Martiris 2011

Secure Private Data

Gegevensbescherming in Oracle Databases

Inhoudsopgave

Introductie

Voor veel bedrijven bestaat het grootste bedrijfskapitaal uit de data die zij beheren.

Steeds vaker is het nodig om in deze gegevens onderscheid te kunnen maken dat verder gaat dan mogelijk is met de standaard database privileges en rollen in Oracle. Hierbij valt te denken aan toegang verlenen of juist ontzeggen voor specifieke records of het afschermen van gegevens in specifieke kolommen.

Er kunnen verschillende redenen zijn om een fijnmaziger toegang tot data te willen regelen, zoals:

- Combineren van data in tabellen van verschillende eigenaren, bijvoorbeeld als gevolg van consolidatie, waarbij data aan de eigenaar voorbehouden moeten blijven.
- SaaS applicatie (Software as a Service): een gedeelde applicatie waarin gegarandeerd is dat elke klant alleen toegang heeft tot zijn eigen gegevens.
- Need to Know: openstellen van privacy gevoelige gegevens aan specifieke medewerkers en afschermen voor anderen.
- Toepassen van *compliancy* regels zoals Sarbanes-Oxley wetgeving.
- Preventie van datadiefstal en beschermen van gevoelige (productie) gegevens in ontwikkel- en testomgevingen.

Secure Private Data (SPD) kan worden gezien als een uitbreiding op de standaard database privileges en rollen.

Het biedt de mogelijkheid om op rij en kolom niveau gegevens beschikbaar te stellen aan geautoriseerde gebruikers. Autorisaties kunnen ook beschikbaar worden gesteld via applicatie rollen.

SPD beveiligt applicaties transparant, met geen of minimale aanpassingen aan de te beveiligen applicatie. Applicatie logica en security logica zijn gescheiden.

SPD doet zijn werk in de database: gegevens zijn ten alle tijden beschermd, ook als gebruikers buiten de applicatie om de database benaderen, bijvoorbeeld via TOAD of SQL*Plus. Met configuratie is eventuaal af te dwingen dat gebruikers alleen via de applicatie toegang tot gegevens hebben.

Alle opties van de Oracle database ook op SPD van toepassing. Bijvoorbeeld scalability, partitionering, backup etc.

Secure Private Data kent een web based gebruikersinterface waarmee autorisaties gemakkelijk en intuïtief zijn in te regelen. Wijzigen of aanmaken van nieuwe autorisaties is eenvoudig. Nieuwe autorisaties kunnen eenvoudig worden aangemaakt zonder dat de bestaande aangepast hoeven te worden.

Historie

Het concept voor Secure Private Data is initieel bedacht bij TNO Bouw en Ondergrond in Utrecht. In 2008 is dit in een samenwerkingsproject met Martiris ontwikkeld tot een eerste versie van SPD.
Deze eerste versie was specifiek toegespitst op TNO applicatie ‘Dinoloket’. Deze applicatie stelt gegevens over de Nederlandse ondergrond aan diverse partijen beschikbaar.

In 2010 heeft Martiris hier een eigen invulling aan gegeven.
Deze huidige versie is generiek toepasbaar en heeft vele nieuwe functies.

Secure Private Data: Functioneel

SPD biedt in principe drie functionaliteiten:

a) row level security
b) column masking
c) afschermen data voor privileged users

a) Row Level Security

Met SPD kan eenvoudig toegang tot data op rijniveau worden verleend.
Gegevens van verschillende organisaties of bedoeld voor verschillende gebruikers kunnen zo in een gedeelde database bestaan zonder dat deze partijen of gebruikers elkaars data kunnen zien.

b) Column Masking

Het is mogelijk om het lezen van gegevens in kolommen toe te staan aan specifieke gebruikers.
Dit kunnen privacy gevoelige gegevens zijn of bijvoorbeeld Burger Service Nummers, emailadressen, wachtwoorden of inkomens.
Ook kan het gaan om gegevens die zijn voorbehouden aan een bepaalde rol. Te denken valt bijvoorbeeld aan informatie in medische dossiers welke voor artsen toegankelijk moet zijn en voor verpleegkundigen niet.

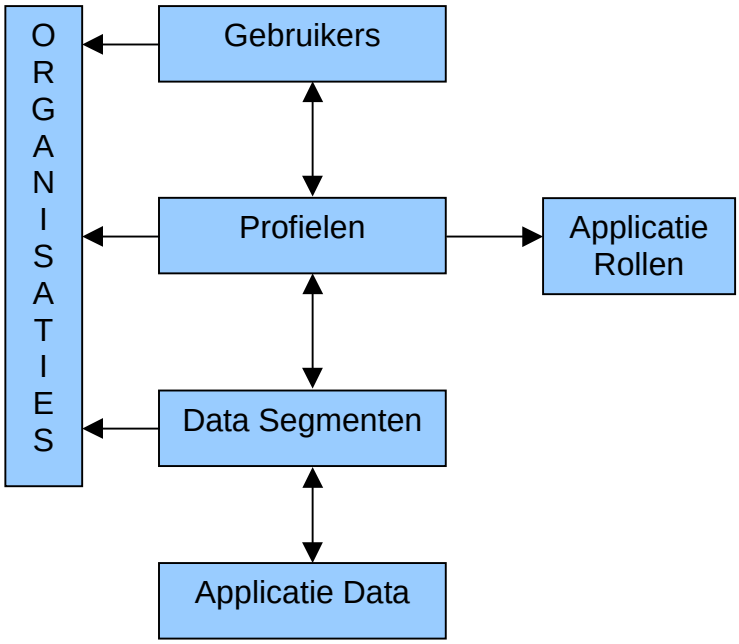
c) Privileged Users

Met SPD beveiligde data zijn ook afgeschermd voor zgn. 'privileged users', dat zijn gebruikers met vergaande privileges. Te denken valt aan applicatiebeheerders of Data Base Administrators.
Veel voorkomend zijn ook situaties waarin ontwikkelaars of testers (vaak extern ingehuurd) hun werk doen in een kopie van de productie omgeving, inclusief alle productie gegevens. Dit kan een beveiligingsrisico zijn.
Met SPD kan eenvoudig toegang tot gevoelige informatie worden beperkt.

Secure Private Data: Concept

Voor *row-level-security* worden in SPD gebruikers en verwijzingen naar applicatiedata geregistreerd. Een verwijzing kan op een enkele rij betrekking hebben (bv. een verwijzing naar een klantnummer of ID) maar ook meerdere records omvatten (bv. een klanttype aanduiding).
Verwijzingen naar data worden gebundeld in data segmenten.

Via profielen worden data segmenten aan gebruikers of aan applicatie rollen gekoppeld.
Voor elk profiel is aan te geven welke rechten het heeft op een data segment.
Leesrechten kunnen gecombineerd worden met willekeurig andere rechten zoals aanmaken, wijzigen en verwijderen.



Figuur 1. Concept data model SPD

Op deze manier is vastgelegd wat voor rechten een gebruiker of een rol heeft op bepaalde rijen. Deze informatie wordt toegepast op het moment dat een gebruiker gegevens in een tabel leest, wijzigt, aanmaakt of verwijdert.

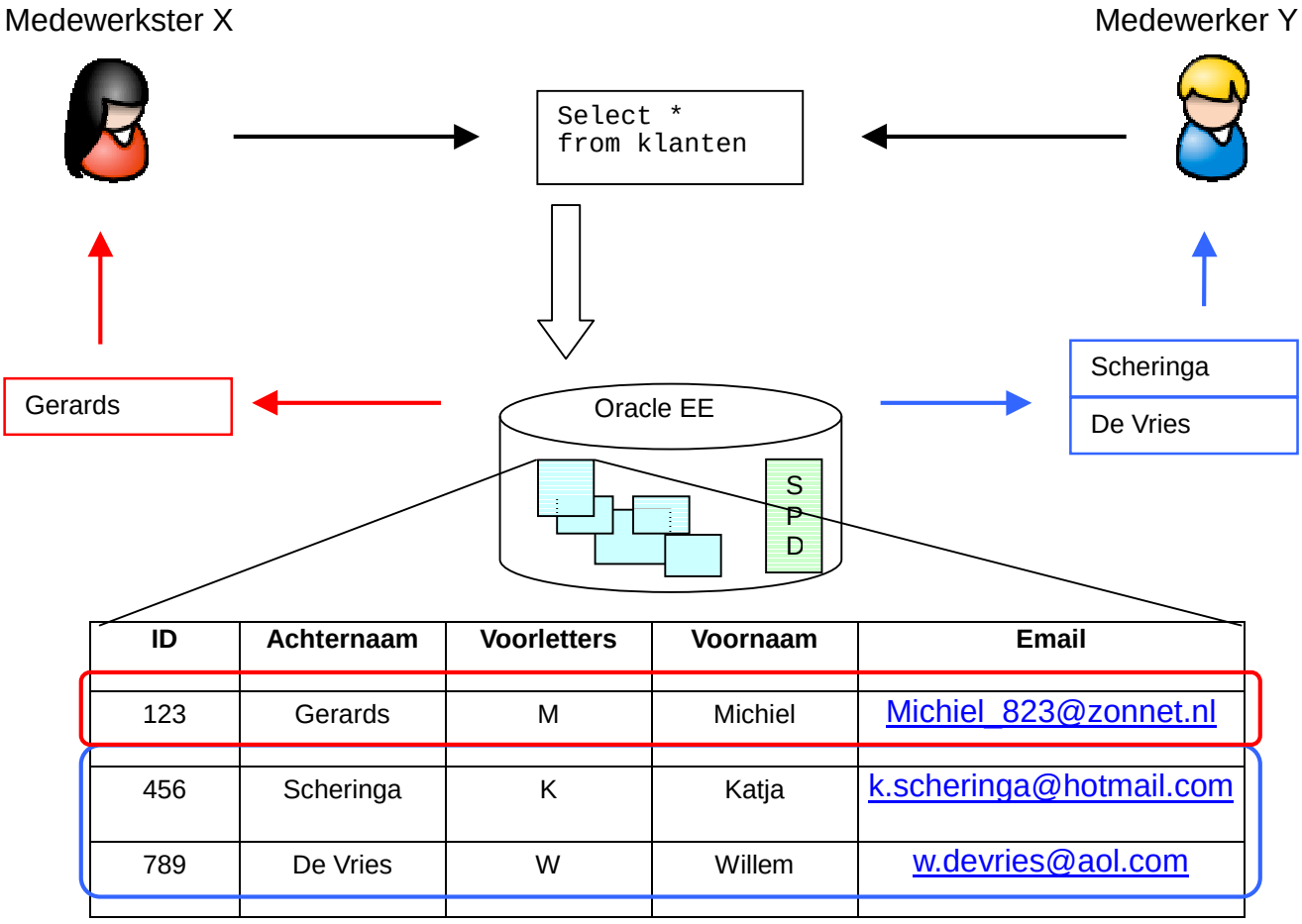
Column-level-security werkt voor hele kolommen en voor alle rijen.
Beperkingen op rij niveau en kolom niveau kunnen gecombineerd worden toegepast.

Virtual Private Database

SPD maakt gebruik van *Virtual Private Database (VPD)*, een standaard en licentievrije feature in de Enterprise Edition van de Oracle Database.
Hiermee wordt onzichtbaar een *'where'* clause toegevoegd aan het statement waarmee dit statement beperkt wordt tot die gegevens waar een gebruiker recht op heeft.
Het zo aangepaste statement wordt alleen toegepast op de dataset waarvoor een gebruiker is geautoriseerd.

Daarnaast is er een optie om VPD te simuleren via views. Voor Oracle gebruikers die werken met de Standard Edition of XE versie van de database biedt dit de mogelijkheid om Secure Private Data te gebruiken zonder VPD.

Figuur 2 laat een zien hoe een identiek select statement door verschillende gebruikers kan leiden tot verschillende uitkomsten.



ID	Achternaam	Voorletters	Voornaam	Email
123	Gerards	M	Michiel	Michiel_823@zonnet.nl
456	Scheringa	K	Katja	k.scheringa@hotmail.com
789	De Vries	W	Willem	w.devries@aol.com

Figuur 2. Row level security.

Beveiliging op meerdere niveaus

Gegevens zijn beveiligd via multi-factor policies.
Toegang tot data kan afhankelijk zijn van:

a) User authenticatie
b) Fysieke locatie

a) User Authenticatie

SPD ondersteunt een middle-tier applicatie architectuur waarin de applicatielaag naar de database connect via een enkele database account.
In SPD kan worden aangegeven welke manier(en) van authenticatie zijn toegestaan en welke niet.
Zo is het mogelijk om een gebruiker alleen toegang tot beveiligde data te verlenen via de applicatie en hem deze toegang te ontzeggen op het moment dat hij rechtstreeks op de de database inlogt.

b) Fysieke locatie

Via IP adres restricties is het mogelijk beperkingen te stellen aan de fysieke locatie vanaf waar gegevens kunnen worden benaderd.
Deze restricties kunnen op meerdere en verschillende niveaus worden ingesteld:

- Voor alle gebruikers van een organisatie
- Voor een individuele gebruiker
- Voor een profiel
- Voor een enkele datagroep

Hiermee kan ingeregeld worden dat alleen vanaf bepaalde werkstations sommige gegevens toegankelijk zijn.
Het is mogelijk om een enkel IP adres op te geven of een bereik.
Ook is het mogelijk om op verschillende niveau's overlappende dan wel elkaar uitsltuitende IP restricties te definieren.

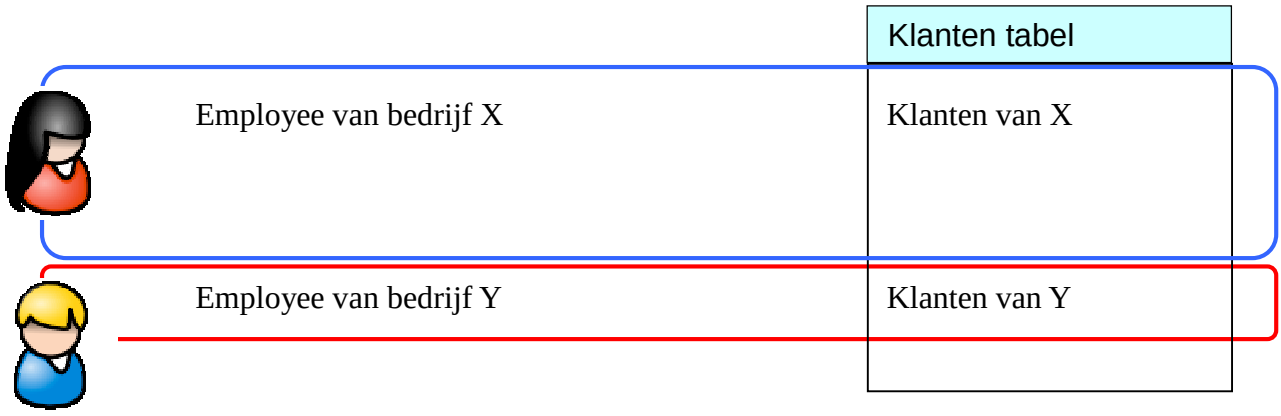
Multi Client

SPD is bij uitstek geschikt om te gebruiken in gedeelde applicaties.

Hierbij is het van belang dat de verschillende partijen alleen toegang hebben tot de eigen gegevens.
Een voorbeeld hiervan is het toenemend gebruik van SaaS applicaties, ofwel *Software as a Service*.

Zowel gebruikers als profielen als datagroepen zijn altijd gekoppeld aan een organisatie. Zo wordt gewaarborgd dat gebruikers alleen toegang hebben tot data van de eigen organisatie (zie figuur 3).

Samenwerken en delen van data tussen organisaties is eventueel mogelijk.



Figuur 3. Multiclient: users hebben alleen toegang tot gegevens van de eigen organisatie.

Partieel Secure

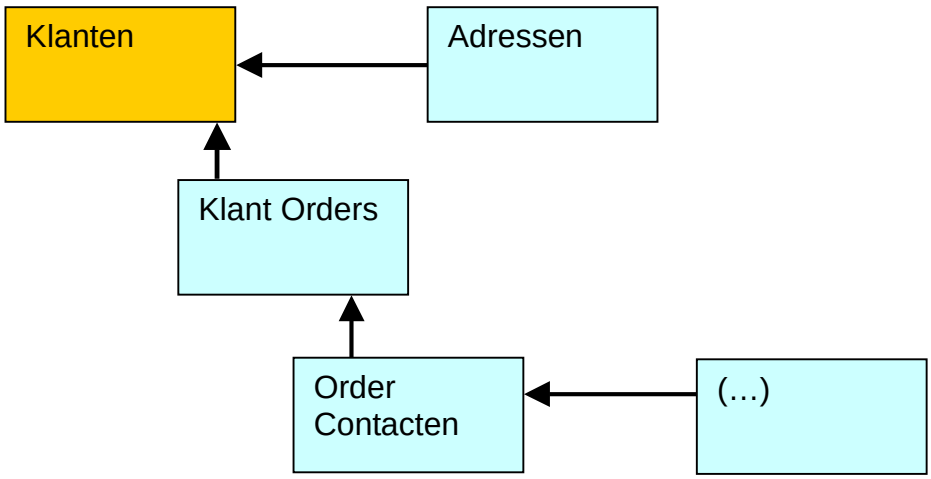
Het is mogelijk om enkel een subset van gegevens in een tabel te beveiligen.
Alleen voor deze subset hoeft dan toegang te worden gedefinieerd.
Gegevens die niet tot deze subset behoren zijn voor iedereen toegankelijk, dat wil zeggen dat SPD geen restricties aan toegang tot deze gegevens stelt.
Uiteraard zijn wel de standaard database privileges en rollen van toepassing op deze gegevens.
Ten opzichte van het opnemen van alle data in SPD biedt dit twee voordelen:
1. De meerderheid van de gegevens is voor iedereen toegankelijk, dus ook voor gebruikers die niet in SPD zijn gedefinieerd.
2. Het beheer in SPD hoeft niet verwijzingen naar alle data in de tabel te omvatten.

Secure by Reference

Vaak zal zich de situatie voordoen dat toegangsrechten voor een tabel ook gelden voor aan deze tabel gerelateerde gegevens.
Met SPD kan de autorisatie voor één hoofdtabel ook toegepast worden op gerelateerde tabellen. Voor de gerelateerde tabellen hoeven geen aparte autorisaties te worden vastgelegd, deze zijn altijd synchroon met de hoofdtabel.
Het beheer wordt hiermee een stuk eenvoudiger.

De relatie tussen hoofdtabel en afgeleide tabellen kan rechtstreeks zijn maar kan ook lopen via een (reeks van) andere afgeleide tabellen.
Ook dan is het nog steeds mogelijk om te refereren aan de waarden waarop toegang tot de master is verleend.

Een voorbeeld is te zien in figuur 4: adressen, klantorders, ordercontacten en daar weer aan gerelateerde data zijn alle terug te leiden tot specifieke klanten.
Een wijziging in toegang op klanten geldt ook voor al deze gerelateerde gegevens.



Figuur 4. Secure by Reference

Column Security

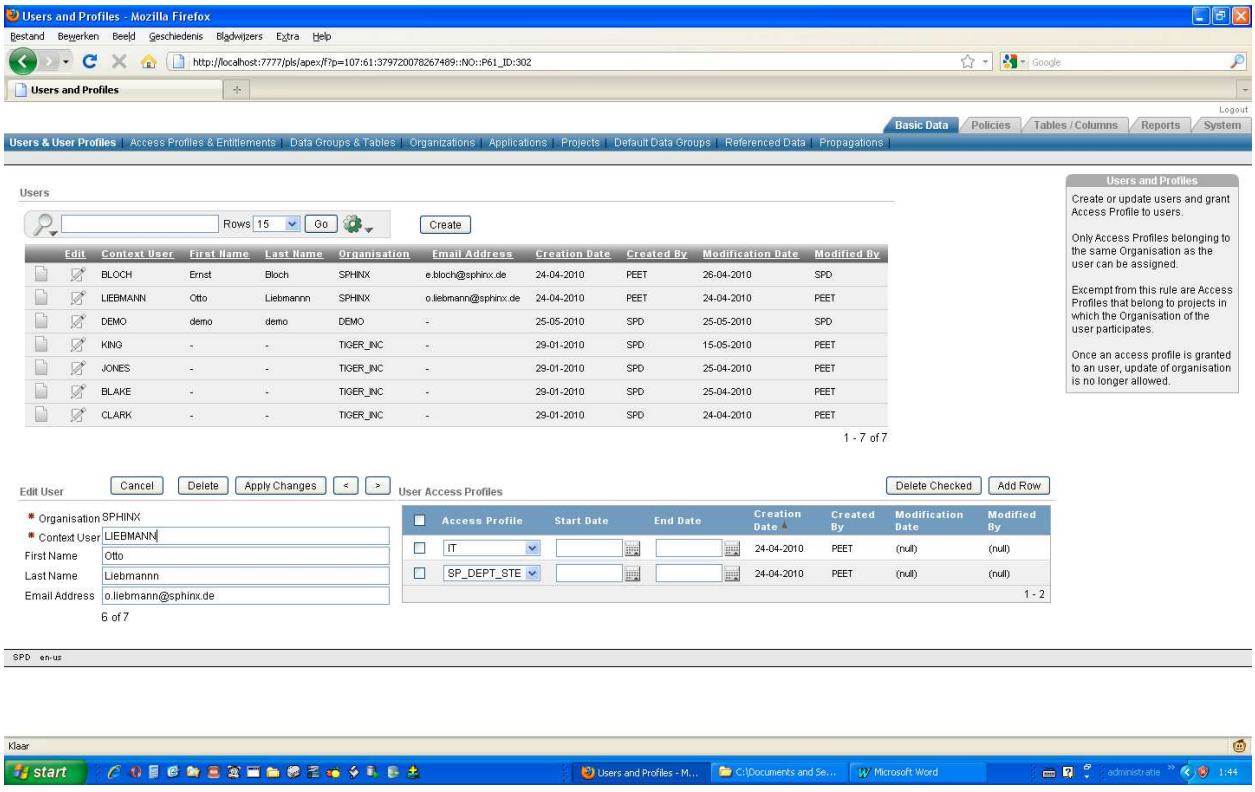
Kolommen kunnen eenvoudig worden gemaskeerd. Data in gemaskeerde kolommen is alleen leesbaar voor geautoriseerde gebruikers.
De keuze voor het maskeren van een kolom kan in een multi-client omgeving per client apart worden ingesteld.
Voor tabellen die slechts gedeeltelijk zijn afgeschemd (Partial Secure) is er de keuzemogelijkheid om het maskeren van kolommen op de niet afgeschermde gegevens toe te passen.

Row level security en kolom masking zijn gecombineerd te gebruiken.

Beheer van Secure Private Data

SPD kan worden beheerd via een web based interface.
Deze biedt overzicht en inzicht op een duidelijke manier.
Elke pagina en de meeste items zijn voorzien van een korte toelichting zodat beheerders gemakkelijk en eenvoudig hun taken kunnen verrichten.

Figuur 5 biedt een voorbeeld van een scherm.



Figuur 5. Voorbeeld beheerscherm SPD

Conclusie

Secure Private Data biedt een eenvoudige en betrouwbare methode om gegevens binnen tabellen te segmenteren en rechten hierop aan gebruikers toe te wijzen.
Deze segmentatie kan zo fijnmazig en flexibel zijn als gewenst en nodig is.
Verdere beveiliging is mogelijk in de vorm van Column Level Security. Gevoelige data in kolommen is zo voorbehouden aan bevoegden.
Gebaseerd op Oracle Virtual Private Database biedt Secure Private Data de zekerheid dat vertrouwlijke informatie in de Oracle database veilig is en blijft.

Martiris
Januari 2011
Versie 1.5

www.martiris.nl/SPD.html
info@martiris.nl
06 1468 4123