



CIBG  
*Ministerie van Volksgezondheid,  
Welzijn en Sport*

## Versleutelen e-mail met Microsoft Outlook

Versie 1.0

Datum 2 december 2010  
Status definitief (UZ68.01)

## Inhoud

<b>1</b>	<b>Inleiding—3</b>
1.1	Doelstelling—3
1.2	Versies—3
1.3	Opbouw van het document en overige documentatie—3
1.4	Document historie—3
<b>2</b>	<b>Versleutelen van e-mail met Microsoft Outlook—4</b>
2.1	Randvoorwaarden—4
2.2	Configuratie Windows Register voor gebruik van UZI-pas in Outlook (script)—4
2.3	Configureren van Outlook voor versleutelen van een e-mail bericht—4
2.3.1	Stap 1: zoek het vertrouwelijkheidcertificaat op van de ontvanger—4
2.3.2	Stap 2: plaats uw UZI-pas in de kaartlezer—4
2.3.3	Stap 3: contactpersoon toevoegen voor ontvanger—5
2.3.4	Stap 4: e-mail bericht maken voor contactpersoon—6
2.4	Openen van een versleuteld e-mail bericht—8
	<b>BIJLAGE: Publieke sleutel overnemen vanuit een eerder ontvangen ondertekende e-mail—10</b>

Copyright CIBG 2010 © te Den Haag

Niets uit deze uitgave mag verveelvoudigd en/of openbaar worden gemaakt (voor willekeurig welke doeleinden) door middel van druk, fotokopie, microfilm, geluidsband, elektronisch of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van CIBG.

## 1 Inleiding

### 1.1 Doelstelling

Met behulp van UZI-passen kunt u e-mail berichten versleutelen zodat deze alleen door u en de ontvanger te lezen zijn. Deze handleiding beschrijft hoe u met de UZI-pas in Microsoft Outlook een e-mail bericht kan versleutelen.

### 1.2 Versies

Bij het opstellen van dit document is gebruik gemaakt van Microsoft Office 2003 op Windows XP. Behalve de lay-out is de werking in nieuwere Office versies vergelijkbaar.

### 1.3 Opbouw van het document en overige documentatie

In hoofdstuk 2 wordt beschreven hoe men met Microsoft Outlook een e-mail kan versleutelen.

Er is een aparte handleiding die beschrijft hoe u met een UZI-pas een e-mail bericht kan ondertekenen.

Het advies is om eerst te zorgen dat u met Outlook e-mail kan ondertekenen voordat u aan de slag gaat met vertrouwelijke e-mail.

### 1.4 Document historie

Versie	Datum	Status	Omschrijving
1.0	2 december 2010	Definitief	Eerste gepubliceerde versie.

## 2 Versleutelen van e-mail met Microsoft Outlook

### 2.1 Randvoorwaarden

Deze handleiding gaat er vanuit dat u beschikking heeft over de volgende zaken:

- 1 Een UZI-pas met bijbehorende PIN-code;
- 2 Een Windows PC waarop de standaard kaartlezer en software voor gebruik van de UZI-pas reeds is geïnstalleerd. Zie <http://www.uziregister.nl/technischesupport/installerenuzipasenkaartlezer/windows/>
- 3 Een Windows PC waarop Microsoft Outlook is geïnstalleerd als onderdeel van Office XP, Office 2003 en Office 2007.
- 4 Een Windows PC waarop u voldoende rechten heeft om software te installeren. Dit is nodig voor enkele aanpassingen in het Windows register.

### 2.2 Configuratie Windows Register voor gebruik van UZI-pas in Outlook (script)

Microsoft Outlook controleert standaard of het e-mailadres van de verzender van een bericht overeenkomt met het e-mailadres in het gebruikte certificaat. In de certificaten van de UZI-pas is bewust geen e-mailadres opgenomen. Hierdoor is de UZI-pas op meerdere werkplekken (e-mailadressen) te gebruiken en hoeft ook niet vervangen te worden bij een wijziging van het e-mailadres van de pashouder. Wel vereist deze werkwijze een aanpassing in het register van Windows om de controle op het e-mailadres uit te zetten<sup>1</sup>.

Op de website van het UZI-register staat bij deze handleiding het script 'Register\_Aanpassing\_Outlook.reg' om de configuratie van uw versie van Outlook aan te passen. Dit script voert de vereiste aanpassing in het register uit voor Office XP, Office 2003, 2007 en 2010.

### 2.3 Configureren van Outlook voor versleutelen van een e-mail bericht

#### 2.3.1 Stap 1: zoek het vertrouwelijkheidcertificaat op van de ontvanger

Om iemand een versleutelde e-mail te sturen heeft u zijn vertrouwelijkheidcertificaat nodig. Outlook gebruikt de sleutel uit dit certificaat om het bericht te versleutelen. Alleen de ontvanger die beschikt over de bijbehorende UZI-pas kan het bericht lezen.

De certificaten zijn terug te vinden in de zogenaamde LDAP database. De zoekpagina voor deze LDAP is te vinden via:

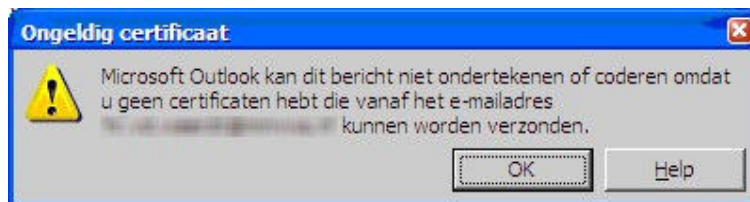
<http://www.uziregister.nl/ikhebeenuzipas/uitgegevenuzipassen/>

In BIJLAGE 1 is een alternatief aangegeven voor deze stap: het overnemen van het vertrouwelijkheidcertificaat uit een eerder ontvangen e-mail.

#### 2.3.2 Stap 2: plaats uw UZI-pas in de kaartlezer

**Belangrijk!** Om een encrypt bericht te kunnen versturen moet ook de UZI-pas van de verzender in de kaartlezer zitten. Dit geldt ook als men het bericht alleen wilt versleutelen en niet wilt ondertekenen! Zo niet dan krijgt u onderstaande foutmelding:

<sup>1</sup> De technische achtergrond en details van de oplossing staan in het Microsoft Support artikel How to turn off e-mail matching for certificates in Outlook. Zie: <http://support.microsoft.com/default.aspx?scid=kb;en-us;276597>



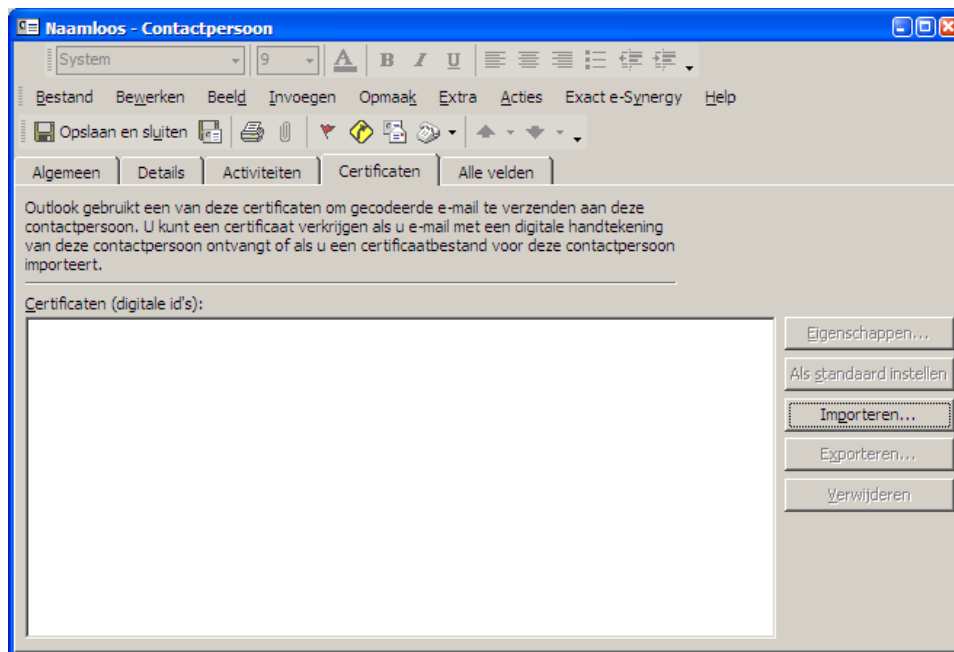
De reden hiervan is dat in de 'verzonden items' van de verzender het bericht versleuteld wordt opgeslagen op basis van het encryptie certificaat van de verzender. Outlook heeft dus 2 encryptiecertificaten nodig: van de ontvanger en de verzender.

**Belangrijk!** Als u later de verzuurde versleuteld berichten wilt lezen in de 'verzonden items' moet u de UZI-pas in het systeem hebben en de PIN invoeren. Zonder uw UZI-pas kan u zelf uw verzonden en versleutelde e-mail berichten niet meer lezen! Deze mail is niet meer te openen na verlies of defect van uw UZI-pas, ook niet met een nieuwe UZI-pas.

### 2.3.3

#### Stap 3: contactpersoon toevoegen voor ontvanger

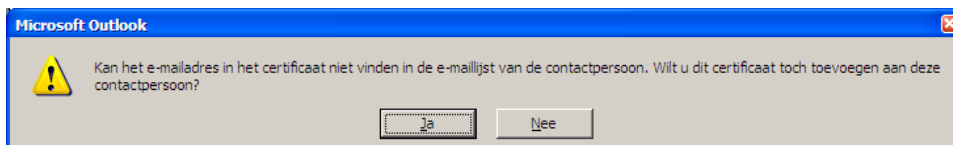
- Voeg in 'Contactpersonen' een nieuwe contactpersoon toe voor de geadresseerde aan wie u een versleutelde e-mail wilt versturen.
- Importeer in het tabblad 'Certificaten' het vertrouwelijkheidcertificaat van de geadresseerde.



- Via de knop importeren kan een certificaat (publieke sleutel) worden toegevoegd aan de contactpersoon waar u het versleutelde bericht naar toe wilt sturen.
- Dit certificaat is te downloaden van <http://www.uziregister.nl/ikhebeenuzipas/uitgegevenuzipassen/>. Hier vult u de gegevens in van de persoon in kwestie, deze persoon dient dus wel in het bezit te zijn van een UZI-pas of een servercertificaat. Waarna u het vertrouwelijkheid certificaat van die persoon download.

<b>Status</b>	Aktief
<b>CERTIFICATEN</b>	
<b>Download certificaat Functie</b>	
<a href="#">Certificaat 1</a>	Vertrouwelijkheid
<a href="#">Certificaat 2</a>	Authenticatie
<a href="#">Certificaat 3</a>	Elektronische handtekening

In de certificaten die het UZI-register uitgeeft wordt geen e-mail adres opgeslagen. Bij het toevoegen komt er een melding dat het e-mailadres van het contact niet overeenkomt met het certificaat maar die melding kunt u negeren.



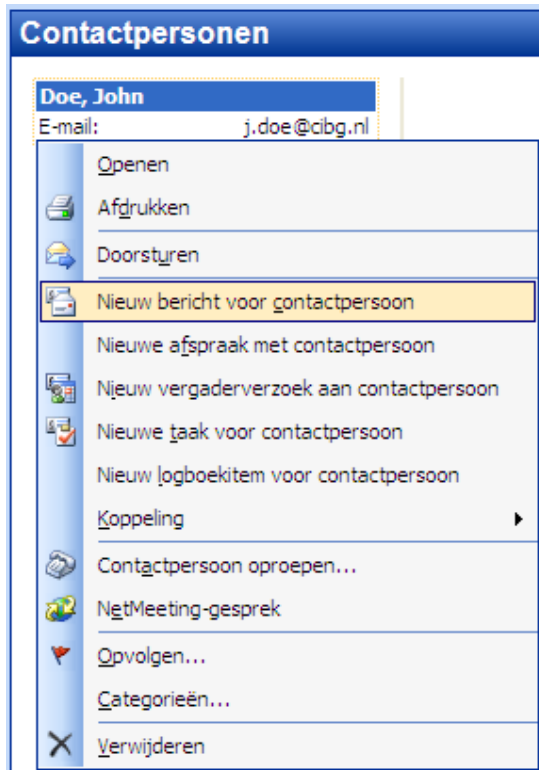
- Klik hier dus op 'Ja' en daarna op 'Opslaan en sluiten'

2.3.4

*Stap 4: e-mail bericht maken voor contactpersoon*

Er kan nu een nieuw e-mail bericht worden gemaakt met in het Aan veld de zojuist aangemaakte contactpersoon.

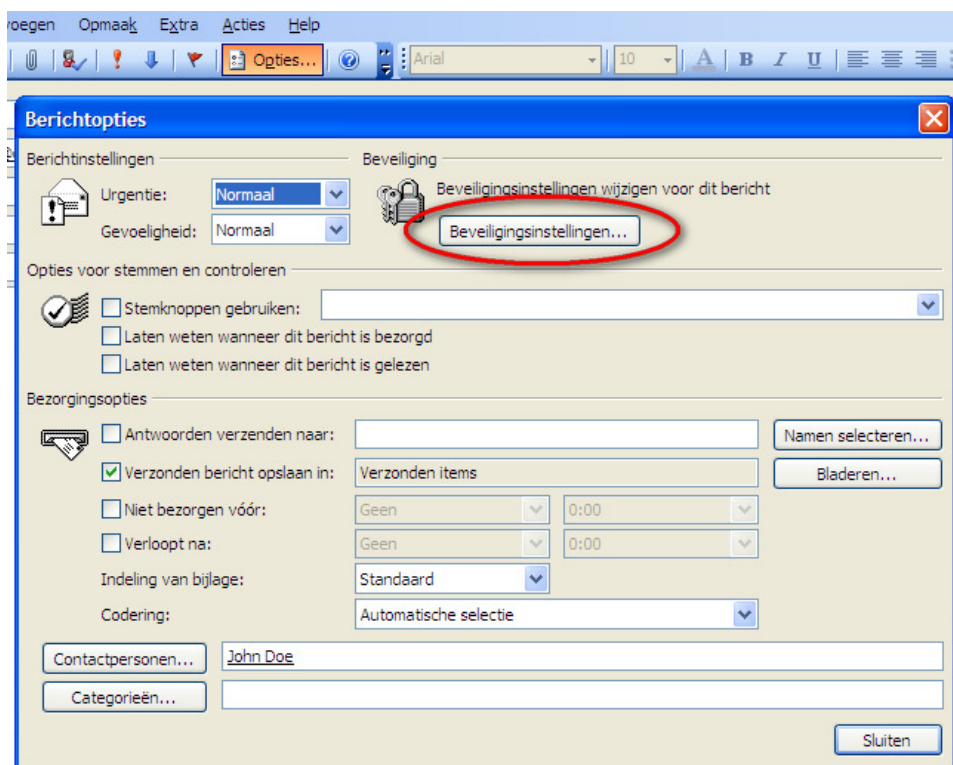
- Klik in de contacten met de rechtermuis op het betreffende contact
- Kies 'aanmaken' en 'nieuw bericht voor contact'



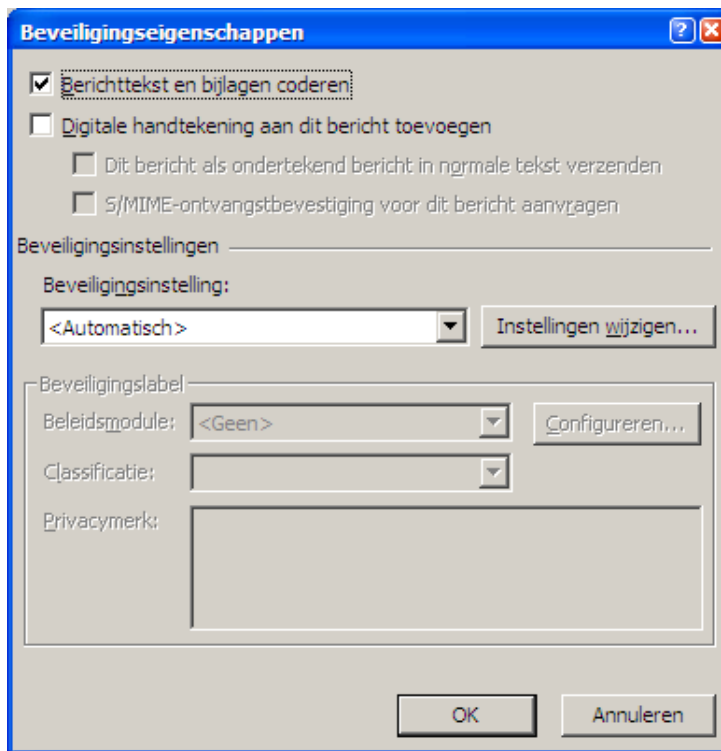
- Klik daarna op het volgende icoon om uw bericht te versleutelen.




- Als alternatief kunt u ook op de volgende wijze uw bericht versleutelen. Ga daarvoor in het bericht naar 'Opties' en dan 'Beveiligingsinstellingen'.



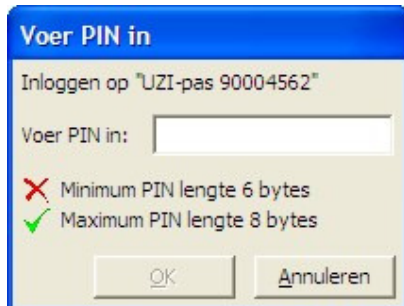
- Check daar het vinkje voor codering. Het eerder genoemde icoon moet dan zichtbaar zijn, waarmee wordt aangeduid dat het bericht versleuteld is.



#### 2.4 Openen van een versleuteld e-mail bericht

Bij de ontvanger zal dit icoon  voor het ontvangen bericht staan, dit kunt u zien als een bevestiging dat het bericht daadwerkelijk versleuteld is verstuurd. Voordat u verder gaat dient de UZI-pas in de kaartlezer te zitten.

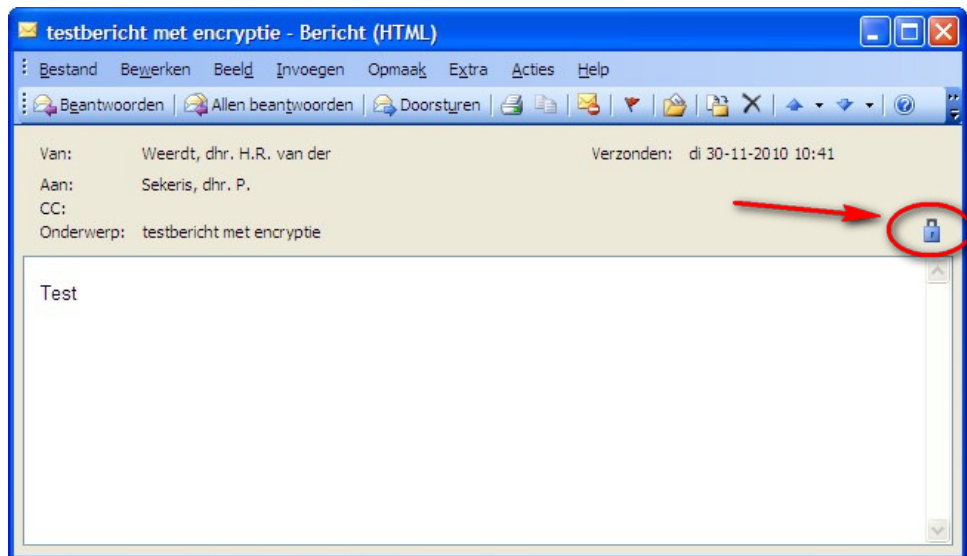
- Door vervolgens op het bericht te dubbelklikken verschijnt het PIN venster. Voer hier uw pincode in en klik vervolgens op "OK".



- Zodra er geen UZI-pas in de kaartlezer zit verschijnt de volgende melding.



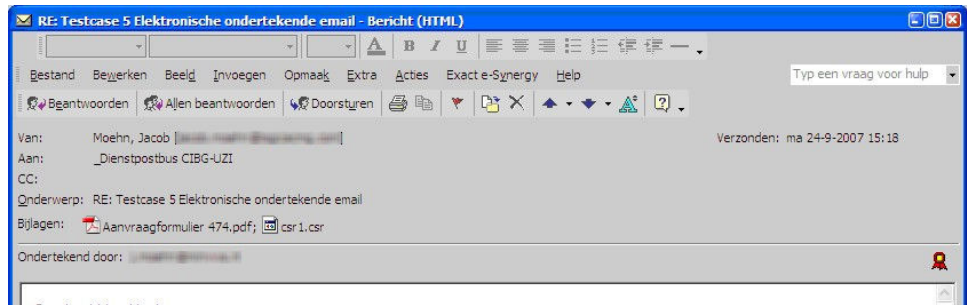
- Nadat de correcte pincode is ingevoerd zal het bericht geopend worden. Aan de hand van het icoon (het slotje) kunt u zien dat het een versleuteld bericht betreft.



## BIJLAGE: Publieke sleutel overnemen vanuit een eerder ontvangen ondertekende e-mail

Als een collega op een eerder tijdstip al een digitaal ondertekend bericht heeft toegezonden dan kan vanuit dat bericht de publieke sleutel worden gehaald en later opnieuw worden gebruikt<sup>2</sup>. Dit gaat als volgt:

- Open het bericht waarin de digitale handtekening zit.

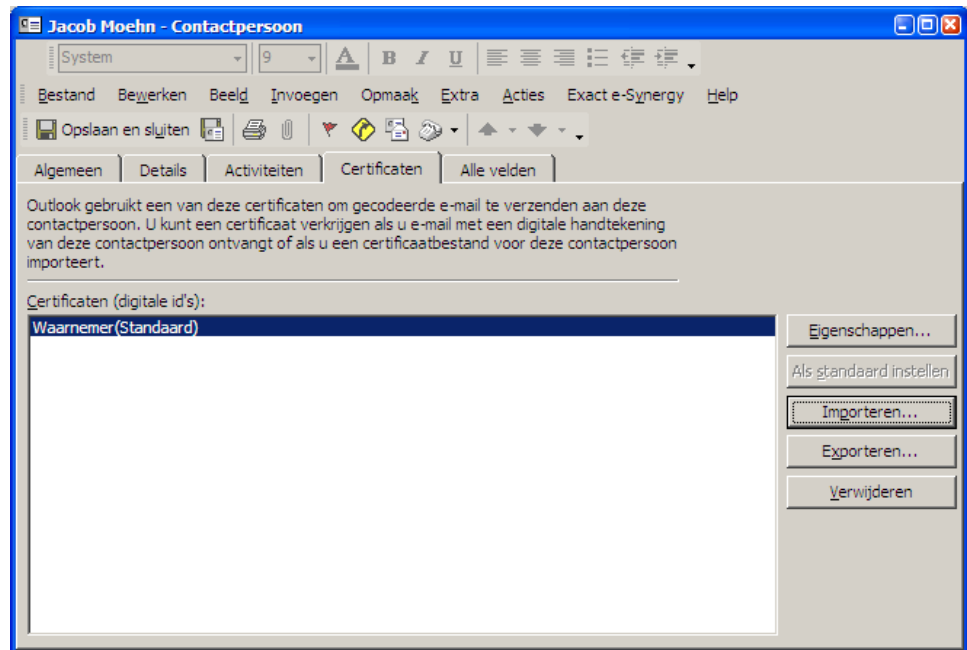


- Klik met de rechtermuisknop op de naam van de afzender en kies voor de optie toevoegen aan contactpersoon.



<sup>2</sup> Voorwaarde is dat de verzender heeft aangevinkt om dit certificaat mee te sturen bij de beveiligingsopties.

- Het volgende scherm verschijnt. In het tabblad 'Certificaten' is het certificaat (de publieke sleutel) van de verzender terug te vinden (dit certificaat kan eventueel worden geëxporteerd en worden opgeslagen).



- Klik vervolgens op "Opslaan en sluiten".

De contactpersoon is nu met certificaat opgeslagen in de lijst met contactpersonen en kan later worden gebruikt.