Sagsnr. 1-30-82-2-11
Udbudsmateriale - Offentlig udbud
Udbud af Region Midt tilkobling til Interregionalt Billedindeks
Bilag 2.9

Præsentation af BSK – regionens identity and access management platform

Dato 28-05-2010
JakobBækgaard Riis
Programleder BSK
Tel. +45 29 13 58 61
Version 3.0

BrugerStamdataKataloget (BSK) er regionens centrale it-løsning til håndtering af adgange til regionens fælles it-systemer.

BSK skal bl.a. være med til at sikre rettidig, effektiv bruger-administration og øget sikkerhed.

Visionen er, at BSK på baggrund af viden om medarbejderens rolle og organisatoriske tilknytning automatisk tildeler en række adgange til it-systemer, som medarbejderen kan tage i brug allerede på første arbejdsdag. Når en medarbejder forlader Region Midtjylland, skal BSK tilsvarende sikre, at medarbejderens systemadgange lukkes.

Alle medarbejdere i regionen er registreret i BSK og har dermed et regionsID. regionsID består af et brugernavn og en adgangskode, og anvendes i en række af regionens fælles it-systemer hvorved der opnås simplified logon (ét brugernavn og ét password).

Visionen med BSK

- at personale- og medarbejderinformation kun registreres én gang
- at nyt personale har adgang til alle de it-systemer de skal anvende, første dag de møder på deres nye arbejdsplads
- at personale altid har adgang til de nødvendige it-systemer og de rigtige rettigheder, der hvor de arbejder, også selv om de er ansat flere steder i organisationen
- at personale- og medarbejderinformation kun vedligeholdes af kilden (dataejer)
- at samtlige registrerede informationer til enhver tid er korrekte, opdaterede, dækkende, dokumenterede og tilgængelige for netop de systemer og parter der skal anvende dem

Programmål for BSK

- at igangsætte og videreføre de organisatoriske processer, der er nødvendige for at opfylde programmets visioner og formål
- at signalere at Region Midtjylland er én organisation

- at synliggøre opbygningen af en fælles identitet i Region Midtjylland

BSK data

BSK registrerer data om den enkelte bruger, herunder:

- Stamdata
  - regionsID
  - CPR
  - Stilling
- Kontaktinformation
  - Mail
  - Telefon
- Organisatorisk tilknytning i andre systemer
  - Lønsystem
  - ESDH

BSK vil på sigt også kunne levere data om de organisatoriske enheder, brugeren er tilknyttet, herunder:

- Ledelse
- Kontaktinformationer
  - Adresser
  - Telefonnr
  - Webadresse
  - Outlook funktionspostkasse
- Andre stamdata, fx
  - EAN nr
  - ØS afdelingsnumre
  - SKS koder

Det tekniske

BSK er en hændelsesbaseret platform som tilbyder en række standard snitflader til synkronisering af stamdata, både dem som gælder for brugeren af selve systemet, men også fagsystemets stamdata om medarbejderne.

Platformen tilbyder høj tilgængelighed, fejltolerant setup og god performance. Databasen understøtter eventstyret synkronisering helt ned til attributniveau som sammen med den unikke replikeringsteknologi sikre en meget effektiv skalerbarhed.

Standardsnitflader som BSK tilbyder til autentifikation (navn/password validering) og eventuel autorisation:

- SOAP service; BSKAuth se vedlagte bilag WebService LoginModule (BSKAuth) og WebService LoginModule (BSKAuthNSP)
- LDAP
- Synkronisering af navn/password (såfremt password bliver forsvarligt krypteret), øvrige brugerstamdata, autorisationer og data i øvrigt til applikationsdatabase gennem nedenfor nævnte snitflader.

Standard integrationer (synkroniseringssnitflader) er lavet til mange applikationer, og indenfor HR systemer kan nævnes PeopleSoft og SAP HR. Men udover de standardiserede integrationer benytter BSK sig af såkaldte ”drivere”, som kan forbinde til applikationen på forskellige måder. Der kan nævnes følgende (udsnit):

Databaser

IBM DB2, Informix, Microsoft SQL Server, MySQL, Oracle, Sybase, JDBC

Directories

Critical Path InJoin Directory, IBM Directory Server (SecureWay), iPlanet Directory Server, Microsoft Active Directory, Microsoft Windows NT Domain, Netscape Directory Server, Novell eDirectory, Oracle Internet Directory, Sun ONE Directory Server, LDAP

Scripting Systems

Scripting Driver, Scripting Open Source Scripts Overview, sasldb Integration Scripts, Scripting Driver Scripts - Google Apps Driver, Windows Domain/Local Account Scripts, Exchange 2007 Scripts

Andre

Delimited Text, Health Level 7 (HL7), DSML, Schools Interoperability Framework (SIF), SOAP, SPML, XML

Valget af integrationssnitflade afhænger at mange forskellige forhold, som vil være for omfattende at udarbejde en standard tjekliste for. Derfor afholder BSK programmet forud for igangsætning af integrationen, en screeningsproces sammen med system leverandøren. Vi anbefaler altid at gennemføre en screening af nye systemer inden regionen beslutter sig for at underskrive kontrakt på et nyt system. Screeningfasen kan normalt gennemføres inden for en uge, og kræver involvering af systemejer (3-5 timer), system leverandøren (2-3 timer) og BSK repræsentanter.

Bilag - WebService LoginModule (BSKAuth)

Navn

Web Service: LoginModule
Metode/operation: BSKLogin

Formål

Formålet med metoden er at kunne få verificeret et brugernavn og password, og kunne hente en brugers adgange til alle eller et specifikt system.

Tilgang

Metoden stilles til rådighed via HTTP transport protokol over en sikker forbindelse (SSL). Der anvendes XML-baseret SOAP protokol, så kommunikationen sker via XML. Service description sker via generet WSDL.

Kriterier

Følgende søgeparameter skal angives:

XML navn	Beskrivelse
Username (String)	Brugerens Username
Password (String)	Brugerens Password
System (String)	Angivelse af et specifikt system

System kan være blankt, hvilke vil medføre at alle brugerens rettigheder vil blive returneret.

Udtræksfelter

Følgende Udtræksoplysninger dannes:

XML navn	Beskrivelse
Status (int)	Angiver om brugeren er verificeret eller ej. • 1 = Login ok • 3 = Login ok. Password skal skiftes inden for ”PasswordDays” dage. • 7 = Login ok, Gracelogins. • 8 = Login fejlede = Username eller password forkert. • 16 = Login fejlede = Account Locked • 128 = Anden fejl som f.eks. webservice kan ikke kontakte BSK.
StatusMessage (String)	Dansk tekst, som beskriver evt. fejl, skal benyttes såfremt status ikke er 1, dette sikre en ensartet dialog med brugerene uanset applikaiton.
RoleScope (String[])	En liste af roller og på hvilket niveau rettigheden er

	givet. Såfremt listen er tomt har personen ingen rettigheder til det pågældende system og vil derfor normalt skulle nægtes adgang.
PasswordDays(int)	Antal dage til password skal skiftes, kun relevant såfremt Status er 3.
PasswordGrace(int)	Antal Gracelogins tilbage, kun relevant såfremt Status er 5.
PasswordChangeURL (String)	URL til password skifte, såfremt bruger manuelt skal skifte password via redirect. Istedet for denne URL ønskes nedenstående ChangePassword metode benyttet, således password skifte virker ”seemless” i applikationen.

Bilag - WebService LoginModule (BSKAuthNSP)

BSKAuth SOAP servicen er udvidet med 3 ekstra metoder: LoginNSPASync, LoginNSPSync, GetSAMLTicketID. LoginNSPASync er beskrevet nedenfor, øvrige kan rekvireres efter behov.

Formål

Formålet med metoden er at kunne få verificeret et brugernavn og password, og kunne hente en brugers adgange til alle eller et specifikt system. Derudover genereres der en BSKTicketNSP til bruge i metoden GetSAMLTicketID. Ved godkendt login startes en ny asynkron process som kommunikerer med SOSI gatewayen og får dannet en SAMLTicket og SAMLTicketID, denne kan hentes via metoden GetSAMLTicketID. Der returneres til det kaldende system lige efter godkendt login, og der ventes derfor ikke på generering SAMLTicket.

Denne metode er tiltænkt brugt hvor man har behov for hurtig login uden afventning på generering af SAMLTicketID på SOSI gateway.

Tilgang

Metoden stilles til rådighed via HTTP transport protokol over en sikker forbindelse (SSL). Der anvendes XML-baseret SOAP protokol, så kommunikationen sker via XML. Service description sker via generet WSDL.

Kriterier

Følgende søgeparameter skal angives:

XML navn	Beskrivelse
Username (String)	Brugerens Username
Password (String)	Brugerens Password
System (String)	Angivelse af et specifikt system.

System kan være blankt hvilke vil medføre at alle brugerens rettigheder vil blive returneret.

Udtræksfelter

Følgende Udtræksoplysninger dannes:

XML navn	Beskrivelse
Status (int)	Angiver om brugeren er verificeret eller ej. • 1 = Login ok • 3 = Login ok. Password skal skiftes inden for ”PasswordDays” dage. • 7 = Login ok, Gracelogins. • 8 = Login fejlede = Username eller password forkert. • 16 = Login fejlede = Account Locked • 128 = Anden fejl som f.eks. webservice kan ikke kontakte BSK. • 512 = Login OK, men bruger har ikke Digital Signatur.
StatusMessage (String)	Dansk tekst, som beskriver evt. fejl, skal benyttes

	såfremt status ikke er 1, dette sikre en ensartet dialog med brugerene uanset applikaiton.
RoleScope (String[])	En liste af roller og på hvilket niveau rettigheden er givet. Såfremt listen er tomt har personen ingen rettigheder til det pågældende system og vil derfor normalt skulle nægtes adgang.
PasswordDays(int)	Antal dage til password skal skiftes, kun relevant såfremt Status er 3.
PasswordGrace(int)	Antal Gracelogins tilbage, kun relevant såfremt Status er 5.
PasswordChangeURL (String)	URL til password skifte, såfremt bruger manuelt skal skifte password via redirect. Istedet for denne URL ønskes nedenstående ChangePassword metode benyttet, således password skifte virker "seemless" i applikationen.
BSKTicketNSP	ID generet af BSK til senere forspørgsel via metoden GetSAMLTicketID.
BSKTicketNSPTimeOut	Tidsstempel for hvornår BSKTicketNSP udløber
NSPTicketServerName	Hvilken NSP platform har udstedt SAMLTicket og herunde SAMLTicketID. (Multivalue)

Flow