



Telewerken



Inhoudsopgave

1.	Inleiding	4
1.1.	Achtergrond	4
1.2.	In het kort	4
2.	Gebruikerservaring	5
2.1.	Aanloggen met SMS Tokens	5
2.2.	Telewerkportaal – direct in het hoofdmenu	5
3.	Oplossing	6
3.1.	Basis is secure SSL VPN Appliance	6
3.2.	Beveiliging is succesfactor voor telewerken	6
3.3.	Grafische vormgeving in huisstijl	7
3.4.	Modellen en specificaties	7
3.5.	Sterke authenticatie met SMS tokens	8
3.6.	SMS Provider	9
	Appendix: Bedrijfsprofiel Motiv	10

Inleiding

1.1. Achtergrond

Telewerken is niet meer weg te denken. Sommigen kiezen ervoor om 's avonds nog even snel de e-mail te controleren, anderen werken bijvoorbeeld een vaste dag in de week thuis. Vanuit de technologie kent telewerken twee uitdagingen: telewerken moet eenvoudig functioneren. Bij voorkeur via internet. Ten tweede dient de beveiliging goed te zijn geregeld. Het mag niet zo zijn dat hackers via een telewerkvoorziening kunnen inbreken of dat gevoelige gegevens in handen van derden komen. Motiv biedt telewerken waar de beveiliging vanzelfsprekend goed is geregeld. In deze brochure leest u alles over de huidige oplossingen voor veilig telewerken.

1.2. In het kort

De basis van onze oplossing is een telewerkvoorziening die werkt vanaf elke pc met een standaard web-browser. Met behulp van zogenoemde SSL VPN-technologie kunnen gebruikers via een beveiligde webpagina toegang krijgen tot interne systemen inclusief bekende applicaties zoals Microsoft Outlook, Microsoft Office, intranet en standaard (web)applicaties. Om te voorkomen

dat hackers misbruik maken van de telewerkvoorziening, is een extra toegangscontrole met SMS tokens ingebouwd. De gebruiker logt in met z'n standaard gebruikersnaam en bijbehorend wachtwoord. Binnen een paar seconden krijgt hij/zij vervolgens een eenmalige zes-cijferige code op zijn persoonlijke mobiele telefoon. Na het invoeren van deze code krijgt de gebruiker toegang tot de telewerkvoorziening.

De telewerkvoorziening werkt met standaard PC's met Microsoft Windows, Macintosh en LINUX. Wel is het zo dat de gebruiker (zelf) een PC thuis tot zijn/haar beschikking moet hebben. Voor het gebruik van SMS tokens is het gebruik van een mobiele telefoon noodzakelijk.

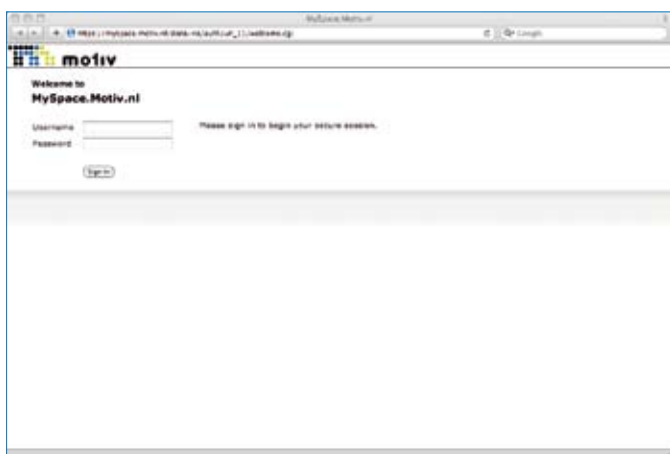
De oplossing kan op twee manieren worden geïmplementeerd. Als eerste als maatwerk op locatie van de klant. Maximale flexibiliteit op specifieke hard- en software van de klant. Ten tweede leverbaar als een dienst voor een vaste prijs per gebruiker via internet. Onze centraal beveiligde telewerkvoorziening wordt in dit geval gekoppeld aan de ICT-omgeving bij de klant.



Gebruikerservaring

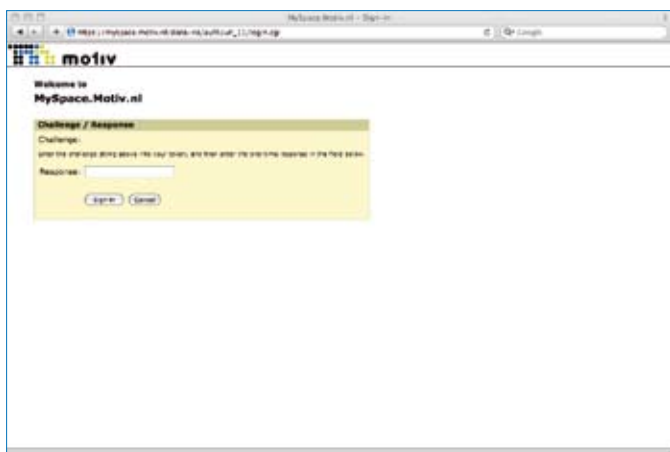
2.1. Aanloggen met SMS Tokens

Log in met een willekeurige PC met internet. Veilig telewerken is beschikbaar voor Microsoft Windows, Macintosh MAC OS (Safari browser) en Linux. De site is beveiligd met een zogenoemd SSL-certificaat (zichtbaar slotje in de webbrowser). De gebruikersnaam en wachtwoord is dus niet zichtbaar voor derden (lees: hackers).



Figuur 1: inlogscherm voor telewerken via elke webbrowser

Gebruik normale gebruikersnaam en bijbehorend wachtwoord. En klik op Sign in. Vervolgens krijg je binnen een paar seconden een flash SMS'je. In deze SMS staat een code van zes cijfers. Tik deze code over in het scherm.

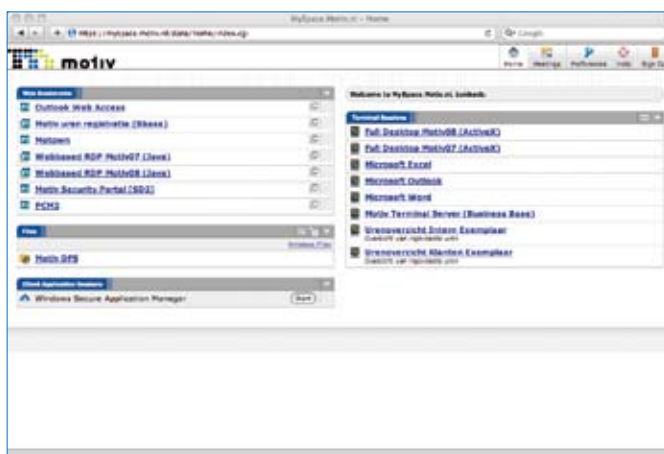


Figuur 2: Sterke authenticatie met SMS token

De gebruiker is nu succesvol aangemeld. Dit is alles.

2.2. Telewerkportaal – direct in het hoofdmenu

Nu verschijnt het hoofdmenu (webpagina) met hyperlinks naar een set van (web)applicaties. Standaard wordt een set van applicaties ondersteund. Voorbeelden zijn Outlook Web Access, intranet, Windows Terminal Server en Citrix. Deze applicaties kunnen we snel beschikbaar stellen via de oplossing voor Motiv telewerken.



Figuur 3: Hoofdmenu voor telewerken via de webbrowser

Standaard worden de volgende applicaties direct vanuit het hoofdmenu ondersteund:

- Alle web based applicaties zoals Outlook Web Access (OWA) en intranet;
- Citrix (via activeX of Java) of Windows Terminal Services (WTS);
- Webapplicaties zoals Oracle Applications en Siebel;
- File sharing via een drive mapping (network connect) of via een webbrowser (met download en upload file).



Oplossing

In veel gevallen worden de standaard webapplicaties zoals OWA direct aangeboden. Voor de overige en standaard kantoorapplicaties (zoals Microsoft Office) geldt dat deze via Citrix of WTS worden aangeboden. Zie ook het screenshot op de vorige pagina.

Motiv Veilig Telewerken is een geïntegreerde totaaloplossing, die werknemers toegang biedt tot toepassingen en bedrijfssystemen via een centraal webportaal. De belangrijkste aspecten die hierbij een rol spelen zijn beveiliging, transparante toegang, passende weergave op basis van uw gebruikte apparatuur (PC, Thin Client, PDA, telefoon) en het personaliseren van informatie op basis van functierollen. De inzet van een transparant portaal heeft verschillende voordelen. Zo zijn uw medewerkers niet langer gebonden aan een vaste werkplek, maar kunnen ze 24 uur per dag overal waar een internetaansluiting is, bedrijfsinformatie ontsluiten. Dat draagt sterk bij aan de flexibiliteit en wendbaarheid van uw organisatie en die van uw medewerkers. Daarnaast hoeft u niet ingrijpend te investeren in aanpassingen aan uw bestaande IT-infrastructuur. Die blijft volledig in tact.

3.1. Basis is secure SSL VPN Appliance

De SSL-VPN security appliance is een veilige, schaalbare en flexibele oplossing voor telewerken. De SSL VPN appliance is een telewerkportaal. De portal is via een versleutelde verbinding (https) via internet bereikbaar.



De belangrijkste eigenschappen van de oplossing zijn hieronder puntsgewijs weergegeven:

- Role based. Op de appliance worden rollen gedefinieerd waar gebruikers aan gekoppeld kunnen worden. Binnen een rol wordt gedefinieerd welke eigenschappen een sessie dient te hebben. Dit geldt zowel voor autorisaties (tot welke resources krijgt een gebruiker toegang), als voor randvoorwaarden waar de gebruikers aan dienen te voldoen (bijvoorbeeld of de client aan bepaalde security eisen voldoet). Binnen het systeem vindt een mapping plaats tussen de gebruikers en de van toepassing zijnde rollen;
- Granulariteit van toegang op basis van rechten en gebruikt platform (security policy);
- In de meeste gevallen kunnen gebruikers bij de SSL VPN-appliance profiteren van single-sign-on. Dat wil zeggen dat zij zich slechts één keer hoeven aan te melden om toegang te krijgen tot alle relevante interne informatiesystemen.
- Gebruikers authenticeren via centrale user directories (bijvoorbeeld LDAP of Active Directory). Het systeem hoeft geen eigen userlijst bij te houden;
- Meerdere portals mogelijk, ieder met een geheel eigen "look and feel";
- Verschillende vormen van toegang voor verschillende gebruikersgroepen huidige en toekomstige, bijvoorbeeld tijdelijke toegang tot een bepaalde applicatie voor derden.
- Ondersteuning diversiteit aan platformen met verschillende typen webbrowsers (Java of ActiveX);
- Ondersteuning aan diverse besturingssystemen. Zo worden bijvoorbeeld Windows, Linux, Mac en Solaris als client ondersteund, maar ook PDA's kunnen toegang verkrijgen tot de diensten;
- Mogelijkheden voor het implementeren van een diepgaande security policy, waarbij lokale data volledig afgeschermd kan worden van de werkplek en versleuteld wordt opgeslagen gedurende de sessie. Na afloop van de sessie wordt deze data definitief verwijderd.

3.2. Beveiliging is succesfactor voor telewerken

Beveiliging is een zeer belangrijke randvoorwaarde voor het telewerken. Zonder beveiliging is niet haalbaar om (interne) informatie over internet te lezen of te verwerken. Onze oplossing biedt een scala aan mogelijkheden voor passende beveiliging.

- De telewerkportaal is gebaseerd op een security appliance van Juniper Networks. Deze appliance is uit zichzelf zeer sterk beschermd tegen aanvallen vanaf internet. De systemen zijn aan

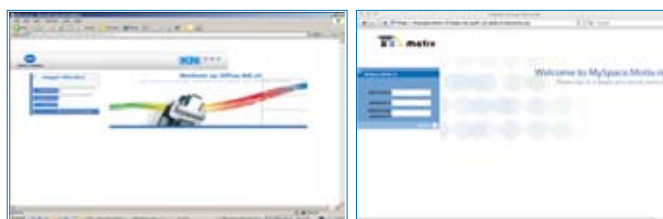
diverse security testen blootgesteld. Voor overheid is er zelfs een speciale versie met EAL-certificering. De appliance is bovendien als absolute marktleider op het gebied van SSL VPN volgens analist Gartner.

- Sterke authenticatie door middel van tokens. Zie tekst en voorbeeld in paragraaf 3.5. Naast de SMS tokens biedt Motiv ook de RSA tokens. Deze digitale sleutels moeten wel worden uitgedeeld aan medewerkers. Het werken met SMS tokens is eenvoudiger, sneller en bovendien goedkoper.
- **Host Security Checker**
Preventieve controle van de PC van de gebruiker op beveiligingsinstellingen. Deze optie is alleen zinvol als de PC een PC/notebook van kantoor is.
- **Cache cleaner**
Voor Windows-gebaseerde werkplekken biedt Cache Cleaner de mogelijkheid om tijdelijk lokaal opgeslagen data, zoals cookies, temp-files, of applicatie cache, van de PC te verwijderen na een SSL-VPN sessie. Hiermee wordt voorkomen dat bepaalde vertrouwelijke informatie achteraf teruggevonden kan worden op de PC. Tevens voorkomt Cache Cleaner het permanent opslaan van gebruikersnamen, wachtwoorden en andere informatie welke gebruikers in webformulieren invullen.
- **Secure Virtual Workspace (SVC)**
De Secure Virtual Workspace gaat nog een stuk verder dan Cache Cleaner. Met behulp van de Host Checker functionaliteit kan op Windows gebaseerde werkplekken een zogenaamde Secure Virtual Workspace worden gecreëerd. Dit is een mechanisme wat er voor zorgt dat alle activiteiten van een gebruiker op de portal plaatsvinden in een volledig beschermd gedeelte van de werkplek. Secure Virtual Workspace versleutelt alle informatie die door applicaties naar de harddisk of het Windows register worden geschreven en vernietigt alle informatie over zichzelf en de SSL-VPN sessie bij het afsluiten hiervan. De SSL-VPN omgeving zorgt ervoor dat de Secure Virtual Workspace client wordt gedownload naar de gebruiker op het moment dat deze zich aanmeldt. Deze client creëert een versleuteld virtueel filesystem en een versleutelde virtuele registry op de PC. Voor het draaien van de Secure Virtual Workspace hoeft de gebruiker geen lokale administrator-rechten op de PC te hebben. SVC kent een aantal beperkingen waardoor dit niet voor alle type (web)-applicaties geschikt is.

3.3. Grafische vormgeving in huisstijl

Tegen meerprijs kan Motiv naast alle implementatie en support services ook het ontwerp op maat leveren. Hierbij moet worden de volgende zaken meegenomen in het project:

- Token met eigen design – zie voorbeelden in de kantlijn¹
- Alle inlog- en uitlog pagina's in eigen huisstijl
- Kleurgebruik en basiszaken van het portaal in de eigen huisstijl (voor zover mogelijk in de appliance)



Figuur 4: voorbeelden van custom design van de SSL VPN Portal

3.4. Modellen en specificaties

Juniper kent een drietal SSL VPN appliances voor de zakelijke markt. Het verschil in de modellen zit voornamelijk in de capaciteit van de appliances. Het aantal gelijktijdige gebruikers is hoger bij een groter model.

Functie	2500	4500	6500
Aantal gelijktijdige gebruikers (maximaal)	100	1.000	>10.000
Aantal gelijktijdige gebruikers (minimale/maximaal) (maximaal)	25/100	50/1.000	50/10.000
Griepandemielicentie - optioneel (dertig dagen maximaal aantal gebruikers)	nee	ja (1.000)	ja (10.000)
Maximale virtualisatie (ondersteuning van vlags e.d.)	nee	optie	optie
Basisapplicaties <ul style="list-style-type: none"> • Web (HTML, Java, ActiveX) • Citrix (ICA, Secure Access Gateway) • WTS (RDP) • File shares • Web shares 	ja	ja	ja
Clustering en load balancing	HA	HA	HA/LB

Alle apparatuur wordt geleverd inclusief een set met licenties en inclusief de software modules network connect (transparante netwerkverbindingen over SSL) en secure application manager (beschikbaar stellen van specifieke applicaties). Daarbij kan de apparatuur worden uitgebreid met de speciale pandemielicentie.

¹ Logo of beeldmerk wordt gedrukt in hart van het token (cirkel van 18,5mm x 18,5mm)

3.5. Sterke authenticatie met SMS tokens

De SMS authenticatie is een vorm van sterke authenticatie op basis van de software van SecurEnvoy. SecurAccess maakt het mogelijk om vertrouwde personen veilig op het bedrijfsnetwerk te laten inloggen. Problemen met wachtwoord - of tokenbeheer en social engineering aanvallen zijn nu definitief verleden tijd. Een elegante oplossing voor een zwaarwegend zakelijk probleem.

SecurAccess is eenvoudig in gebruik. Het gepatenteerde systeem stuurt een passcode van zes cijfers via SMS naar de mobiele telefoon van de gebruiker. De SecurAccess security server leest rechtstreeks alle benodigde gegevens uit de Microsoft Active Directory en andere veelgebruikte directory servers zoals eDirectory. Daardoor is het niet nodig om gebruikers opnieuw te creëren of te synchroniseren in een aparte database. Het systeem kan eenvoudig beheerd worden via de dynamische webpagina's van SecurEnvoy, die veilig en ook op afstand toegankelijk zijn. Zodra het mobiele nummer van een gebruiker in de Active Directory is opgenomen, kan de gebruiker direct aan de slag.

Voordelen van SMS authenticatie

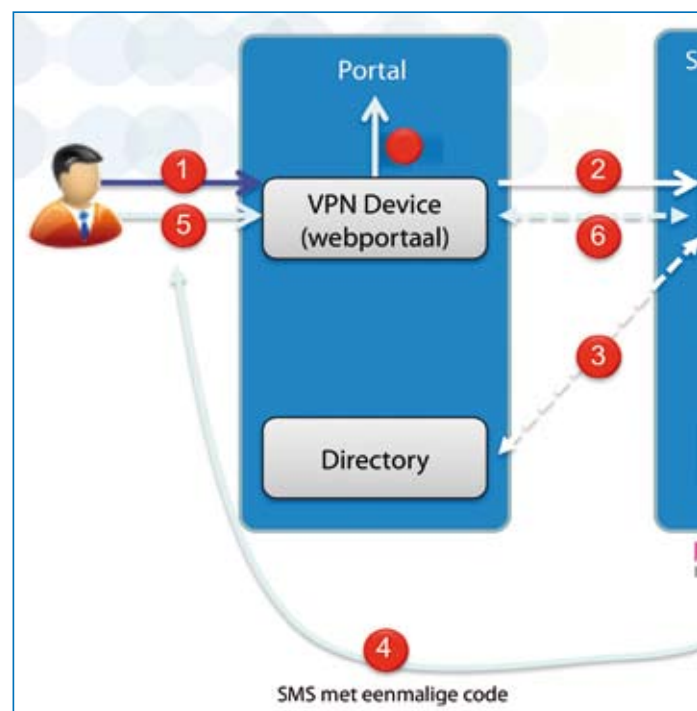
- Krachtige, betaalbare, gebruiksvriendelijke two-factor-authenticatie (gebruikersnaam plus wachtwoord en daarna tokencode via SMS). Met dit systeem maakt u van elke mobiele telefoon een SMS-token. Er is geen specifieke software op de mobiele telefoon nodig.
- Er zijn geen extra hardware tokens nodig.
- Reductie in beheerkosten door dat er geen distributie van tokens nodig is.
- Geen problemen met niet-functionerende hardware bij eindgebruikers.
- Rechtstreeks leesrechten in de bestaande Active Directory, e-Directory, Sun Directory, OpenLDAP (gebruikersnaam, wachtwoord of pincode en mobiele nummer).
- Eenvoudige authenticatiecode van zes cijfers via SMS tekstbericht.
- Eenmalige passcodes voorkomen kwetsbaarheden als gevolg van password guessing of password cracking;
- Flash SMS waarmee een SMS'je eenmalig op de mobiele telefoon verschijnt en na lezen automatisch wordt verwijderd (mits de telefoon deze functie ondersteunt).

De sterke authenticatie werkt met elke mobiele telefoon die SMS'jes kan ontvangen. De oplossing werkt met twee componenten:

- SecurEnvoy SecureAccess server (Windows of Linux). Deze server kan ook op een VMware omgeving worden geplaatst. De server verzorgt de sterke authenticatie. Sterke authenticatie is een combinatie van iets wat een gebruiker weet (wachtwoord)

en iets wat de gebruiker heeft (mobiele telefoon waar de SMS op binnenkomt). Sterke authenticatie met SMS tokens wordt door beveiligingsspecialisten en EDP-auditors als noodzakelijk gezien voor beveiliging van telewerken over internet.

- Interface voor versturen van SMS'jes. De SMS'jes kunnen met een speciale SIM-box worden verstuurd (eigen SIM-kaart van bedrijf nodig) of kunnen als dienst worden afgenomen van een SMS provider. Motiv adviseert gebruik te maken van SMS provider Mollie. Bijbestellen gaat eenvoudig via de website van de SMS Service Provider. De prijs per SMS is plusminus 10 cent. Motiv kan beide opties direct leveren.

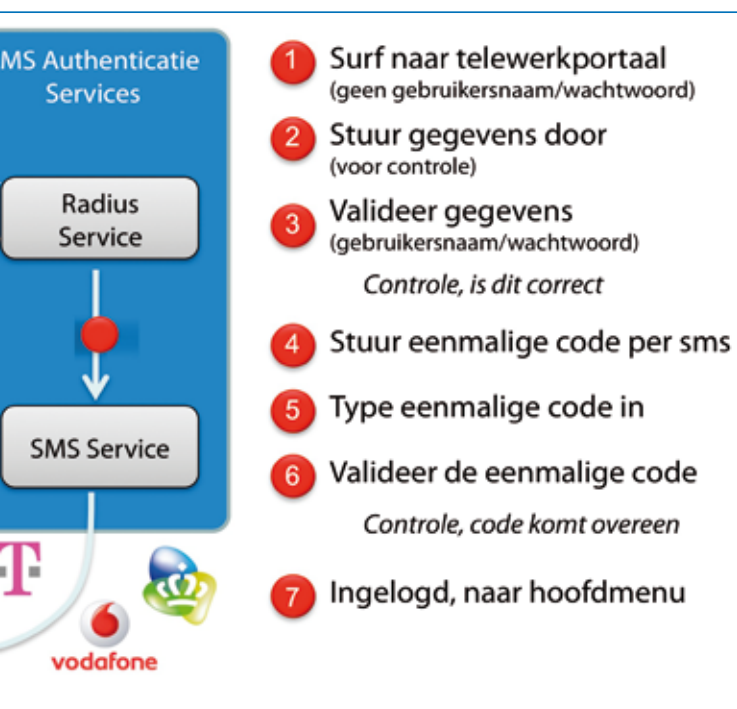


In Figuur 5 wordt het authenticatieproces weergegeven in 7 stappen:

1. De gebruiker logt, op basis van zijn/haar directory credentials (gebruikersnaam plus wachtwoord), in op de SSL VPN portal (Radius agent) bij de klant.
2. De Radius agent stuurt een verzoek naar de SecurEnvoy server voor validatie van de ingevoerde gebruikersnaam en wachtwoord.
3. De Radius server controleert deze credentials op zijn beurt weer bij de LDAP server van de klant. Wanneer de credentials door de directory server zijn gevalideerd stuurt deze een bericht naar de Radius server om aan te geven of de credentials correct zijn. Daarnaast voorziet de directory server de Radius server van het mobiele telefoonnummer van de gebruiker.
4. De Radius server stuurt, wanneer de credentials goed zijn bevonden, een passcode uit naar een SMS provider op het

Internet. De SMS provider stuurt de, door de Radius server gegenereerde, passcode naar het telefoonnummer verkregen uit de directory server.

5. De gebruiker krijgt een challenge pagina te zien in de browser (type de code van het SMS-bericht in) en geeft de ontvangen eenmalige passcode in op deze pagina van de SSL VPN-portal.
6. De SSL VPN-portal verifieert de passcode bij de SecureEnvoy server. De server geeft een antwoord terug naar de SSL VPN portal, waarin wordt aangegeven of de passcode correct is bevonden.
7. Indien akkoord krijgt de gebruiker toegang tot de diensten achter de SSL VPN portal.



Figuur 5: Functionele weergave Managed Authentication Services

3.6. SMS Provider

Motiv adviseert voor deze SecurEnvoy installatie een SMS bundel bij een SMS Provider af te nemen. Motiv werkt met één van de market-leiders in Nederland voor het versturen van SMS. Via een koppeling met de SecurEnvoy worden de SMS'jes bij de provider aangeboden, die ze vervolgens met directe koppelingen naar de verschillende (Nederlandse) operators verstuurd. De SMS Provider levert meerdere bundels die 24 maanden geldig blijven. Voor de kwaliteit van deze bundels zijn meerdere opties mogelijk.

De klant of Motiv kan eenvoudig via internet een SMS bundel inkopen bij de provider. Met een gebruikersnaam en wachtwoord kan de SMS

bundel worden uitgebreid. Ook is het mogelijk om meldingen per SMS tekstbericht te ontvangen als het saldo te laag wordt. Om een indicatie te geven van gemiddeld gebruik van SMS authenticatie adviseert Motiv 125 SMS-jes per gebruiker per jaar in te kopen.

Wat is sterke authenticatie

Voordat een gebruiker toegang tot het informatiesysteem krijgt, zal hij/zij zich moeten identificeren. Normaal gesproken doet een gebruiker dit door het invoeren van een gebruikersnaam en bijbehorend wachtwoord. Wachtwoorden kunnen relatief eenvoudig worden geraden of gekraakt. Om die reden wordt dit controlemechanisme ook wel zwakke authenticatie genoemd. Door meerdere controlemechanismen te combineren is er sprake van sterke authenticatie. Hierbij zijn drie vormen van bewijs bruikbaar:

1. **Kennis, iets wat je weet zoals een wachtwoord of een pincode;**

Iets wat je weet is bijvoorbeeld een wachtwoord, een PINcode of een geheime zin. Het is de bedoeling dat dit bewijs geheim is, het mag niet uitlekken om diefstal van de identiteit tegen te gaan. Een hacker zal proberen de identiteit van iemand over te nemen door een wachtwoord te raden of te kraken. Om die reden wordt in professionele omgevingen dan ook het gebruik van complexe wachtwoorden afgedwongen, die periodiek gewijzigd moeten worden.

2. **Bezit, iets wat bij je hebt zoals een zogenoemd token of mobiele telefoon.**

Dit betekent dat het bewijs van de identiteit wordt geleverd door het gebruikmaken van een fysiek herkenningsteken, dat door of namens het autoriserende systeem werd uitgereikt. Te denken valt aan een 'token' zoals een chipkaart (de smartcard) een USB-sleutel, of een zogenoemd SMS token. Voor controle wordt een eenmalig unieke code per SMS verstuurd naar een bekend mobiel telefoonnummer van de gebruiker. Deze moet de gebruiker – ter controle dat die de telefoon in bezit heeft – invoeren.

3. **Persoonlijke eigenschap, iets wat je bent zoals een vingerafdruk.**

Een uniek identificerend kenmerk van een persoon wordt opgeslagen in een authenticatiedatabase. Een voorbeeld is een vingerafdruk of irisherkenning.

SMS authenticatie met SecurEnvoy is een combinatie van iets wat iemand weet (wachtwoord/pincode) plus iets wat een gebruiker heeft (mobiele telefoon). Daarmee biedt de oplossing een gedegen vorm van sterke authenticatie. Deze vorm is uitstekend en toepasbaar voor telewerken via internet en toegang tot webapplicaties met persoonlijke of gevoelige informatie.

Appendix: Bedrijfsprofiel Motiv

Motiv is sinds 1998 actief als sparringpartner, systems integrator en probleemoplosser voor klanten die zoeken naar innovatieve ICT-oplossingen voor de ondersteuning van hun bedrijfsprocessen. Rode draad in onze activiteiten is de beveiliging van netwerken en gegevens. Of het nu gaat om het optimaal beveiligen van een netwerk of de veilige toegang tot een database, Motiv biedt de juiste oplossing op basis van de in eigen huis opgebouwde expertise. Die combineren we met de geavanceerde producten van toonaangevende leveranciers als Microsoft, Oracle, Juniper Networks en RSA Security.

Sparringpartner - Veel klanten weten wat ze willen en hoe ze het willen, maar schakelen ons toch in om te bepalen of en hoe het beter kan. Zij vertrouwen op onze kennis en expertise op het gebied van databases, netwerken en security en weten dat onze consultants altijd tot het uiterste gaan om creatieve invalshoeken te bedenken bij elke klantvraag.

Probleemoplosser - Uiteraard vragen klanten ons ook gewoon om een concreet probleem op te lossen of een concrete vraag te beantwoorden. En daarbij zoeken we steeds naar onderscheidend vermogen met een creatieve en heldere aanpak.

Systems integrator - De complexiteit van IT-infrastructuren neemt nog met de dag toe. Daarom doen veel klanten een beroep op Motiv bij de integratie van nieuwe technologie in de bestaande omgeving. Zo halen we samen met de klant het uiterste uit alle IT-investeringen.

Probleemoplosser - Uiteraard vragen klanten ons ook gewoon om een concreet probleem op te lossen of een concrete vraag te beantwoorden. En daarbij zoeken we steeds naar onderscheidend vermogen met een creatieve en heldere aanpak.

Transparant

Voor beheer en ondersteuning beschikt Motiv over mogelijkheden voor telefonische ondersteuning, proactief beheer op afstand en bewaking. Uniek is de Service Desk van Motiv, die klanten via het web in een oogopslag alle actuele informatie biedt over apparatuur, wijzigingen, storingen en andere relevante zaken.

Klanten

Motiv is actief in verschillende sectoren en werkt onder meer voor financiële instellingen, telecom- en service providers, lokale en centrale overheden en vele commerciële en dienstverlenende organisaties.





Motiv
Poortdijk 13
NL - 3402 BM IJsselstein

T +31 [0]30 - 68 77 007
F +31 [0]30 - 68 77 006

www.motiv.nl
info@motiv.nl