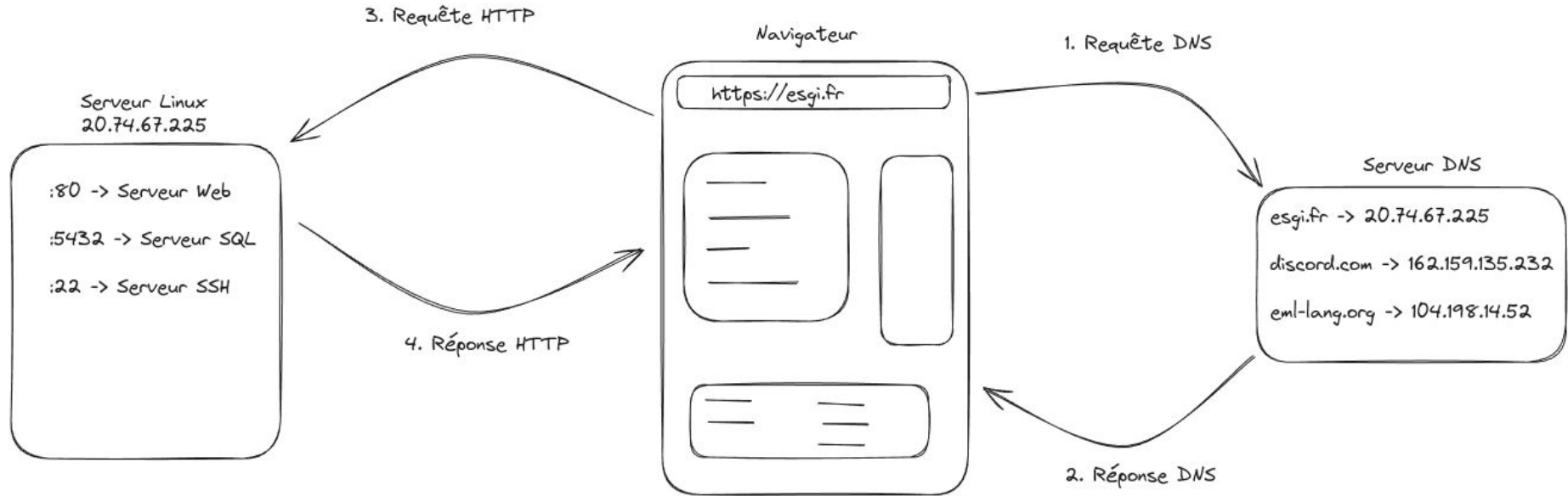


Protocoles d'Authentification

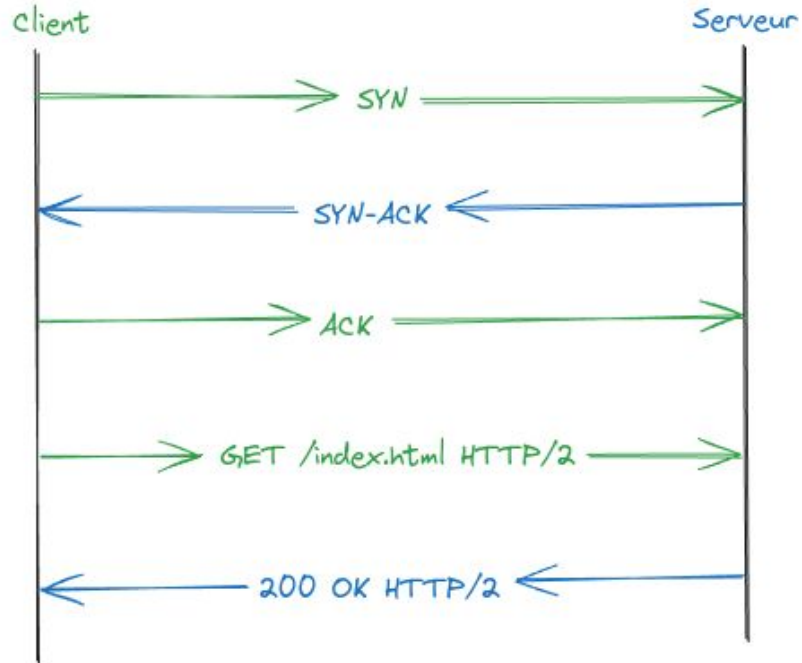
Amin NAIRI <anairi@esgi.fr>

<https://slash.nairi.cloud/s/positionnement-4iw1>

Séance 1 : Introduction aux protocoles d'authentification



Séance 1 : Introduction aux protocoles d'authentification



Requête	Réponse
<pre>POST /users HTTP/2 Host: esgi.fr Content-Type: application/json Content-Length: 1234 { "email": "user@domain.com", "password": "s3cr3t" }</pre>	<pre>200 OK HTTP/2 Content-Type: application/json Content-Length: 1234 { "userId": "a1b2c3d4" }</pre>

Séance 1 : Introduction aux protocoles d'authentification

Time-based One-Time Password (TOTP)

Initialisation

Utilisation

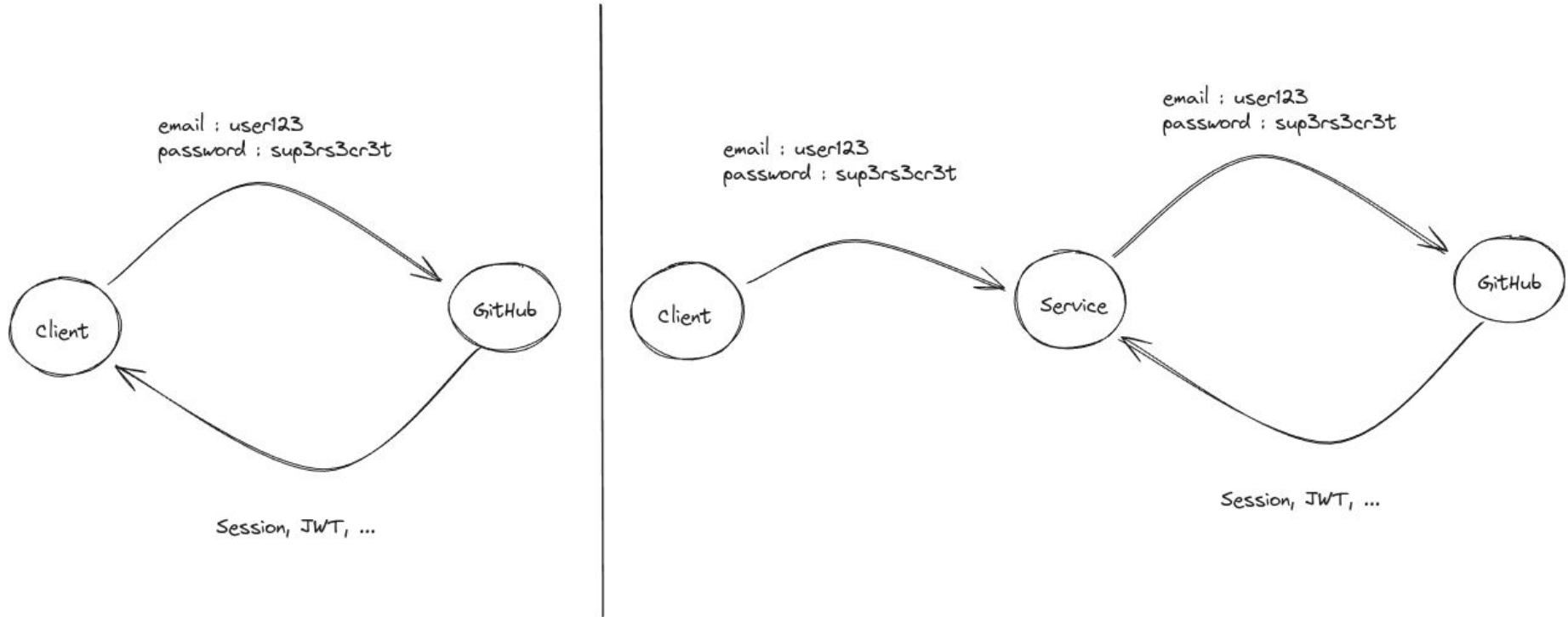
Algorithme

1. Création d'une chaîne de caractères aléatoire côté serveur
2. Partage via un QRCode
3. Enregistrement de la chaîne de caractères dans une application supportée
Ex: Google Authenticator

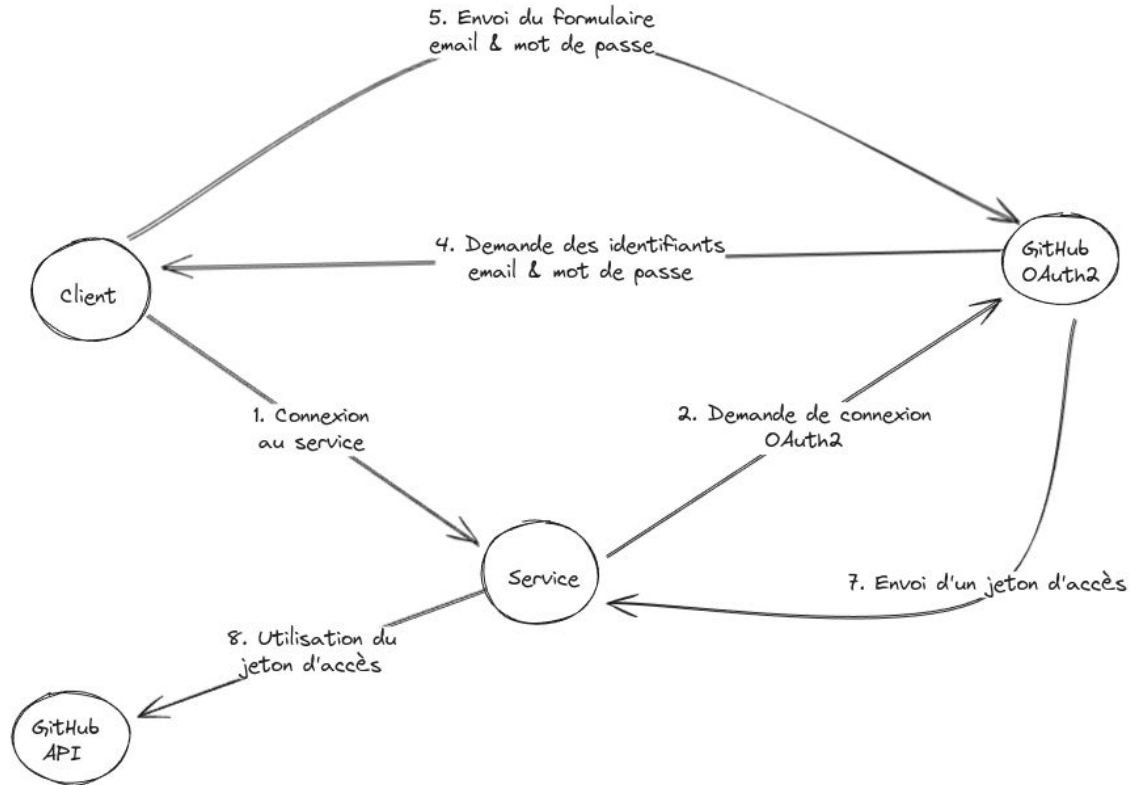
1. Inscription via email et mot de passe
2. Vérification des informations
3. Demande d'entrée du TOTP
4. Vérification côté serveur
5. Autorisation

1. Récupération de la chaîne de caractères aléatoire
2. Récupération du nombre de secondes UNIX
3. Division par un intervalle (ex: 30 secondes)
4. Réunion des deux dans un appel de fonction (HMAC-SHA256)
5. Troncation aux 6 premiers nombres

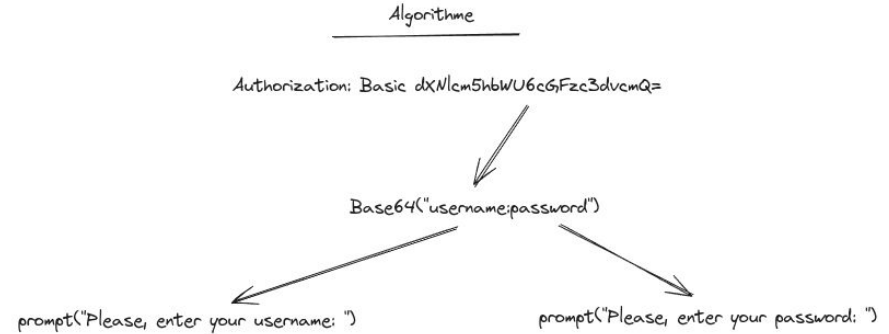
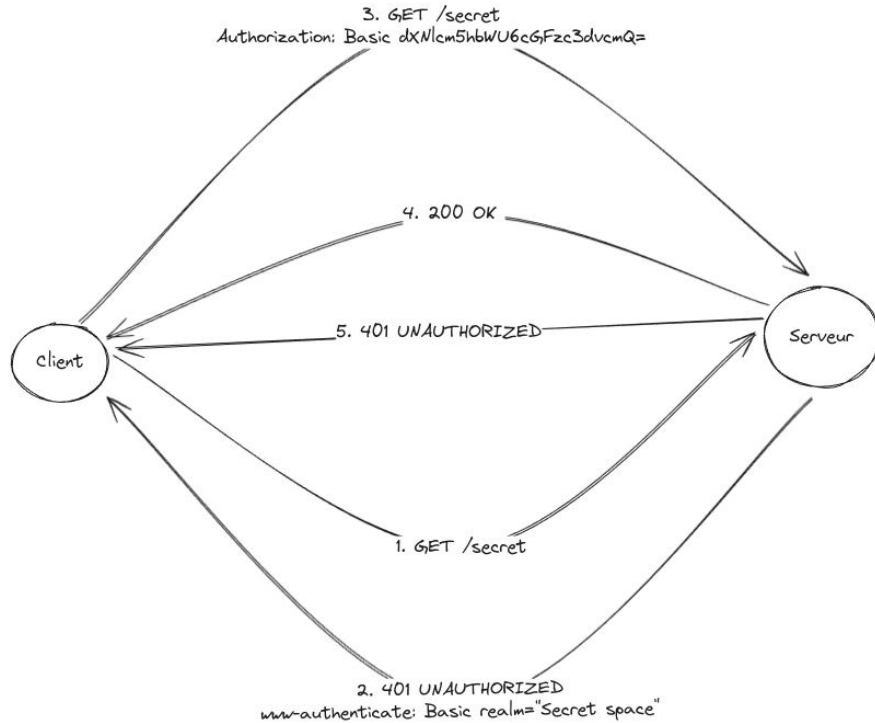
Séance 1 : Introduction aux protocoles d'authentification



Séance 1 : Introduction aux protocoles d'authentification



Séance 1 : Introduction aux protocoles d'authentification



Séance 1 : Exercice

- Implémenter une authentification basique
- Utiliser Node.js pour le côté serveur
- Utiliser la librairie http
- Utiliser l'objet Buffer pour l'encodage
- Ne pas utiliser de HTML

Séance 2 : Cookies & Sessions

Requête	Réponse
<pre>GET /profile HTTP/2 Host: esgi.fr Cookie: PHPSESSID=9872947; theme=dark</pre>	<pre>200 OK HTTP/2 Content-Type: text/html Content-Length: 1234 </DOCTYPE html> <html> ...</pre>

Séance 2 : Cookies & Sessions

Requête

```
POST /login HTTP/2
Host: www.example.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 43

email=user@domain.com&password=pass
```

Réponse

```
HTTP/2 200 OK
Set-Cookie: PHPSESSID=abcdef1234567890; Expires=987192837
Content-Type: text/html

</DOCTYPE html>
<html>
...
```