made**Safe**™

madesafe

User Guide

www.madesafe.com

jbe

Handleiding bij madeSafe

- **madeSafe Cd-rom**
- **madeSafe brochure met alle functies**
- **madeSafe overzichtsbrochure**
- **madeSafe sticker**
- **INTERNETTOEGANG NODIG OM madeSafe TE REGISTREREN**
- **PC-cillin 2002** (proefversie)- een complete virus- en hackerbeveiliging voor uw computer en PDA.
- **Ability Office –** alle software die uw bedrijf nodig heeft. Het biedt u een krachtige tekstverwerker, een spreadsheet, een relatiedatabase en een fotobewerkingsprogramma.

madeSafe Security Companion SE

Naast de MadeSafe Security Companion zijn nog een aantal andere versies leverbaar. In deze handleiding wordt daar naar verwezen. Voor elke versie geldt dat upgrades en service integraal beschikbaar zijn via de knoppen boven aan de interface van de madeSafe Companion.

- **kenmerken**
- Veilige e-mail en Active Stealth Technology, verkrijgbaar als upgrade voor £9.99

- Extra opslagruimte online voor vault, verkrijgbaar voor £9.99

- Standaard Internet-filter op de Home Edition, verkrijgbaar als upgrade voor £19.99

Inhoudsopgave

Hoofdstuk 1 Starten met madeSafe Companion

Wat doet madeSafe?

- Zorgt ervoor dat persoonlijke- en bedrijfsinformatie veilig, beveiligd en verborgen wordt opgeslagen.
- Beschermt de PC tegen hackers.
- Verstuurt op een veilige wijze e-mails
- Accepteert gesproken opdrachten.
- Beheert en controleert persoonlijke veiligheidseisen via één gebruikersvriendelijke interface.
- Houdt het Internet veilig voor kinderen.
- Slaat bestanden op en haalt 'secure files' (beveiligde bestanden) op vanaf elke willekeurige plek ter wereld, zelfs wanneer uw PC gestolen is!
- De multi user versie maakt het mogelijk om op elk gewenst moment nieuwe gebruikers toe te voegen.
- Veel extra functies en upgrades voor het aanpassen van madeSafe aan uw persoonlijke en specifieke behoeften.

madeSafe garandeert de best mogelijke gegevensbescherming- en beveiliging. madeSafe is wereldleider in encryptie software. De kunstmatige intelligentie is in staat het hoofd te bieden aan bedreigingen, die door de voortschrijdende techniek, van een steeds hoger niveau zijn.

Security Companion

De madeSafe Security Companion™ is een grafische interface, met zeer gebruikersvriendelijke encryptie software. De functies van madeSafe om bestanden te beveiligen zijn eenvoudig en direct te benaderen..

De madeSafe Security Companion™ heeft vier verschillende functionaliteiten voor gegevenssbeveiliging en voor optimalisering van PC-prestaties.

. De functies zien er als volgt uit:

- Knoppen voor Profiel en Uitbreiding
- Optimalisering en hulpprogramma's voor opslag
- Bestand, drive en vensters met directory’s
- Encryptie

Encryptie

De supersnelle wereldleidende 448-bit encryptie is slechts met één handeling (klik) te bewerkstelligen. Snelheid en encryptiegraad zijn volledig instelbaar. Bescherm hiermee uw vertrouwelijke persoonlijke- en professionele informatie tegen hackers en niet geauthoriseerde gebruikers.

Beveiligde e-mail

Super encrypted e-mailbijlagen kunnen zonder problemen over de hele wereld gestuurd worden. De geadresseerde kan het bericht decoderen zonder zelf madeSafe te hebben.

Krachtige hulpprogramma's

Een krachtige combinatie van beveiligingsopties

Scan – controle van een gekozen drive op vertrouwelijke bestanden.
Opruimen – verwijdering van niet actuele bestanden (dit geeft extra vrije ruimte op de harde schijf), verwijdering van de toetsaanslagenhistorie (om te voorkomen dat hackers beveiligde bestanden, nieuwe bestanden en bestandsdata kunnen vinden).
Versnipperen – veilige definitieve verwijdering van een bestand of document.
Stealth –madeSafe's Active Stealth Technology garandeert de ultieme beveiliging voor alle encrypted gegevens en zorgt ervoor dat de bestanden niet weergegeven worden in de directory's.

Internetfilter – madeSafe Shield

Enkele hoofdfuncties en kenmerken van SHIELD:

- ✓ Blokkeren van ongewenste websites.
- ✓ Filteren van sites met behulp van URL database en Meta Tags I.E: (trefwoord en omschrijving)
- ✓ Constante bijwerking van de De URL-database van geblokkeerde sites.
- ✓ Mogelijkheid tot uitschakeling van Pop-up-vensters.
- ✓ Ouder/beheerder controle (de gebruiker heeft hierop geen rechten).
- ✓ Toevoegen van aangepaste URL's en trefwoorden.
- ✓ Controle van gebruikers die toegang proberen te krijgen tot geblokkeerde sites.
- ✓ Het programma werkt onopvallend in de taakbalk.
- ✓ Registratie van alle Internetverkeer (bezochte sites, aantal keren en gebruikers).

Ultraveilig opslaan en ophalen

Gebruik Vault voor het dupliceren van de belangrijkste vertrouwelijke informatie op onze ultraveilige madeSafe website. Voor veilig kopieëren en ophalen. Wereldwijd, 24 uur per dag, 365 dagen per jaar. De toegang wordt u persoonlijk toegekend.

Multi-user opties, netwerkgereed

Extra gebruikersvergunningen, gegevensbescherming en beveiliging voor het hele bedrijf.

Uitbreiding van bestaande madeSafe toepassingen voor meerdere gebruikers. Elke upgrade maakt een uitbreiding van drie gebruikers mogelijk.

Diensten en opties

Een groot aantal diensten garanderen volledige veiligheid:

Bescherming tegen verloren wachtwoord

Opslag van wachtwoorden voor beveiligde bestanden in onze encrypted kluis.

Veiligheidscontrole

Downloadable software voor een complete veiligheidscheck-up van uw netwerk of PC.

Diefstaldetectie

Een geïntegreerd hulpprogramma stuurt in geval van diefstal een e-mail zodra met de desbetreffende PC verbinding wordt gezocht met het Internet.

madeSafe helpdesk

Algemene telefonische ondersteuning, degelijke technische ondersteuning en begeleiding om madeSafe producten zo optimaal mogelijk te gebruiken.

madeSafe verzekering

Profiteer van de voordelen van onze wereldwijde all-riskverzekering voor laptop of PC.

Upgrades en updates

Levenslang recht op productverbetering, gratis updates, kortingen en speciale aanbiedingen.

Vault upgrade: De opslagruimte van de kluis is op elk moment naar wens uit te breiden.

Internetfilter upgrade: regelmatige upgrades voor de Internet-categorieënfilter teneinde up-to-date te blijven en continu beschermd tegen ongewenste zaken.

Installeren van madeSafe

Systeemvereisten

madeSafe werkt in een Microsoft Windows-omgeving. Wanneer u werkt met Windows zult u de integratie van madeSafe Security Companion in uw bureaublad zeker waarderen.

Minimale systeemvereisten voor de installatie van madeSafe:

- IBM™ PC of compatibel
- Microsoft® Windows 95, 98, 2000, NT, ME of Windows XP
- 486 processor of hoger
- 16MB RAM
- 100MB ruimte op de harde schijf
- Een webbrowser (bij voorkeur IE4 of Netscape 4 of hoger)
- VGA of hoger met 256 kleuren
- Cd-rom
- Internet-toegang met een **geldig** E-mail-account
- Geluidskaart en microfoon (optioneel)

Installatie

Volg onderstaande procedure om madeSafe te installeren

1 Start Windows (wanneer dit nog niet opgestart is).

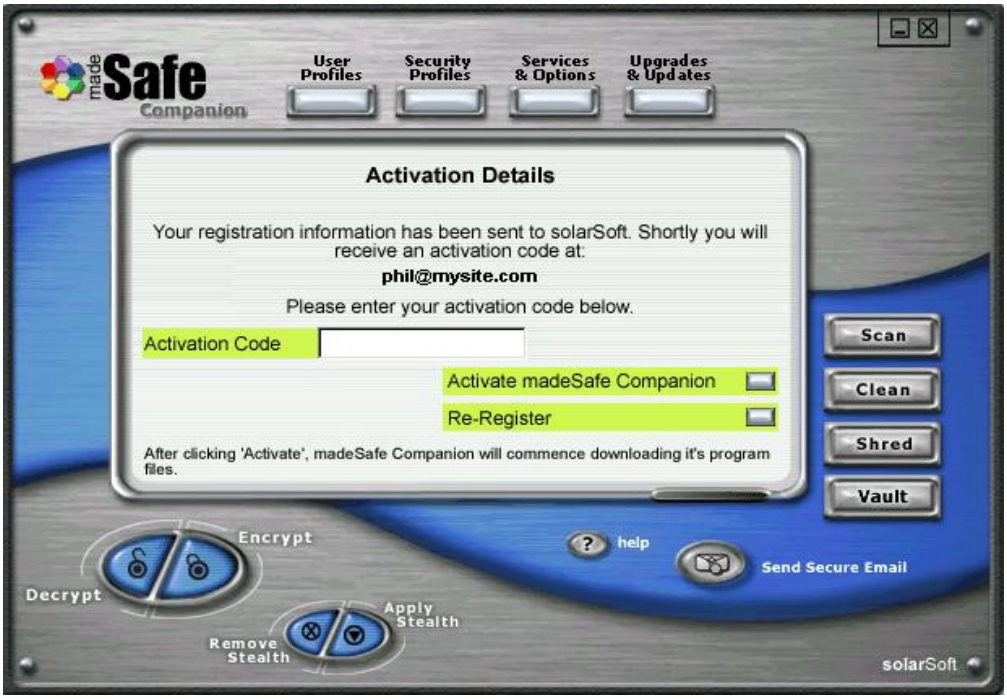
2 Doe de madeSafe CD in het CD-ROMstation.

3 Klik in het openingsscherm op ***Install madeSafe*** en volg nu de instructies op het scherm.

Installatie en registratie

Na installatie vraagt het programma om een hoofd\beheerdersaccount te openen. Vul dan naam, e-mail-adres en een bevestigend (minimaal uit 8 tekens bestaand) wachtwoord in. (BELANGRIJK! VERGEET DE HOOFDWACHTZIN NIET) daarna voert u de cd-code in voor de registratie.

onze server vraagt u nu (via een beveiligde e-mail) specifieke informatie, benodigd om u een persoonlijke activeringscode te verstrekken. Voer de verkregen code in in het activeringsvak (bij voorkeur door kopieëren en plakken) en klik dan op '***Activate***'. Nu worden de componenten gedownload die het gebruik van madeSafe mogelijk maken.



Hoofdstuk 2 Configuratie van Security Companion

De hoofdgebruiker wordt tijdens de installatie en registratie ingesteld.
De hoofdwachtzin kan niet worden veranderd, maar de naam wel. Selecteer de naam en vul een nieuwe naam in. Daarna klikken op ***Apply change***.
Om een gebruiker toe te voegen klikt u op het pulldown menu en selecteert een nieuwe gebruiker, voer de naam en de wachtzin in. Daarna klikken op ***Apply change***.
Het verwijderen van een gebruiker is net zo gemakkelijk. Selecteer de gebruiker via het menu en klik op ***Delete selected user***. Klik op ***Finished*** om terug te keren naar het hoofdmenu.
De hoofdgebruiker heeft volledige toegang tot de bestanden van andere gebruikers.

Bedrijfs-setup

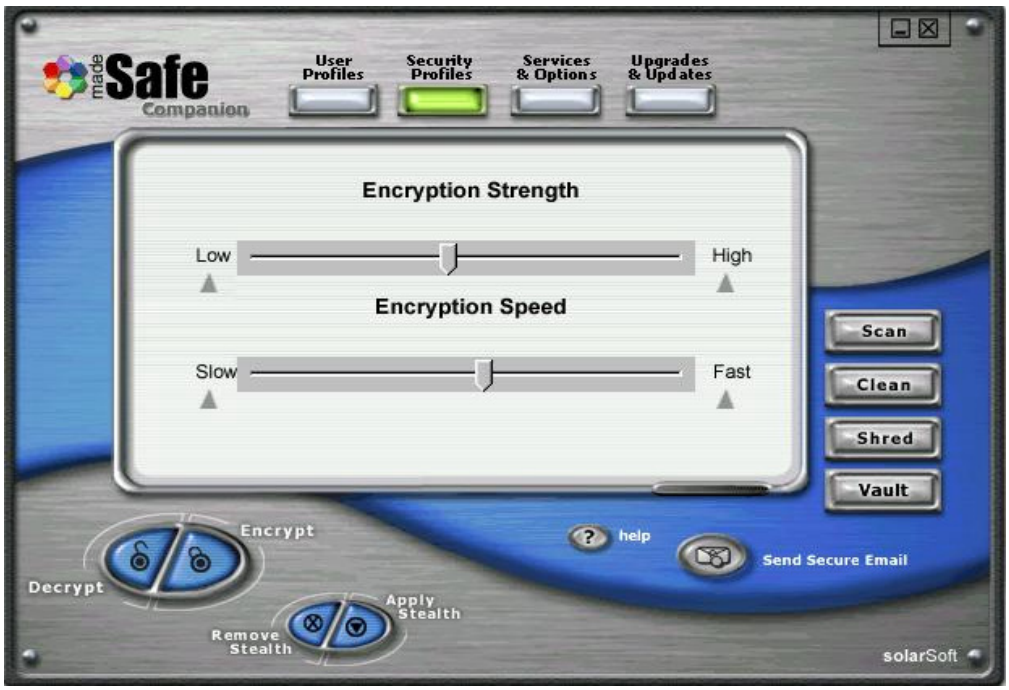
De hoofdgebruiker moet madeSafe Companion eerst op zijn/haar eigen computer installeren en activeren, alvorens installatie op de computers van de andere gebruikers kan plaatsvinden. Nu moet tijdens de installatie niet de cd-code worden ingevuld, maar voert de hoofdgebruiker ***Network*** in en klikt op ***Activate***.
De hoofdgebruiker wordt hierop gevraagd om in het netwerk te zoeken naar de hoofdgebruikersinstallatie.
b.v. \\Admin\C:\ProgramFiles\solarsoft\madesafe.
NB: de drive op de computer van de hoofdgebruiker moet een gemeenschappelijke schijf zijn.
klik op ***OK*** nadat de directory is gevonden om de installatie te voltooien.
De hoofdgebruiker kan alle accounts nu vanaf zijn/haar computer beheren.
De hoofdgebruiker kan zich nu bij elke computer aanmelden waarop madeSafe is geïnstalleerd (met behulp van een tweede of derde gebruikersnaam en wachtwoord) en heeft tevens toegang tot alle encrypted gegevens.

WAARSCHUWING: PORBEER GEEN GEGEVENS TE DECODEREN DIE NIET **DOOR UZELF** ENCRYPTED ZIJN!!!

Voorbeeld: EEN TWEEDE GEBRUIKER PROBEERT EEN BESTAND TE DECODEREN DAT DOOR DE HOOFDGEBRUIKER IS ENCRYPTED: DIT HEEFT TOT GEVOLG DAT HET BESTAND WORDT VERNIETIGD!!!

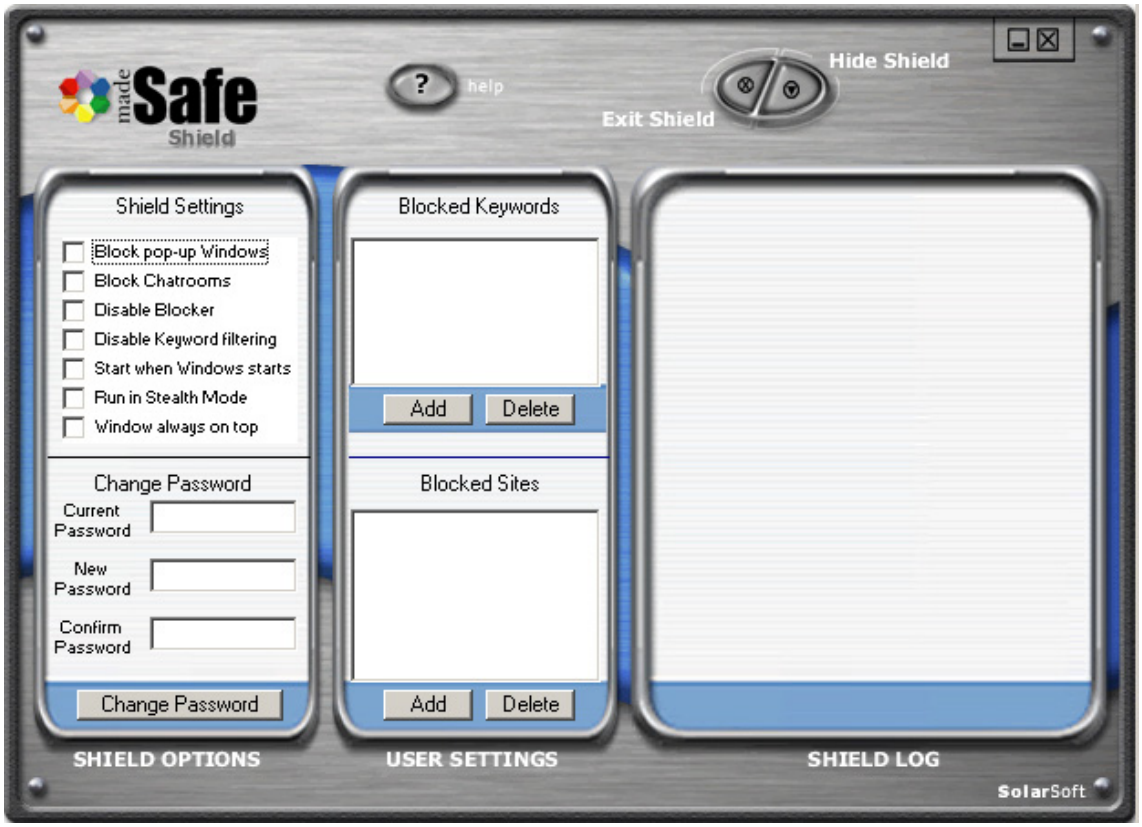
Beveiligingsprofielen

madeSafe biedt de volgende drie functionaliteiten:***Encryption Setup***, ***Filtering Setup*** en ***Database***. De Encryption Setup heeft twee schuifbalken (zie onder) waarmee de encryptiegraad of de snelheid van de encryptie kan worden geregeld. De snelheid neemt af wanneer de encryptiegraad wordt verhoogd. Evenzo neemt de encryptiegraad af wanneer de snelheid wordt verhoogd.



Internet-filter

Filter Setup: met deze opties kan het surfgedrag op internet volledig naar wens aangepast worden. Alleen de hoofdgebruiker kan de filteropties configureren.



Bij het zoeken van toegang tot het filter (Shield) wordt via de taakbalk gevraagd om een wachtwoord. Het standaard wachtwoord is Password. Dit kan op een later tijdstip worden gewijzigd.

Filteropties
Block pop-up windows– een functie om reclamevensters te blokkeren.
Block chatrooms– blokkeert de toegang tot alle chat-ruimtes.
Disable blocker– het filterprogramma wordt hiermee uitgeschakeld.
Disable keyword filtering- hiermee wordt het blokkeerprogramma voor trefwoorden uitgeschakeld.
Start when Windows starts– deze functie start het filter automatisch en tegelijk met Windows op.
Run the Stealth mode– hiermee kan het programma onopvallend op de achtergrond functioneren.
Windows always on top– zorgt ervoor dat het het filter in elk venster op de voorgrond aanwezig is.

Blocked Keywords – madeSafe heeft een ingebouwde lijst met trefwoorden, waaraan naar wens trefwoorden kunnen worden toegevoegd.
Blocked Sites – hiermee kunnen bepaalde websites worden geblokkeerd.

Shield Log – hiermee worden alle Internet-activiteiten op de PC geregistreerd. De informatie bevat naam, datum, tijd en bezochte websites.

Beveiligingsdatabase

Met deze functie kan de hoofdgebruiker de beveiligingsinstellingen aanpassen. Een bedrijf heeft bijvoorbeeld te maken heeft met autoverkoop en de winstmarges zijn binnen het bedrijf niet openbaar. Door simpelweg "winstmarges" aan de database toe te voegen weigert madeSafe iedereen behalve de hoofdgebruiker toegang tot alle bestanden die gaan over "winstmarges". De database kan onbeperkt worden aangevuld met trefwoorden.

Encryptie

Encryptie is nog nooit zo eenvoudig geweest. Kies eerst de drive, daarna de desbetreffende map en tenslotte het bestand of de bestanden die u wilt encrypten, klik vervolgens op de knop ***Encrypt.***

Dat is alles! Deze bestanden zijn nu **alleen** voor diegene, die ze encrypt heeft, toegankelijk.

Bestanden ontgrendelen (decoderen) is net zo gemakkelijk. Selecteer de encrypte bestanden en klik op ***Decrypt***.

Encrypte bestanden worden herkend aan de extensie: ENC

Stealth

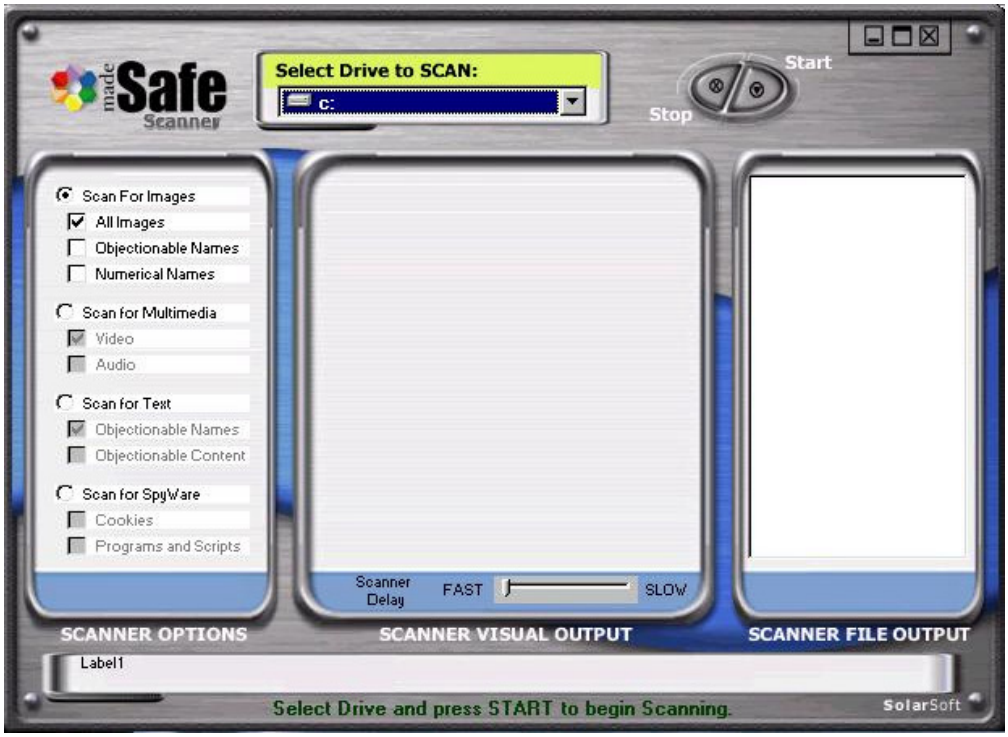
Voor ultieme beveiliging kunt u Stealth als extra optie kiezen. Wanneer Stealth op encrypte bestanden wordt toegepast, worden deze onzichtbaar bij het normaal browsen op een harde schijf. Selecteer de map met de encrypte bestanden en klik op ***Apply Stealth***. De encrypte bestanden zijn nu niet langer zichtbaar in de directory's.

Om de verborgen bestanden te bekijken moet de desbetreffende directory worden geselecteerd, kies vervolgens de knop ***Remove Stealth***.

Stealth verbergt alleen encrypte bestanden. Alle andere bestanden blijven zichtbaar in de map.

Scan

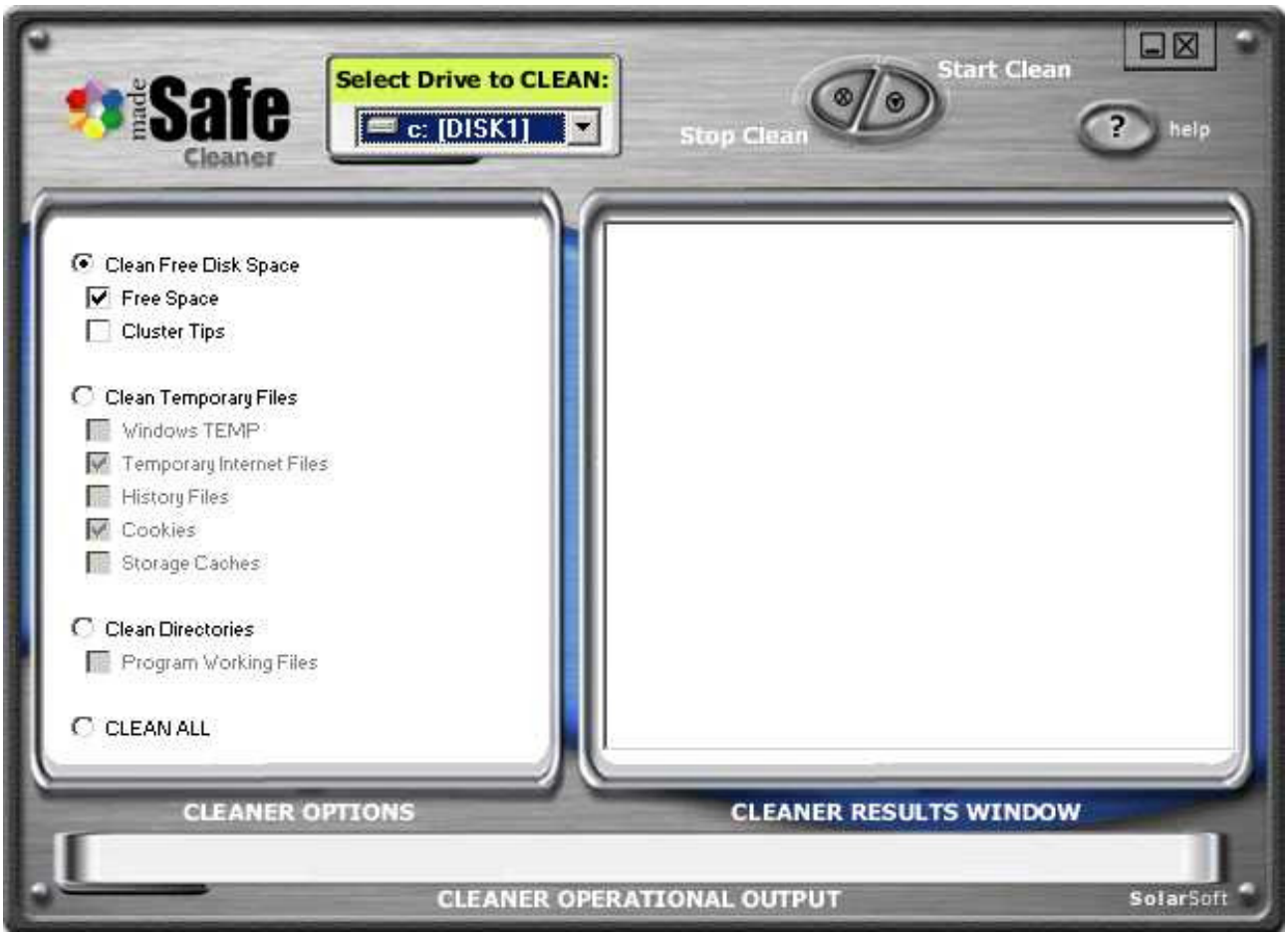
Een functie om de harde schijf te controleren op ongewenste zaken. Er kan gezocht worden naar naar beelden, video en tekst of elk ander type bestand dat verdacht mocht zijn.



Selecteer het type bestand waarnaar gezocht moet worden en klik op ***START***. Het middelste venster toont de gevonden bestanden. Dit proces kan worden vertraagd zodat de bestanden langer zichtbaar worden. Het rechter venster laat een overzicht zien van de gevonden bestanden. Van hieruit kunnen ze ingezien worden.

Opruimen

Een functie om de harde schijf te reorganiseren, zodat er schijfruimte op de computer vrijkomt. Niet actuele of niet gebruikte bestandsclusters worden gewist. Tevens wordt de toetsaanslagenhistorie verwijderd, om te voorkomen dat hackers wachtwoorden en bestanden kunnen opsporen. Deze functie kan het best worden gebruikt na het versnipperen van een of meerdere bestanden. Omdat deze functie grondig te werk gaat, kan dit enige tijd in beslag nemen, uiteraard afhankelijk van de gekozen opruimwerkzaamheden.



Versnipperen

Een krachtig programma voor het vernietigen van computerbestanden. Een eenmaal versnipperd bestand kan nooit meer worden hersteld en is definitief verdwenen. Dus:‘’bezint eer ge begint’’.

Er wordt u gevraagd of u zeker weet of u het bestand wilt verwijderen.

Beveiligde e-mail

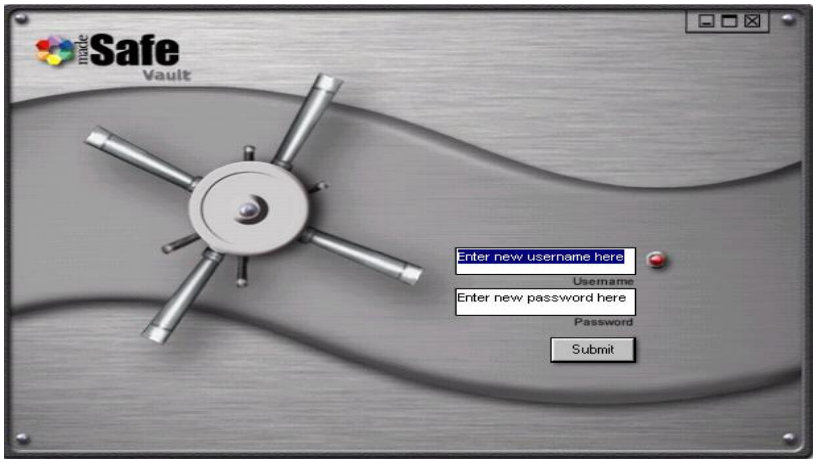
Deze procedure maakt het mogelijk om om superencrypted bestanden te versturen over de hele wereld, zonder dat de geadresseerden zelf madeSafe op hun computer geïnstalleerd hebben.

Selecteer het gewenste beveiligingsniveau (***High Security*** of ***Low Security***) Nu wordt gevraagd om de te beveiligen e-mailbijlage te selecteren. De madeSafe assistent leidt u door het hele proces. In de verzonden e-mail staan instructies voor de ontvanger over hoe de bijlage te openen. (de geadresseerde moet WinZip op zijn/haar computer geïnstalleerd hebben). Daarnaast heeft de geadresseerde van u een wachtwoord nodig om de bijlage te decoderen.

Instructies voor Vault

Vault is gemakkelijk te gebruiken. Zodra u uw gebruikersnaam en wachtwoord heeft ingevoerd krijgt u het bovenstaande scherm te zien. Er kunnen 10 laden worden gebruikt. U kunt elke lade een willekeurige nieuwe naam geven.
De lade wordt geopend door op het groene lampje te klikken. De inhoud van de lade wordt nu zichtbaar.

Bestanden kunnen eenvoudigweg door verslepen in de kluis of in een open lade gezet worden. Het programma vraagt of u het bestand nu of later wilt versturen. Als u kiest voor later, dan worden de bestanden in een wachtrij geplaatst. Wanneer u klaar bent met het selecteren, klikt u op de knop ***Send Files***. De procedure voor het ophalen van bestanden verloopt in omgekeerde volgorde. Selecteer de bestanden in de kluis en klik op de knop ***Receive Files***.
Terwijl de kluis gevuld wordt met bestanden, geeft de capaciteitsmeter aan hoeveel ruimte er nog over is. Wanneer de kluis voor 85% vol is, adviseert het systeem om de kluisruimte uit te breiden. Voor tarieven en verdere instructies verwijst het systeem u naar de website.



Toegang tot madeSafe Vault via een externe verbinding

NB: Een madeSafe programma is niet nodig om toegang te krijgen tot madeSafe Vault

volg de onderstaande procedure voor internationale toegang tot madeSafe Vault 24/7:

1) Open uw Internet-browser en voer in: www.madesafevault.com
2) Voer uw cd-code in (het nummer voor installatie op de hoes van de CD). Voer uw actuele Vault wachtwoord in.
3) Alvorens u de beveiligde bestanden kunt ophalen en decoderen, moeten er drie bestanden gedownload worden. Deze bestanden vindt u op de pagina ***Welkom bij uw Vault***.
4) Deze procedure geldt voor elke PC die gebruikt wordt voor toegang tot madeSafe Vault.

Hoofdstuk 3 Wat betekent uw persoonlijke veiligheid voor u?

De belangrijkste kwestie in de 21e eeuw

De opslag van vertrouwelijke persoonlijke- en bedrijfsinformatie wordt door de huidige technische ontwikkelingen steeds meer bedreigd. (diefstal, fraude en vernietiging) .

De commerciële noodzaak van elektronische centralisering van gevoelige informatie geeft ruim baan aan hackers en cyberterroristen. Op zowel emotioneel- als op financieel vlak kunnen inbraken van dergelijke figuren catastrofale gevolgen hebben. In een van haar laatste publicaties wees de FBI er op dat de grootste dreiging en de meest fraude zich afspeelt binnen de eigen organisatie.

Iedereen loopt risico!

Niet alleen bedrijven lopen risico op het Internet. Telkens wanneer u, vanuit uw eigen huis, een verbinding maakt met het Internet, biedt dit indringers een mogelijkheid zich een weg te banen naar uw PC en uw persoonlijke informatie

Huidige beveiligingsoplossingen

De huidige beveiliging tegen deze dreiging is onder te verdelen in drie categorieën:
firewall, anti-virus en eenvoudige encryptiesoftwarepakketten.

De veelheid aan virussen en de steeds geavanceerder technieken om ze aan te maken, zorgen ervoor dat anti-virus software onmisbaar blijft voor personen en bedrijven. De software beschermt onder andere tegen virussen die een PC blokkeren, programma's ontwrichten en zichzelf via e-mail kunnen verspreiden, Echter anti-virussoftware heeft geen enkele funcionaliteit om de vertrouwelijkheid van de data te beschermen.

Firewalls (zowel hardware als software) hebben in verleden bewezen relatief weinig bescherming te bieden tegen een vastberaden hacker. Ook beschermen Firewalls niet tegen ongeautoriseerde gebruikers binnen de eigen organiatie. Encryptie van gegevens lijkt dus de beste oplossing. Maar de huidige encryptiesoftware is vaak te gecompliceerd of biedt (met het oog op de steeds verdergaande technologische ontwikkelingen) geen 100% beveiliging.

Deze dreiging kan het hoofd geboden worden door een nieuwe wijze van denken en nieuwe technieken.

Het antwoord is:

Stelt u zich het volgende voor:

U bent een goede netwerkbeheerder en u heeft de beste maatregelen getroffen voor de beveiliging van uw netwerk. De firewall functioneert met alle nieuwste patches. De routers zijn correct geconfigureerd. Elke toestemming voor gebruiker of groep is gecontroleerd. Op zekere dag moet u bij de directie verschijnen. Deze meldt u dat verschillende klanten gereclameerd hebben over het feit dat hun creditcardnummers zijn belast zonder hun toestemming. Bovendien is de creditcard van het bedrijf ook zonder toestemming voor 15.000 euro belast. Een gedetailleerde inspectie van de logboekbestanden laat een paar doorbraakpogingen zien, echter zonder succes. Na een tweede en derde controle moet geconcludeerd worden dat het gaat om iemand binnen het bedrijf.zelf. U controleert de logins op de server waar de klantgegevens zijn opgeslagen. De enige logins zijn die van uzelf. U gaat vervolgens naar de server waar de financiële gegevens van uw bedrijf zijn opgeslagen.De enige logins daar zijn van de directeur. De tijdmarkering van de login geeft aan dat er een login van de directeur was, ten tijde dat hij ergens een conferentie bezocht. Van uw eigen logins vond er ook een plaats toen u de hele dag in vergadering was met het hoofd van de IT-afdeling. Iemand heeft dus fysiek toegang tot uw servers en is in de gelegenheid om gebruikersinformatie te stelen, inclusief namen en wachtwoorden van gebruikers.

Dit is weliswaar een fictieve situatie, maar regelmatig spelen dergelijke zaken zich in werkelijkheid af. Wanneer iemand fysiek toegang heeft tot uw server kan hij/zij alle informatie op de server benaderen. Op deze manier kan het netwerk gekraakt worden en informatie gestolen of gekopieerd. Dit kan alleen voorkomen worden door de toegang tot de servers te beperken. Fysieke beveiliging beperkt zich uiteraard niet tot alleen servers, maar geldt ook voor laptops en werkstations. Dit gaat u als klant aan, maar is ook essentieel voor de IT-professional.

Het antwoord is:

Hoofdstuk 4 Probleemoplossing

VEEL GESTELDE GESTELDE VRAGEN

1) **Hoe encrypt ik een persoonlijk bestand?**

Open de companion en selecteer de schijf waarop het te ecncrypten bestand staat in de ‘drive list’. Selecteer de desbetreffende directory en markeer het bestand. Klik op de knop ‘***Encrypt***’. Alleen u kunt het bestand nu lezen.

2) **Hoe kan ik een encrypted bestand identificeren/decoderen?**

Encrypte bestanden zijn herkenbaar aan het bestandstype.ENC Markeer ze en klik op '***Decrypt***' om ze te ontsluiten.

3) **Ik heb enkele bestanden encrypt en nu kan ik ze niet vinden.**

Tijdens de encryptie heeft u mogelijk Stealth toegepast. Selecteer de directory en klik op ***'Remove Stealth'***. Nu wordt Stealth van ALLE encrypte bestanden verwijderd.

4) **Ik heb mijn wachtwoord vergeten. Hoe kan ik mijn gegevens herstellen?**

Solarsoft adviseert in deze om het wachtwoordbeschermingprogramma aan te schaffen.Om uw wachtwoord weer terug te vinden, volgt u de procedure voor verloren wachtwoorden. Zonder dit wachtwoordbeschermingsprogramma zijn de bestanden onherstelbaar.

5) **Ik heb gevoelige informatie die ik permanent van mijn computer wil verwijderen. Hoe moet ik dit doen?**

Markeer in companion het bestand dat u blijvend wilt verwijderen en klik vervolgens op ***Shred*** Het bestand wordt nu onherstelbaar vernietigd.

6) **Ik heb madeSafe Home en wil mijn eigen kluis (Vault) hebben. Hoe moet ik dit doen?**

Om Vault aan te schaffen klikt u in companion op ‘***Upgrade’***.Volg verder de instructies op het scherm.

7) **De kinderen klagen over een slecht werkend internet.Wat is de ooprzaak?**

Sommige Internet-pagina's verschijnen in een nieuw venster. Deze functie is als standaard geactiveerd. Om deze functie te deactiveren klikt u op het pictogram in de werkbalk, kies dan voor ***Disable pop-up windows***.

8) **Kan ik encrypte e-mail versturen wanneer de geadresseerde geen madeSafe heeft?**

Ja. Klik op de knop ***Send secure e-mail*** en de madeSafe assistent leidt u door het hele proces.

Hoofdstuk 5 Verklarende woordenlijst

Active Stealth Technology™
Met de Active Stealth Technology van madeSafe kunt u reeds encrypte gegevens zodanig verbergen, dat een hacker of indringer geen enkele complete bron of ingang kan vinden.

Algoritme (hekje)
Een aantal wiskundige regels (logica) die gebruikt worden voor het maken van berichten en sleutels/handtekeningen.

Algoritme (encryptie)
Een aantal wiskundige regels (logica) die gebruikt worden voor encryptie en decodering.

Anti-virus
Software die een PC beschermt tegen virussen vanuit het Internet. Dergelijke virussen beschadigen PC's met alle nadelige gevolgen van dien.

Asymmetrische sleutels
Een afzonderlijk maar geïntegreerd sleutelpaar dat bestaat uit een algemene- en een persoonlijke sleutel. Elke sleutel is enkelvoudig toepasbaar. Dit betekent dat een sleutel die gebruikt wordt voor het encrypten van informatie, niet gebruikt kan worden om dezelfde informatie te decoderen.

Autorisatie
Het verlenen van officiële goedkeuring, toegang of wettelijke bevoegdheid aan een rechtspersoon.

Bestandsoverdrachtprotocol (FTP)
FTP is een programma dat gebruikt wordt om bestanden vanuit PC of netwerk op Internet plaatsten.

Beveiliging
Bescherming tegen ongeautoriseerde toegang tot computergegevens, hardware, telecommunicatielijnen en softwaretoepassingen.

Blind signature
De optie om documenten te ondertekenen zonder de inhoud te kennen, vergelijkbaar met een zogenaamde "notary public".

Block cipher
Een symmetrische decoder die werkt op onbewerkte tekstblokken en sleuteltekst, normaal 64 bits.

Blowfish
Een uitgebreide block cipher, symmetrisch algoritme

Certificaten
Een digitale ID die uitgegeven wordt door een erkende uitgever om gegevensoverdracht via het internet te verifiëren en te valideren.

Cipher-tekst
Onbewerkte tekst, omgezet in een geheim formaat door een encrypted algoritme. De oorspronkelijke onbewerkte tekst kan worden gedecodeerd met een ontcijferingssleutel.

Cliënt
Een computer die op een server is aangesloten. Wanneer uw PC bijvoorbeeld wordt aangesloten op een ISP of bedrijfsnetwerkcomputer, is uw PC de cliënt en is de ISP of bedrijfsnetwerkcomputer de server.

Codering
Beschermt een e-mailbericht en bijbehorende gevoelige documenten.

Companion™
madeSafe Security Companion is een gemakkelijk te gebruiken interface die u één omgeving biedt vanwaaruit producten, upgrades en diensten van madeSafe bereikbaar zijn.

Cookie
Een klein stukje informatie dat een webserver via uw webbrowser kan opslaan op uw harde schijf en later via uw browser terug kan lezen. Websites verzamelen informatie over hun bezoekers op basis van een hulpprogramma dat een Cookie wordt genoemd. Het gaat hier om commerciële informatie over het surfgedrag van de bezoeker. De door de cookie verzamelde informatie wordt op de harde schijf van de bezoeker opgeslagen. Dus wanneer u een site meer dan een keer bezoekt, opent die site uw cookiebestand om te zien wat u eerder hebt bekeken. Zo komen de desbetreffende sitebeheerders erachter op welke gebieden uw interesses liggen. Cookies zijn automatisch opgenomen in zowel Netscape Navigator als Microsoft Internet Explorer, maar kunnen uitgeschakeld worden

Cryptografie
De kunst en wetenschap van het maken van cryptische teksten

Data-integriteit
Een methode die garandeert dat informatie niet is gewijzigd of aangepast via een ongeautoriseerde of onbekende weg.

Decoderen (1)
Het opheffen van de beveiliging van een e-mailbericht en ondersteunende documenten.

Decoderen (2)
Methode voor het decoderen van encrypted informatie zodat die weer leesbaar wordt. De ontvanger van de informatie gebruikt een persoonlijke sleutel om te decoderen.

DES (Data Encryption Standard)
Een 64-bit block cipher, symmetrisch algoritme dat ook bekend staat als Data Encryption Algorithm (DEA) bij ANSI en DEA-1 bij ISO. Een algemeen gebruikte standaard.

Digitale certificaten
Documenten die worden uitgegeven door erkende uitgevers. Zij waarborgen de authenticiteit van een webdocument of URL. Een digitaal certificaat is een encrypted gegevensbestand dat met een wachtwoord beveiligd is en dat naast het verzonden bericht, ook de identificatie van de gebruiker bevat. Weliswaar kan elke computer (tijdens verzending op het internet) toegang krijgen tot het bestand, maar alleen de geadresseerde kan het certificaat decoderen en lezen.

Digitale handtekening
Een beveiligingstechniek voor unieke identificatie van de bron van een document of toepassing.

Echtverklaring
Procedure waarmee de identiteit van een gebruiker, die probeert toegang te krijgen tot het systeem, wordt vastgesteld.

EES (Escrowed Encryption Standard)
Een voorgestelde standaard van de Amerikaanse regering voor de zogenaamde “escrow” van persoonlijke sleutels.

Erkende uitgever
Een organisatie die de digitale certificaten met betrekking tot de identiteit van de zender van een e-mail of bestand, afgeeft,

Extranet
Extranetten zijn netwerken die intranetten van ondernemingen verbinden met het wereldwijde Internet. Extranetten zijn in principe ontworpen voor commerciële doeleinden. Het maakt een snelle uitwisseling van informatie mogelijk.

Faciliteit Shred
De faciliteit Versnipperen van madeSafe verwijdert een bestand of document veilig en definitief. Zonder ook maar één spoor achter te laten en zonder enige mogelijkheid tot herstel.

Filteren van Internet-categorieën
Het filteren van Internet-categorieën is een standaardfunctie van madeSafe Home en een upgrade voor Madesafe Mobile en Business.

Firewall
Een beveiligingssprocedure die een computersysteem programmeert om de informatiestroom tussen het Internet en computers waarop een Intranet-draait, te beheersen. Deze barrière verhindert dat van buitenaf toegang wordt verkregen tot een intern bedrijfsnetwerk. Het interne netwerk heeft via de firewall indirect toegang tot het Internet. *Zie Proxyserver.*

Geldigheid
Geeft de mate van het vertrouwen weer dat de sleutel inderdaad behoort tot de vermeende eigenaar.

Hacker
Een persoon die zonder toestemming in computersystemen binnendringt. *Zie Kraker*

Het World Wide Web
(a.k.a., WWW, W3, Het Web) een algemeen gebruikt Internet hypertext-informatiesysteem dat gebaseerd is op het HTTP protocol en de HTML taal.

HTTPS
Staat voor een veilige Internetserver met een veilig protocol om hypertekst-documenten te transporteren op het Internet.

Hyper Text Mark-up Language (HTML)
De taal waarin webpagina's en e-mailberichten worden geschreven en opgemaakt.

Hyper Text Transfer Protocol (HTTP)
Het protocol dat gebruikt wordt om hypertekst-documenten te transporteren.

Hyperlink
Een woord of zin met een onderstreping of een andere accentuering, waarop met de muis geklikt kan worden om naar een ander document te gaan.

Integriteit
De verzekering dat gegevens tijdens de verzending of de overdracht. niet (door ongeautoriseerde personen) geschonden worden.

Internet
De grootste computernetwerken ter wereld. Internet verbindt de computernetwerken van vele universiteiten, staten/provincies, regio's, landen en bedrijven met elkaan.

Internet Service Provider (ISP)
Een Internet-aanbieder voor gebruikers met een inbelverbinding en/of bedrijfsnetwerken. De provider biedt hierin maatwerk.

Internet-filter

Een softwareproduct dat het Internet online filtert zodat kinderen of werknemers geen toegang kunnen krijgen tot ongewenste websites. *Zie Filteren van Internet-categorieën.*

Intranet
Een intern Internet van een bedrijf of organisatie, uitsluitend intern bedoeld. Intranet is dan ook niet openbaar en zit verborgen achter de firewall van een bedrijf.

ISO (International Organization for Standardization)
Een instantie, verantwoordelijk voor een groot aantal technische normen.

Kraker
Een persoon die de kopieerbeveiliging van software verwijdert of omzeilt. Meestal door een wijziging in de software aan te brengen.

Kunstmatige intelligentie
Een tak van de computerwetenschap, gericht op het ontwikkelen van een technologie die intelligent menselijk gedrag kan imiteren.

Message Authentication
Proces dat de geldigheid garandeert van de zender en de ontvanger van een e-mailbericht.

Onbewerkte tekst
Tekens in een vorm, leesbaar voor mens of machine.

Opruimfaciliteit
De opruimfaciliteit van madeSafe reorganiseert de harde schijf en brengt gegevens op orde. Zodat weer meer ruimte beschikbaar komt.

PGP
'Pretty Good Privacy.' Een algemeen maar toch persoonlijk sleutel-cryptografiesysteem dat bestaat uit twee sleutels. De eerste is een publieke sleutel die doorgegeven wordt aan alle ontvangers van een bepaald gecodeerd bericht. De tweede is een persoonlijke sleutel die gebruikt wordt voor het decoderen van ontvangen berichten.

PKI (Public Key Infrastructuur)
Een algemeen certificaatsysteem voor het verkrijgen van de publieke sleutel van een (rechts)persoon. Met die garantie dat het om de juiste sleutel gaat en deze niet is herroepen.

Private sleutel
Het geheime gedeelte van een sleutelpaar, gebruikt om informatie te ondertekenen en te decoderen. Deze persoonlijke sleutel is uitsluitend bij de gebruiker bekend.

Proxy (server)

Een server die functioneert als een firewall (barrière) en bemiddelt tussen een beveiligd netwerk en het Internet.

Publieke sleutel
Data, gebruikt om berichten, opgesteld in een publieke sleutel encryptie, te decoderen. De publieke sleutel kan, zoals de naam al zegt, gerust openbaar gemaakt worden omdat deze niet gebruikt kan worden voor het decoderen van berichten.

S/MIME
Zie Multipurpose Internet Mail Extensions (MIME).

Scanfaciliteit
De scanfunctie van madeSafe scant drives op materiaal dat de door de hoofdgebruiker als ongewenst wordt gezien.

Secure Cellular Architecture™
Persoonlijke producten van madeSafe (home en mobiel) die zorgen voor een veilig encrypted 448-bit cel rond bepaalde data of bestanden. Dit garandeert een veilig multi-user gebruik, geautoriseerd en beheerd door de systeembeheerder.
madeSafe Business biedt een hoofd-user-cell met extra cellen voor een aantal gebruikers. Elke cel biedt dezelfde encryptieniveaus en functionaliteiten. De hoofdgebruiker heeft echter alle rechten, alsmede de eindcontrole.

Secure Electronic Transactions (SET)
Veilige Internetprotocollen voor de elektronische verwerking van geld.

Secure Multipart Internet Mail Encoding (S/MIME)
Protocol voor verzending van veilige e-mail.

Secure Socket Layer (SSL)
Technologie van Netscape voor interne programmabeveiliging, gericht op identificatie van zender en geadresseerde van over het Intranet verzonden informatie.

Server
Een computer die informatie uitwisselt of verbindingen legt met andere computers op een bepaald netwerk. *Zie cliënt*

Simple Mail Transport Protocol (SMTP)
Een Internetprotocol voor het versturen van e-mail.

Single Line Internet Protocol (SLIP)
Een gedateerd communicatieprotocol voor seriële inbelverbindingen met het Internet.

Sleutel
Een digitale code die gebruikt wordt om berichten en bestanden te ondertekenen, te encrypten en te verifiëren. Sleutels bestaan uit sleutelparen en worden aan zogenaamde ‘sleutelhangers’ bewaard.

Sleutelbeheer
Procedure voor een veilige aanmaak en opslag, alsmede een nauwkeurige distributie van cryptografische sleutels voor geautoriseerde geadresseerden.

Sleutelhanger
Een set sleutels Elke gebruiker heeft een persoonlijke sleutelhanger en een publieke sleutelhanger.

Sleutellengte
Het aantal bits vertegenwoordigt de lengte van de sleutel. Hoe langer de sleutel, hoe sterker deze is.

Smart Encryption™
De madeSafe encryptietechniek gecombineerd met kunstmatige intelligentie heet Smart Encryption**™.** De producten van madeSafe hebben standaard 448-bit dual end superencryptie. Het niveau van de encryptie kan worden aangepast (bijvoorbeeld ten behoeve van de snelheid) in het beveiligingsprofiel van madeSafe Companion.**™**

Steganografie
Het verbergen van informatie binnen andere informatie. Een tekstbestand kan bijvoorbeeld verborgen zijn in een afbeelding of in een geluidsbestand. Bij het bekijken van de bestanden of het afspelen ervan is niets te merken.

Symmetrische sleutel
Een conventionele geheime sleutel en enkel sleutelalgoritme, waarbij de encryptie- en decoderingssleutel gelijk zijn of van elkaar afgeleid kunnen worden. madeSafe gebruikt deze symmetrische sleutel.

Tijdmarkering
Het vastleggen van de tijd waarin bepaalde informatie tot stand komt of reeds bestaat.

Transmission Control Protocol/Internet Protocol (TCP/IP)
Een reeks van standaarden (protocol) voor de gegevensoverdracht tussen het Internet en aangesloten computers, alsmede voor de foutcorrectie.

Two Fish
Een block cipher, symmetrisch algoritme

Uniform Resource Locator (URL)

Het site-adres dat wordt gebruikt om de locatie van een webpagina te bepalen.(HTML document). Dit is de formele technische naam voor een tekstreeks die voorziet in een Internet-adres en de wijze van benadering hiervoor.

Vault™
Met Vault kunt u encrypte gegevens op onze ultraveilige madeSafe website kopieëren. Zodat u 24 uur per dag, 365 dagen per jaar een backup heeft van uw informatie. Elke upgrade van madeSafe Vault bestaat uit veelvouden van 5MB.

Veilig kanaal
Een website die een veilige overdracht garandeert van alle informatie die ernaar wordt verzonden.

Verificatie
Vergelijking van een handtekening, gemaakt met een persoonlijke sleutel met dezelfde handtekening, gegenereerd met een publieke sleutel.

Encryptie
Een beveiligingstechniek die toegang tot informatie onmogelijk maakt door de informatie om te zetten in cipher-tekst (encrypte, onleesbare tekst). De cipher-tekst moet door de Internet-gebruiker worden gedecodeerd voordat deze leesbaar is.
Encryptie kan voor vele doelen worden ingezet. Denk hierbij bijvoorbeeld aan de beveiliging van gevoelige computerbestanden, de overdracht van financiële informatie via het Internet en gesprekken via digitale mobiele telefoons.

VPN (Virtual Private Network) een op Intranet gebaseerd besloten netwerk dat een openbaar netwerk (Internet) weer verbindt met een ander netwerk.

Wachtwoord
Een reeks van persoonlijk gekozen tekens of een woord dat toegang verschaft tot een PC of netwerk.

Wachtzin
Voor een effectieve beveiliging is een wachtzin te prefereren boven een enkel wachtwoord; 'key crunching' zet dit vervolgens om in een willekeurige sleutel.

Willekeurig getal
Een manier om een of meerdere unieke sleutels samen te stellen die voor een indringer onvoorspelbaar zijn.

Zoekmachine
Programma's die aan de hand van opgegeven sleutelwoorden automatisch en systematisch het Internet afspeuren.

Hoofdstuk 6 Technische ondersteuning

Solarsoft garandeert een optimale service en ondersteuning. Wij staan u graag op professionele wijze bij in het gebruik van onze madeSafe software en diensten.

Registratie

Registratie van uw madeSafe producten geeft u recht op Internetondersteuning, updates en speciale aanbiedingen.

Klantenservice

Op onze website: www.madesafe.com. vindt u uitgebreide informatie. Natuurlijk kunt u ons ook e-mailen: sales@madesafe.com.

Gratis Internet-ondersteuning

Gratis Internet-ondersteuning vraagt u aan via de knop ***Help*** in madeSafe Companion. Van maandag t/m vrijdag, van 09:00 - 17:00 uur kunt u ook direct hulp zoeken via www.madesafe.com/support.

Telefonische ondersteuning

Voor alle madeSafe producten biedt Solarsoft gratis technische ondersteuning per telefoon. Toegang hiertoe verkrijgt u via de knop ***Services & Options*** in madeSafe Companion.

Hoofdstuk 7 Auteursrecht & Handelsmerken

SOLARSOFT LIMITED. ALLE RECHTEN VOORBEHOUDEN

Deze software is uitsluitend bedoeld voor gebruik door de oorspronkelijke koper en voor gebruik in het opbouwen van één veilige cel. In het madeSafe Business product worden twee extra 'werker'-cellen geboden als onderdeel van de licentie. Gebruiksrecht wordt verleend aan rechtmatige gebruikers voor het lezen van de software op de bijgevoegde CD vanuit hun medium naar het geheugen van een computer uitsluitend voor het doel van de uitvoering hiervan. De verkoop of andere distributie van deze software is wettelijk verboden.

Deze handleiding valt onder het auteursrecht en alle rechten zijn voorbehouden. Deze handleiding mag niet in zijn geheel, noch gedeeltelijk worden gekopieerd, gefotokopieerd of vertaald worden, noch gereduceerd worden tot een elektronisch medium of een machinaal leesbare vorm zonder voorafgaande schriftelijke toestemming van Solarsoft Limited. Wij behouden ons het recht voor om wijzigingen aan te brengen in dit document en/of product zonder verdere kennisgeving.

Solarsoft Limited garandeert dat de cd-media waarop de software is aangebracht vrij zij van materiaal- en fabricagefouten en dat de software substantieel functioneert in overeenstemming met de specificaties in het bijgesloten schriftelijke materiaal. Solarsoft Limited geeft geen andere garantie of bevestiging, uitdrukkelijk of niet-uitdrukkelijk met betrekking tot de software en de documentatie, de kwaliteit, prestatie, verkoopbaarheid of geschiktheid daarvan voor een bepaald doel. Bovendien geeft Solarsoft Limited geen garantie dat de software behoorlijk functioneert in elke omgeving of in alle toepassingen. Solarsoft Limited behoudt zich het recht voor om wijzigingen aan te brengen in de software en in de inhoud van de handleiding zonder de verplichting om enige persoon of organisatie van de herziening of wijziging in kennis te stellen.

madeSafe, Smart Encryption, Active Stealth Technology, Secure Cellular Architecture, Companion en Vault zijn alle geregistreerde handelsmerken die eigendom zijn van Solarsoft Ltd. Microsoft® Windows 95/98/Me/NT/2000/XP zijn geregistreerde handelsmerken van Microsoft Corporation. Alle overige handelsmerken worden erkend. Solarsoft®2001. Alle rechten voorbehouden.

Hoofdstuk 8 Contact opnemen

Wij stellen persoonlijk contact met onze klanten zeer op prijs. U kunt ons altijd bellen. Onze website houdt u op de hoogte van de nieuwste ontwikkelingen en biedt u de benodigde ondersteuning.

Solarsoft Limited
Phillips House, Station Road, Hook, Hampshire, Verenigd Koninkrijk. RG27 9HD

Tel: +44 (0) 870 872 8210 Fax: +44 (0) 1256 769770
Web: http: www.madeSafe.com

Hoofdstuk 9 Informatie over assistent

Wanneer de assistent zichtbaar is, zijn de knoppen niet actief. Voor informatie over de functies klikt u op de knop waarvoor u hulp wenst. De madeSafe assistent legt de functie dan uit. Om de assistent uit te schakelen klikt u met de rechtermuisknop op de assistent en kiest ***Hide***. U kunt de assistent ook sluiten met de escape toets.

Hoofdstuk 10 Beknopte handleiding

Setup/Bewerken van gebruikers profielen

Setup/Bewerken van soort van beveiliging

Bekijk de beschikbare opties en diensten

Controleer welke upgrades/updates beschikbaar zijn

Weergave van bestanden in actieve directory

Locatie van doelstation

Scant drive op ongewenst materiaal.

Doel-directory Locatie

Verwijdert tijdelijke bestanden veilig van de harde schijf

Verwijdert bestanden veilig en permanent

Decodeer geselecteerde bestanden

Directe toegang tot persoonlijke kluis

Encrypt geselecteerde bestanden

Toon geselecteerde bestanden

Verberg geselecteerde bestanden

Vraag om hulp via de madeSafe assistent

Verstuur veilige e-mails