S/MIME certificaat

Installeren en gebruik S/MIME in Outlook (Windows)



(Deze pagina is bewust leeg gelaten)

•

Inhoudsopgave

1 Inleiding	4
1.1 Sectigo certificaat downloaden	5
1.2 Certificaat installeren	7
1.3 Mail versturen (encrypted/signed)	12

1 Inleiding

Je kan jouw e-mail digitaal ondertekenen en/of versleutelen met jouw TU Delft mailaccount. Dit gebeurt met S/MIME, waarvoor je een certificaat nodig hebt. Certificaten voor de TU Delft worden door GÉANT uitgereikt. Deze handleiding beschrijft hoe je een certificaat genereerd en hoe je vervolgens S/MIME kan configureren binnen Outlook (Windows).

1.1 Sectigo certificaat downloaden

Allereerst dien je een certificaat te downloaden. Volg onderstaande stappen:

- 1. Open een browser en ga naar <u>https://edu.nl/sectigo-sso</u>
- 2. Zoek jouw onderwijsinstelling door te zoeken op "Delft"
- 3. Klik op "Delft University of Technology" (tudelft.nl)

Find Your Institution Your university, organization or company	
Delft	٩
Examples: Science Institute, Lee@uni.edu, UCLA Remember this choice Learn More	
Delft University of Technology tudelft.nl	

4. In het volgende scherm log je in met je netID + wachtwoord.

f UDelft			
Please login t	o access login-protected servic	es	
Username	your NetID		
Password	your password		
	Login		

- 5. Review de informatie om in te loggen via SURFconext; klik op "Proceed to Cert Manager"
- 6. Je komt in het volgende scherm. Kies hier voor "GÉANT email Signing and encryption" via het dropdown menu:

	Digital Certificate Enrollment
Digital Certificate Enrollment	This is your certificate enrollment form. Once you submit, your certificate will be generated and downloaded to your computer.
This is your certificate enrollment form. Once you submit, your certificate will be generated and downloaded to your computer.	Name Organization Technische Universiteit Delft Email @tudelft.nl
Organization Technische Universiteit Delft	Select your Certificate Profile to enable your enrollment options.
Email @tudelft.nl	Certificate Profile* GÉANT Personal email signing and encryption
Select your Certificate Profile to enable your enrollment options.	GÉANT Personal Authentication GÉANT Personal Automated Authentication
Certificate Profile*	GÉANT Personal email signing and encryption

Kies de volgende instellingen om een werkend certificaat te genereren voor Windows:
 -Term: 365 days

-Enrollment Method: Key Generation

-Key Type: RSA – 2048

-Password: bewaar dit wachtwoord goed, deze heb je later nodig bij het configureren in Outlook

-Key Protection Algorithm: Secure AES256-SHA256

-Vink het vakje aan om akkoord te gaan met de voorwaarden en klik op "Submit" om een certificaat te genereren

Digital Certificate Enrollment	
This is your certificate enrollment form. Once you submit, your certificate will be ge and downloaded to your computer.	nerated
Name	
Organization Technische Universiteit Delft	
Email @tudelft.nl	
Select your Certificate Profile to enable your enrollment options.	
Certificate Profile* GÉANT Personal email signing and encryption	*
Personal Certificate - provides secure email services, and enables you to encry digitally sign email communications, as well as sign and protect some types of doc (but not sign PDF documents).	ypt and ument
Term* 365 days	*
⊖ csr	
Key Type*	*
Descuord in required to unlook the certificate file download to protect private key	
Password*	8
Password Confirmation*	8
Choose key protection algorithm.	
Algorithm Secure AES256-SHA256	*
I have read and agree to the terms of the EULA	
Submit	

8. Het certificaat wordt gegenereerd, dit kan even duren



9. Er verschijnt een melding dat het certificaat succesvol is gegenereerd en gedownload.



Let op: Bewaar dit certificaat (certs.p12) goed voor toekomstig gebruik! Houd er rekening mee dat je jouw eigen versleutelde e-mail alleen kunt decrypten met het certificaat waarmee je deze eerder hebt versleuteld. Als je dit certificaat kwijtraakt, kan je het originele bericht niet terughalen!

1.2 Certificaat installeren

Nu het certificaat is gedownload kan je deze configureren in Outlook. Volg onderstaande stappen: 10. Open Outlook en klik op "*File*" bovenin je werkbalk en kies onderin voor "*Options*":



11. Klik vervolgens op "Trust Center" -> "Trust Center Settings":



12. Klik vervolgens op "Email security" -> "Import/Export"



13. In het volgende scherm klik je op "**Browse**" om te navigeren naar het S/MIME certificaat die in stap 9 is aangemaakt/gedownload. Vul het bijbehorende wachtwoord in en klik op "**OK**"

Import the Dig password you	jital ID from the file to your entered while exporting th	computer. You must e certificate to this t	t use the file.
Import File:	C:\Users \Dow	nloads\certs. B	owse
Password:	•••••		
Digital ID			
) Export your Export the Dig protect this in	Digital ID to a file jital ID information into a fi formation.	le. Enter a password	I to help
) Export your Export the Dig protect this in Digital ID:	Digital ID to a file ital ID information into a fi formation.	le. Enter a password	i to help elect
Export your Export the Dig protect this in Digital ID: Filename:	Digital ID to a file ital ID information into a fi formation.	ie. Enter a password	elect
Export your 1 Export the Dig protect this in Digital ID: Filename: Password:	Digital ID to a file iital ID information into a fi formation.	le. Enter a password	l to help elect
Export your I Export the Dig protect this in Digital ID: Filename: Password: Confirm:	Digital ID to a file ital ID information into a fi formation.	le. Enter a password	elect

14. Er verschijnt een nieuwe melding. Klik hier op "**OK**"

Importing	a new private exchange key	tificate to t	his file. X
	An application is creating a Pro	tected item.	
	CryptoAPI Private Key		
	Security level set to Medium	Set Sec	urity Level
	ОКС	ancel	Details

15. Kies vervolgens voor settings:

Trust Center	
Trusted Publishers	Encrypted email
Privacy Options	Figure Frequent contents and attachments for outgoing messages
Form-based Sign-in	Add digital signature to outgoing messages
Email Security	Send clear text signed message when sending signed messages
Attachment Handling	Request S/MIME receipt for all S/MIME signed messages
Automatic Download	Default Setting:
Macro Settings	Digital IDs (Certificates)
Programmatic Access	Digital IDs or Certificates are documents that allow you to prove your identity in ele Publish to GAL
	Read as Plain Text

16. Zorg ervoor dat de volgende vinkjes zijn gezet. Klik vervolgens op "*Choose*" om te verifiëren dat het juiste certificaat is geselecteerd (GEANT Personal CA4, controleer ook "valid from" datum).

Change Security Settings		×		
Security Setting Preference	25			
Security Settings Name:				
My S/MIME Settings (/	@tudelft.nl)	~		
Cryptography Format:	S/MIME	\sim		
🗹 Default Security Sett	ing for this cryptographic message	format		
Default Security Sett	ing for all cryptographic messages		Windows Security	×
Security Labels	. New Delete		Select a Certificate	
Certificates and Algorit	hms			
Signing Certificate:		Choose	S=	
Hash Algorithm:	SHA1 ~		Issuer: GEANT Personal	CA 4
Encryption Certificate:	-	Choose	Valid From: 12-4-2024	to 13-4-2025
Encryption Algorithm:	AES (256-bit) V		Click here to view certif	icate properties
Send these certificat	es with signed messages			
	ОК	Cancel	ОК	Cancel
			1	

17. Indien dit het geval is, klik op "**OK**" -> "**OK**". Vervolgens vink je het volgende vakje aan in Trust Center om je uitgaande berichten standaard te voorzien van een digitale handtekening: "**Add digital signature to outgoing messages**":

Trust Center	?	×
Trusted Publishers Privacy Options	Encrypted email	
Form-based Sign-in Email Security	 Add digital signature to outgoing messages Send clear text signed message when sending signed messages Request S/MIME receipt for all S/MIME signed messages 	
Automatic Download Macro Settings	Default Setting: My S/MIME Settings (A.Gorgees@tudelft.nl) Digital IDs (Certificates)	
Programmatic Access	Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions. <u>Publish to GAL Import/Export</u>	
	Read as Plain Text	

De optie "*Send clear text signed message when sending signed messages*" is standaard ingeschakeld om ervoor te zorgen dat de ontvangers die geen S/MIME-beveiliging hebben, de berichten kunnen lezen die jij verzendt (aanbevolen om dit ingeschakeld te laten).

De optie "*Request S/MIME receipt for all S/MIME signed messages*" kan je aanvinken als je wilt verifiëren dat jouw digitaal ondertekende e-mailbericht ongewijzigd is ontvangen door de beoogde ontvangers. Wanneer je deze optie selecteert, worden de verificatiegegevens in een afzonderlijk bericht naar jou verzonden.

18. Tip: In Trust Center Settings, klik op "Publish to GAL...".



Hiermee publiceer je jouw certificaat naar de "Global Address List". Dit is een gecentraliseerde directory van emailadressen en contactinformatie binnen het e-mailsysteem van een organisatie. Op deze manier kunnen gebruikers encrypted e-mails naar jou sturen zonder dat ze je eerst aan hun Outlook-contacten hoeven toe te voegen (dit wordt later in de handleiding beschreven). In sommige gevallen kan het tot 48 uur duren voordat het S/MIME-certificaat is gepubliceerd in de GAL via de functionaliteit "Publish to GAL".

19. **Succes**! Je bent nu klaar met het configureren van je S/MIME instellingen. Sluit nu alle schermen door op "**OK**" te klikken.

1.3 Mail versturen (encrypted/signed)

Ga nu terug naar het beginscherm van Outlook en klik op "*New Email*" om een nieuwe mail op te stellen. Klik op "*Options*" boven in je werkbalk. De opties "*Encrypt*" en "*Sign*" zijn hier zichtbaar. "*Sign*" is nu standaard ingeschakeld door de instellingen uit de vorige stap. Dit is te zien doordat deze knop gemarkeerd is.

ଅ୨୦↑↓୫∽⊽		Dit is een testmai	il - Message (HTML)
File Message Insert Draw O	ptions Format Te	ext Review Help	Acrobat Q Tell me what you want to do
Aa Colors ~ A Fonts ~ Page Colors ~ Bcc From Effects ~	Encrypt Sign U	Jse Voting Calendary Request a Deliver	y Receipt Save Sent Delay Direct Item To ~ Delivery Replies To
Themes Show Fields	Encrypt	Tracking	العا More Options
To Send			
Subject Dit is een testmai			
Dit is een testmail			

Indien je een bericht wilt encrypten klik je op "**Encrypt**". Klik vervolgens op "**Send**". Er volgt een pop-up venster ter bevestiging. Klik op "**Allow**".

$\square ~ \bigcirc ~ \bigcirc ~ \uparrow ~ \Downarrow ~ \bullet ~ \bullet$	Dit is een testmail - Message (HTML)
File Message Insert Draw Options F	Format Text Review Help Acrobat 🛛 🖓 Tell me what you want to do
Colors × Page Themes Effects × Colors × Bcc Fonts × Page Themes Show Fields	Sign Request a Delivery Receipt Use Voting Buttons ~ Request a Read Receipt Tracking Ts More Options Ts
То	Windows Security X
Send Cc	Credential Required
Subject Dit is een testmail	Do you want to allow the app to access your private key?
Dit is een testmail	Key description : CryptoAPI Private Key
	FG-
	Allow Don't allow

Het bericht wordt nu encrypted verstuurd. De ontvanger ziet het volgende bij het ontvangen van de mail. Dit icoontje toont aan dat het bericht encrypted is verstuurd.

Focused Other	
! 🌣 🗅 🖉 From 🥜	Subject
∼ Today	
	Dit is een testmail

Bij het openen van de mail is het volgende te zien: **Signed by**: mailadres@tudelft.nl gevolgd door een tweetal icoontjes (encrypted + signed icoon):



Note: om een bericht encrypted te versturen is het noodzakelijk dat het publieke certificaat van de ontvangende partij bekend is. Dit doe je door een "signed" mail te openen die je hebt ontvangen en deze persoon vervolgens toe te voegen aan jouw contacten. Open een "signed" mail -> rechtermuisknop op de naam van de persoon -> Add to Outlook Contacts -> Save & Close:



Je contactpersoon is nu succesvol opgeslagen aan jouw Outlook-contacts. Door de contactpersoon gegevens te openen kan je de certificaat eigenschappen bekijken (indien beschikbaar): klik op "**Certificates**" -> Properties

