



IT- og Telestyrelsen

Ministeriet for Videnskab
Teknologi og Udvikling

Anbefaling til unik Id-nøgle

Kolofon:

OIO Referencemodel for tværgående brugerstyring

Denne anbefaling kan frit anvendes af alle. Citeres fra anbefalingen i andre publikationer til offentligheden skal angives korrekt kildehenvisning.

Forslag til anbefalinger for tværgående brugerstyring udarbejdes af IT- og Telestyrelsen, IT-strategisk kontor, som sekretariat for OIO It-Arkitekturkomiteen.

Kontaktperson:

It-Arkitekt Søren Peter Nielsen, email: spn@itst.dk

Telefon 25 67 07 83 (direkte)

It-Arkitekt Anders Dalsgaard, email: ada@itst.dk

Telefon 25 65 32 08 (direkte)

Ministeriet for Videnskab, Teknologi og Udvikling

IT- og Telestyrelsen

IT-strategisk kontor

Holsteinsgade 63

DK-2100 København Ø

Telf. +45 35 45 00 00

Fax. +45 35 45 00 10

<http://www.itst.dk>

itst@itst.dk

Indholdsfortegnelse

1	Indledning.....	4
1.1	Opsummering.....	4
1.2	Formål	4
1.3	Baggrund for anbefaling	4
1.4	Anvendelsesområde	5
2	Nuværende situation.....	6
3	Forudsætninger.....	7
4	Baggrund - XRI.....	8
5	Anbefalet opbygning af unik id-nøgle generelt.....	9
6	Anbefalet opbygning af id-nøgle til borger med OCES certifikat.....	10
7	Eksempler	11
8	Appendix A – Information om XRI	14
9	Appendiks B - Yderligere information.....	15

1 Indledning

At kunne identificere en bruger entydigt er af afgørende betydning for sikkerhed i it-systemer. Både mht. autentifikation, sporbarhed og kobling af data på tværs af systemer.

Der vil i mange situationer være behov for en såkaldt id-nøgle, som kan sammenknytte information om en given bruger i en given kontekst. Samtidig skal den samme person kunne optræde som it-bruger i forskellige sammenhænge med forskellige id-nøgler.

Denne anbefaling omhandler en sådan id-nøgle.

1.1 Opsummering

I dette dokument anbefales det, at man anvender en standard til oprettelse af en entydig id-nøgle til identifikation af et datasæt med brugerinformation. Standarden skal bygge på XRI, som står for 'Extensible Resource Identifier'.

Den anbefalede standard muliggør, at man på tværs af systemer/organisationer kan garantere, at den id-nøgle, man kobler til sine brugere, er unik og entydig.

Anbefalingen skal ses som et alternativ til eksisterende metoder som f.eks. anvendelse af CPR-nummer, der har den uheldige omstændighed, at det kan henføres direkte til en person og ikke kan indskrænkes til kun at kunne anvendes i en given kontekst.

1.2 Formål

Formålet med en unik id-nøgle er at identificere brugere entydigt på tværs af it-systemer og tid dvs. sporbarhed samt at kunne udveksle information om brugere. Denne vejledning har til formål at hjælpe systemejere til at lave en arkitektur baseret på en unik id-nøgle, således at brugere kan identificeres entydigt på tværs af systemer og tid. Kravet om entydighed på tværs af tid sikrer, at id-nøgler ikke genbruges og dermed altid vil kunne benyttes til at identificere en bruger entydigt. Anbefalingen er tænkt som et supplement og i nogle tilfælde som et muligt alternativ til eksisterende metoder.

1.3 Baggrund for anbefaling

It-brugere er i dag typisk registreret i flere forskellige systemer, uden at der altid er nogen konsistent måde til at fastslå, om forskellige brugerkonti repræsenterer den samme bruger. I nogle tilfælde er det muligt at anvende brugerens CPR-nummer til at matche forskellige brugerkonti, fordi CPR-nummeret er garanteret unikt.

Imidlertid kan samme person være registreret i it-systemer i forskellige sammenhænge, der ikke har noget med hinanden at gøre. Eksempler på forskellige sammenhænge en bruger kan være registreret i, er: som borger, som ansat med et givet sæt jobfunktioner og som vikar i en anden organisation med et andet sæt jobfunktioner.

Det er således ikke muligt altid at sammenknytte brugerinformation ved hjælp af CPR-nummer; dels fordi det i nogle situationer kan være i konflikt med persondataloven, dels fordi anvendelse af CPR-nummer ikke i sig selv gør det muligt at afgrænse sammenknytningen af brugerinformationer til de data, der vedrører en given kontekst for brugeren (fx som *borger* eller *sagsbehandler i en socialforvaltning* etc.)

1.4 Anvendelsesområde

Den anbefalede unikke id-nøgle vil primært være rettet mod at koble en unik id-nøgle til brugere, der oprettes i organisationers brugerkataloger. Føres denne id-nøgle med over i globale/lokale it-systemer, som brugeren får adgang til, kan man sikre, at data hørende til den enkelte bruger kan kobles på tværs af systemer. Endvidere vil anvendelsen af denne unikke id-nøgle i loggen til it-systemer kunne sikre sporbarhed, såfremt dette skulle blive nødvendigt.

Sporbarheden forudsætter dog, at den udstedende organisation sikrer en kobling mellem bruger og person.

2 Nuværende situation

Ved autenticitetssikring af en bruger i et it-system anvendes traditionelt en eller flere af følgende data:

- CPR-nr.
- Bruger-id/initialer
- Digital signatur
- Identifikation ud fra en profil bestående af attributter

Disse data kan/skal anvendes til at matche information/data på tværs af systemer hørende til den samme bruger.

CPR-nummer er unik mht. personer inden for Danmarks grænser. Det knytter sig ikke til ansættelsesforholdet men udelukkende til personen. Anvendelse af CPR-nummer kan være privatlivskrænkende i forbindelse med borgernes adgang til systemer. Her er det vigtigt, at de enkelte it-systemer overholder persondataloven, og at CPR-nr. ikke kompromitteres.

Bruger-id/initialer er ikke unikke på tværs af systemer eller over tid. Ofte genbruges disse, hvilket vanskeliggør sporbarhed. Hvis forskellige systemer anvender forskellige bruger-id'er for samme bruger, er det en vanskelig opgave at koble brugere fra forskellige systemer samt at identificere personer ud fra en log.

Digital Signatur giver entydighed inden for den enkelte udbyder. Ved flere udbydere skal udbyderens id inkluderes, for at certifikatet er unikt, og en entydig identifikation af brugeren derved kan sikres. Teknologien bag Digital Signatur er ikke låst, hvilket kan give udfordringer på sigt, hvis teknologien ændrer sig. Specielt vil flere udbydere give udfordringer på sigt.

Identifikation ud fra en profil kan give entydig identifikation af en bruger afhængigt af profilens indhold. Der findes pt. ingen standardprofil til identifikation. Dvs. at det er op til det enkelte it-system at lave egne regler for identifikation.

Alle fire metoder anvendes i dag til at autenticitetssikre personer i it-systemer. Med personer menes her både borgere i det danske samfund og offentligt ansatte.

Brugere af it-systemer på tværs af organisationer afføder et behov for oprettelse af en unik id-nøgle, der kan koble brugerkonti på tværs af systemer, domæner etc. Hvis der til hver bruger evt. i et givet ansættelsesforhold, knyttes en unik id-nøgle, vil denne kunne anvendes til entydigt og nemt at identificere den pågældende bruger og ikke mindst sikre sporbarhed i loggen.

3 Forudsætninger

Ved udveksling af data mellem it-systemer vedr. brugeroplysninger kan der f.eks. benyttes SAML 2.0, som anbefalet i OIO-Kataloget over offentlige it-standarder.

Den SAML 2.0-profil, der beskriver en bruger, vil ofte have behov for at indeholde en unik id-nøgle. Dette kan være et CPR-nummer, et certifikat hørende til digital signatur eller evt. en ny unik id-nøgle.

Et unikt id oprettes samtidig med oprettelsen af brugeren i kataloger som f.eks. LDAP og ikke samtidig med oprettelse af personen. Det er underordnet, om der er tale om en borger eller en medarbejder. Hvis dette unikke id følger brugeren, vil personen altid kunne identificeres entydigt. Ved provisionering til andre systemer vil data og brugerinformation kunne kobles til anvendelse af dette unikke id.

4 Baggrund - XRI

Som unik id-nøgle anbefales anvendelsen af XRI. XRI står for 'Extensible Ressource Identifier'. Den er udviklet af 'OASIS XRI Technical Committee'. XRI giver en standard syntaks- og løsningsprotokol for abstrakte identifikatorer, som er uafhængig af lokation, system, protokol, domain, ejer, autoritet etc.

XRI opdeles i tre forskellige kontekstområder svarende til, hvorledes det enkelte XRI navngives. Der anvendes tre forskellige symboler hørende til de tre forskellige kontekstområder:

Type	Globalt kontekst	Global Kontekst Symbol	Eks. I-Names	Eks. I-Number
Person	Individer	=	=Mary.Jones.Smith	=:2D37.90C1.FA48
Forretning/ Organisation	Alle former for organisationer	@	@Johnson.Brothers	@:1057.A22C.4E83
Generel	Generelle koncepter, emner, items	+	+printer +printer/HP1100	+:2640 +:2640/:3364

'Global Kontekst Symbol' benyttes til at definere den abstrakte globale kontekst af en autoritet.

Vi betragter udelukkende I-Names i dette dokument.

Se Appendix A for yderligere information eller læs om anvendelse og definition af XRI, ver. 2.0 på:

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xri

5 Anbefalet opbygning af unik id-nøgle generelt

Princippet i opbygningen af id-nøglen består af følgende led:

- Identifikation af landetilknytningen for organisationen, der opretter brugeren
- Identifikation af den oprettende organisation via CVR-nummer
- Et tidsstempel
- Identifikation af den enkelte bruger ved udstedende organisations egen systematik

På landsplan registreres et XRI I-Name, her kaldet xri://@DK-XRI af Videnskabsministeriet eller anden passende myndighed. @DK-XRI kan opløses til et I-NUMBER, men dette er ikke aktuelt i forhold til denne anbefaling.

Alle xri, der anvendes i dette regi, skal således starte med xri://@DK-XRI. Dette sikrer, at de unikke identifikatorer, der oprettes, også er unikke globalt.

Herefter følger CVR-nr. Dette indikerer lokation for, hvor den pågældende ressource, person etc. er blevet registreret. Hvis organisationen har eget XRI (orgXRI) kan dette erstatte CVR. Det er i dette tilfælde organisationens eget ansvar at sikre entydighed, MEN der skal stadig startes med xri://@DK-XRI.

Dernæst skal følge et tidsstempel (UTC) for oprettelse.

Ovenstående giver mulighed for følgende xri'er:

Xri://@DK-XRI*[CVR]/[tidsstempel]/xxxx

Xri://@DK-XRI*(@[orgXRI])/[tidsstempel]/xxxx

'xxxx' er en streng, som den enkelte organisation selv har ansvaret for. Dette kan f.eks. være initialer, et løbenr. eller personlige XRI'er.

For at illustrere anvendelsen vil der i næste afsnit blive gennemgået 3 eksempler, så anvendelsen af XRI som id-nøgle bliver tydeliggjort.

6 Anbefalet opbygning af id-nøgle til borger med OCES certifikat

Borgere med OCES certifikat har allerede fået tildelt en entydig id-nøgle i forbindelse med udstedelsen af OCES certifikatet. Dette er PID'en. Denne anvendes i dette specialtilfælde til at generere en unik XRI-nøgle. PID'en kan resolves til et CPR-nummer.

Denne id-nøgle kan anvendes til at knytte borgerens data sammen på tværs af systemer.

Princippet i opbygningen af id-nøglen består af følgende led:

Identifikation af landetilknytningen for organisationen, der opretter brugeren

PID'en

Dvs.

Xri://@DK-XRI/pid/<PID>

Uanset hvilken ingang borgeren bruger til Told & Skat vil borgeren således have den samme PID og dermed kan borgerens rekords linkes sammen.

7 Eksempler

Eksempel 1: Kommunalt ansat

Ole Jensen, ansat i socialforvaltningen i Bjergdal kommune. Ole Jensens initialer er OJEN. Ole Jensen har endvidere registreret sit eget personlige XRI under det globale context symbol '=' som: xri://=Ole.Jensen CVR-nummer for Bjergdal kommune er 19437019. Ole Jensen registreres i de lokale brugerkataloger d. 02. august, 2005 kl. 16.42.¹

Dette giver følgende xri, hvis initialerne anvendes.

- `xri://@DK-XRI*19437019/($d/2005-08-02T16:16:42+01:00Z)/OJEN`

Under antagelse af, at initialer IKKE genbruges internt i kommunen, vil denne identifikator være unik globalt.

Hvis Ole Jensens eget XRI anvendes kunne en xri se således ud:

- `xri://@DK-XRI*19437019/($d/2005-08-02T16:16:42+01:00Z)/(=Ole.Jensen)`

Ole Jensen er også borger i Bjergdal kommune. Dette giver følgende xri, hvis initialerne anvendes:

- `xri://@DK-XRI*19437019/($d/2005-08-02T16:16:43+01:00Z)/OJEN`

, og hvis Ole Jensens eget xri anvendes:

- `xri://@DK-XRI*19437019/($d/2005-08-02T16:16:43+01:00Z)/(=Ole.Jensen)`

Bemærk, at der her forudsættes, at en person IKKE registreres som borger og ansat i samme moment (sekund), da dette vil give den samme id-nøgle. Dette anses for at være meget lidt sandsynligt.

Hvis nu Bjergdal Kommune endvidere havde registreret registreret sit eget personlige XRI under det globale context symbol @ som: xri://@Bjergdal.Kommune så ville ovenstående 4 xri'er kunne laves om til:

`xri://@DK-XRI*(@Bjergdal.Kommune)/($d/2005-08-02T16:16:42+01:00Z)/OJEN`

`xri://@DK-XRI*(@Bjergdal.Kommune)/($d/2005-08-02T16:16:42+01:00Z)/(=Ole.Jensen)`

`xri://@DK-XRI*(@Bjergdal.Kommune)/($d/2005-08-02T16:16:43+01:00Z)/OJEN`

`xri://@DK-XRI*(@Bjergdal.Kommune)/($d/2005-08-02T16:16:43+01:00Z)/(=Ole.Jensen)`

Ole Jensen får således knyttet 2 forskellige id-nøgler til sig. Alt efter hvilken rolle han tilgår it-systemer med, vil den tilhørende bruger være tilknyttet et unikt id, der entydigt fortæller, hvilken sammenhæng (rolle/jobfunktion etc.) han går på det enkelte it-system med. Anvendes dette f.eks. i loggen til it-systemet, vil den enkelte systemejer kunne identificere Ole Jensen og dennes kontekst som bruger entydigt.

¹ XRI metadata repræsentation af et tidsstempel er: `$d/YYYY-MM-DDTHH24:MI:SS+XX:00Z`, hvor `XX:00` er afvigelsen fra GMT.

Bemærk, at tidsstempel er med. Dette er for at kunne styre opsigelser og genansættelser. I disse tilfælde vil en udeladelse af et tidsstempel medføre, at der kan opstå dubletter. Og netop i ovenstående eksempel, hvor personen både er borger og ansat, ville dette resultere i dubletter.

Ovenfor er anvendt initialer. Man kunne have anvendt et løbenummer i stedet. Det vigtigste er, at der til hver bruger bliver knyttet et entydigt id i brugerkataloget.

Eksempel 2: Ansat på Odense Universitetshospital

Mette Hansen, ansat på børnecenteret på Odense Universitetshospital. Mette Hansens initialer er MHAN. CVR-nummer for Odense Universitetshospitals børnecenter er 25528107. Fyns amt har CVR-nummer 40556311. Ovenstående giver følgende xri, hvis amtet opretter Mette Hansen som bruger.

*xri://@ DK-XRI *40556311/(\$d/2005-08-01T16:10:42+01:00Z)/MHAN*

Hvis det er børnecenteret selv, der opretter Mette Hansen som bruger, bliver Xri'en:

*xri://@ DK-XRI *25528107/ (\$d/2005-08-01T16:10:42+01:00Z)/MHAN*

Eksempel 3: Borger i Bjergdal – anvendelse af løbenummer.

Bent Broberg er borger i Bjergdal. Bent Broberg ønsker adgang til kommunens it-systemer, og han oprettes i disse. Han tilknyttes en XRI:

xri://@DK-XRI(@Bjergdal.Kommune)/(\$d/2005-08-02T16:16:52+01:00Z)/0000122 eller*

*xri://@DK-XRI*19437019/(\$d/2005-08-02T16:16:52+01:00Z)/0000122*

0000122 er et løbenummer, som styres af Bjergdal kommune. Ved oprettelse af brugeren knyttes xri-nummeret til Bent Broberg, og det vil således entydigt kunne identificere denne person ved anvendelse.

I forbindelse med kommunalreformen skifter Bjergdal navn i forbindelse med sammenlægningen med Højborg kommune. Det nye navn bliver Højdal. Dette er umiddelbart uden betydning for de XRI'er, der allerede er eksisterende i systemerne, idet de er unikke og følger brugeren ved migrering til andre brugerkataloger etc. Nye XRI'er skal dog benytte det nye navn. Hvis nu Bent Broberg tilflytter kommunen efter kommunesammenlægningen, så vil han få tilknyttet et nyt XRI, som hedder:

xri://@DK-XRI(@Højdal.Kommune)/(\$d/2007-08-04T16:16:52+01:00Z)/0000345*

(Det antages, at Højdal i dette tilfælde har registreret @Højdal.Kommune. CVR-nummer er endnu ukendt)

Eksempel 4: Borger i Bjergdal – anvendelse af PID.

Bent Broberg er borger i Bjergdal. Bent Broberg ønsker adgang til kommunens it-systemer, og han oprettes i disse. Han har fået udstedt et OCES certifikat med pid= 279815395 . Han tilknyttes en XRI:

xri://@DK-XRI/pid/ 279815395

Denne id-nøgle forbliver uændret, uanset hvor Bent Broberg bor eller flytter hen. Dvs. den kan koble samtlige data sammen hørende til borgeren, uanset hvor id-nøglen er tilknyttet.

8 Appendix A – Information om XRI

XRI bygger oven på IRI (Internationalized Resource Identifier), som igen bygger oven på Universal Resource Identifier (URI). Målet med XRI er at give det samme uniforme identifikationslag for abstrakte identifikatorer, som URI og IRI giver for konkrete identifikatorer i dag. XRI skal således kunne fortolkes til URI's/IRI's.

URN (Uniform Resource Names) giver kun persistence, mens XRI's giver persistence og flytbarhed.

Bedste brugerscenarie for en abstrakt identifikator er muligheden for at opretholde en persistent reference til en ressource, når den flytter eller ændrer adresse.

URL (Uniform Resource Locator = http URI's) bruger en fysisk location – dvs. den fejler, når ressourcen flyttes.

XRI opfylder kravene for URN som specificeret i *RFC1737*.

Det er en abstrakt adresse, der løser problemet med at opretholde en persistent adresse for mennesker, organisationer og ressourcer uanset hvilke forandringer, der sker i kontaktdata.

XRI-adresselaget består af 2 lag, der bygger oven på 'DNS names' og 'IP-num':

- I-Numbers

Identifiser som er registreret på en ressource (system, fil, printer, person, organisation etc.), og som aldrig bliver reassigned. Dette nummer kan således anvendes til at repræsentere netværksressourcen i netværket.

- I-Names

Logisk navn, der kan opløses til et 'I-Number'. I modsætning til 'I-Numbers' kan de overføres til en anden ressource af ejeren.

I-Names kaldes også 'Universal Private Addresses'

I-Names og I-Numbers er 'persistent, potable, private identifiers'. De kaldes også XRI-synonymer.

Første trin i en persistent identifikation af en ressource er at tildele en identifikator, som ikke afhænger af ressourcens netværksplacering (el. organisatoriske tilhørsforhold) og adgangsmekanisme, da de begge kan ændres over tid. Dette kaldes en abstrakt identifikator, idet den ikke kan transformeres til en ressource direkte via en protokol, men skal 'løses' til en konkret identifikator i stedet, f.eks. en URI.

Hvis en ressource flytter, så skal ændringen foretages i løsnings servicen. Dvs. når man kalder denne med en given XRI, vil den returnere den nye adresse.

Hvis XRI skal skifte navn, så skal løsnings servicen returnere den gamle, der så igen kan løses til ressourcen.

Bemærk, at anvendelsen af xri ikke er et forsøg på at lave en unik bruger-id, men at kunne binde data sammen på tværs af systemer via en unik id-nøgle samt at kunne identificere den bagvedliggende person. Man har ikke behov for at anvende f.eks. 'user-id' i xri'en. Det er kun en logisk indikator.

XRI er bagud-kompatible med DNS og IP-adresser. Domæne-navne og IP-adresser kan således anvendes som 'I-Names'. Endvidere understøtter XRI flere niveauer. Et firma kan registrere et top-level 'I-Name' og dernæst 'assigne' lokale 'I-Names' til dets ressourcer (f.eks. underafdelinger, personer mm). Der er ingen begrænsning på dybden af dette, men en flad struktur er at foretrække for at bevare overblikket.

9 Appendiks B - Yderligere information

Dette fællesoffentlige arbejde i forbindelse med tværgående brugerstyring er beskrevet på

<http://www.oio.dk/arkitektur/brugerstyring>

Information om nogle af de aktiviteter inden for it-sikkerhed, som Videnskabsministeriet varetager findes på

<http://www.oio.dk/sikkerhed>

Information vedrørende arbejdet med at implementere en fælles standard for styring af it-sikkerhedsprocesser i staten findes på

<http://www.oio.dk/itsikkerhed/isis>