

**To:** [redacted] ( [redacted] ) - [redacted] [redacted] [redacted] @logius.nl]; [redacted] 2 [redacted] [redacted] [redacted] @webweaving.org]  
**Cc:** [redacted] [redacted] [redacted] [redacted] ( [redacted] ) - Logius [redacted] [redacted] @logius.nl]  
**From:** [redacted] [redacted] [redacted] ( [redacted] )  
**Sent:** Mon 9/28/2020 2:45:06 PM  
**Subject:** RE: Technische deadline (OCSP/CRL published revoke) G3  
**Received:** Mon 9/28/2020 2:45:06 PM

M2M, ingebouwd in de app

---

**Van:** [redacted] [redacted] ( [redacted] ) - [redacted] <[redacted]@logius.nl>  
**Verzonden:** maandag 28 september 2020 16:36  
**Aan:** [redacted] [redacted] ( [redacted] ) <[redacted]@minvws.nl>; [redacted] [redacted] [redacted] [redacted] <[redacted]@webweaving.org>  
**CC:** [redacted] [redacted] [redacted] [redacted] ( [redacted] ) - Logius <[redacted]@logius.nl>  
**Onderwerp:** RE: Technische deadline (OCSP/CRL published revoke) G3

Hoi [redacted]

Ik ben zo concreet als mogelijk en tracht vanuit mijn rol zo goed mogelijk aan te geven waar rekening mee gehouden kan worden.

De vraag is hier volgens mij of de Coronamelder een website of M2M verkeer is.  
 Ik ken de Coronamelder niet dus het lijkt mij niet verstandig dat ik daarover speculeer.

Met vriendelijke groet,

[redacted]

NB Nu met de juiste [redacted] in de cc

---

**Van:** [redacted] [redacted] ( [redacted] ) <[redacted]@minvws.nl>  
**Verzonden:** maandag 28 september 2020 15:26  
**Aan:** [redacted] [redacted] ( [redacted] ) - [redacted] <[redacted]@logius.nl>; [redacted] [redacted] [redacted] [redacted] <[redacted]@webweaving.org>  
**CC:** [redacted] [redacted] ( [redacted] ) - Logius <[redacted]@logius.nl>  
**Onderwerp:** RE: Technische deadline (OCSP/CRL published revoke) G3

Dag [redacted]

Dank voor je reactie. In het kader van samen het land redden en zorgen dat CoronaMelder blijft werken kopieer ik [redacted] in (die overigens ook zelf in het CA/b forum zit).

Jouw antwoord geeft nog geen antwoord op onze concrete vraag. Is mijn interpretatie correct dat we voor CoronaMelder dus geen risico lopen?

Met vriendelijke groet,

[redacted] [redacted]  
 [redacted] Informatiebeleid / [redacted] (CIO)

.....  
**Ministerie van Volksgezondheid, Welzijn en Sport**

Postbus 20350 | 2500 EJ | Den Haag

[redacted] [redacted] [redacted] | [redacted] @minvws.nl | [redacted]

.....  
**T** [redacted]  
 [redacted] @minvws.nl  
 .....

**Van:** 5.1.2e, 5.1.2e (5.1.2e) - 5.1.2e <5.1.2e@logius.nl>

**Verzonden:** maandag 28 september 2020 15:17

**Aan:** 5.1.2e, 1., (5.1.2e) <5.1.2e@minvws.nl>

**CC:** 5.1.2e, 1., (5.1.2e) - Logius <5.1.2e@logius.nl>

**Onderwerp:** FW: Technische deadline (OCSP/CRL published revoke) G3

Geachte heer 5.1.2e Beste 5.1.2e

In antwoord op de vraag in hoeverre er zekerheid is te verkrijgen rondom de december datum het volgende.

De certificaatwissel die plaats vindt als gevolg van het actieplan wordt aangevlogen met als eerste prioriteit het voorkomen van uitval van (vitale) systemen.

Om het vertrouwen van webbrowsers in het PKI Overheidstelsel te behouden is een actieplan opgesteld met daarin een drietal deadlines.

Wij kunnen de werking van certificaten na verloop van deadlines niet meer garanderen.

Dat betekend;

dat het gebruik van publiek vertrouwde certificaten uitgegeven onder de G3 root voor websites na 1 oktober risico's in zal houden.

Dat het gebruik van publiek vertrouwde certificaten uitgegeven onder de G3 root voor M2M verkeer na 31 december risico's in zal houden.

Dat het gebruik van publiek vertrouwde certificaten uitgegeven onder de G3 root na 31 januari risico's in zal houden.

Ik las in onderstaande wisseling de opmerking over de informele signalen vanuit Logius.

Wij willen perse voorkomen dat bij gebruikers van certificaten de indruk gaat ontstaan dat de deadlines zoals gedeeld op het CA/b forum zonder penalty kunnen verlopen.

Wij lopen namelijk het risico dat webbrowsers onze voortgang op het vervangingsplan onvoldoende vinden en hier consequenties aan willen verbinden.

De informele signalen kunnen verklaard worden vanuit de vele gevallen van zogenaamd "dual use". De situatie waarin hetzelfde Publiek vertrouwde certificaat wordt gebruikt voor zowel een website als voor M2M verkeer. Deze veel voorkomende "dual use" situatie dwingt het stelsel PKI Overheid tot terughoudendheid met betrekking tot intrekking omdat voor M2M de deadline 31 december is in tegenstelling tot de 1 oktober voor websites. Dit terwijl intrekken Dus voor browsers juist de belangrijkste basiseis van toepassing is.

In zeer uitzonderlijke gevallen kunnen wij – zoals bekend - dispensatie verlenen voor het gebruik van certificaten uitgegeven onder de G3 root waarbij de datum van 31 december de uiterste mogelijkheid is.

In de hoop en verwachting met deze uitleg te hebben geholpen,

Met vriendelijke groet,

5.1.2e

Humor, Paradox, Change

.....  
**Logius**

**Ministerie van Binnenlandse Zaken en Koninkrijksrelaties**

Wilhelmina van Pruisenweg 52 | 2595 AN | Den Haag

Postbus 96810 | 2509 JE | Den Haag

5.1.2e

5.1.2e

@logius.nl

.....  
**M**

5.1.2e

5.1.2e

@logius.nl

[www.logius.nl](http://www.logius.nl)

.....  
**Dienst Digitale Overheid**