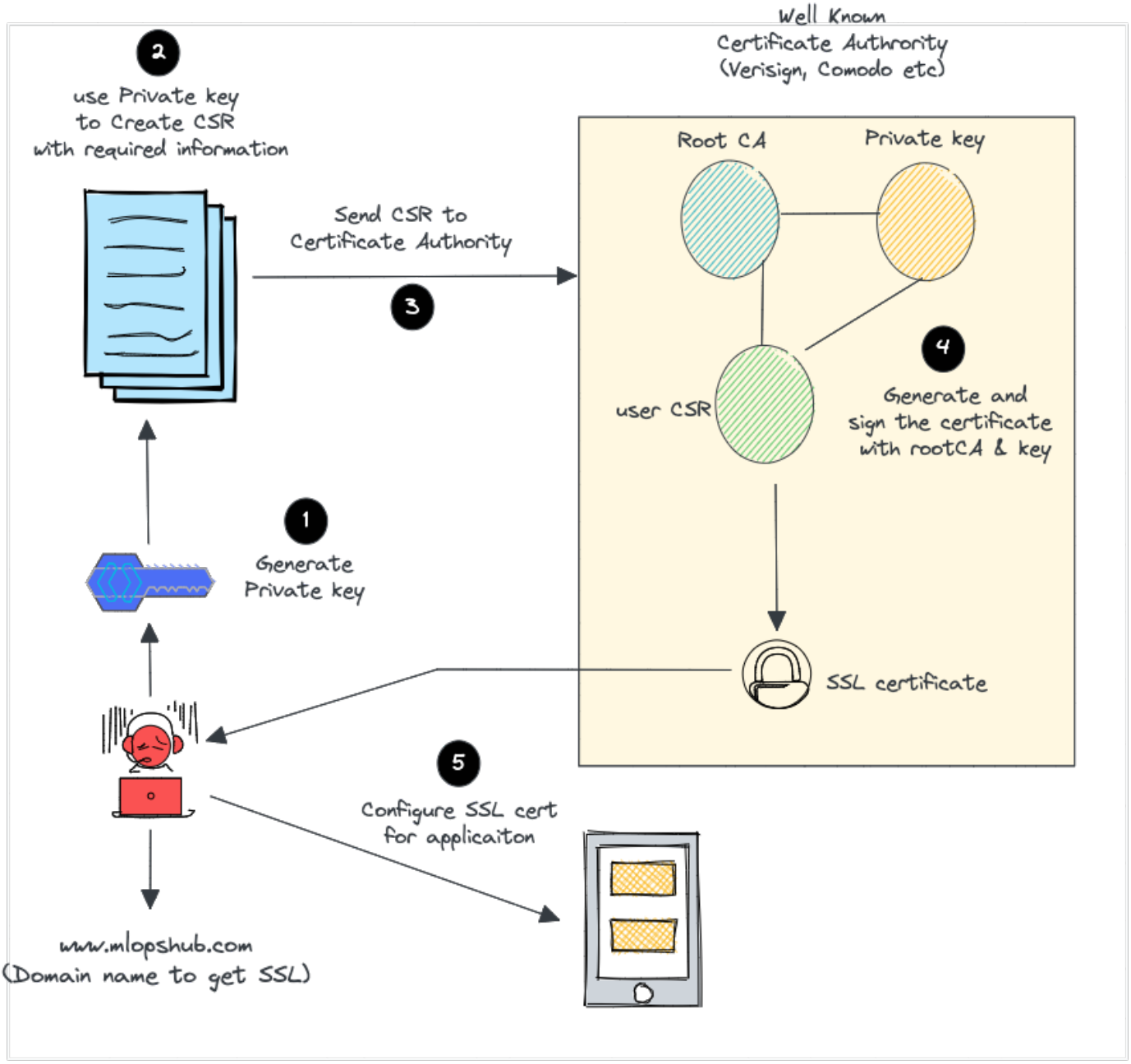
SSL Certificate 101

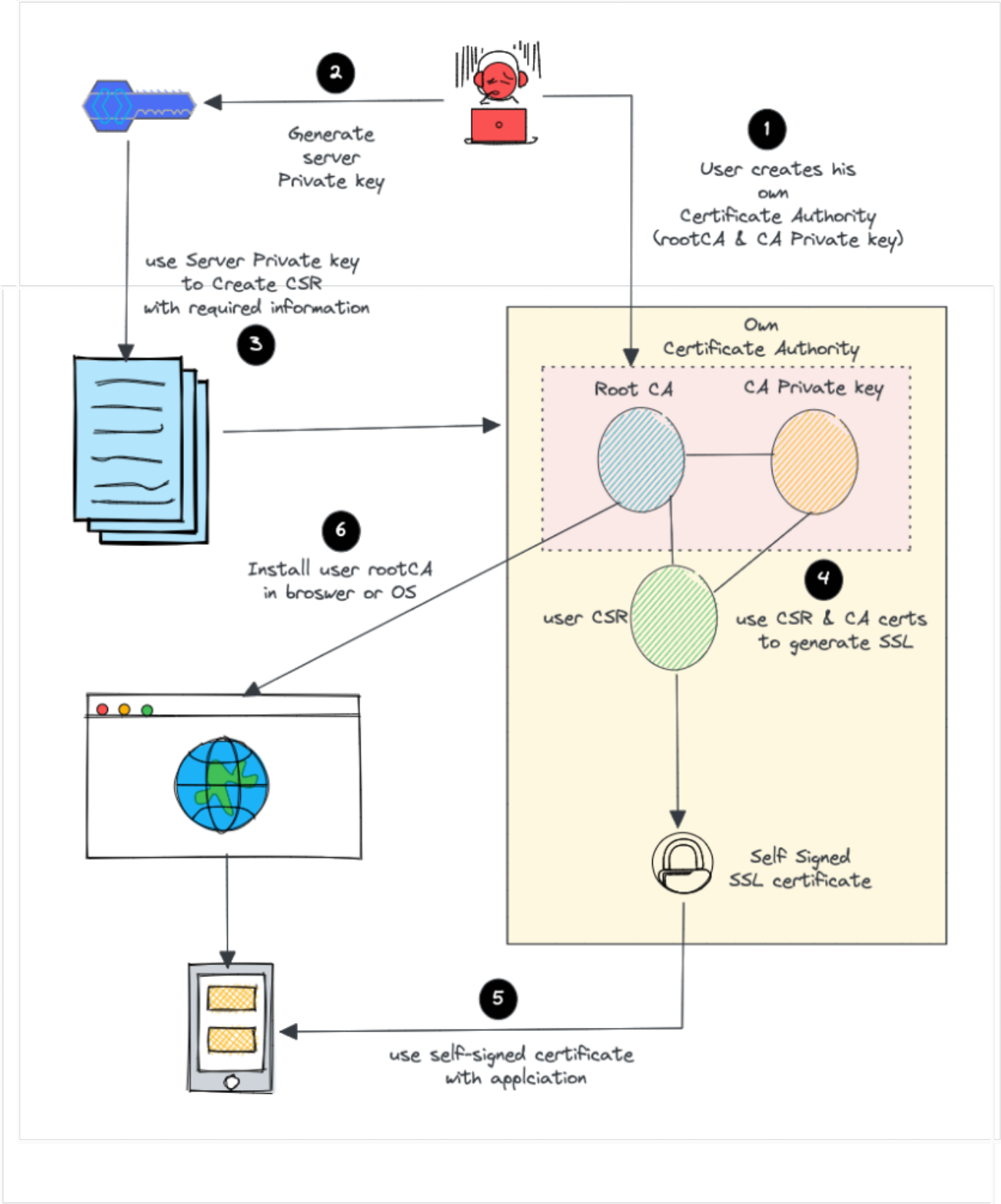
How to generate a self-signed certificate

If you wish to generate a certificate from an actual Certificate Authority then the flow is done like such:



I will only be explaining how to generate a self-signing certificate because the process is essentially the same, except that you abstract out the CA as a thirty party that will handle the request for you automatically.

To create create a self-signed certificate (a certificate that's signed by a CA that YOU own) this is the steps:



1. Create your own root CA certificate and root CA private key

To get started with creating self-signed certificate you will need to first create your root CA private key and root CA certificate.

Running the following command will generate a private key and name the file as `server.key` to indicate that this is the private key for the server.

```
openssl genrsa -out root.key
```

To generate the root CA certificate run the following command:

```
openssl req -x509 -days 365 -key root.key -out root.cer
```

This will generate a root certificate with the server private key that's valid for 365 days. You can validate this certificate by running and you can see the expiration date of this certificate.

```
openssl x509 -in root.cer -text
```

> Note that you must provide a common name field in order to validate the certificate trust chain.

2. Create your server private key and certificate signing request

Go ahead and generate your server's private key with the following command.

```
openssl genrsa -out server.key
```

Now then you will need to create a certificate signing request with your server's private key.

```
openssl req -new -key server.key -out server.csr
```

> When prompted to enter in a common name field you will also need to enter it in otherwise, you cannot validate the certificate trust chain.

3. Use CSR to create server certificate

The following command will use the certificate signing request (who to sign the certificate for) and the root server's certificate information and the private key to create a server certificate signed by the root CA hosted by ourselves.

```
openssl x509 -req -in server.csr -CA root.cer -CAkey root.key -CAcreateserial -out server.crt
-days 365
```

4. Validate certificate chain

Finally, to validate that the output server certificate is indeed created and signed by the root server we can run the following command:

```
openssl verify -CAfile root.cer server.crt
```

If everything is good, then you should see the output `server.crt: OK`

What is Self-Signed Certificate

All root CA certificates are self-signed in the sense that the root CA certificate is created using the certificate's own private key. Nothing special about them besides that the organization owns them are a trusted entity by the general public and have good reputation in owning and issuing out certificates.

You can also generate your own self-signed certificate.

What is PEM files

https://origin-blog.mediatemple.net/work-life/ssl-certificate-101-everything-you-need-to-know/

- What is PEM files
- What is X.509 file types
- How the hell does certificate work

Revision #3
Created 2023-11-08 01:24:57 UTC by Tamarine
Updated 2024-04-13 01:21:00 UTC by Tamarine