

# Hotdesking met SmartCards . . .

## Algemeen

In steeds meer bedrijven en instellingen is het noodzakelijk dat medewerkers informatie snel en eenvoudig maar wel veilig kunnen benaderen en wijzigen vanaf diverse werkplekken.

Hotdesking is de techniek die dit mogelijk maakt. Hotdesking is een techniek die al lang bestaat in de telefoniewereld, het zogenaamde "follow-me" principe. Het toestel volgt mij waar ik maar ga.

Dit principe is ook heel goed mogelijk met IT-werkplekken. Dat het hierbij belangrijk is dat de medewerker direct toegang heeft tot de juiste informatie, maar ook slechts de informatie die ingezien mag worden is evident. Snelheid én beveiliging zijn randvoorwaarden om hotdesking succesvol toe te passen.

Nieuwe mogelijkheden die Microsoft omgevingen standaard al bieden kunnen nu ingezet worden om bij een optimale ervaring van de gebruiker de beveiliging toch te laten voldoen aan de hoogste eisen. Daar waar een gebruiker in seconden toegang krijgt vanaf een willekeurige werkplek tot zijn volledige werkplek, is ondertussen een solide check uitgevoerd of de verbinding wel veilig is en of hij of zij wel degene is waarvoor hij of zij zich uitgeeft.

Het toverwoord: Standaard software, SmartCards en vooral: digitale certificaten.

## Digitale certificaten

De laatste jaren wordt steeds meer gebruik gemaakt van certificaten ten behoeve van authenticatie-doeleinden. Dit omdat enkel de combinatie gebruikersnaam/wachtwoord niet meer voldoende veilig is en het wachtwoord kan worden onderschept. Door certificaten op een met een PIN code beveiligde SmartCard te plaatsen ontstaat een veilige manier van Two-Factor authenticatie.

Two-Factor authenticatie gaat uit van het principe dat er twee zaken nodig zijn om te authenticeren. Namelijk iets wat je hebt, de SmartCard en iets wat je weet, de PIN code.

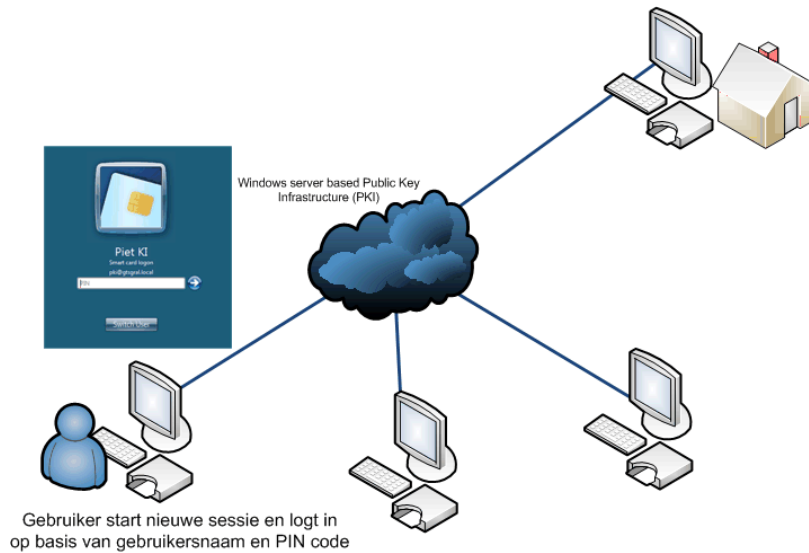
Met de huidige generatie SmartCards is het mogelijk om meerdere certificaten op een SmartCard te plaatsen. Hierdoor wordt het mogelijk om de SmartCard niet alleen voor het aanmelden in Windows te gebruiken, maar ook bijvoorbeeld om aan te melden bij beveiligde websites.

## Hoe werkt het?

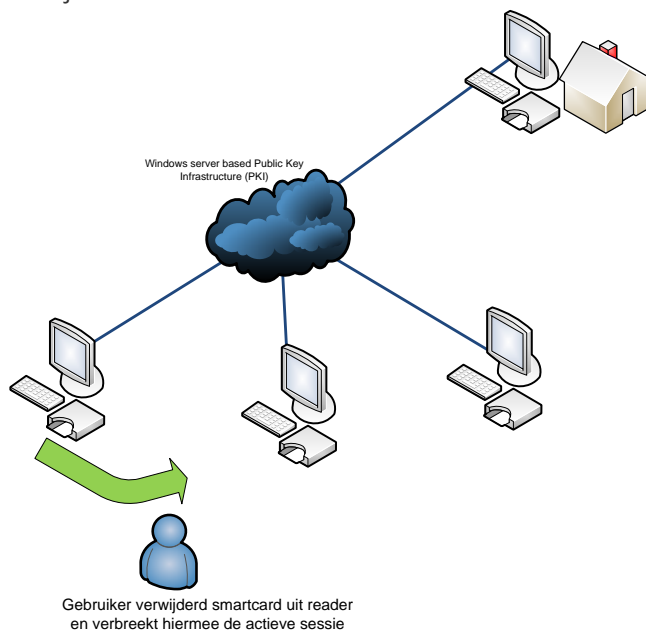
De basis van hotdesking is het feit dat de werkplek van de gebruiker altijd beschikbaar is op de centrale IT-omgeving of in de Cloud. De gebruiker meldt zich initieel gewoon aan en krijgt toegang tot zijn of haar werkplek. Er wordt een nieuwe "sessie" aangemaakt. Bij het aanmelden hoeft een gebruiker niet



meer te doen dan het plaatsen van zijn of haar SmartCard en het invoeren van zijn of haar PIN code.

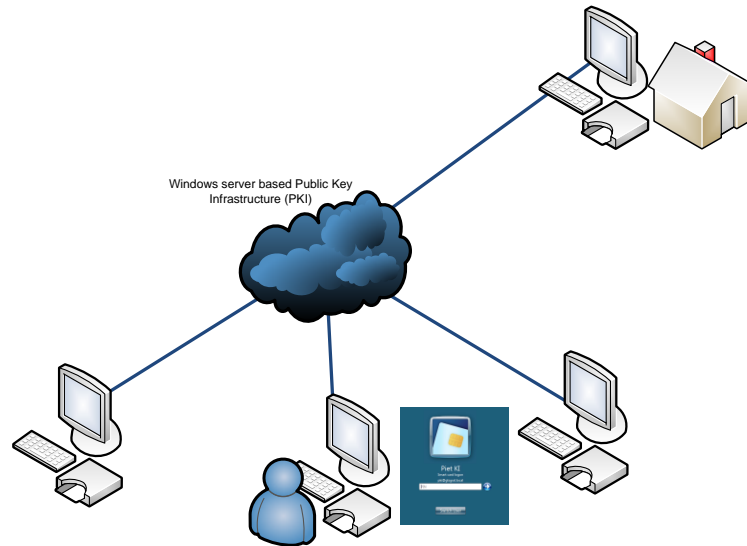


Zodra de gebruiker van zijn of haar werkplek weg gaat hoeft men niet uit te loggen, het verwijderen van zijn of haar SmartCard is voldoende. De sessie wordt verbroken (maar niet beëindigd!) wanneer de SmartCard wordt verwijderd.



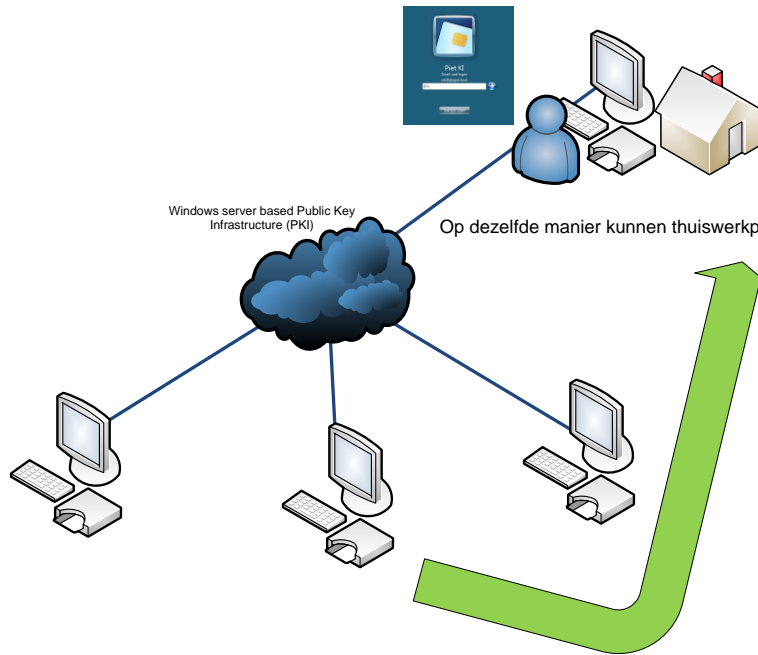


Aangekomen bij een andere werkplek volstaat het plaatsen van de SmartCard en het invoeren van de PIN code om weer direct verder te kunnen werken. Er wordt de benodigde beveiliging opgezet en gecontroleerd, en de verbinding met de "sessie" hersteld.



Gebruiker plaatst smartcard en logt in met gebruikersnaam en PIN code  
De verbinding met de verbroken sessie wordt hersteld en de gebruiker kan direct weer verder werken.

Wanneer een gebruiker thuis de beschikking heeft over een werkplek met SmartCard reader kan zelfs thuis op dezelfde manier worden verder gewerkt.



Op dezelfde manier kunnen thuiswerkplekken worden beveiligd





## Functionaliteit geïntegreerd in het OS.

Door gebruik te maken van de standaard functionaliteit in Microsoft Windows client- en server OS-en is vanaf Windows Vista en Server 2008 bij gebruik van de juiste SmartCards geen extra software installatie meer vereist.

Alle benodigde functionaliteit zit standaard in het OS. Het wijzigen van de PIN code van de gebruiker bijvoorbeeld is geïntegreerd in het aanmeldscherm van Windows.



## Veilig bij design

De in Microsoft Windows Server geïntegreerde Public Key Infrastructure (PKI) is volkomen veilig. Bij het aanmelden wordt gecontroleerd of gebruikerscertificaten zijn ingetrokken, zodat niet geautoriseerde gebruikers niet aan kunnen melden.

De SmartCards zelf zijn beveiligd met een PIN code en worden automatisch geblokkeerd wanneer er drie keer een verkeerde PIN code is ingevoerd.

## Snel

Het hele proces van SmartCard insteken en vervolgens weer toegang hebben tot de volledige desktop is binnen 10 seconden afgehandeld!

## Beheer

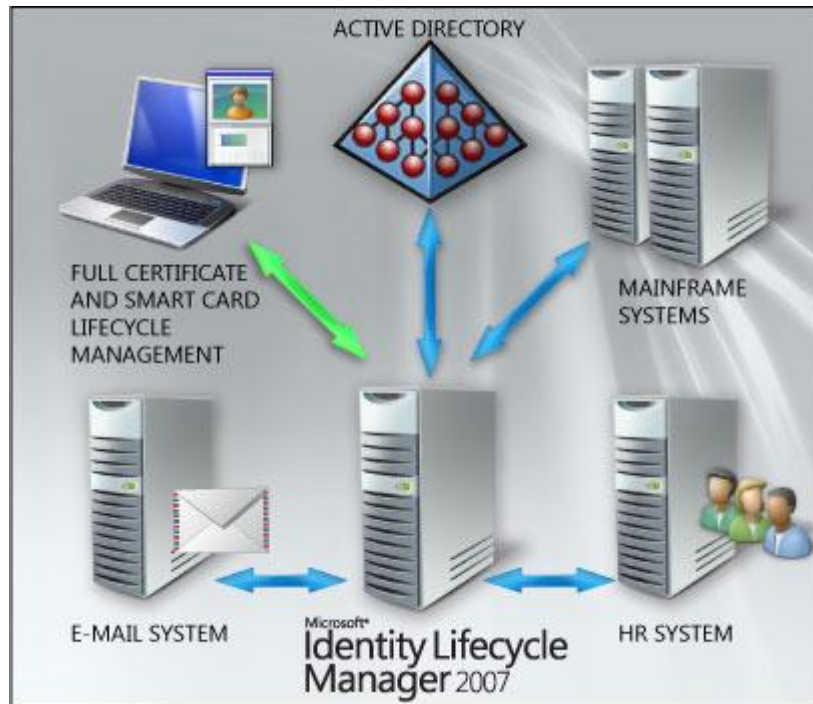
Voor kleinere omgevingen volstaan de standaard door Windows en SmartCard fabrikant geboden beheertools. Tools voor het uitgeven van SmartCards zijn standaard in de meeste Microsoft Operating Systems inbegrepen.



### Identity Lifecycle management

Voor grotere omgevingen is wellicht een extra SmartCard management platform noodzakelijk. Een voorbeeld hiervan is Microsoft Identity Lifecycle Manager 2007 (ILM 2007). ILM 2007 bevat Certificate Lifecycle manager welke de automatisering van de complete SmartCard lifecycle omvat.

Zaken als uitgifte, beheer en rapportage en een self service portal voor gebruikers zitten standaard inbegrepen in ILM 2007. Dit alles volkomen geïntegreerd met Microsoft Active Directory en Certificate Services.



Indien u meer informatie wenst over deze toepassing, neem dan contact met ons op.

GTS-GRAL (NL) B.V.  
Turbinestraat 3b  
3903 LV Veenendaal

Tel.: 0318-550884  
Info@gtsgral.nl  
www.gtsgral.nl