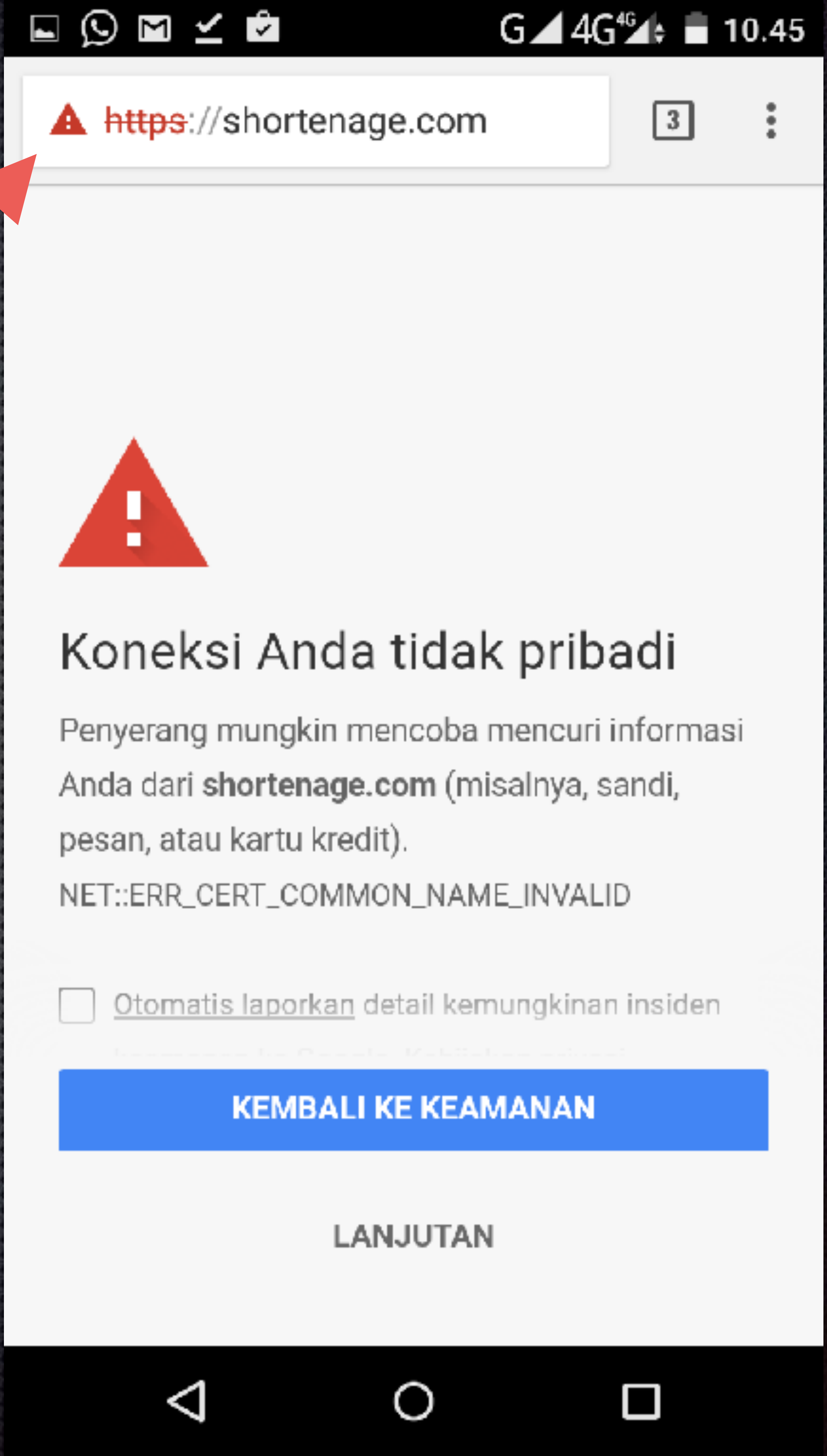
Membuat Sertifikat SSL di Warkop

Azis Kurniawan

Lets begin

(WARMINDO)
Sedia:
Makanan :
-Indomie Goreng
-Indomie Rebus
-Martabak Indomie Goreng
-Martabak Indomie Goreng Rendang
-Gorengan
-Telur 1/2 Matang
Minuman :
-Ichi Ocha
-Air Mineral Club
-Es Teh Manis
-Energy Drink
-Soda Susu Enaak
-Es Jeruk
-Kopi
-Kopi Susu

Perhatikan



~~https~~://shortenage.com

Koneksi Anda tidak pribadi

Penyerang mungkin mencoba mencuri informasi Anda dari **shortenage.com** (misalnya, sandi, pesan, atau kartu kredit).

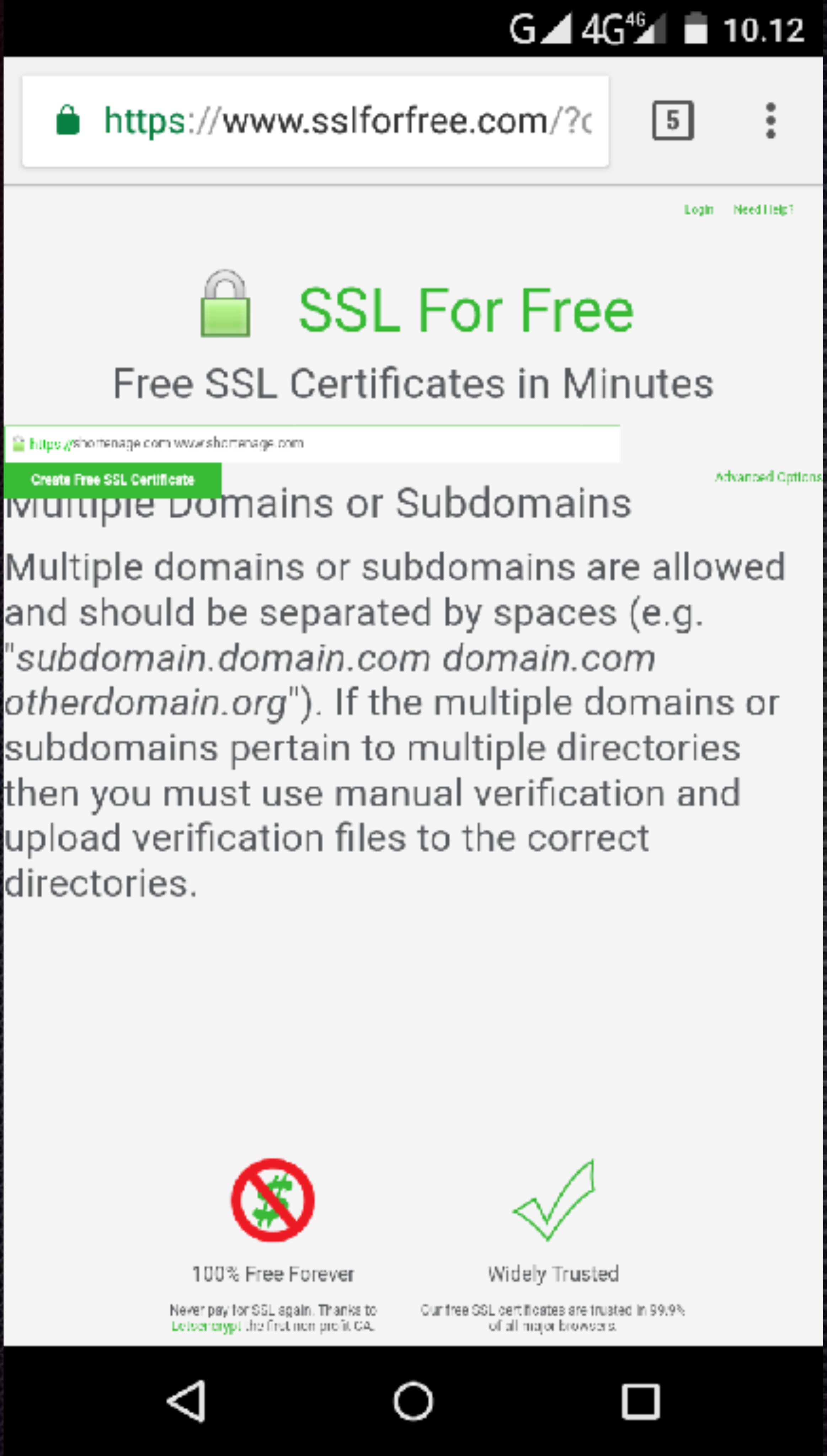
NET::ERR_CERT_COMMON_NAME_INVALID

□ Otomatis laporkan detail kemungkinan insiden

Yang dibutuhkan

- Smartphone (disarankan Android)
- Aplikasi unzip yang terinstall dalam smartphone
- Web browser yang mendukung javascript

Buka https://www.sslforfree.com/


G 4G 10.12
https://www.sslforfree.com/?c
5
Login
Need Help?

SSL For Free

Free SSL Certificates in Minutes

https://shortenage.com www.shortenage.com
Create Free SSL Certificate
Advanced Options

Multiple Domains or Subdomains

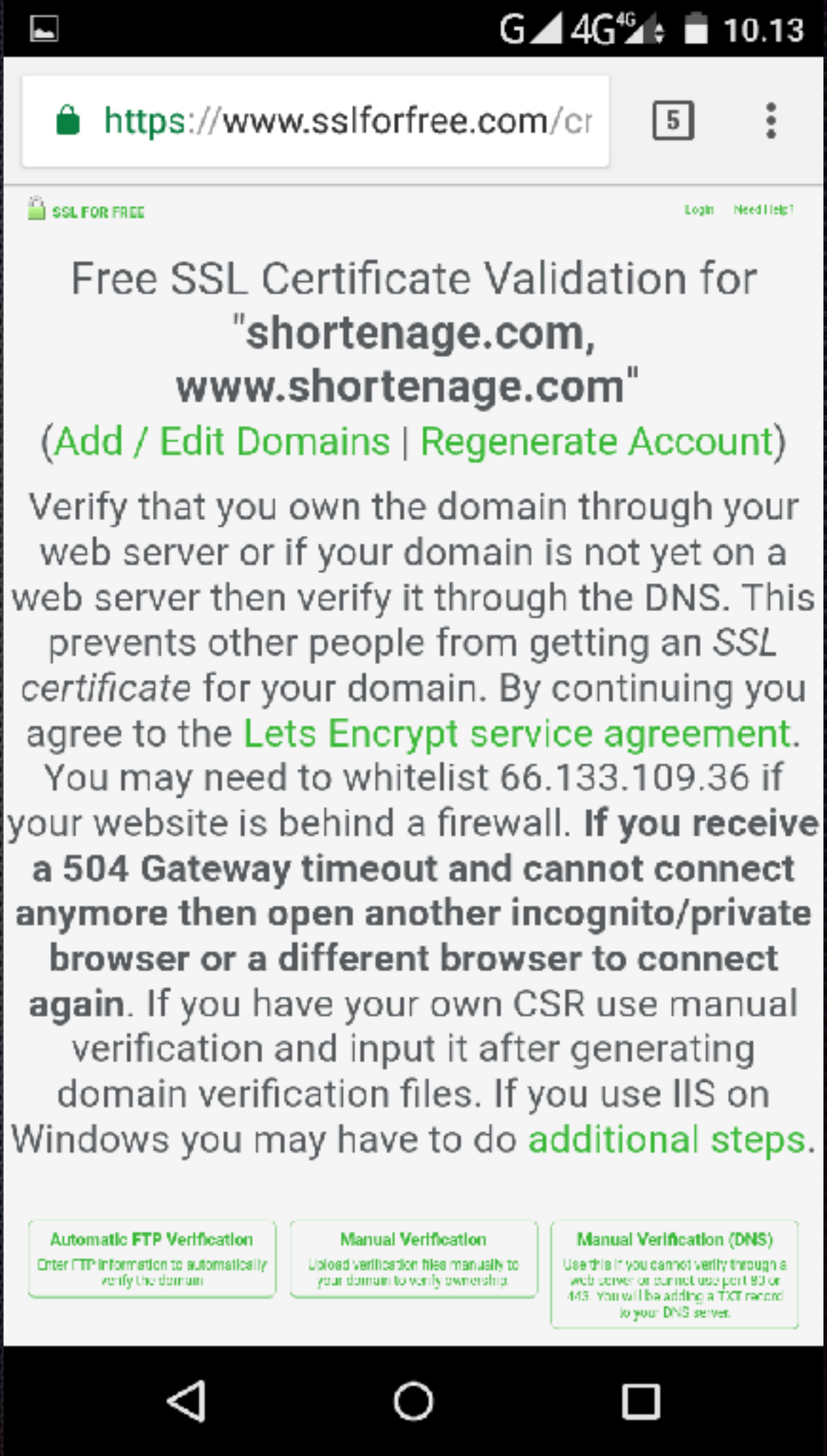
Multiple domains or subdomains are allowed and should be separated by spaces (e.g. "*subdomain.domain.com domain.com otherdomain.org*"). If the multiple domains or subdomains pertain to multiple directories then you must use manual verification and upload verification files to the correct directories.

100% Free Forever

Never pay for SSL again. Thanks to Letsencrypt the first non profit CA.

Widely Trusted

Our free SSL certificates are trusted in 99.9% of all major browsers.



Free SSL Certificate Validation for "**shortenage.com, www.shortenage.com**"

(Add / Edit Domains | Regenerate Account)

Verify that you own the domain through your web server or if your domain is not yet on a web server then verify it through the DNS. This prevents other people from getting an *SSL certificate* for your domain. By continuing you agree to the Lets Encrypt service agreement. You may need to whitelist 66.133.109.36 if your website is behind a firewall. **If you receive a 504 Gateway timeout and cannot connect anymore then open another incognito/private browser or a different browser to connect again**. If you have your own CSR use manual verification and input it after generating domain verification files. If you use IIS on Windows you may have to do additional steps.

Automatic FTP Verification

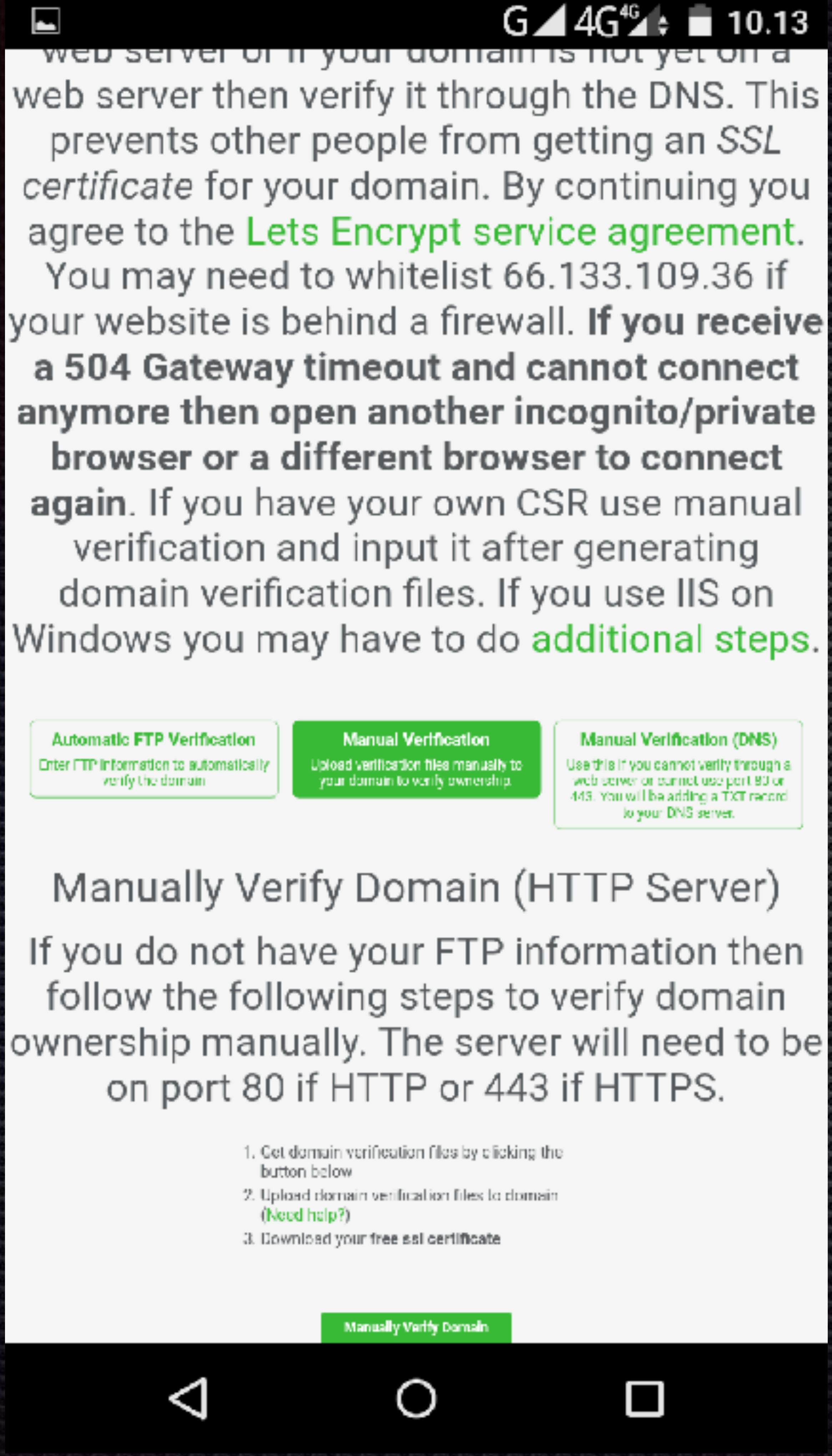
Enter FTP information to automatically verify the domain

Manual Verification

Upload verification files manually to your domain to verify ownership.

Manual Verification (DNS)

Use this if you cannot verify through a web server or cannot use port 80 or 443. You will be adding a TXT record to your DNS server.



web server or if your domain is not yet on a web server then verify it through the DNS. This prevents other people from getting an *SSL certificate* for your domain. By continuing you agree to the Lets Encrypt service agreement. You may need to whitelist 66.133.109.36 if your website is behind a firewall. **If you receive a 504 Gateway timeout and cannot connect anymore then open another incognito/private browser or a different browser to connect again**. If you have your own CSR use manual verification and input it after generating domain verification files. If you use IIS on Windows you may have to do additional steps.

Automatic FTP Verification
Enter FTP information to automatically verify the domain

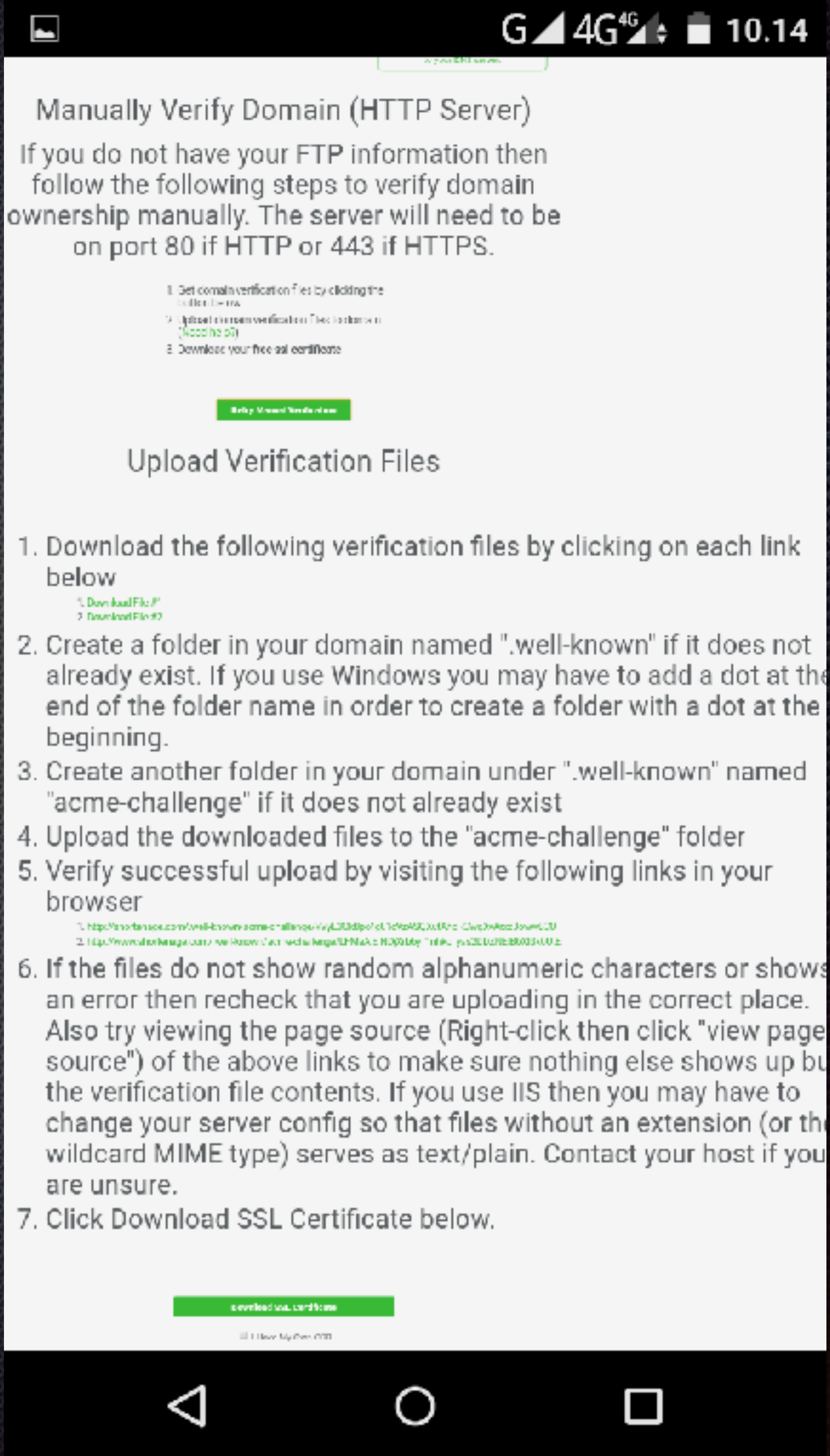
Manual Verification
Upload verification files manually to your domain to verify ownership.

Manual Verification (DNS)
Use this if you cannot verify through a web server or cannot use port 80 or 443. You will be adding a TXT record to your DNS server.

Manually Verify Domain (HTTP Server)

If you do not have your FTP information then follow the following steps to verify domain ownership manually. The server will need to be on port 80 if HTTP or 443 if HTTPS.

1. Get domain verification files by clicking the button below
2. Upload domain verification files to domain (Need help?)
3. Download your **free ssl certificate**



Manually Verify Domain (HTTP Server)

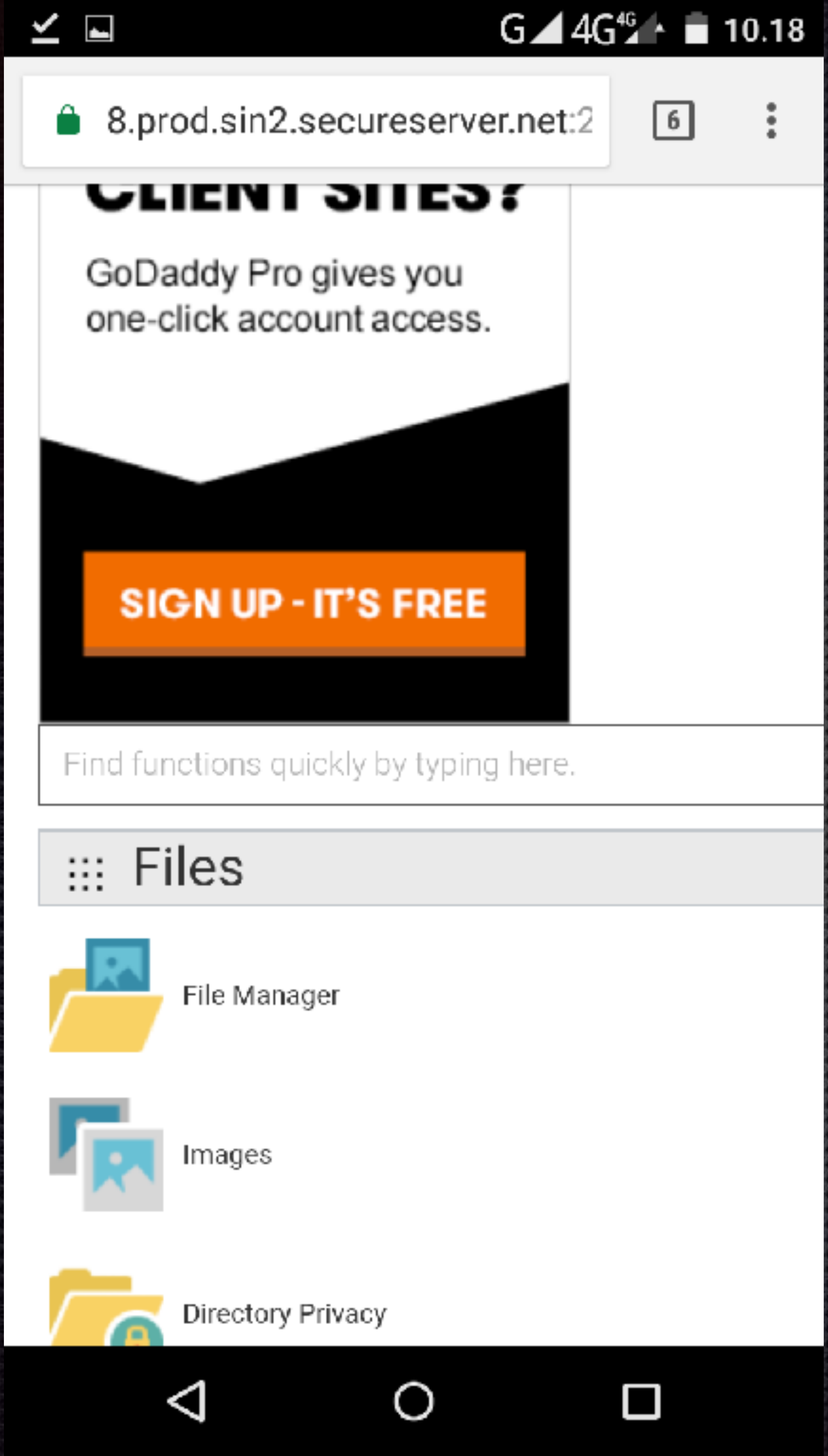
If you do not have your FTP information then follow the following steps to verify domain ownership manually. The server will need to be on port 80 if HTTP or 443 if HTTPS.

1. Get domain verification files by clicking the button below
2. Upload domain verification files to domain (Need help?)
3. Download your free ssl certificate

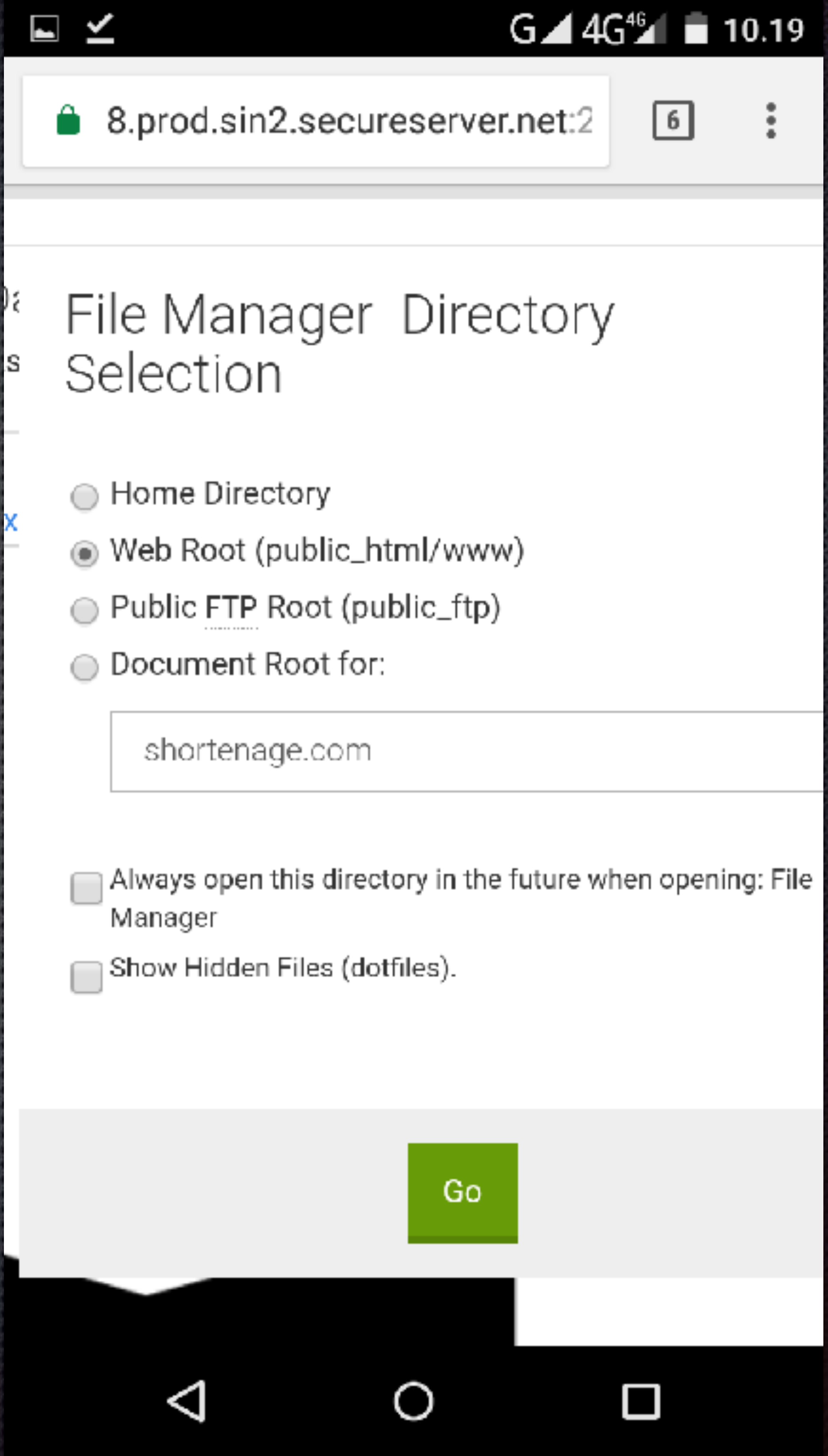
Upload Verification Files

1. Download the following verification files by clicking on each link below
   1. Download File #1
   2. Download File #2
2. Create a folder in your domain named ".well-known" if it does not already exist. If you use Windows you may have to add a dot at the end of the folder name in order to create a folder with a dot at the beginning.
3. Create another folder in your domain under ".well-known" named "acme-challenge" if it does not already exist
4. Upload the downloaded files to the "acme-challenge" folder
5. Verify successful upload by visiting the following links in your browser
   1. [illegible]
   2. [illegible]
6. If the files do not show random alphanumeric characters or shows an error then recheck that you are uploading in the correct place. Also try viewing the page source (Right-click then click "view page source") of the above links to make sure nothing else shows up bu the verification file contents. If you use IIS then you may have to change your server config so that files without an extension (or th wildcard MIME type) serves as text/plain. Contact your host if you are unsure.
7. Click Download SSL Certificate below.

□ I Have My Own CSR



GoDaddy Pro gives you one-click account access.



File Manager Directory Selection

○ Home Directory

● Web Root (public_html/www)

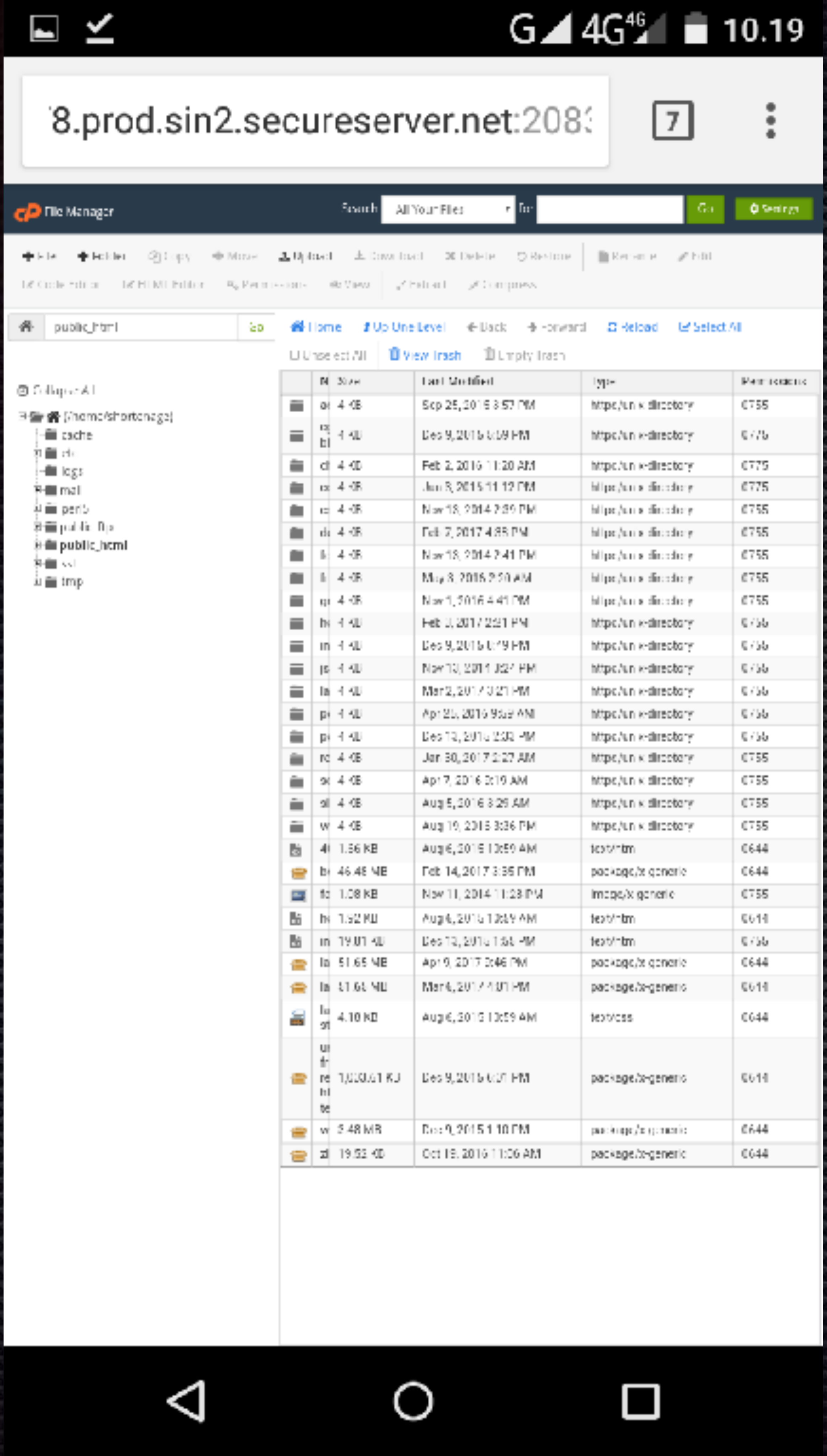
○ Public FTP Root (public_ftp)

○ Document Root for:

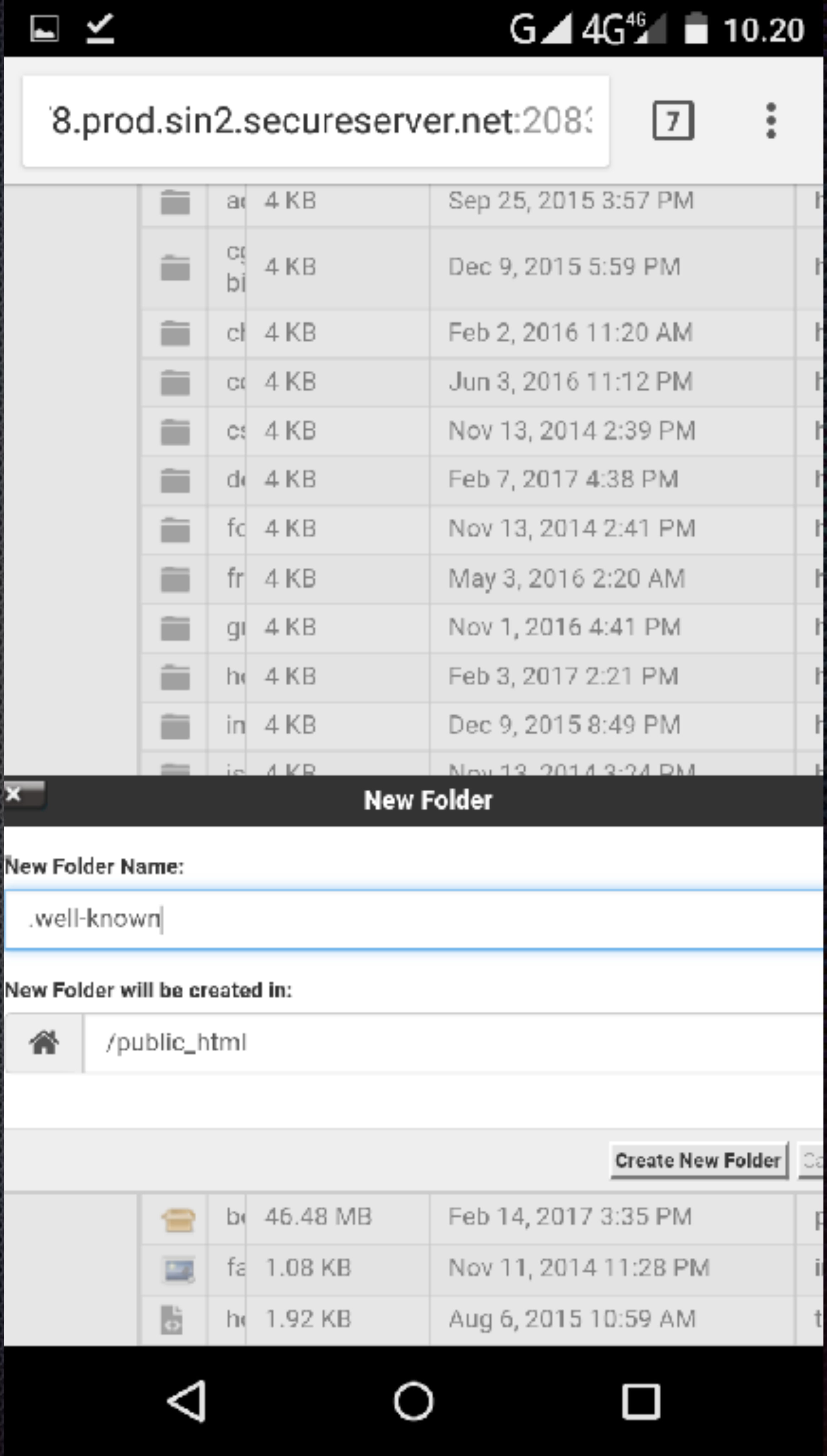
shortenage.com

□ Always open this directory in the future when opening: File Manager

□ Show Hidden Files (dotfiles).


10.19
8.prod.sin2.secureserver.net:2083
File Manager
Search All Your Files for Go ⚙ Settings
+ File + Folder Copy Move Upload Download Delete Restore Rename Edit
Code Editor HTML Editor Permissions View Extract Compress
public_html Go
Home Up One Level Back Forward Reload Select All
Unselect All View Trash Empty Trash
Collapse All
(/home/shortenage)
cache
etc
logs
mail
perl5
public_ftp
public_html
ssl
tmp

	N	Size	Last Modified	Type	Permissions
	ac	4 KB	Sep 25, 2015 3:57 PM	httpd/unix-directory	0755
	cg bi	4 KB	Dec 9, 2015 5:59 PM	httpd/unix-directory	0755
	ch	4 KB	Feb 2, 2016 11:20 AM	httpd/unix-directory	0775
	co	4 KB	Jun 3, 2016 11:12 PM	httpd/unix-directory	0775
	cs	4 KB	Nov 13, 2014 2:39 PM	httpd/unix-directory	0755
	de	4 KB	Feb 7, 2017 4:38 PM	httpd/unix-directory	0755
	fo	4 KB	Nov 13, 2014 2:41 PM	httpd/unix-directory	0755
	fr	4 KB	May 3, 2016 2:20 AM	httpd/unix-directory	0755
	gi	4 KB	Nov 1, 2016 4:41 PM	httpd/unix-directory	0755
	he	4 KB	Feb 3, 2017 2:21 PM	httpd/unix-directory	0755
	in	4 KB	Dec 9, 2015 8:49 PM	httpd/unix-directory	0755
	js	4 KB	Nov 13, 2014 3:24 PM	httpd/unix-directory	0755
	la	4 KB	Mar 2, 2017 3:21 PM	httpd/unix-directory	0755
	pe	4 KB	Apr 25, 2016 9:59 AM	httpd/unix-directory	0755
	pe	4 KB	Dec 13, 2016 2:32 PM	httpd/unix-directory	0755
	rc	4 KB	Jan 30, 2017 2:27 AM	httpd/unix-directory	0755
	sc	4 KB	Apr 7, 2016 3:19 AM	httpd/unix-directory	0755
	sl	4 KB	Aug 5, 2016 3:29 AM	httpd/unix-directory	0755
	w	4 KB	Aug 19, 2015 3:36 PM	httpd/unix-directory	0755
	40	1.36 KB	Aug 6, 2015 10:59 AM	text/html	0644
	be	46.48 MB	Feb 14, 2017 3:35 PM	package/x-generic	0644
	fa	1.08 KB	Nov 11, 2014 11:28 PM	image/x-generic	0755
	ht	1.92 KB	Aug 6, 2015 10:59 AM	text/html	0644
	in	19.01 KB	Dec 13, 2016 1:56 PM	text/html	0644
	la	51.65 MB	Apr 9, 2017 2:46 PM	package/x-generic	0644
	la	51.66 MB	Mar 4, 2017 4:01 PM	package/x-generic	0644
	lu st	4.10 KB	Aug 6, 2015 10:59 AM	text/css	0644
	ur tr re ht te	1,030.61 KB	Dec 9, 2015 6:27 PM	package/x-generic	0644
	w	5.48 MB	Dec 9, 2015 1:10 PM	package/x-generic	0644
	zi	19.53 KB	Oct 19, 2016 11:06 AM	package/x-generic	0644



ac	4 KB	Sep 25, 2015 3:57 PM	h
cg bi	4 KB	Dec 9, 2015 5:59 PM	h
ch	4 KB	Feb 2, 2016 11:20 AM	h
co	4 KB	Jun 3, 2016 11:12 PM	h
cs	4 KB	Nov 13, 2014 2:39 PM	h
de	4 KB	Feb 7, 2017 4:38 PM	h
fo	4 KB	Nov 13, 2014 2:41 PM	h
fr	4 KB	May 3, 2016 2:20 AM	h
gi	4 KB	Nov 1, 2016 4:41 PM	h
he	4 KB	Feb 3, 2017 2:21 PM	h
in	4 KB	Dec 9, 2015 8:49 PM	h
js	4 KB	Nov 13, 2014 3:24 PM	h

New Folder

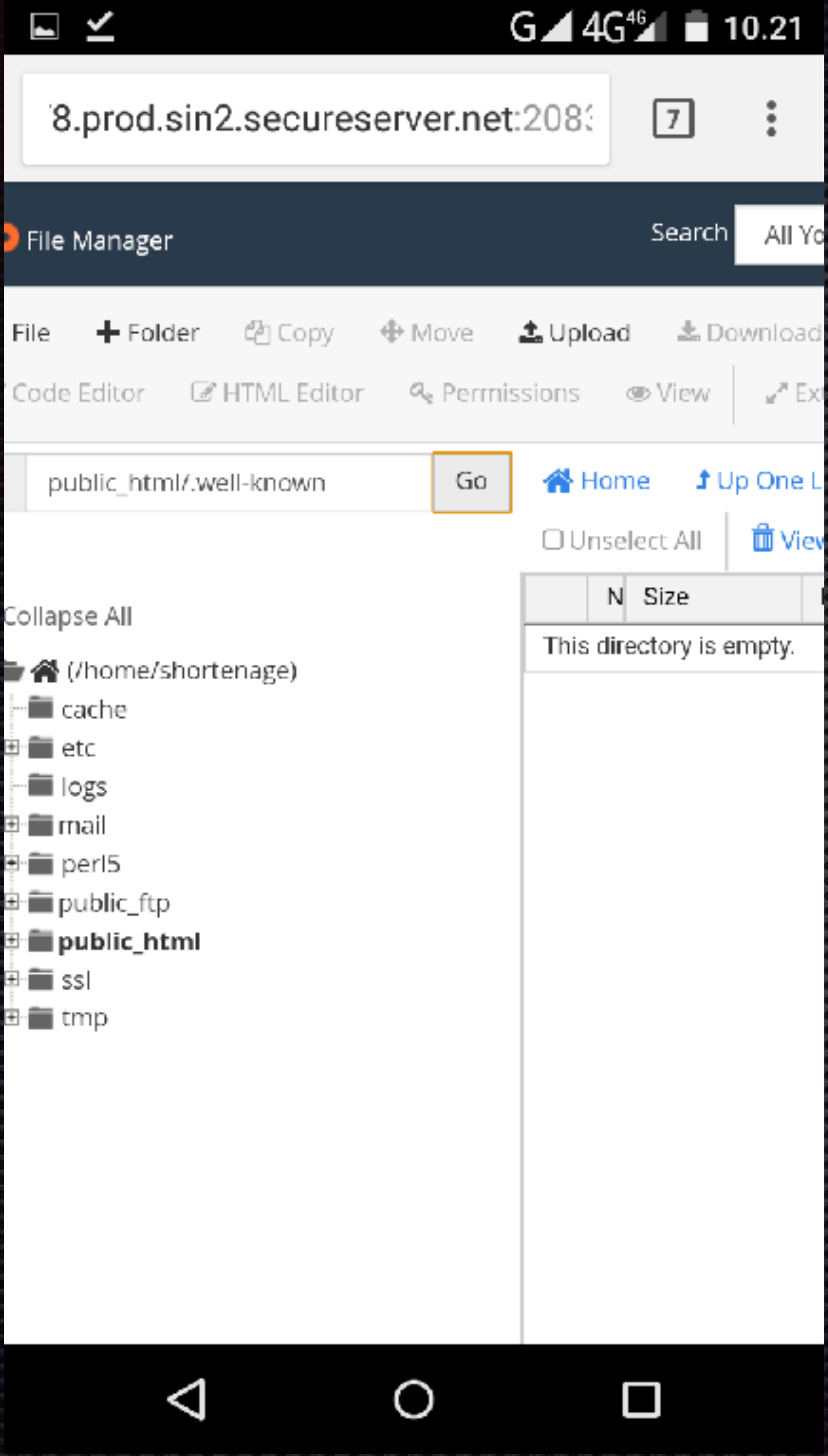
New Folder Name:

.well-known

New Folder will be created in:

/public_html

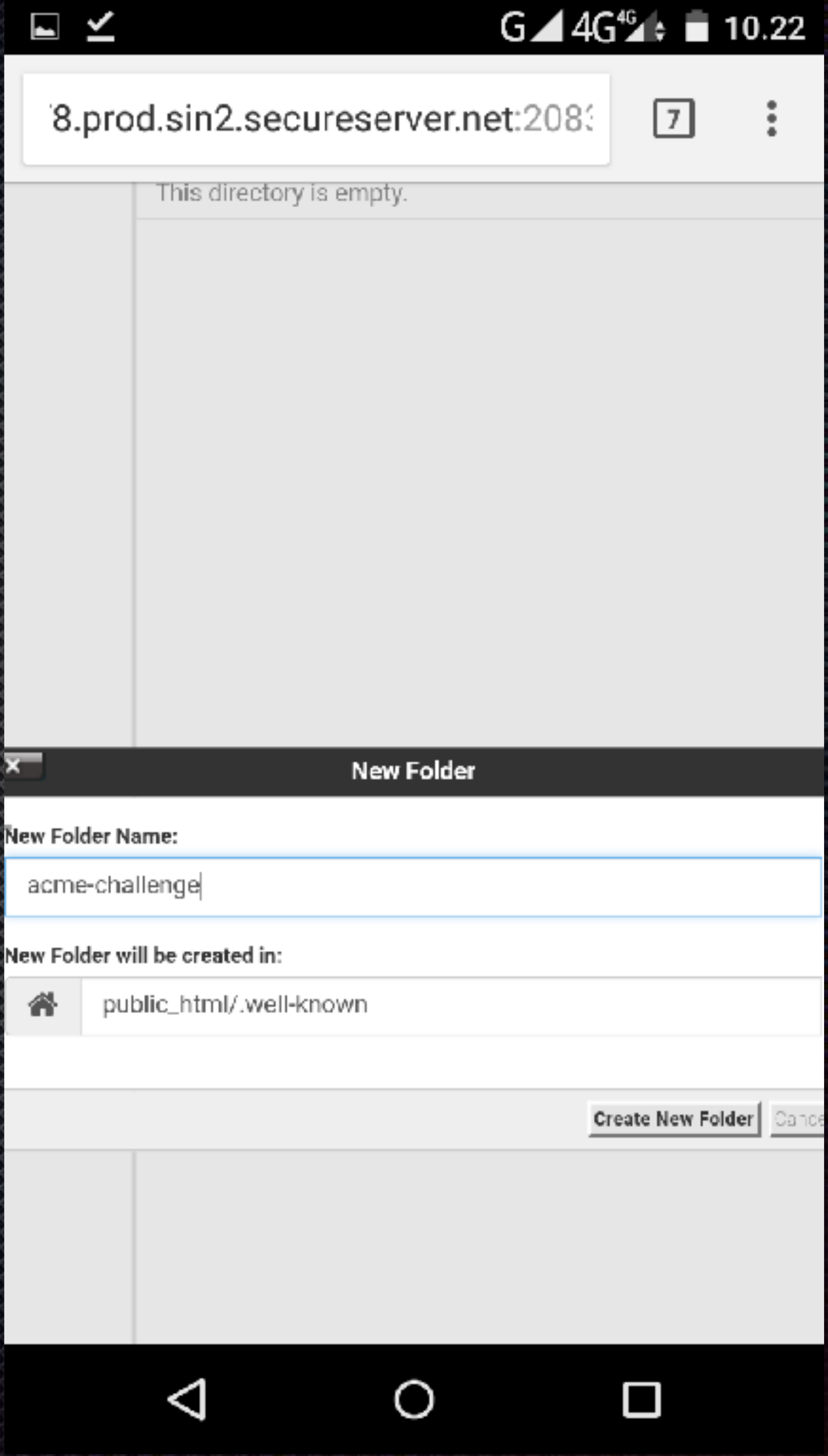
be	46.48 MB	Feb 14, 2017 3:35 PM	p
fa	1.08 KB	Nov 11, 2014 11:28 PM	i
ht	1.92 KB	Aug 6, 2015 10:59 AM	t



8.prod.sin2.secureserver.net:208

public_html/.well-known

This directory is empty.

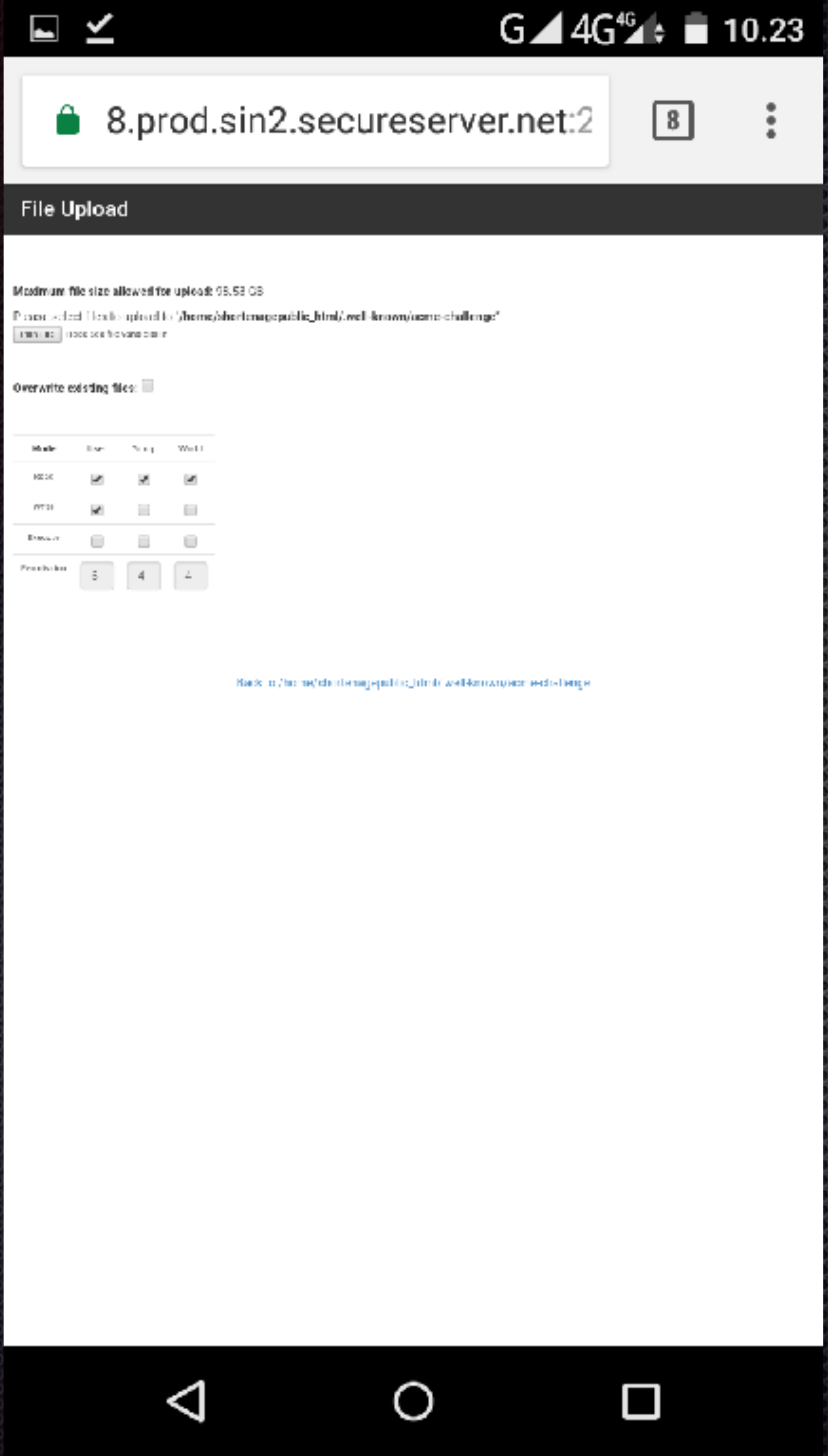


8.prod.sin2.secureserver.net:208

This directory is empty.

New Folder Name: acme-challenge

New Folder will be created in: public_html/.well-known



File Upload

Maximum file size allowed for upload: 95.58 GB

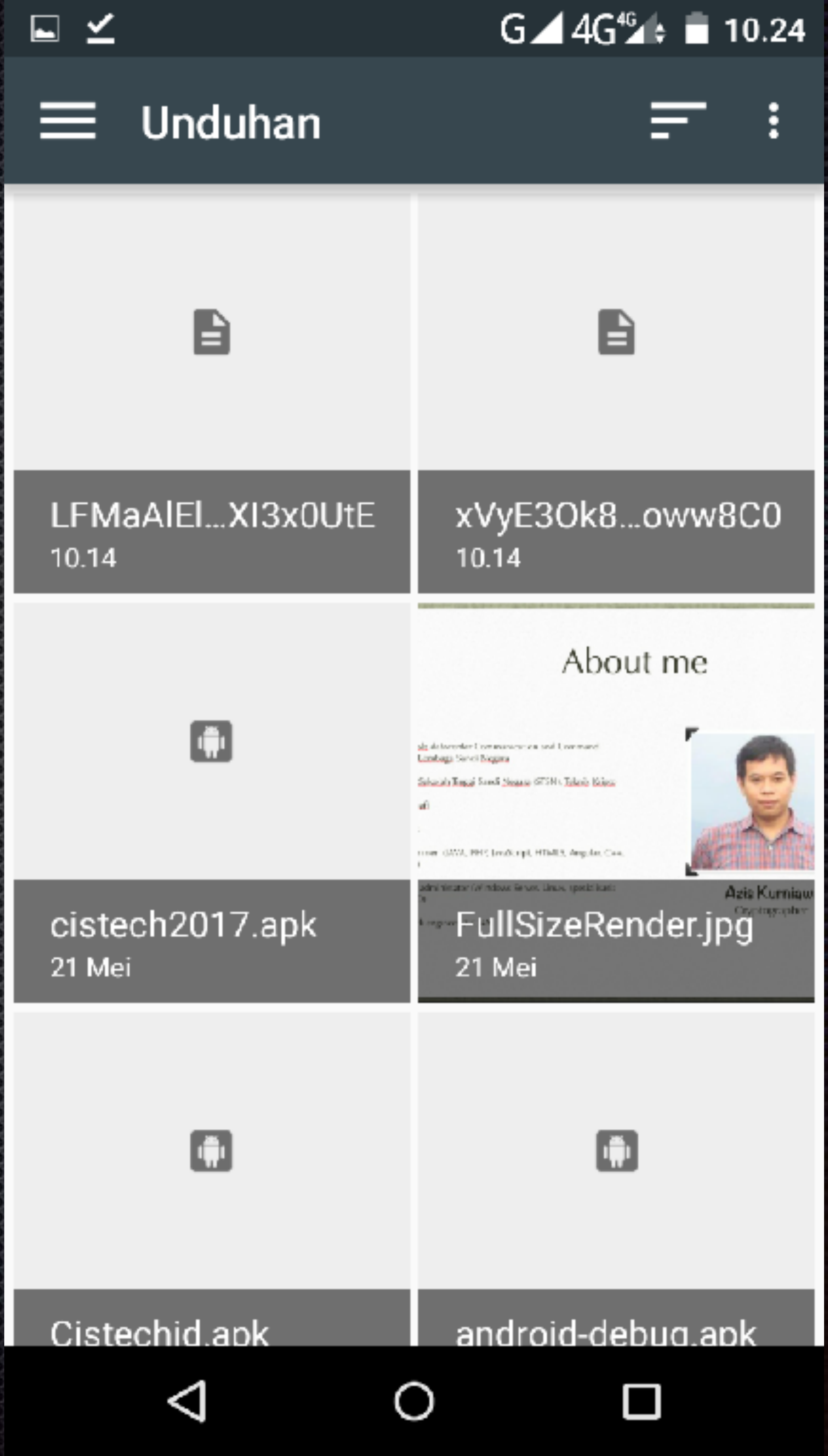
Please select file to upload to "/home/shortenage/public_html/.well-known/acme-challenge"

Browse... No file selected.

Overwrite existing files: □

Mode	User	Group	World
Read	☑	☑	☑
Write	☑	□	□
Execute	□	□	□
Permission	6	4	4

Back to /home/shortenage/public_html/.well-known/acme-challenge



LFMaAlEl...XI3x0UtE
10.14

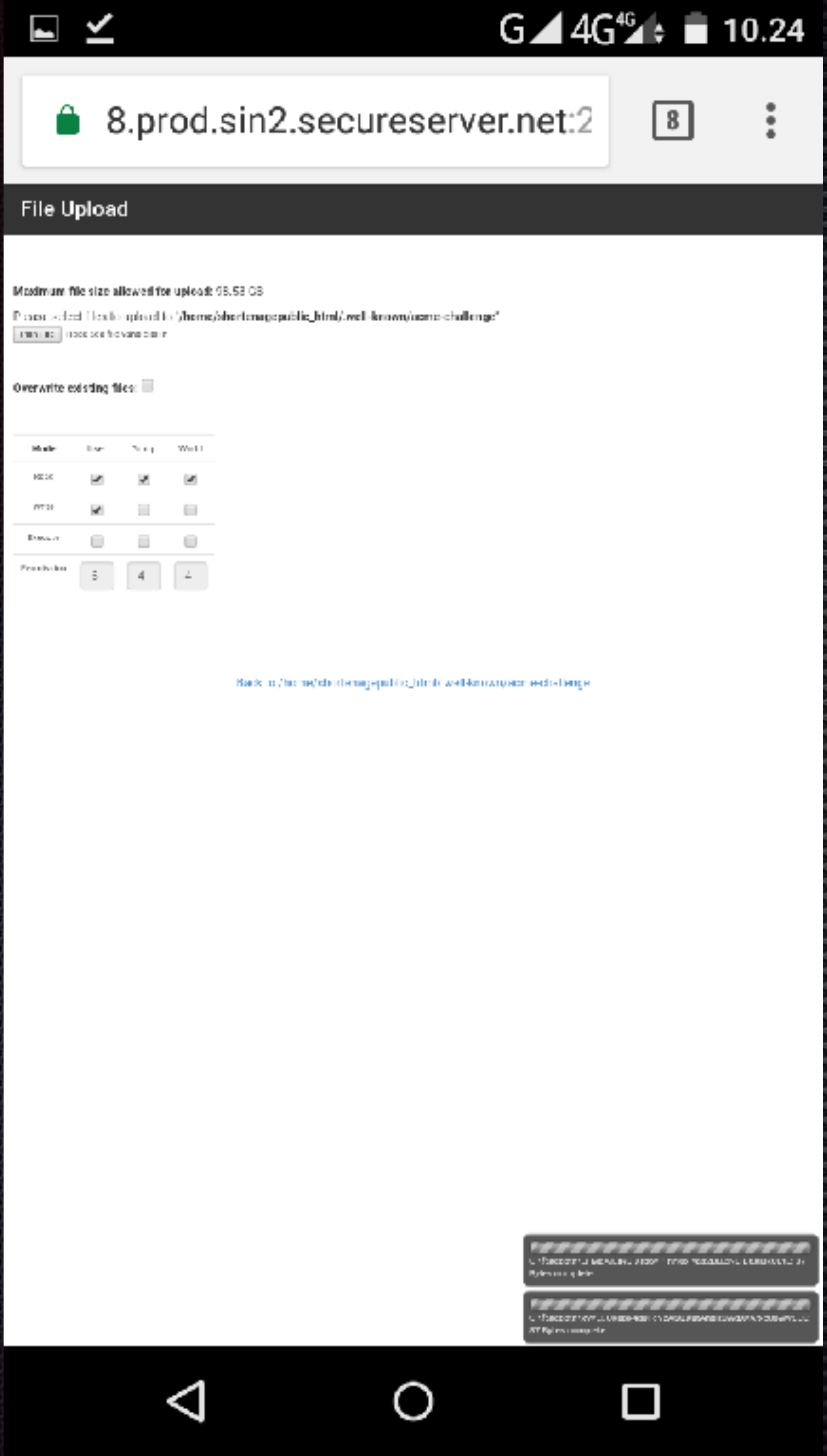
xVyE3Ok8...oww8C0
10.14

cistech2017.apk
21 Mei

FullSizeRender.jpg
21 Mei

Cistechid.apk

android-debug.apk



File Upload

Maximum file size allowed for upload: 95.53 GB

Please select files to upload to '/home/shortenage/public_html/.well-known/acme-challenge'

Choose files No file chosen

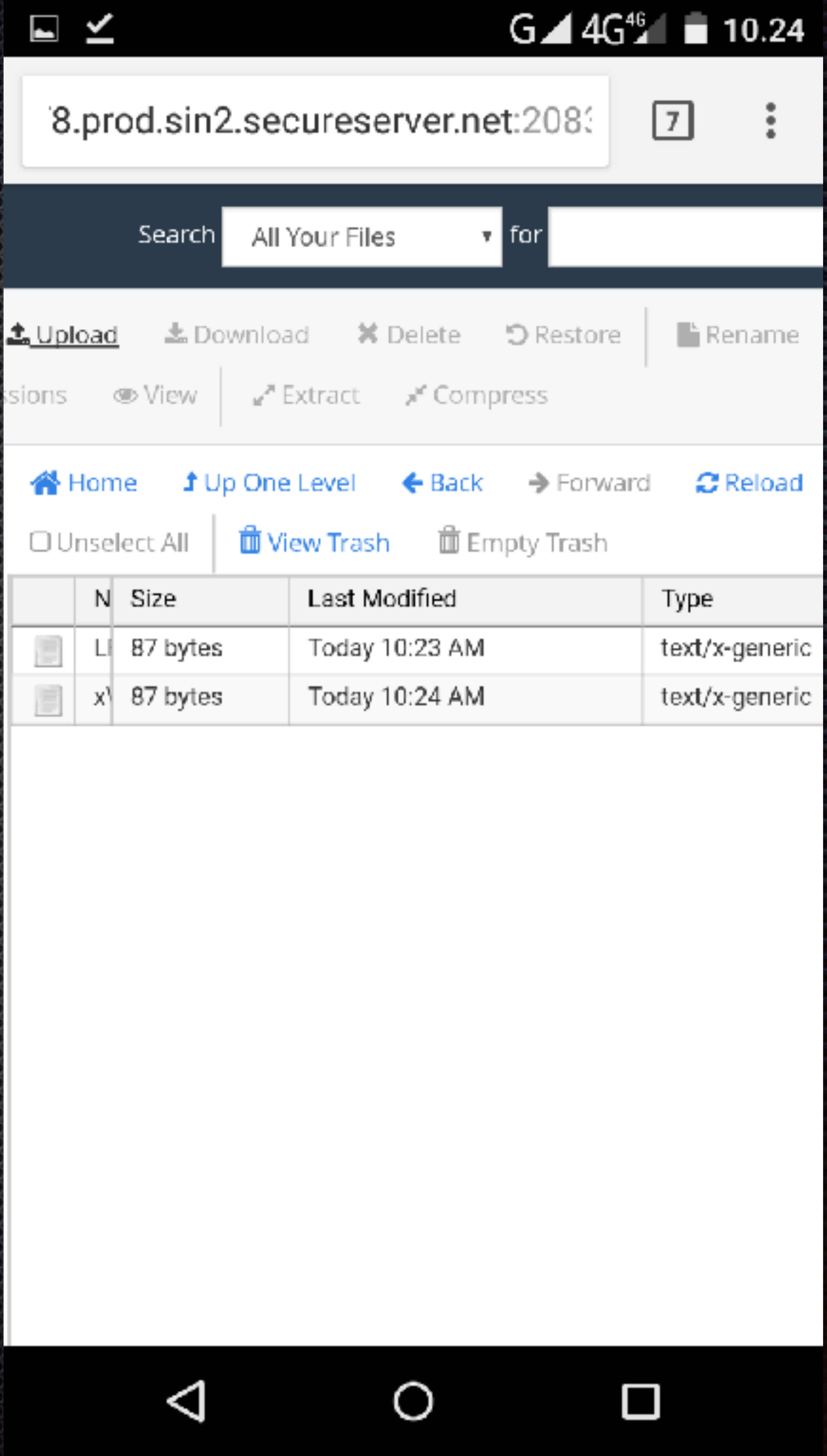
Overwrite existing files: □

Mode	User	Group	World
Read	☑	☑	☑
Write	☑	□	□
Execute	□	□	□
Permission	6	4	4

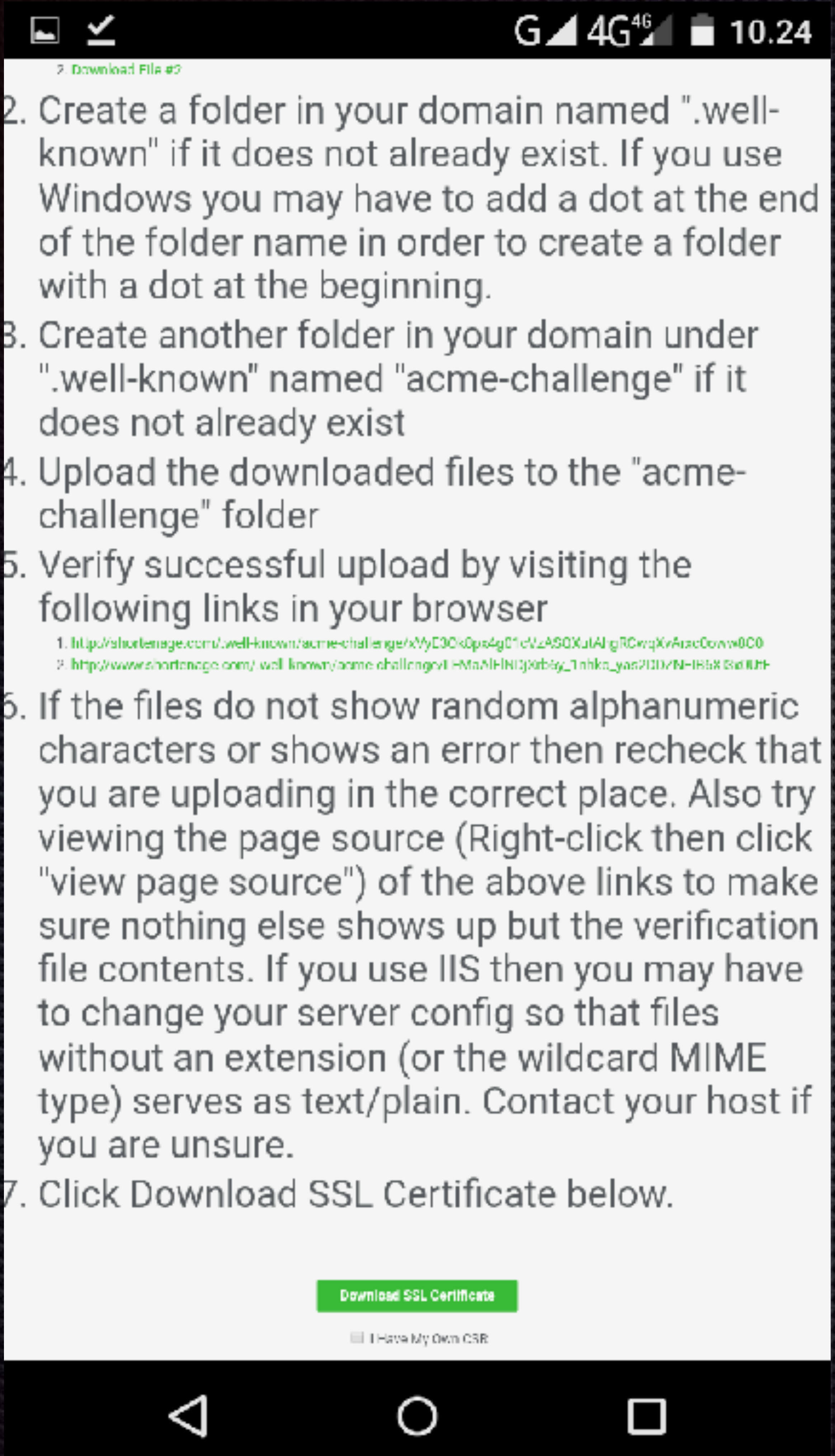
Back to /home/shortenage/public_html/.well-known/acme-challenge

[illegible] 87 bytes complete

[illegible] 87 bytes complete



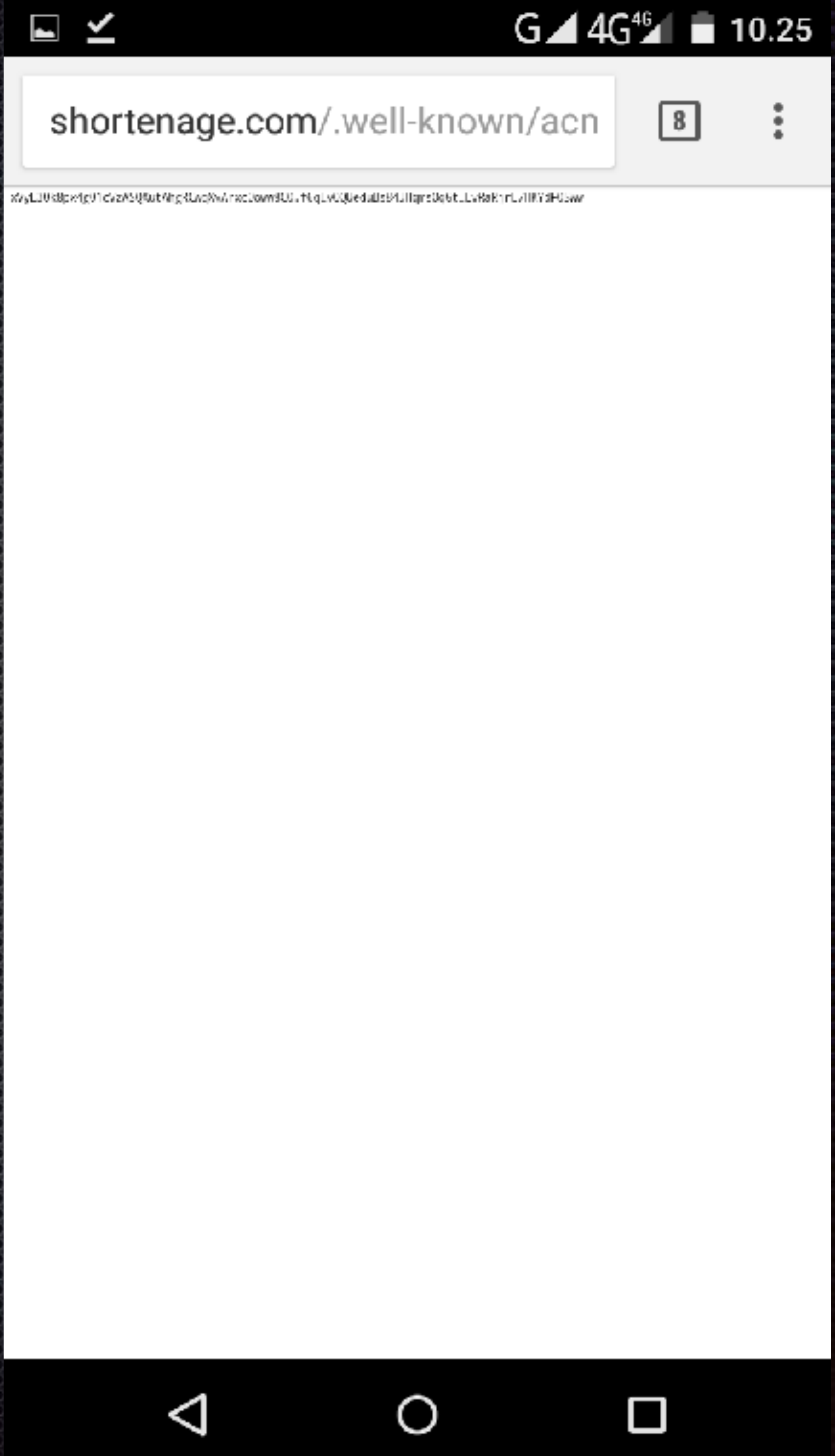
N	Size	Last Modified	Type
LI	87 bytes	Today 10:23 AM	text/x-generic
x\	87 bytes	Today 10:24 AM	text/x-generic



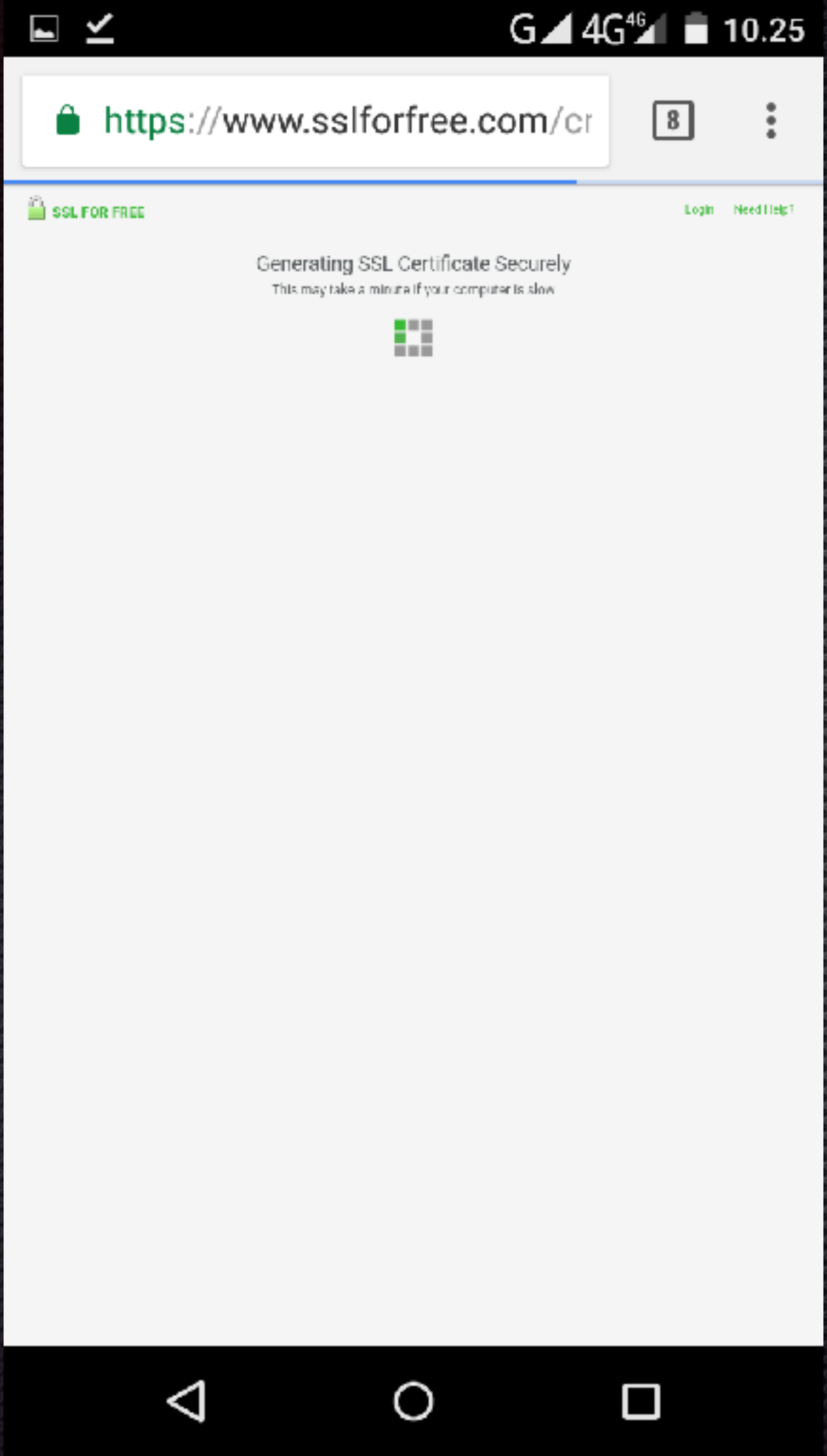
2. Download File #2

2. Create a folder in your domain named ".well-known" if it does not already exist. If you use Windows you may have to add a dot at the end of the folder name in order to create a folder with a dot at the beginning.
3. Create another folder in your domain under ".well-known" named "acme-challenge" if it does not already exist
4. Upload the downloaded files to the "acme-challenge" folder
5. Verify successful upload by visiting the following links in your browser
   1. http://shortenage.com/.well-known/acme-challenge/xWyD3Ok0ps4g01cVzASQXutAhgRCwqXvArxcOovw0C0
   2. http://www.shortenage.com/.well-known/acme-challenge/tHMaAlHRCjXrb6y_1nhko_yas2I3D7N-I86X3dQUH
6. If the files do not show random alphanumeric characters or shows an error then recheck that you are uploading in the correct place. Also try viewing the page source (Right-click then click "view page source") of the above links to make sure nothing else shows up but the verification file contents. If you use IIS then you may have to change your server config so that files without an extension (or the wildcard MIME type) serves as text/plain. Contact your host if you are unsure.
7. Click Download SSL Certificate below.

□ I Have My Own CSR

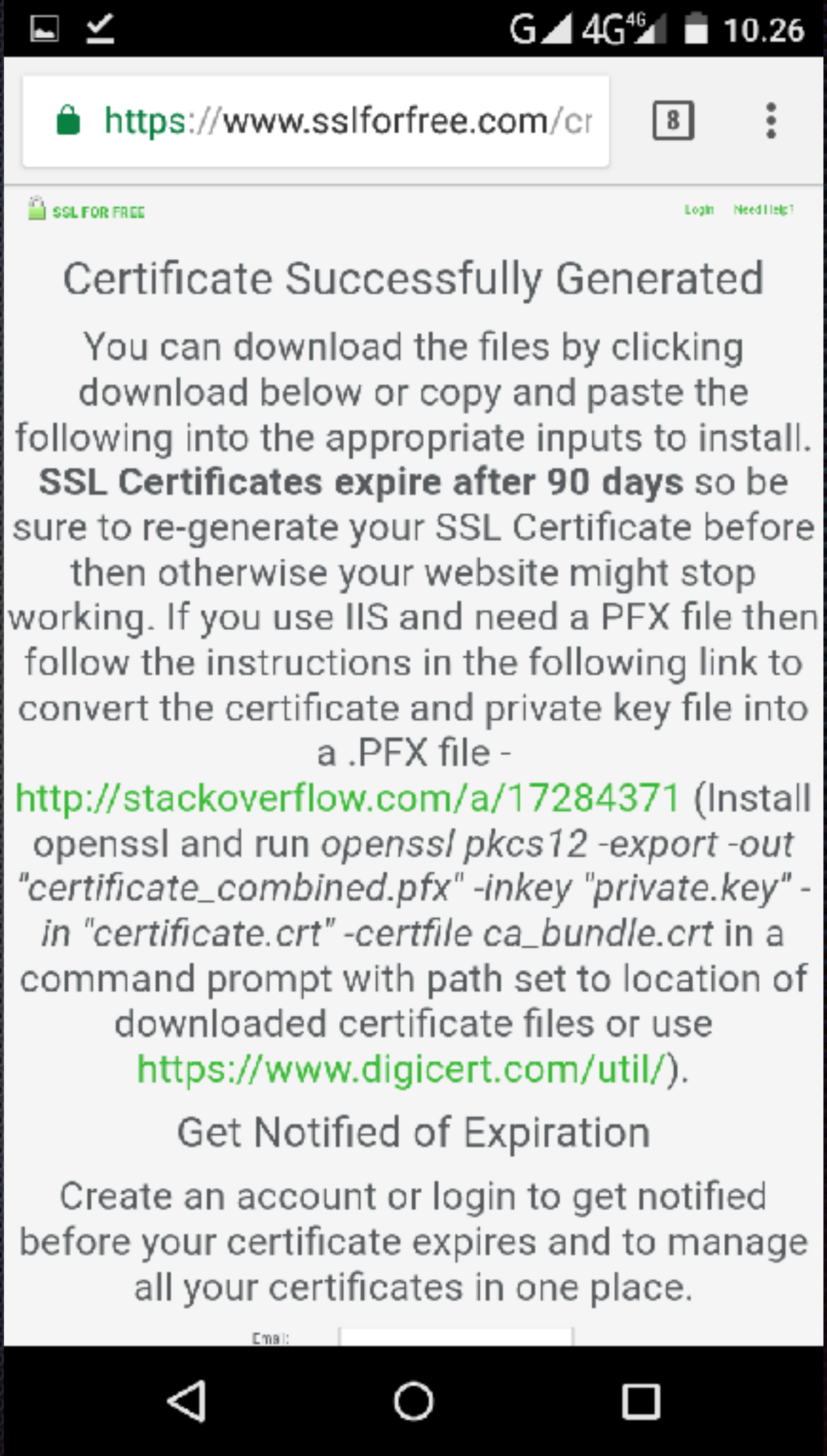


xWyL30k0px4g01cVzASQXutAhgRCwqXvArxcOovw0C0.flqLvOQedaUsPLJIlqrsUobt_LvRaKnrL7IIRYdHUaw



Generating SSL Certificate Securely

This may take a minute if your computer is slow



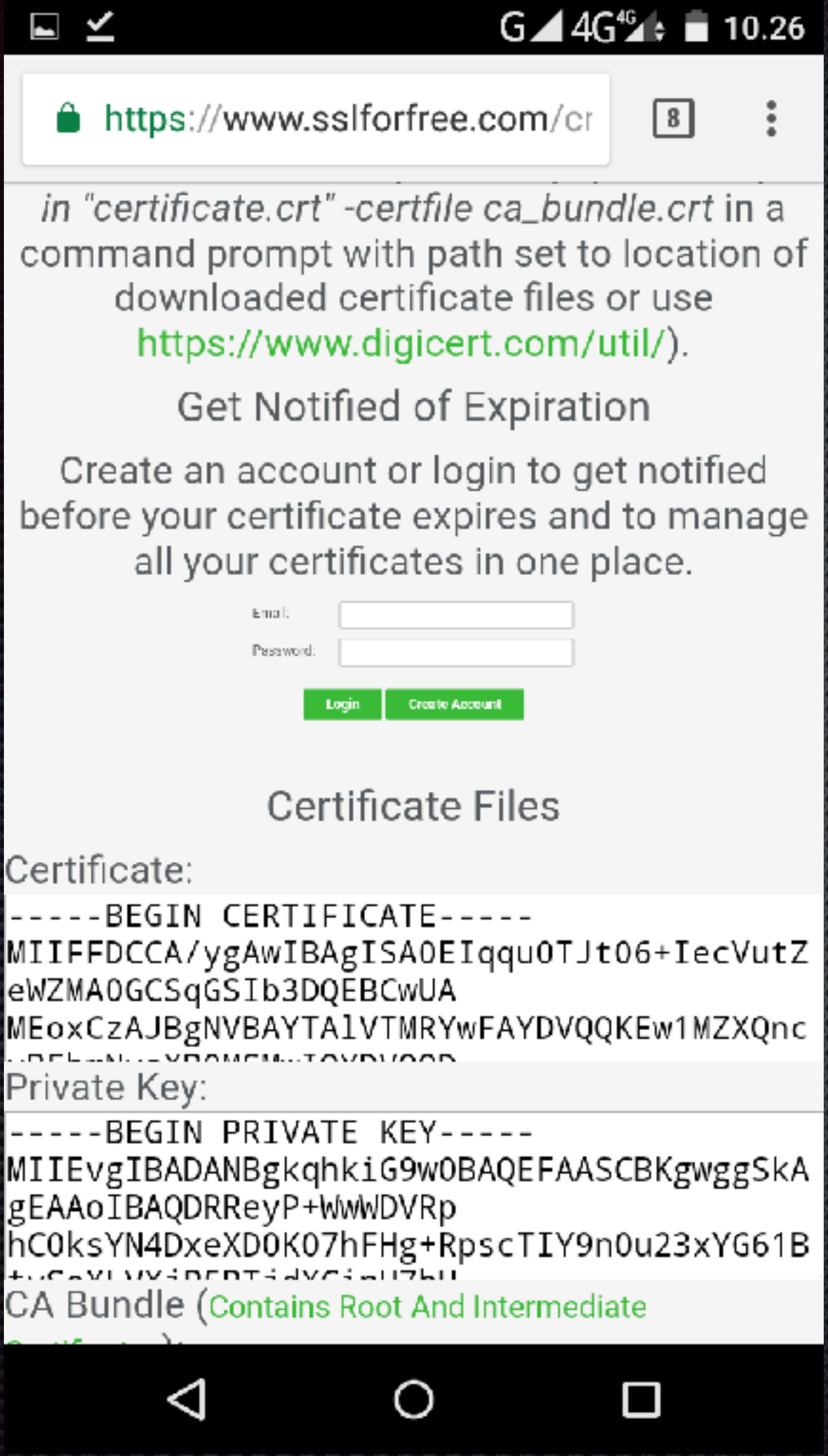
Certificate Successfully Generated

You can download the files by clicking download below or copy and paste the following into the appropriate inputs to install. **SSL Certificates expire after 90 days** so be sure to re-generate your SSL Certificate before then otherwise your website might stop working. If you use IIS and need a PFX file then follow the instructions in the following link to convert the certificate and private key file into a .PFX file - http://stackoverflow.com/a/17284371 (Install openssl and run *openssl pkcs12 -export -out "certificate_combined.pfx" -inkey "private.key" -in "certificate.crt" -certfile ca_bundle.crt* in a command prompt with path set to location of downloaded certificate files or use https://www.digicert.com/util/).

Get Notified of Expiration

Create an account or login to get notified before your certificate expires and to manage all your certificates in one place.

Email:



in "certificate.crt" -certfile ca_bundle.crt in a command prompt with path set to location of downloaded certificate files or use https://www.digicert.com/util/).

Get Notified of Expiration

Create an account or login to get notified before your certificate expires and to manage all your certificates in one place.

Email:

Password:

Certificate Files

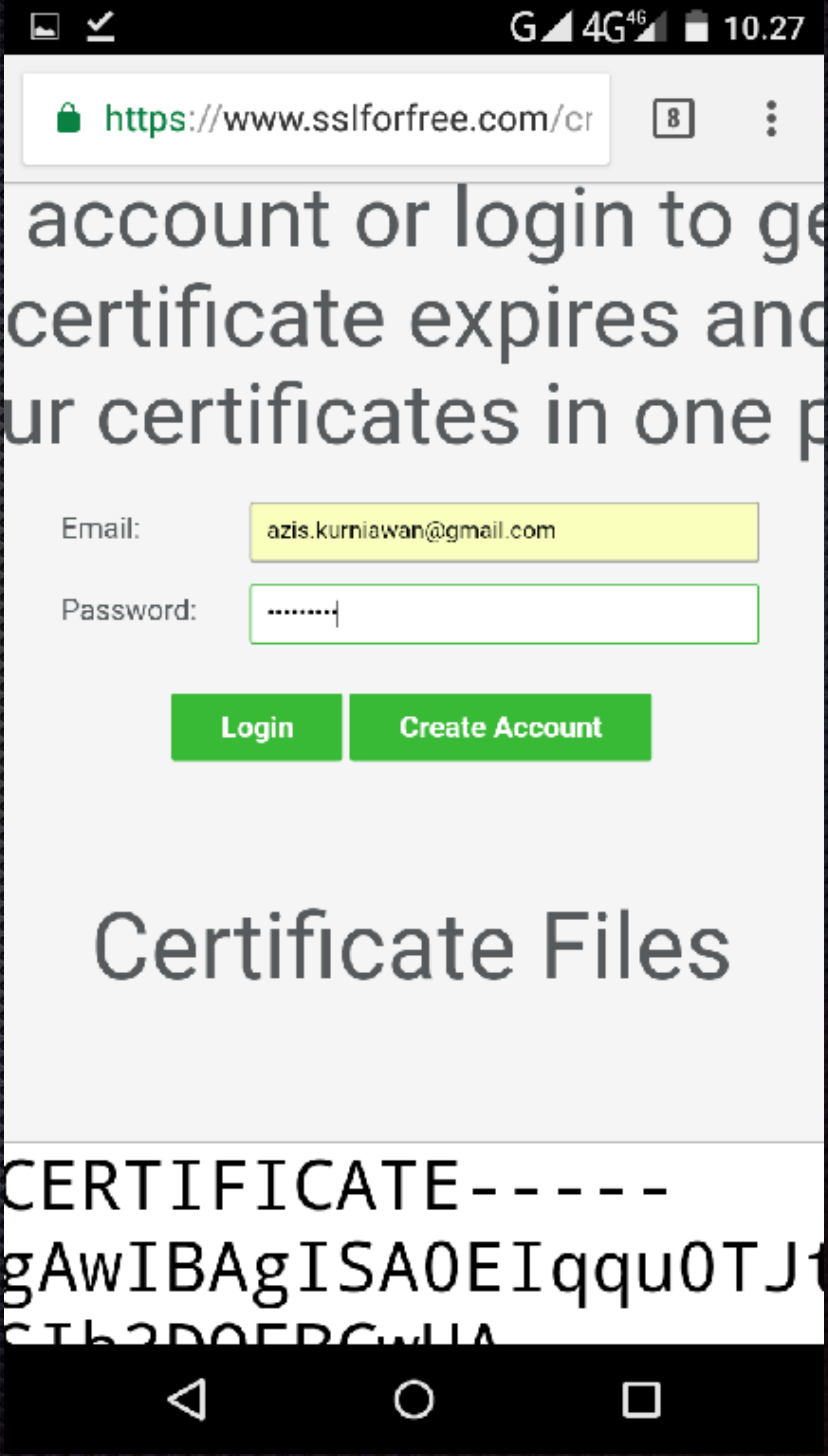
Certificate:

```
-----BEGIN CERTIFICATE-----
MIIFFDCCA/ygAwIBAgISA0EIqqu0TJt06+IecVutZ
eWZMA0GCSqGSIb3DQEBCwUA
MEoxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQnc
```

Private Key:

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkA
gEAAoIBAQDRReyP+WwWDVRp
hC0ksYN4DxeXD0K07hFHg+RpscTIY9n0u23xYG61B
```

CA Bundle (Contains Root And Intermediate



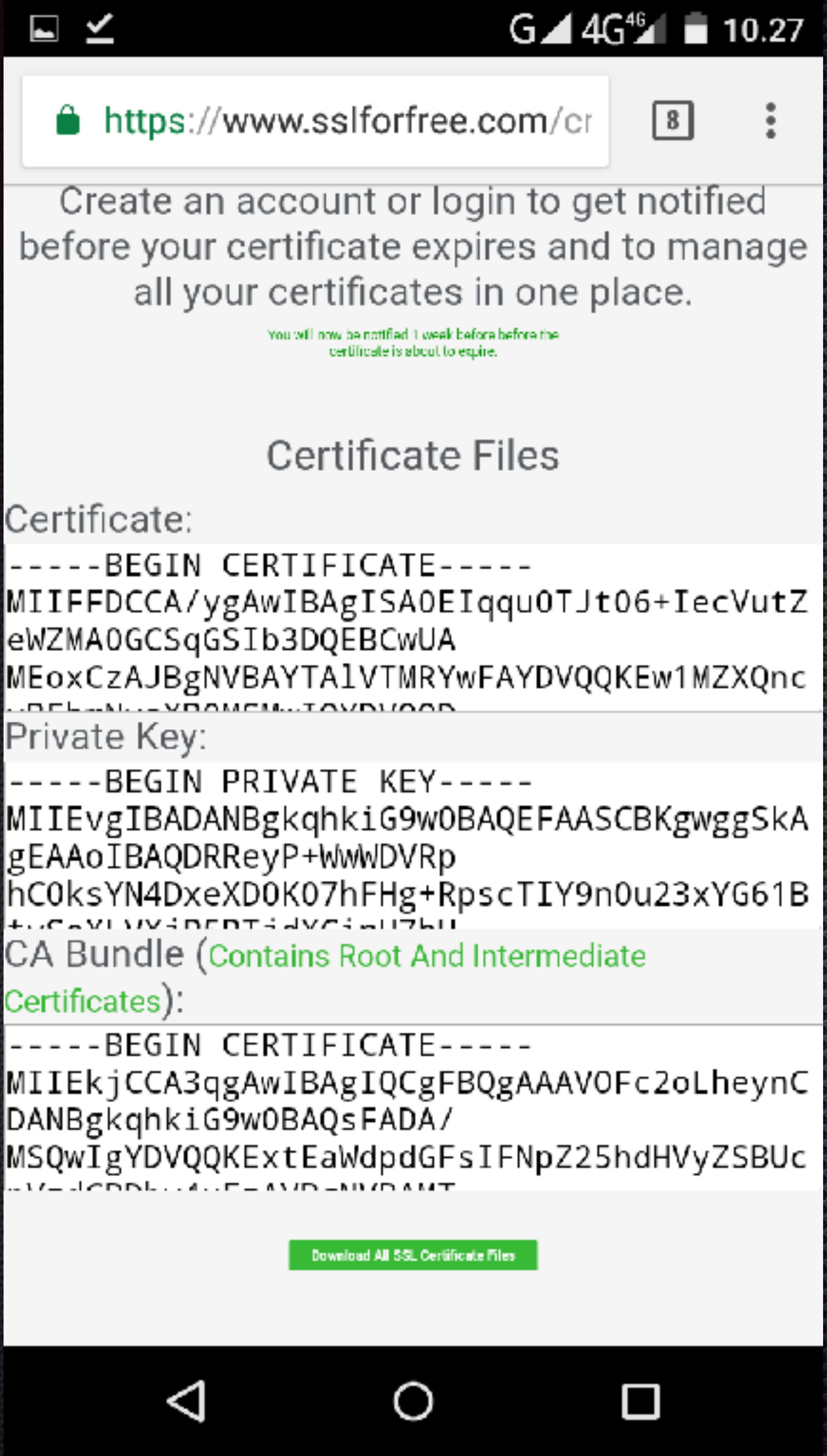
account or login to ge
certificate expires and
ur certificates in one p

Email: azis.kurniawan@gmail.com

Password: ••••••••••

Certificate Files

```
CERTIFICATE-----
gAwIBAgISA0EIqqu0TJt
```



Create an account or login to get notified before your certificate expires and to manage all your certificates in one place.

You will now be notified 1 week before before the certificate is about to expire.

Certificate Files

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIFFDCCA/ygAwIBAgISA0EIqqu0TJt06+IecVutZ
eWZMA0GCSqGSIb3DQEBCwUA
MEoxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQnc
```

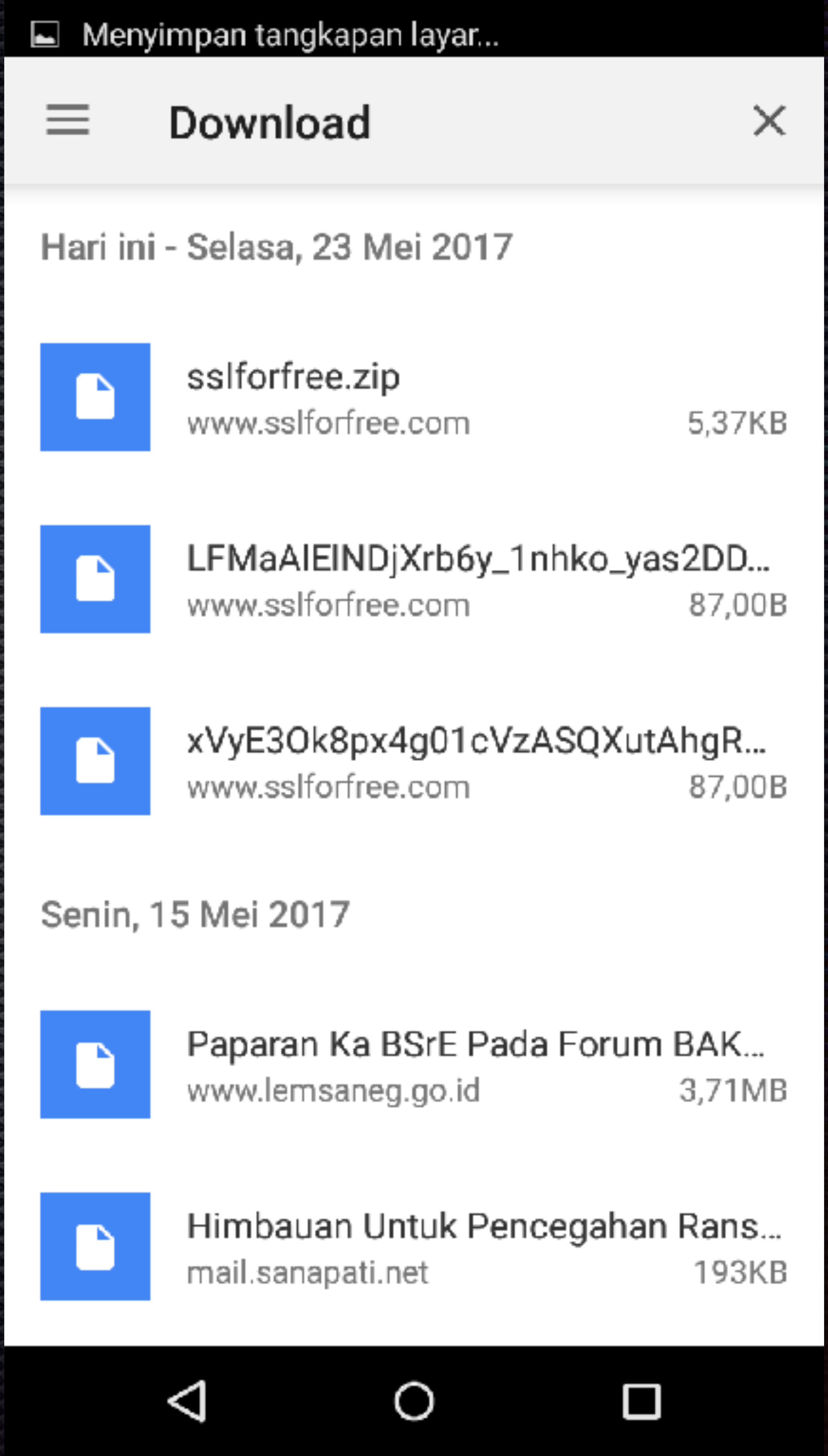
Private Key:

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkA
gEAAoIBAQDRReyP+WwWDVRp
hC0ksYN4DxeXD0K07hFHg+RpscTIY9n0u23xYG61B
```

CA Bundle (Contains Root And Intermediate Certificates):

```
-----BEGIN CERTIFICATE-----
MIIEkjCCA3qgAwIBAgIQCgFBQgAAAVOFc2oLheynC
DANBgkqhkiG9w0BAQsFADA/
MSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUc
```

Download All SSL Certificate Files


Menyimpan tangkapan layar...

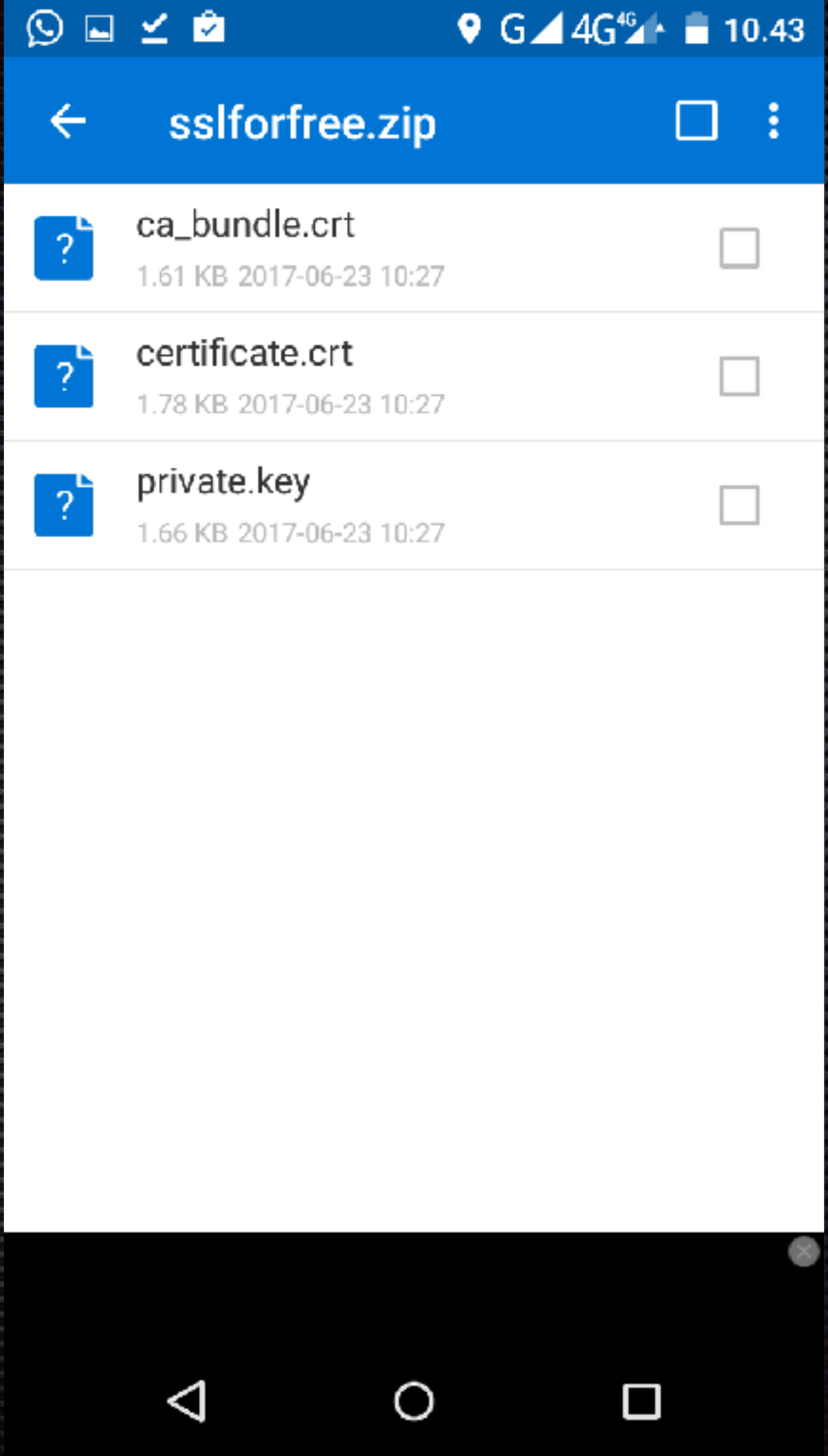
Download

Hari ini - Selasa, 23 Mei 2017

sslforfree.zip	www.sslforfree.com	5,37KB
LFMaAIEINDjXrb6y_1nhko_yas2DD...	www.sslforfree.com	87,00B
xVyE3Ok8px4g01cVzASQXutAhgR...	www.sslforfree.com	87,00B

Senin, 15 Mei 2017

Paparan Ka BSrE Pada Forum BAK...	www.lemsaneg.go.id	3,71MB
Himbauan Untuk Pencegahan Rans...	mail.sanapati.net	193KB

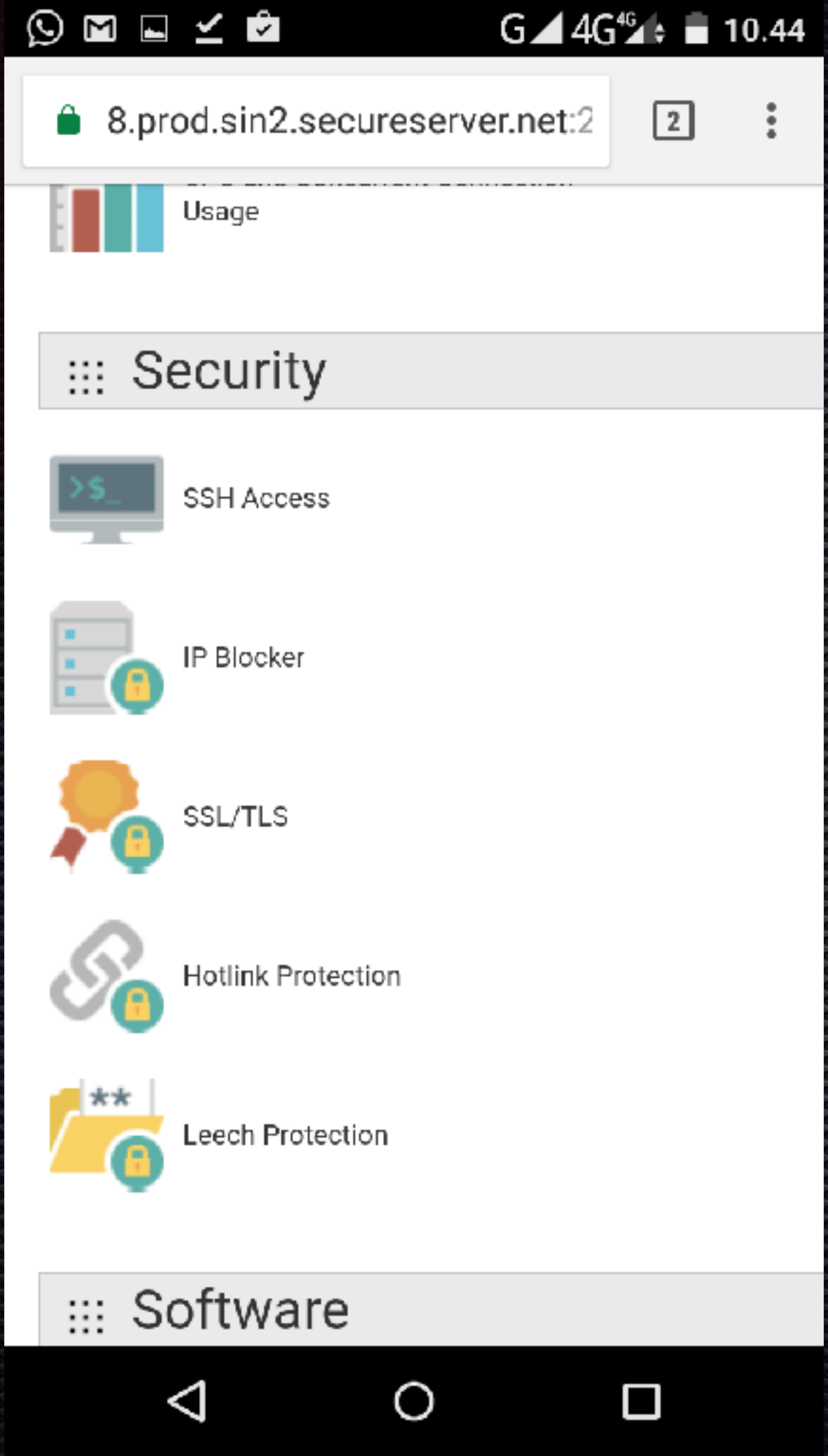


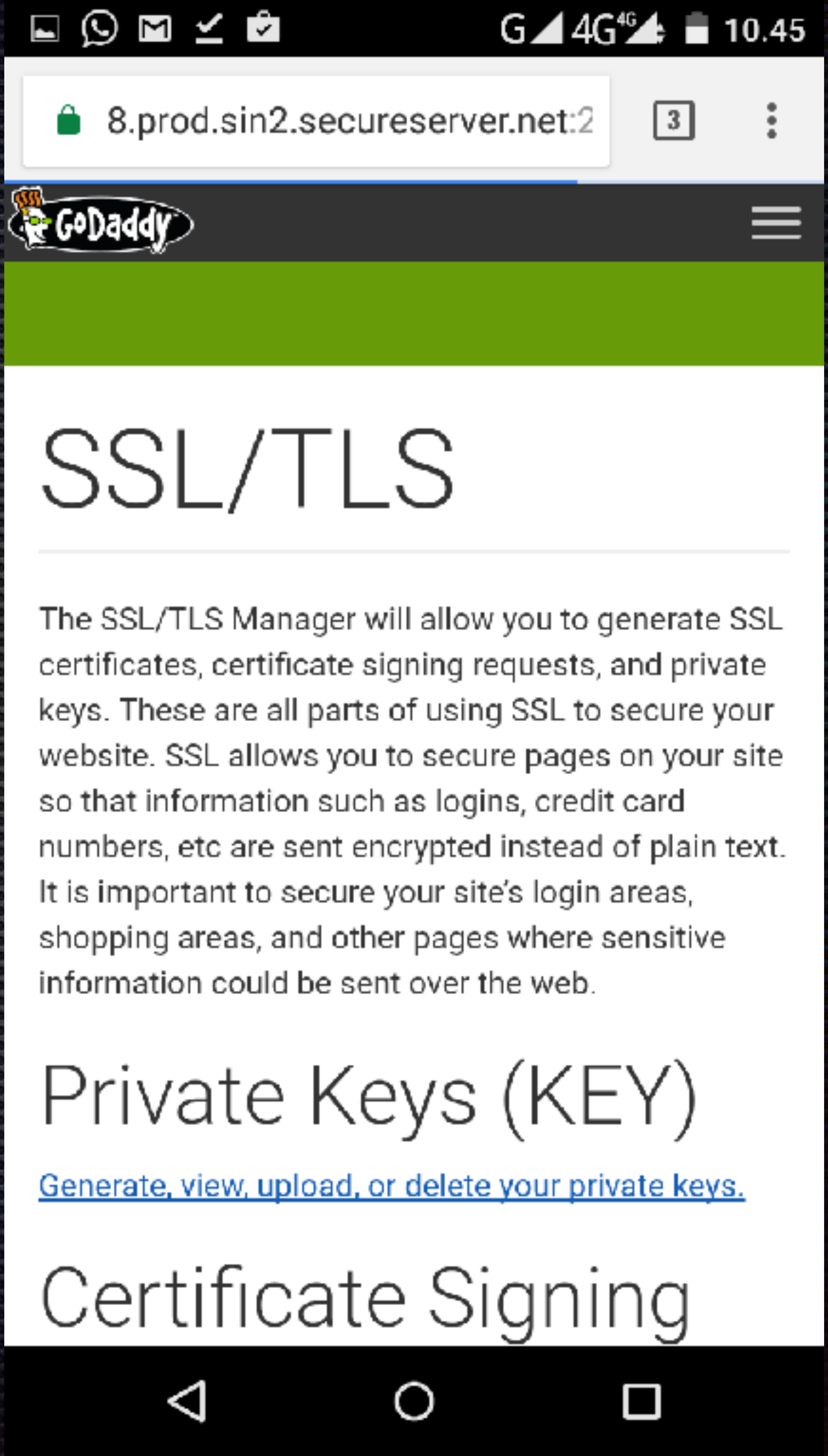
sslforfree.zip

ca_bundle.crt
1.61 KB 2017-06-23 10:27 □

certificate.crt
1.78 KB 2017-06-23 10:27 □

private.key
1.66 KB 2017-06-23 10:27 □





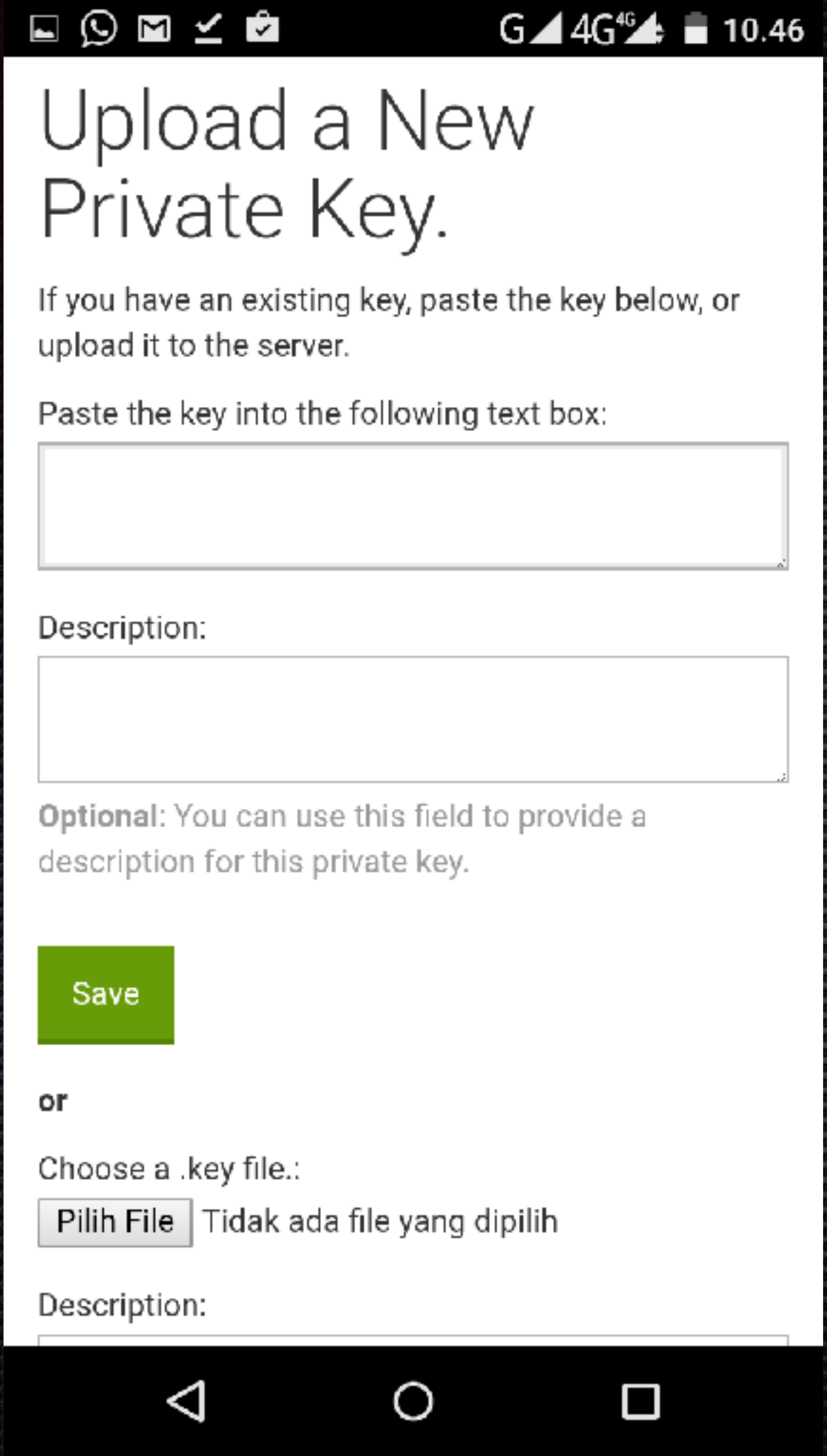
SSL/TLS

The SSL/TLS Manager will allow you to generate SSL certificates, certificate signing requests, and private keys. These are all parts of using SSL to secure your website. SSL allows you to secure pages on your site so that information such as logins, credit card numbers, etc are sent encrypted instead of plain text. It is important to secure your site's login areas, shopping areas, and other pages where sensitive information could be sent over the web.

Private Keys (KEY)

Generate, view, upload, or delete your private keys.

Certificate Signing



Upload a New Private Key.

If you have an existing key, paste the key below, or upload it to the server.

Paste the key into the following text box:

Description:

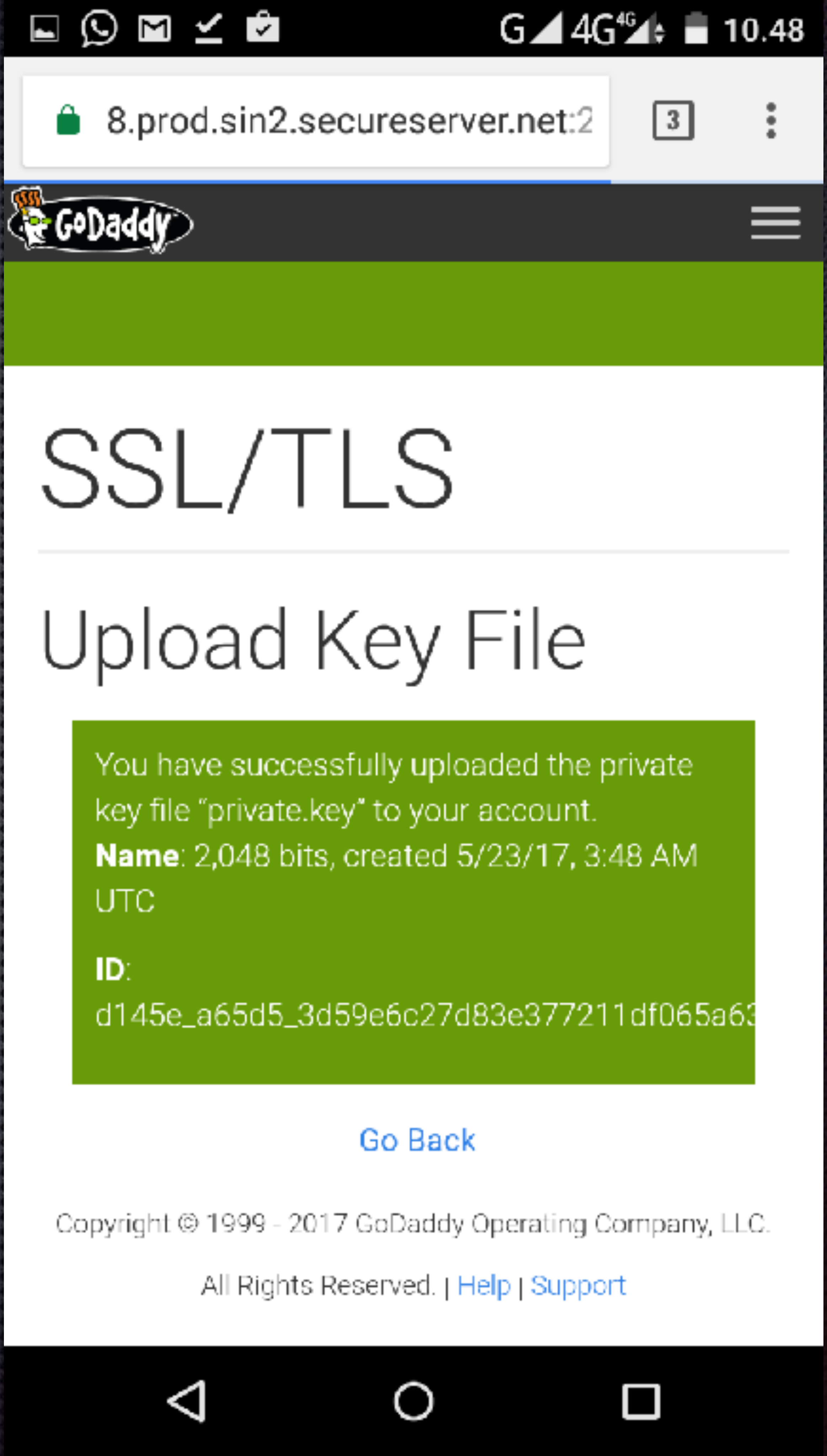
Optional: You can use this field to provide a description for this private key.

or

Choose a .key file.:

Tidak ada file yang dipilih

Description:



SSL/TLS

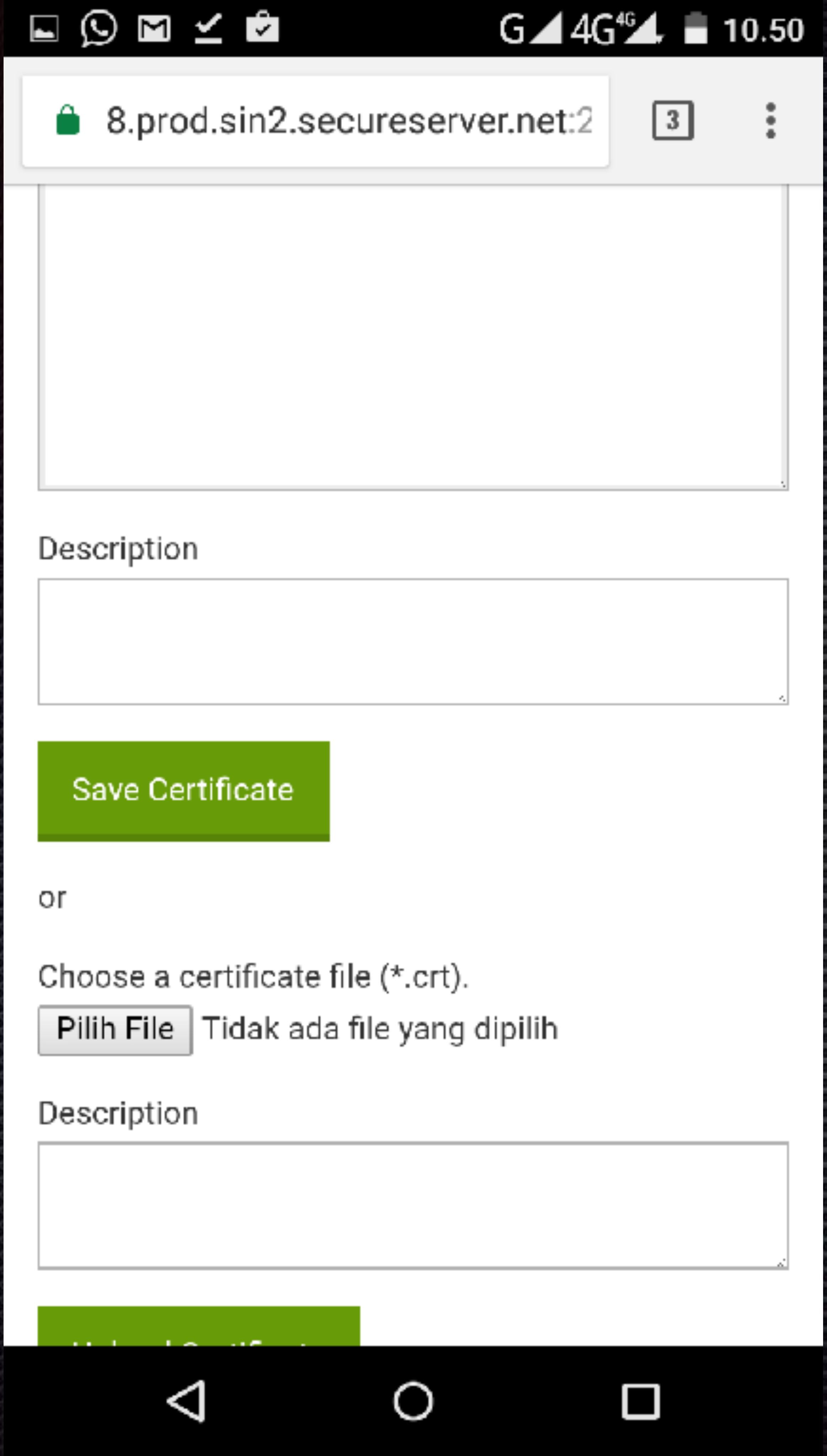
Upload Key File

You have successfully uploaded the private key file “private.key” to your account.
Name: 2,048 bits, created 5/23/17, 3:48 AM UTC

ID:
d145e_a65d5_3d59e6c27d83e377211df065a63

Copyright © 1999 - 2017 GoDaddy Operating Company, LLC.

All Rights Reserved. | Help | Support



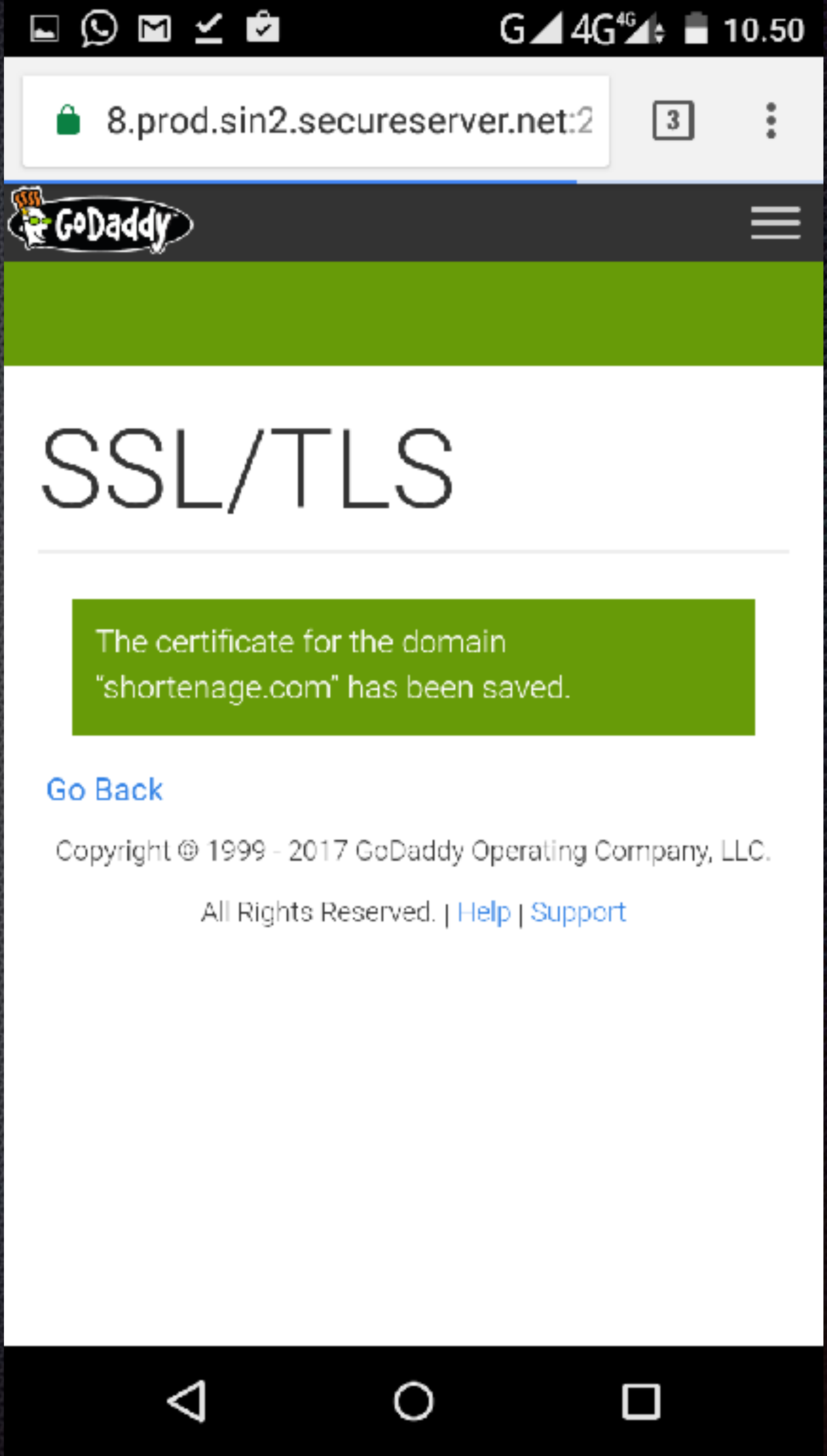
Description

or

Choose a certificate file (*.crt).

Tidak ada file yang dipilih

Description

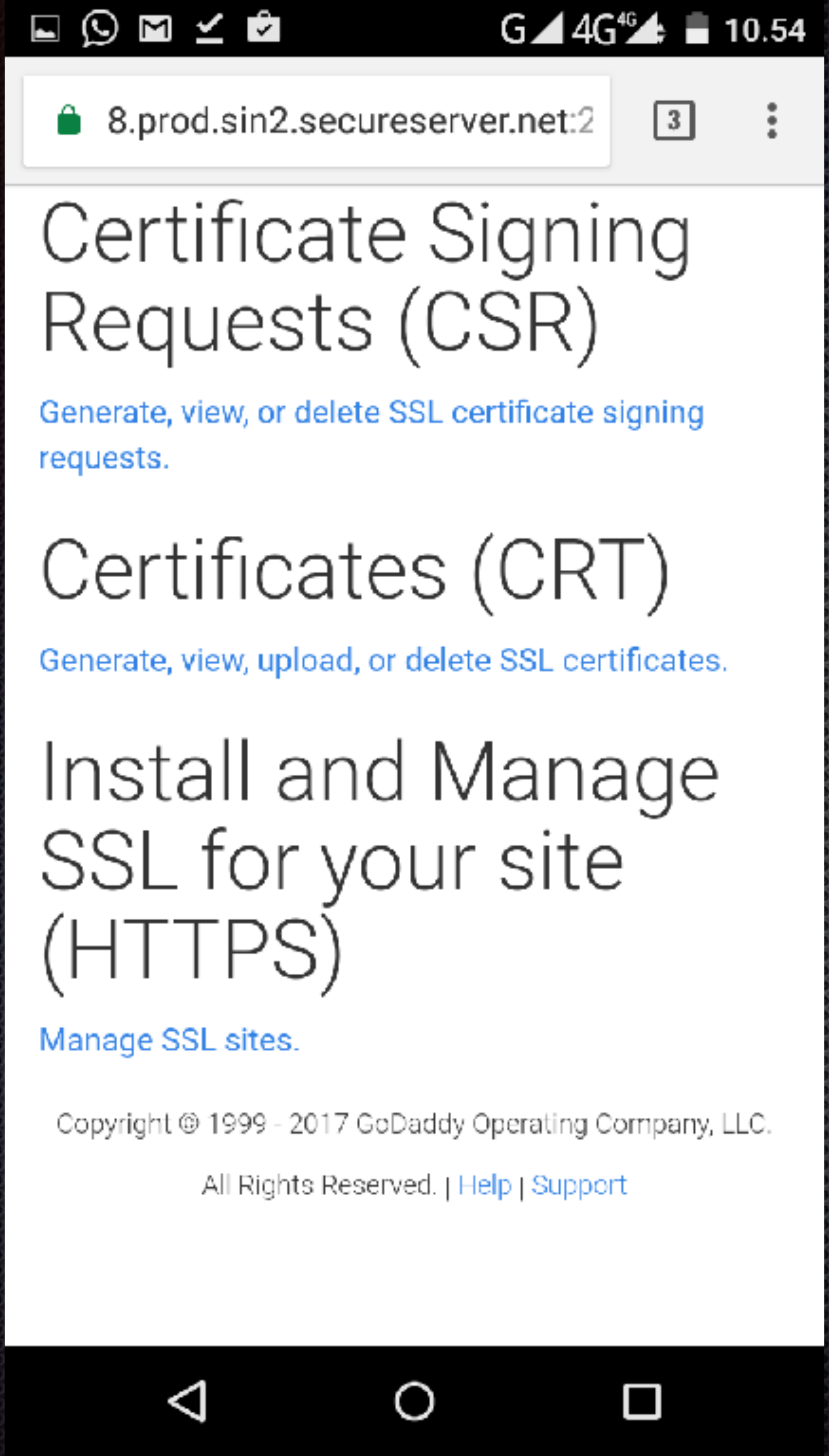


SSL/TLS

The certificate for the domain "shortenage.com" has been saved.

Copyright © 1999 - 2017 GoDaddy Operating Company, LLC.

All Rights Reserved. | Help | Support



Certificate Signing Requests (CSR)

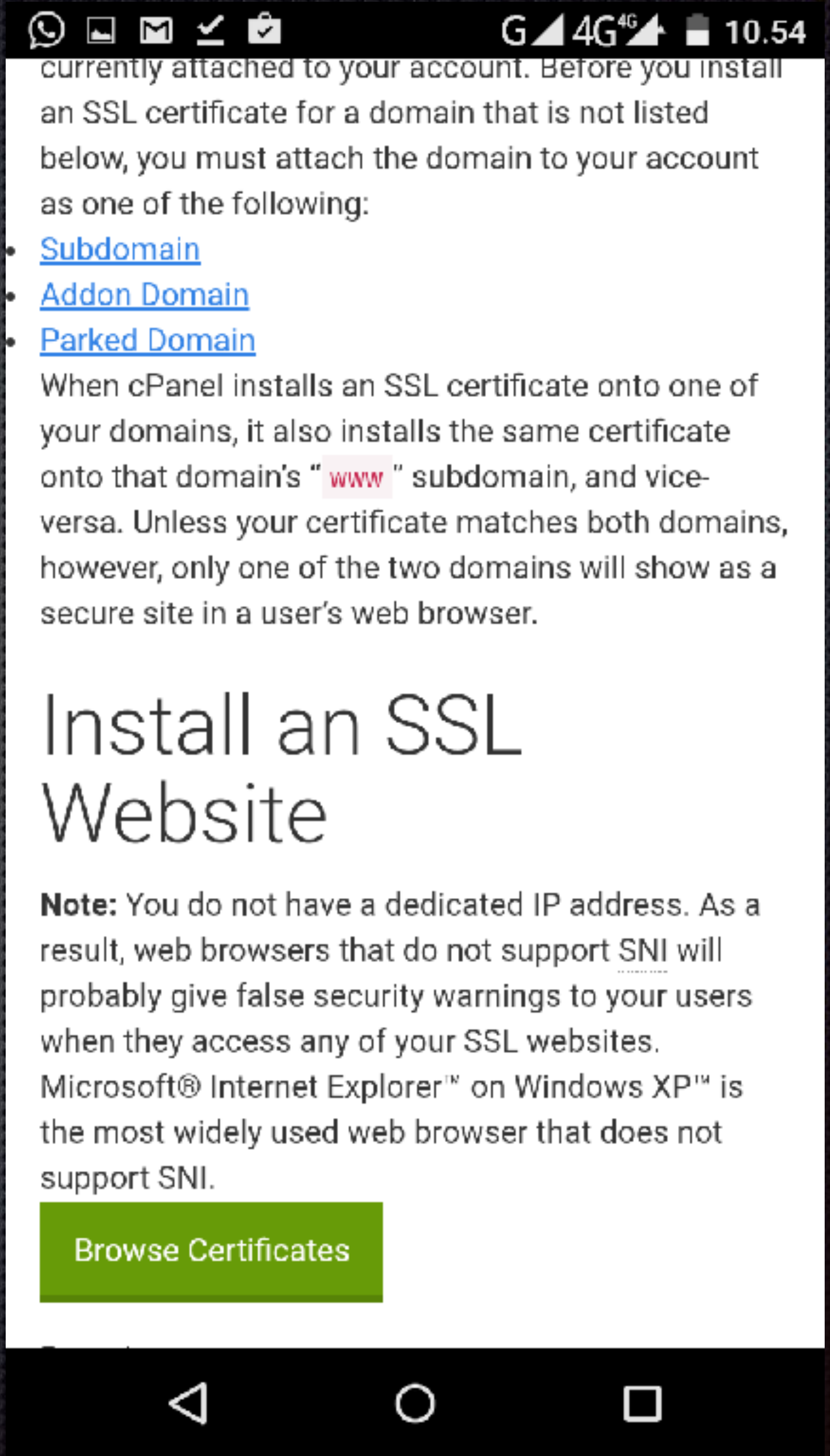
Generate, view, or delete SSL certificate signing requests.

Certificates (CRT)

Generate, view, upload, or delete SSL certificates.

Install and Manage SSL for your site (HTTPS)

Manage SSL sites.



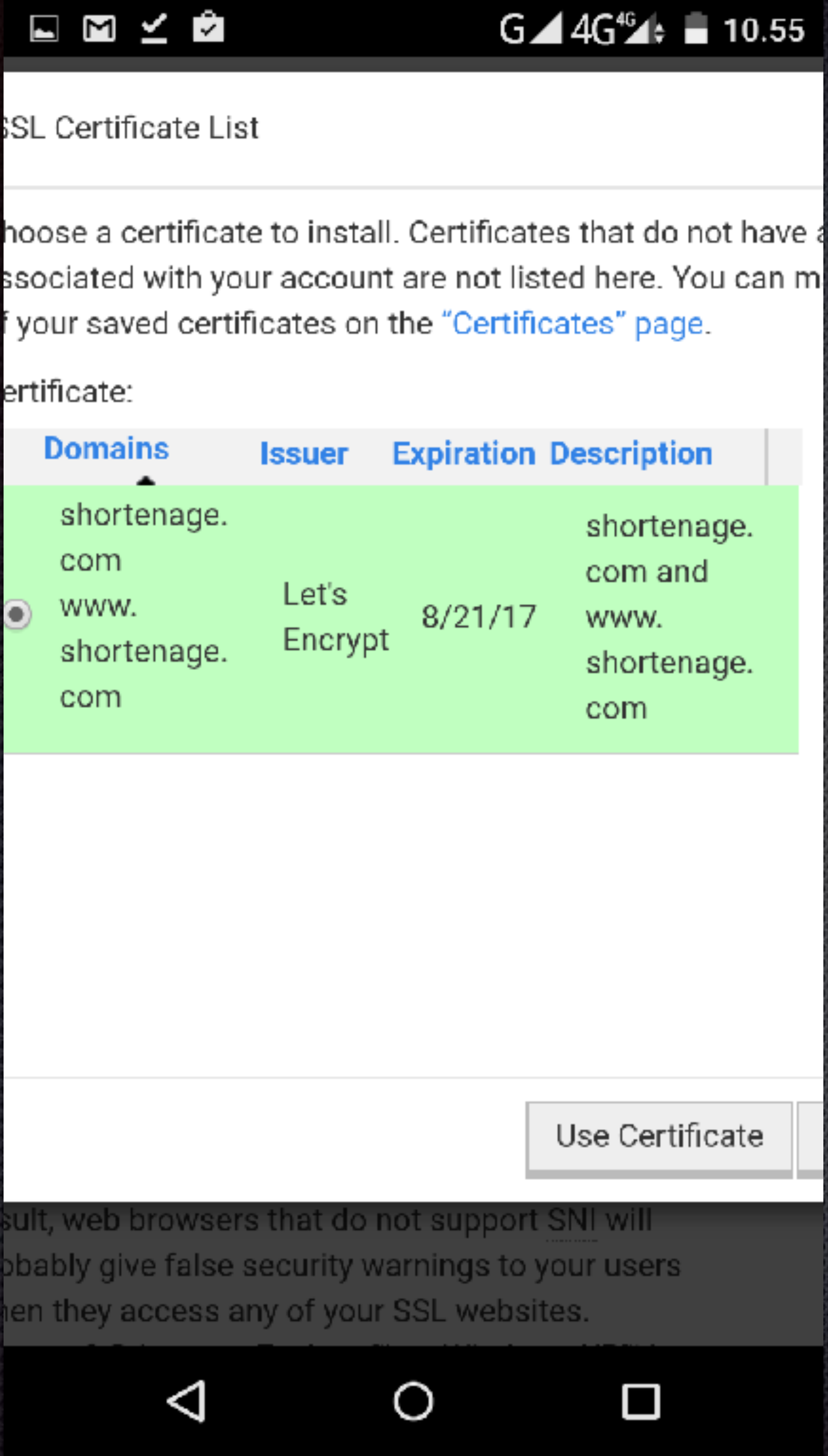
currently attached to your account. Before you install an SSL certificate for a domain that is not listed below, you must attach the domain to your account as one of the following:

- Subdomain
- Addon Domain
- Parked Domain

When cPanel installs an SSL certificate onto one of your domains, it also installs the same certificate onto that domain's "www" subdomain, and vice-versa. Unless your certificate matches both domains, however, only one of the two domains will show as a secure site in a user's web browser.

Install an SSL Website

Note: You do not have a dedicated IP address. As a result, web browsers that do not support SNI will probably give false security warnings to your users when they access any of your SSL websites. Microsoft® Internet Explorer™ on Windows XP™ is the most widely used web browser that does not support SNI.



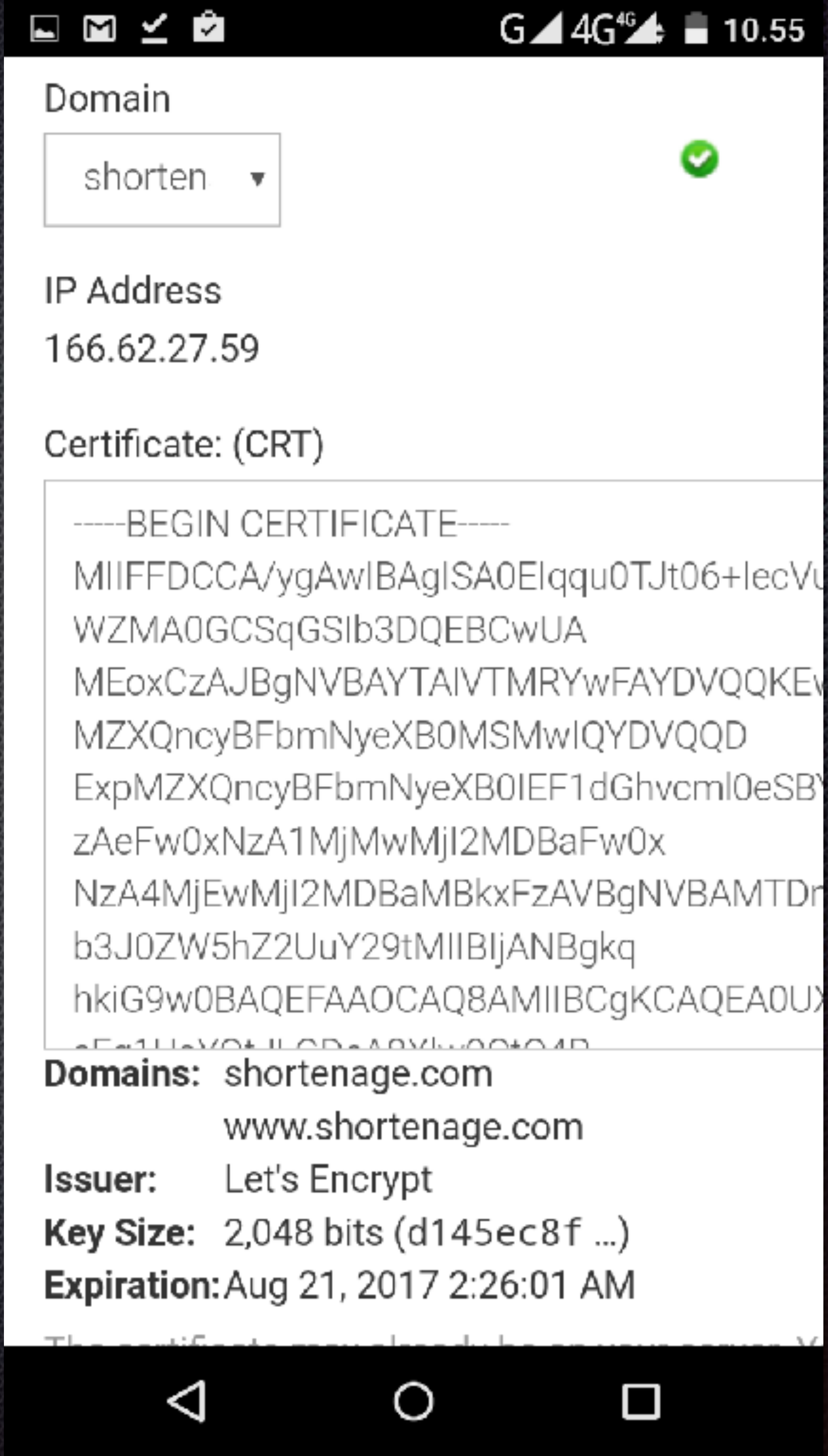
SSL Certificate List

hoose a certificate to install. Certificates that do not have a
ssociated with your account are not listed here. You can m
f your saved certificates on the "Certificates" page.

ertificate:

	Domains	Issuer	Expiration	Description
●	shortenage.com www.shortenage.com	Let's Encrypt	8/21/17	shortenage.com and www.shortenage.com

sult, web browsers that do not support SNI will
obably give false security warnings to your users
en they access any of your SSL websites.



Domain

shorten ▾ ✓

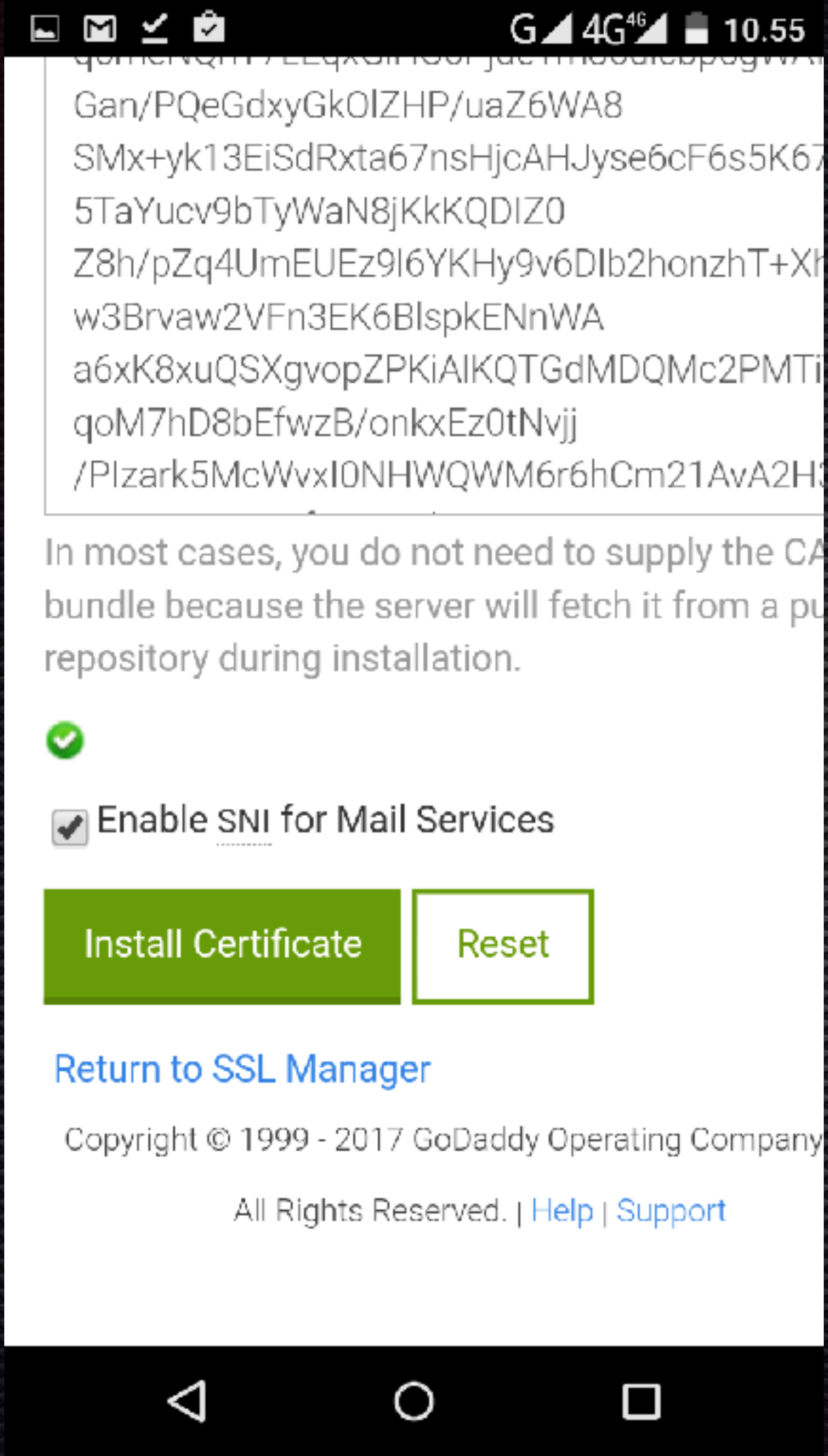
IP Address

166.62.27.59

Certificate: (CRT)

```
-----BEGIN CERTIFICATE-----
MIIFFDCCA/ygAwIBAgISA0Elqqu0TJt06+lecV
WZMA0GCSqGSIb3DQEBCwUA
MEoxCzAJBgNVBAYTAlVTMRYwFAYDVQQKE
MZXQncyBFbmNyeXB0MSMwIQYDVQQD
ExpMZXQncyBFbmNyeXB0IEF1dGhvcml0eSB
zAeFw0xNzA1MjMwMjI2MDBaFw0x
NzA4MjEwMjI2MDBaMBkxFzAVBgNVBAMTD
b3J0ZW5hZ2UuY29tMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0U
```

Domains: shortenage.com
www.shortenage.com
Issuer: Let's Encrypt
Key Size: 2,048 bits (d145ec8f ...)
Expiration: Aug 21, 2017 2:26:01 AM



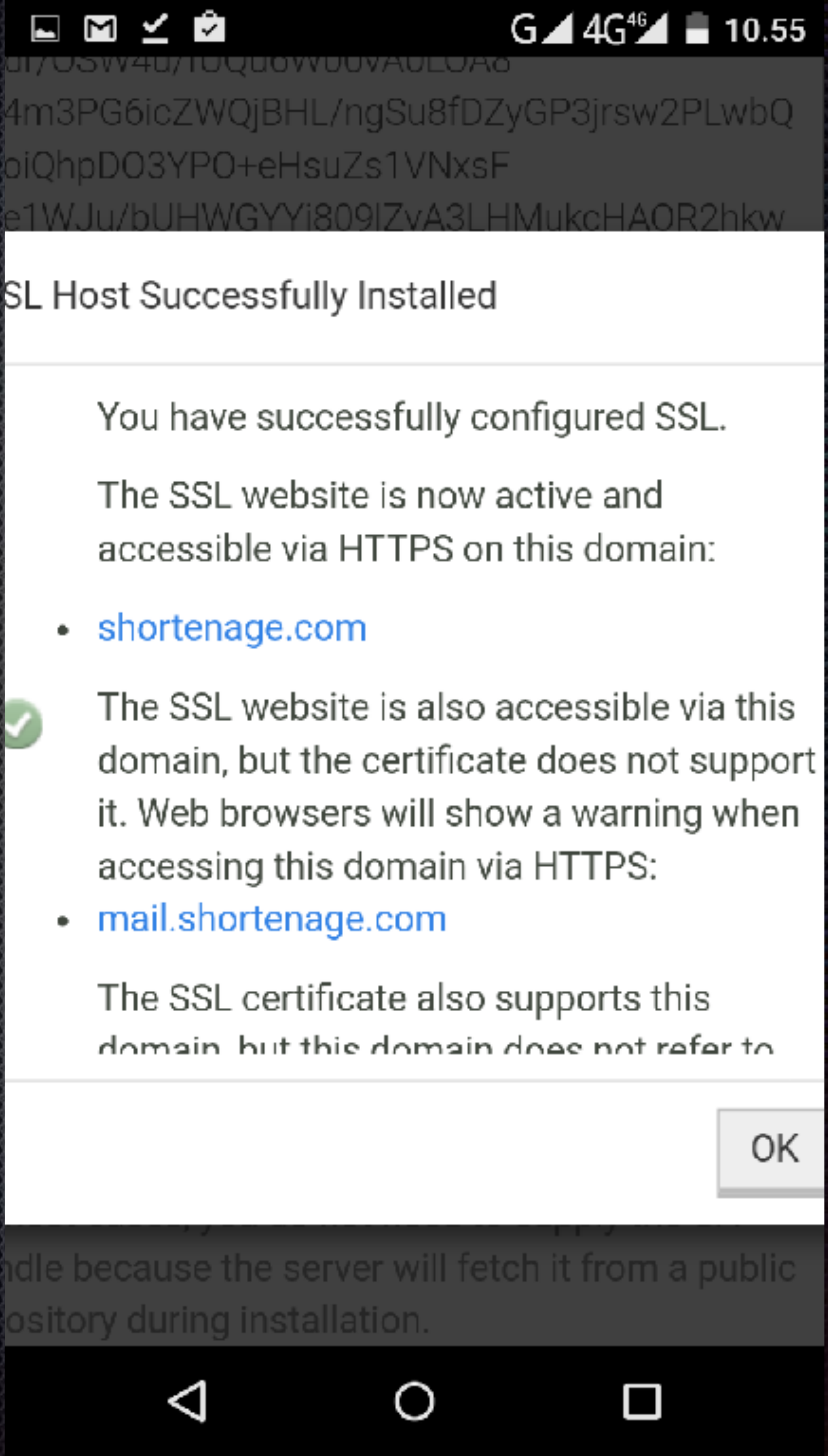
```
Gan/PQeGdxyGkOIZHP/uaZ6WA8
SMx+yk13EiSdRxta67nsHjcAHJyse6cF6s5K67
5TaYucv9bTyWaN8jKkKQDIZ0
Z8h/pZq4UmEUEz9I6YKHy9v6DIb2honzhT+Xh
w3Brvaw2VFn3EK6BIspkENnWA
a6xK8xuQSXgvopZPKiAIKQTGdMDQMc2PMTi
qoM7hD8bEfwzB/onkxEz0tNvjj
/PIzark5McWvxI0NHWQWM6r6hCm21AvA2H
```

In most cases, you do not need to supply the CA
bundle because the server will fetch it from a pu
repository during installation.

✓

☑ Enable SNI for Mail Services

Return to SSL Manager



```
4m3PG6icZWQjBHL/ngSu8fDZyGP3jrsw2PLwbQ
oiQhpDO3YPO+eHsuZs1VNxsF
e1WJu/bUHWGYYi809IZvA3LHMukcHAOR2hkw
```

SL Host Successfully Installed

You have successfully configured SSL.

The SSL website is now active and accessible via HTTPS on this domain:

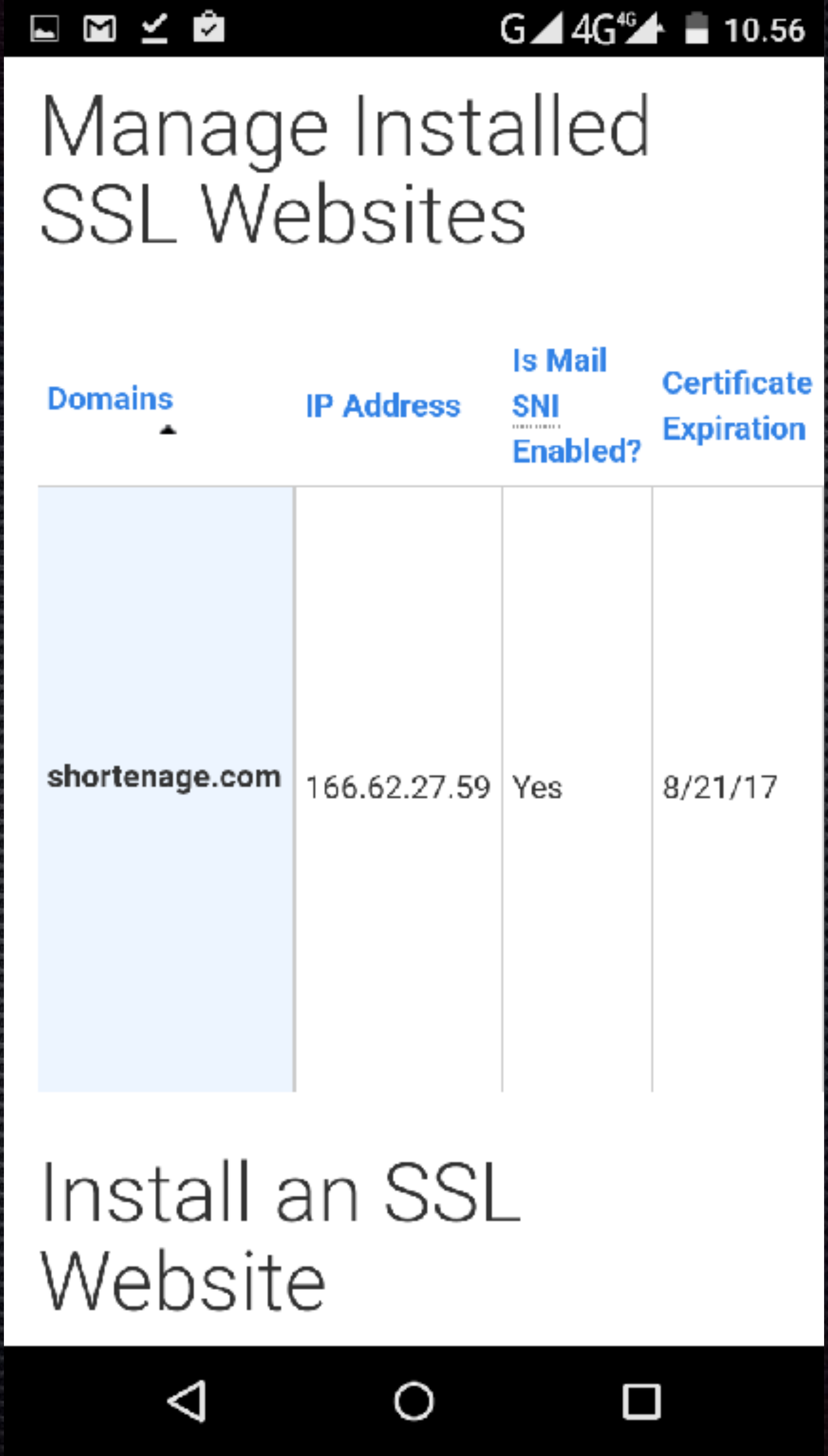
- shortenage.com

✓ The SSL website is also accessible via this domain, but the certificate does not support it. Web browsers will show a warning when accessing this domain via HTTPS:

- mail.shortenage.com

The SSL certificate also supports this domain, but this domain does not refer to

ndle because the server will fetch it from a public
ository during installation.

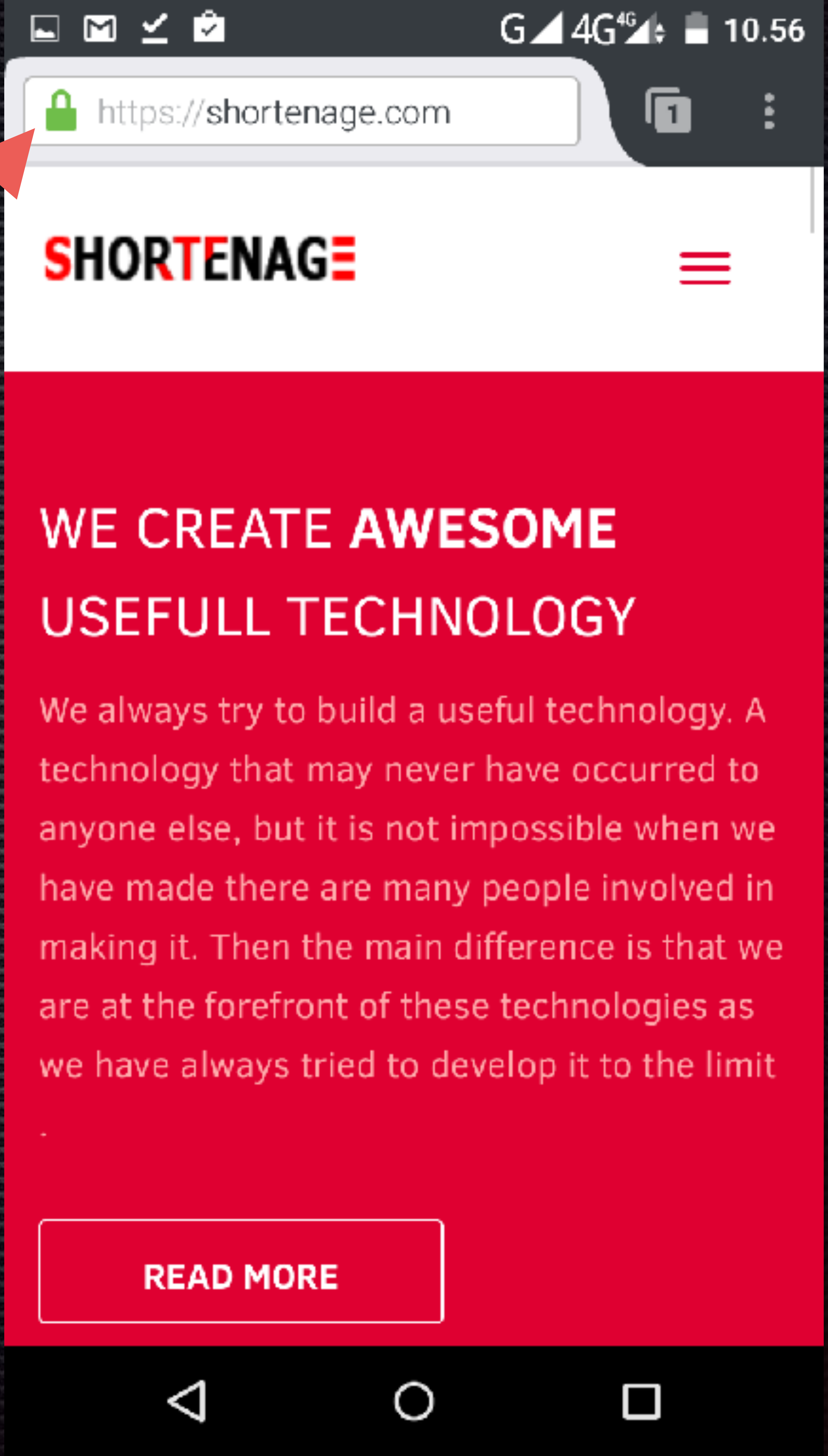


Manage Installed SSL Websites

Domains	IP Address	Is Mail SNI Enabled?	Certificate Expiration
shortenage.com	166.62.27.59	Yes	8/21/17

Install an SSL Website

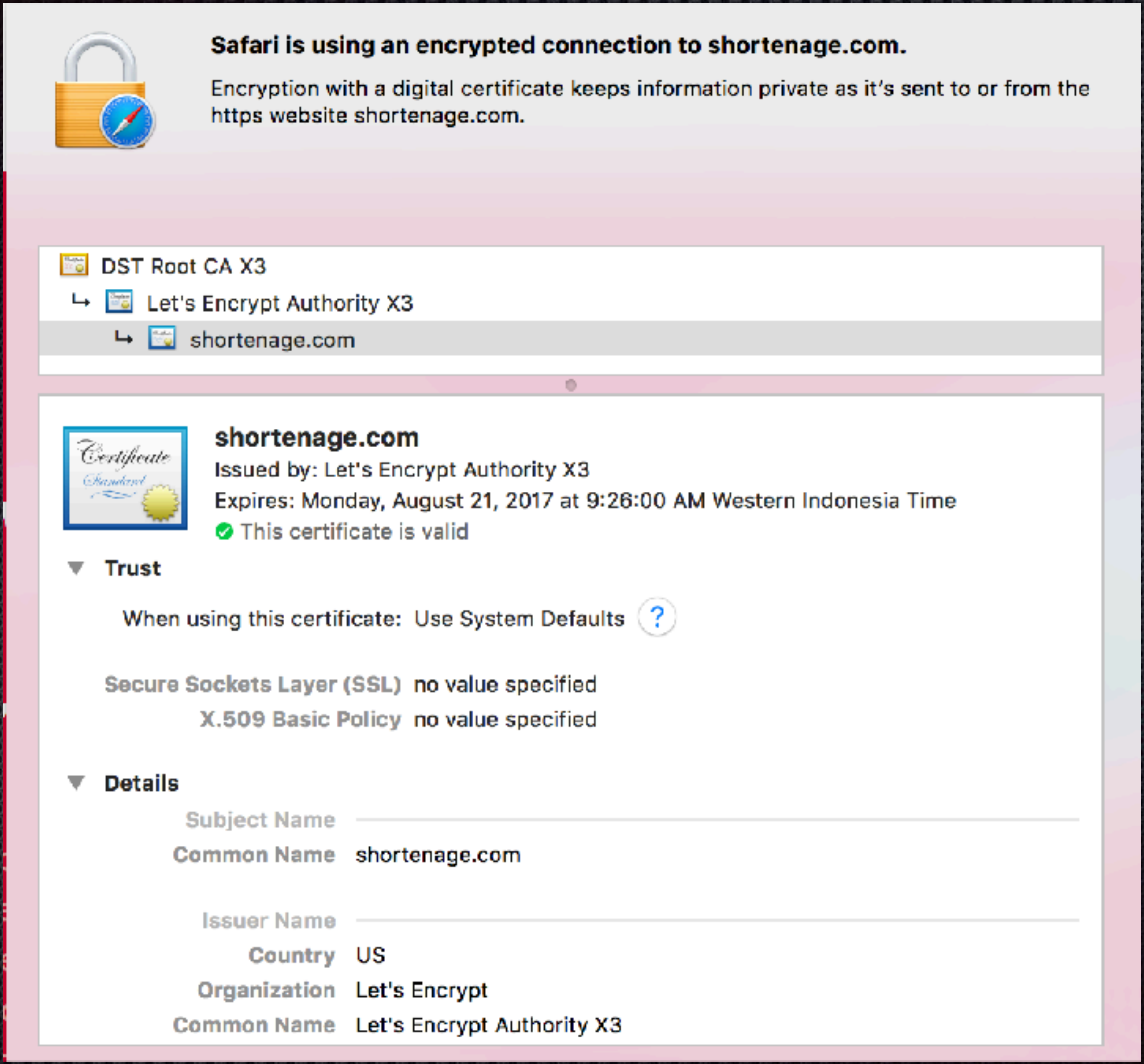
Perhatikan



WE CREATE **AWESOME** USEFULL TECHNOLOGY

We always try to build a useful technology. A technology that may never have occurred to anyone else, but it is not impossible when we have made there are many people involved in making it. Then the main difference is that we are at the forefront of these technologies as we have always tried to develop it to the limit

.



Safari is using an encrypted connection to shortenage.com.

Encryption with a digital certificate keeps information private as it's sent to or from the https website shortenage.com.

DST Root CA X3
↳ Let's Encrypt Authority X3
↳ shortenage.com

shortenage.com
Issued by: Let's Encrypt Authority X3
Expires: Monday, August 21, 2017 at 9:26:00 AM Western Indonesia Time
✓ This certificate is valid

▼ **Trust**

When using this certificate: Use System Defaults ?

Secure Sockets Layer (SSL) no value specified
X.509 Basic Policy no value specified

▼ **Details**

Subject Name
Common Name shortenage.com

Issuer Name
Country US
Organization Let's Encrypt
Common Name Let's Encrypt Authority X3

“Semoga bermanfaat”

Azis Kurniawan