMS och identiteter på nätet

- AMS är en stor producent av elektroniska tjänster
- Vi har Sveriges elfte mest besökta webbplats
- Fram till i våras har endast användarnamn och lösenord använt för identifiering
- Numera även e-legitimationer (BankID, etc.) samt ID-matris
- För att kunna vidareutveckla våra e-tjänster är vi i stort behov av elektronisk identifiering som
  - Är enkel för våra användare
  - Fungerar i många miljöer
  - Är spridd bland våra användargrupper
  - Har en förutsägbar kostnad
  - Vi inte behöver administrera själva

E-legitimationer i Sverige

- Staten har sedan mitten av 90-talet upphandlat e-legitimationer för användning i myndighetstjänster
- Fokus har flyttats från en ren teknisk upphandling av PKI-certifikat till mer inriktat på e-legitimering som tjänst
- Nuvarande ramavtal går ut sista juni nästa år och planeras att ersättas av en ny upphandling med identiska krav
- Det finns dock flera frågor som är aktuella
  - Skall svenska staten själva vara utgivare av elektroniska legitimationer för svenska (!) medborgare?
  - Skall ramavtalskonstruktionen ersättas av ackreditering?
  - Hur kan man utnyttja en gryende identifieringsmarknad?
  - Måste vi ha ”banksäkerhet” i våra myndighetstjänster?

Gemensam elektroniskt ID inom EU

- Inom ramen för IDABC (http://ec.europa.eu/idabc) driver EU-kommisionen ett projekt som syftar till att underlätta ”cross-border” identifiering
- Tanken är att en EU-medborgare skall kunna utnyttja en myndighetstjänst i godtyckligt land med ”godtyckligt” identifieringsinstrument
- Arbetet är just påbörjat och en inventering och problem-identifiering pågår, t.ex.
  - Skall medlemstaterna ge ut de olika identifieringsinstrumenten?
  - Kan man skaffa ett identifieringsinstrument i godtyckligt EU-land?
  - Hur hanterar och kvantifierar man olika säkerhetsnivåer?
  - Hur går det hela till rent tekniskt?
  - Hur gör man om en identifiering ställer tekniska krav på användaren?

Frågor

hakan.z.persson [at] ams.amv.se