Aanbeveling nr. 01/2008 van 24 september 2008

Betreft: aanbeveling met betrekking tot het toegangs- en gebruikersbeheer in de overheidssector (SE/2008/028)

De Commissie voor de bescherming van de persoonlijke levenssfeer, (hierna "de Commissie");

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna "WVP"), inzonderheid artikel 30;

Gelet op de aanvraag van het Sectoraal Comité van het Rijksregister van 12/03/2008;

Gelet op het verslag van de Voorzitter;

Brengt op 24/09/2008 de volgende aanbeveling uit:

I. VOORWERP VAN DE AANVRAAG

1. Op de zitting van het Sectoraal comité van het Rijksregister van 12 maart 2008 werd een machtigingsaanvraag van het Vlaams Energieagentschap behandeld m.b.t. gebruikersbeheer **van** een energieprestatiedatabank. Naar aanleiding van de behandeling van dit dossier stelde het Sectoraal comité vast dat de personen die zich zullen registreren met het oog op het gebruik van de toepassing, verzocht worden om een heel wat informatie te verschaffen zoals diploma, diplomarichting, gevolgde opleiding, correspondentieadres, of men ambtenaar is van een gemeente of van RO Vlaanderen,.... Deze informatie wordt vervolgens, met uitzondering van de naam, de voornamen en het identificatienummer, opgeslagen in de gebruikersgegevensbank zonder een degelijke voorafgaande validatie van de juistheid ervan.

2. Het Sectoraal comité van het Rijksregister heeft erop gewezen dat het aanleggen van gegevensbanken zonder afdoende waarborg van de juistheid van de erin opgenomen gegevens in strijd is met artikel 16, § 2, 1° van de Wet Verwerking Persoonsgegevens, dat stelt dat "de verantwoordelijke van de verwerking er nauwlettend moet over waken dat de gegevens worden bijgewerkt, dat de onjuiste, onvolledige en niet ter zake dienende gegevens, alsmede die welke zijn verkregen of verder verwerkt in strijd met de artikelen 4 tot 8, worden verbeterd of verwijderd".

3. Wanneer deze gegevensbanken worden gebruikt als "betrouwbare" bron voor de verificatie van bepaalde kenmerken van de betrokkene (bvb. arts, notaris, ...), om deze op basis van deze kenmerken toegang te verstrekken tot bepaalde toepassingen en persoonsgegevens, dreigen personen toegang te krijgen tot toepassingen of persoonsgegevens op basis van onjuiste kenmerken. Wat belet bijvoorbeeld iemand om zichzelf een kenmerk aan te meten die hij niet heeft, bijvoorbeeld zorgverstrekker, als dat element toch niet gecontroleerd wordt?

4. Het gevaar bestaat daarenboven dat dergelijke gegevensbanken een officieel cachet krijgen en dat andere instanties er een beroep op doen, er ten onrechte van uitgaande dat ze betrouwbaar zijn omdat ze door een overheidsdienst beheerd worden, met alle gevolgen van dien. Aldus zou het mogelijk worden dat een persoon ten onrechte toegang krijgt tot gegevens op basis van een gefingeerde hoedanigheid. Het is bijgevolg belangrijk dat een aantal vuistregels worden bepaald die bij de uitbouw van een systeem van gebruikers- en toegangsbeheer moeten in acht genomen worden teneinde dergelijke uitwassen te vermijden.

5. Gelet op het feit dat dit een horizontale problematiek is die de bevoegdheid van het Sectoraal Comité van het Rijksregister overstijgt, werd beslist om hierover het standpunt van de Commissie in te winnen.

II. ONDERZOEK

A. Algemeen

6. Ingevolge de elektronische dienstverlening is het onder meer mogelijk om toegang te krijgen tot persoonlijke en/of eventueel gevoelige informatie, of om acties te stellen waaraan (rechts)gevolgen verbonden zijn. Het is dan ook cruciaal dat alleen bevoegde personen en/of organisaties toegang krijgen en zij alleen maar die informatie te zien krijgen of die handelingen kunnen stellen waartoe zij gerechtigd zijn. Dit vereist het uitbouwen van een betrouwbaar systeem van gebruikers- en toegangsbeheer dat bepaalt welke gebruiker/toepassing, in welke hoedanigheid, in welke situatie toegang mag hebben tot welke soorten gegevens m.b.t. welke personen over welke periode.

7. Het gebruikers- en toegangsbeheer bestaat, zoals de term het zelf aangeeft, uit 2 luiken. Het gebruikersbeheer dat volgende aspecten omvat:

- de registratie van de identiteit;
- de identificatie;
- de authenticatie van de identiteit;
- de registratie van de kenmerken en mandaten;
- de verificatie van de kenmerken en mandaten;

en het toegangsbeheer dat de registratie van de autorisaties en de verificatie van de autorisaties dekt.

8. De Commissie staat in de overheidssector (federaal, gemeenschappen, gewesten, lokale besturen, ...) de uitbouw voor van een goed onderling gecoördineerd systeem van gebruikers- en toegangsbeheer dat gebaseerd is op de elektronische identiteitskaart als middel voor identificatie en authenticatie van de identiteit, en op de uitbouw van gevalideerde en gedistribueerde authentieke gegevensbanken (zgn. authentieke bronnen) voor de registratie en verificatie van kenmerken, mandaten en autorisaties. Binnen de overheid worden best afspraken gemaakt opdat voor elk relevant kenmerk, mandaat en autorisatie slecht één gevalideerde authentieke gegevensbank wordt uitgebouwd. Dit vermijdt de risico's voor de bescherming van de persoonlijke levenssfeer die eigen zijn aan de redundante opslag van dezelfde persoonsgegevens in meerdere authentieke gegevensbanken, en ontlast de gebruikers van het meervoudig bewijs van dezelfde kenmerken of mandaten. Dit betekent dat de gevalideerde authentieke gegevensbanken zullen deel uitmaken van de basisdiensten waarop elk gebruikers- en toegangsbeheer, eventueel mits machtiging van het bevoegde sectoraal comité, kan gebouwd worden.

9. Het systeem wordt best uitgebouwd volgens het principe van de "cirkels van vertrouwen". Dit houdt in dat tussen de bij elektronische dienstverlening betrokken instanties duidelijke afspraken worden gemaakt over:

- wie welke authenticaties, verificaties en controles verricht aan de hand van welke middelen en daarvoor verantwoordelijk en aansprakelijk is;
- hoe tussen de betrokken instanties de resultaten van de verrichte authenticaties, verificaties en controles op een veilige wijze elektronisch worden uitgewisseld;
- wie welke loggings bijhoudt;
- hoe ervoor wordt gezorgd dat bij onderzoek, op eigen initiatief van een controle-orgaan of n.a.v. klacht, een volledige tracing (wie, wat, waar, wanneer, waarom) kan geschieden van welke natuurlijke persoon welke dienst of transactie m.b.t. welke burger of onderneming wanneer, via welk kanaal en voor welke doeleinden heeft gebruikt.

Het voordeel van dergelijk systeem bestaat erin dat:

- onnodige centralisatie wordt vermeden;
- onnodige bedreigingen voor de bescherming van de persoonlijke levenssfeer worden vermeden (er gaan bijvoorbeeld geen kopieën van de gevalideerde authentieke bronnen circuleren);
- meervoudige identieke controles en opslag van loggings worden vermeden;
- het met de meest actuele informatie werkt (bijvoorbeeld wanneer een gebruiker een kenmerk verliest zal deze bij aanmelding door het systeem op aangepaste wijze behandeld worden).

B. Terminologie

10. Voor een goed begrip worden de gehanteerde termen hierbij verduidelijkt zodat er geen misverstand kan bestaan over hun draagwijdte:

- de identiteit van de gebruiker is een uniek nummer of een reeks attributen van een gebruiker (natuurlijke persoon, onderneming, vestiging van een onderneming, ...) die toelaten om eenduidig te weten wie de gebruiker is. Dit impliceert dat een gebruiker één en slechts één identiteit heeft. Het feit dat eventueel in bepaalde situaties een pseudoniem gebruikt kan worden, doet daar geen afbreuk aan;

- een kenmerk is een attribuut van een gebruiker, ander dan de attributen die de identiteit van de gebruiker bepalen, zoals een hoedanigheid, een functie in een bepaalde organisatie, een beroepskwalificatie, ... Een gebruiker kan verschillende kenmerken hebben;

- een mandaat is een recht verstrekt door een geïdentificeerde gebruiker aan een andere geïdentificeerde gebruiker om in zijn naam en voor zijn rekening welbepaalde (juridische) handelingen te stellen. Een gebruiker kan aan één of meerdere gebruikers één of meerdere mandaten verstrekken;

- de registratie is het proces waarbij de identiteit van een gebruiker, een kenmerk van een gebruiker of een mandaat met voldoende zekerheid wordt vastgesteld vooraleer middelen ter beschikking worden gesteld aan de hand waarvan de identiteit, een kenmerk of een mandaat kunnen worden geauthentiseerd of geverifieerd;

- de authenticatie van de identiteit is het proces waarbij wordt nagegaan of de identiteit die een gebruiker beweert te hebben de juiste identiteit is om gebruik te kunnen maken van een elektronische dienst. Dit kan geschieden op basis van een controle van:
    - kennis (vb. een paswoord);
    - bezit (vb. een certificaat op een elektronisch leesbare kaart);
    - biometrische eigenschap(pen);
    - een combinatie van meerdere van deze middelen.

- de verificatie van een kenmerk of een mandaat is het proces waarbij wordt nagegaan of een kenmerk of mandaat die een gebruiker beweert te hebben om gebruik te kunnen maken van een elektronische dienst, effectief een kenmerk of een mandaat van deze gebruiker is. Dit kan geschieden:
    - op basis van dezelfde soort middelen als deze gebruikt voor de authenticatie van de identiteit;
    - na authenticatie van de identiteit van een gebruiker, door de raadpleging van een gegevensbank (authentieke bron) waarin kenmerken of mandaten m.b.t. een geïdentificeerde gebruiker worden opgeslagen.

- de autorisatie is de toelating voor een gebruiker om een welbepaalde verwerking te verrichten of een welbepaalde dienst te gebruiken.

C. Ten gronde

11. Cruciaal bij het uitbouwen van het gebruikersbeheer is een goede registratie van de identiteit, de relevante kenmerken en de relevante mandaten. Alles staat of valt met de kwaliteit daarvan. Een kwaliteitsvolle registratie veronderstelt daarenboven dat de beschikbare gegevens up-to-date wordt gehouden. Het belang daarvan ligt voor de hand. Een wijziging van een kenmerk/mandaat van een gebruiker kan immers een weerslag hebben op diens toegangsrechten.

12. Een goede registratie houdt in dat de identiteit van de gebruiker die zich aanmeldt, zijn kenmerken en zijn mandaten worden gecontroleerd aan de hand van authentieke documenten/bronnen waar dit mogelijk is.

13. Vervolgens moet bepaald worden aan de hand van welk instrument zal nagegaan worden wanneer iemand zich aanmeldt om gebruik te maken van een elektronische dienst met wie die dienst te maken heeft: identificeren van de gebruiker en controle of hij degene is die hij beweert te zijn.

14. De Commissie is van oordeel dat de elektronische authenticatie van de identiteit bij voorkeur gebeurt aan de hand van de elektronische identiteitskaart (EID) daar zij de meeste garanties biedt. Ze combineert het bezit van een specifiek document met het beschikken over een bepaalde kennis (pincode). Daarnaast beperken een aantal feitelijke en wettelijke factoren het risico op misbruik ingeval van eventueel verlies/diefstal van de EID:

- **het is een wettelijk beschermd officieel document dat wordt uitgereikt door de overheid;**
- de afwezigheid van de EID zal door de rechtmatige bezitter ervan sneller opgemerkt worden dan deze van andere kaarten die meestal slechts sporadisch gebruikt worden;
- zonder de pincode kan men met de kaart elektronisch niets aanvangen;
- op basis van artikel 6*ter* van de wet van 19 juli 1991 *betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen,* kunnen ingeval van verlies/diefstal op elk moment van de dag of van de nacht de elektronische functies van de kaart geschorst of ingetrokken worden door aangifte van het verlies/diefstal bij helpdesk van het Rijksregister van de natuurlijke personen[1].

[1] Deze helpdesk is vierentwintig uur per dag gedurende zeven dagen per week operationeel (artikel 7 van het koninklijk besluit van 25 maart 2003 *betreffende de identiteitskaarten)*.

15. Het feit dat de identiteit van een gebruiker werd geauthentiseerd volstaat niet altijd om de betrokkene zonder meer toegang te verlenen tot een elektronische dienst. De toegangsrechten tot een elektronische dienst (autorisaties) van een gebruiker in het kader van de elektronische dienst kunnen gekoppeld zijn aan zijn kenmerken en/of mandaten. Een volledig geïntegreerd gebruikers- en toegangsbeheer vereist dus dat op een ondubbelzinnige wijze:

- de relevante kenmerken van een persoon;
- het bestaan van een mandaat tussen een rechtspersoon of natuurlijke persoon waarop een elektronische dienst betrekking heeft en de persoon die deze dienst gebruikt;

kunnen worden gecontroleerd.

16. De verificatie van de kenmerken en/of mandaten zal niet kunnen gebeuren aan de hand van de EID daar zij, naast een instrument voor het plaatsen van een juridisch geldige elektronische handtekening, uitsluitend een instrument voor identificatie en authenticatie van de identiteit is. Dit betekent dat de informatie die deze kaart bevat, zowel in elektronisch leesbare vorm als in met het blote oog zichtbare vorm beperkt is en moet blijven tot:

- die informatiegegevens die noodzakelijk zijn om de houder te identificeren;
- de certificaten (sleutels) die de houder toelaten zich te authenticeren d.w.z. die hem in staat stellen om te bewijzen dat hij daadwerkelijk diegene is wie hij beweert te zijn;
- de certificaten (sleutels) die de houder toelaten om een juridisch geldige elektronische handtekening te plaatsen.

Gegevens die niets te maken hebben met de identificatie en de authenticatie van een fysieke persoon, met de elektronische handtekening, zoals kenmerken en/of mandaten, horen niet thuis op de EID[2].

17. De verificatie van kenmerken en/of mandaten zal dus moeten gebeuren via andere kanalen. Het is niet wenselijk dat men daarbij vertrouwt op niet-gevalideerde informatie die gewoon wordt verstrekt door de gebruiker zelf. Deze elementen moeten gecontroleerd worden aan de hand van een bron die de nodige waarborgen biedt inzake correctheid en actualiteit van de informatie die ze bevat, een gevalideerde authentieke bron. De beheerder van een dergelijke gevalideerde authentieke bron is verantwoordelijk voor de beschikbaarheid en de kwaliteit van de ter beschikking gestelde informatie.

[2] Zie advies van de Commissie nr.13/2005 van 7 september 2005.

18. Een kritische succesfactor van een degelijk elektronisch gebruikers- en toegangsbeheer is onder meer de mate waarin er kan terug gekoppeld worden naar gevalideerde authentieke bronnen. Het ligt dan ook voor de hand dat diegene die een dergelijk beheerssysteem wenst uit te bouwen, moet weten op welke bronnen hij een beroep kan doen. Dit vereist de beschikbaarheid van een inventaris van gevalideerde authentieke bronnen.

19. Dit betekent dat zowel federaal als regionaal o.a. de overheids- en aanverwante diensten moeten geïdentificeerd worden die beschikken over betrouwbare informatie waaruit kenmerken of mandaten van een persoon blijken. Daarnaast dient:

- de authentieke informatie in kaart gebracht worden;
- de elementen waaruit haar kwaliteit blijkt te worden aangegeven;
- deze informatie georganiseerd te worden op een wijze dat ze gemakkelijk kan ontsloten worden met in achtneming van het proportionaliteitsbeginsel.

20. De Commissie is er zich van bewust dat dit geen eenvoudige oefening is. Indien men echter e-government op een veilige manier wil uitbouwen, dan is dit een noodzakelijke oefening. Trouwens, met het oog op de toepassing van de Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 *betreffende diensten op de interne markt* (zgn. dienstenrichtlijn), lijkt zij hoe dan ook gewenst.

21. De dienstenrichtlijn streeft er immers naar om de procedures en formaliteiten voor de toegang tot en de uitoefening van dienstenactiviteiten te vereenvoudigen, dienstverrichters die dit wensen in staat te stellen deze procedures en formaliteiten van op afstand via elektronische weg en/of via één-loket af te wikkelen, en dienstverrichters en afnemers van diensten van op afstand toegankelijke, duidelijke, gebruikersvriendelijke en actuele informatie aan te bieden. Dit impliceert dat lidstaten elkaar wederzijdse bijstand verlenen om de controle op de dienstverrichters en hun diensten te garanderen. Daartoe heeft de Europese Commissie een informatiesysteem voor de interne markt (IMI) ontworpen. Dat systeem zal het mogelijk maken via een verbindingspunt informatie te krijgen over de realiteit van de vestiging, de betrouwbaarheid en professionele competenties van de dienstverrichter.

22. Momenteel zijn er federaal een aantal gegevensbanken operationeel die als gevalideerde authentieke bron worden bestempeld. Denken we bijvoorbeeld aan de Kruispuntbank van Ondernemingen, de gegevensbank van lokale beheerders van bedrijven, gemeenten en OCMW's bij de RSZ(PPO), het kadaster van zorgverstrekkers van de FOD Volksgezondheid, de gegevensbank

met de RIZIV-erkenningen van het RIZIV. Voor een aantal gereglementeerde beroepen zijn er tevens gevalideerde authentieke gegevensbanken beschikbaar. Denken we bijvoorbeeld aan advocaten, notarissen, gerechtsdeurwaarders. Ook op regionaal en lokaal vlak zijn er dergelijke gegevensbanken beschikbaar.

23. Wanneer een systeem van gebruikers- en toegangsbeheer wordt opgezet, dient de betrokken dienstverlener na te gaan voor welke elementen hij kan terugvallen op bronnen die momenteel reeds als een gevalideerde authentieke bron kunnen bestempeld worden. Als dat het geval is moet hij de nodige schikkingen treffen om ze als basisdienst te integreren in zijn systeem.

24. Bij gebrek aan gevalideerde authentieke bron m.b.t. bepaalde kenmerken en/of mandaten moet hij nagaan of daaromtrent bij een derde geen informatie beschikbaar is, die onder bepaalde voorwaarden het cachet van gevalideerde authentieke bron kan krijgen. Vaak beschikt een derde over betrouwbare informatie maar is dit niet bekend met als gevolg dat er geen beroep op gedaan wordt. De houder van die informatie gaat dan ook geen inspanningen doen om die informatie te ontsluiten.

25. Het sluitstuk van het gebruikers- en toegangsbeheer is zoals het begrip aangeeft het toegangsbeheer. Dit bestaat uit de registratie en de verificatie van de autorisaties waarbij:

- de registratie het ingeven impliceert in een authentieke bron van autorisaties door de aanbieder van de elektronische dienst, met specificatie van welke verwerkingen mogen worden verricht m.b.t. welke diensten onder welke voorwaarden (bvb. kenmerken, mandaten, ...) gedurende welke tijdsperiode. Bepaalde gebruikers (vb. lokale beheerders) kunnen de aan hen toegekende autorisaties verder toekennen aan gebruikers die zij aanduiden door het ingeven in een authentieke bron van autorisaties;
- de verificatie impliceert de raadpleging van de relevante authentieke bronnen van autorisaties.

26. Een gebruikers- en toegangsbeheer opgebouwd met inachtneming van de hiervoor uiteengezette richtlijnen zal bijdragen tot het beperken van het risico dat langs elektronische weg ongeoorloofd toegang wordt verkregen tot informatie of ongeoorloofde handelingen worden gesteld.

OM DEZE REDENEN,

de Commissie

beveelt aan dat:

↳ bij de organisatie van het gebruikers- en toegangbeheer de volgende punten in acht worden genomen:

- zorgvuldige registratie van de identiteit, kenmerken en mandaten;
- gebruik van de EID enkel voor identificatie en authenticatie van de identiteit, niet voor kenmerken en mandaten ;
- controle van kenmerken en mandaten aan de hand van gevalideerde authentieke bronnen;
- uitbouwen van cirkels van vertrouwen;
- registreren van de autorisaties in een authentieke bron.

↳ de bevoegde overheid/overheden initiatieven neemt om de bestaande gevalideerde authentieke bronnen te inventariseren evenals bronnen die daartoe onder bepaalde voorwaarden in aanmerking kunnen komen met het oog op het uitbouwen van een betrouwbaar en veilig e-government.

Voor de Administrateur m.v., De Voorzitter,

(get.) Patrick Van Wouwe (get.) Willem Debeuckelaere

Voor eensluidend verklaard afschrift:

Patrick Van Wouwe,
Afdelingshoofd O&RM 02.10.2008