Eleven Labs

SAPIENT BUNDLE

Enhance API confidentiality

Eleven Labs

WHO AM I?

Thierry Thuon

Developer @ Eleven-Labs

github.com/lepiaf

Eleven Labs

API EVERYWHERE

Threat on Internet

- Phishing
- DNS/ARP Cache poisoning
- Trust / compromised CA / intermediate
- Hacker / Government

Countermeasure

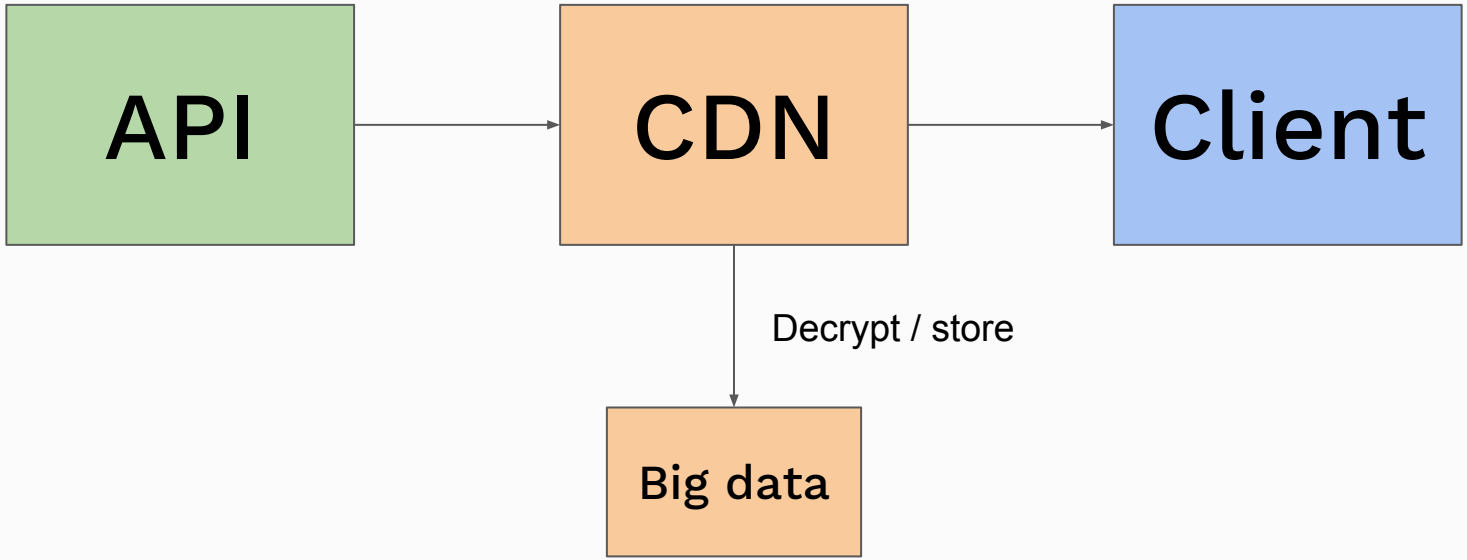
- DNSSEC
- HTTPS / VPN
- Public-key pinning
- Bunker underground fully isolated in Sweden

Eleven Labs

Focus on trust threat

Eleven Labs

Do you trust CDN?



Eleven Labs

Use case to level up trust

- Public API with signed content
- Public API via CDN
- Private API through untrusted network

Eleven Labs

Sapient bundle

Eleven Labs

Let’s talk about the bundle

- Based on sapient library
- Which is based on libsodium
- Which is audited and in PHP core
- Which bring modern cryptography

Eleven Labs

Let’s talk about the bundle

- It ease integration of sapient library in Symfony
- Add a new layer of confidentiality and integrity

Eleven Labs

Show me how easy it is

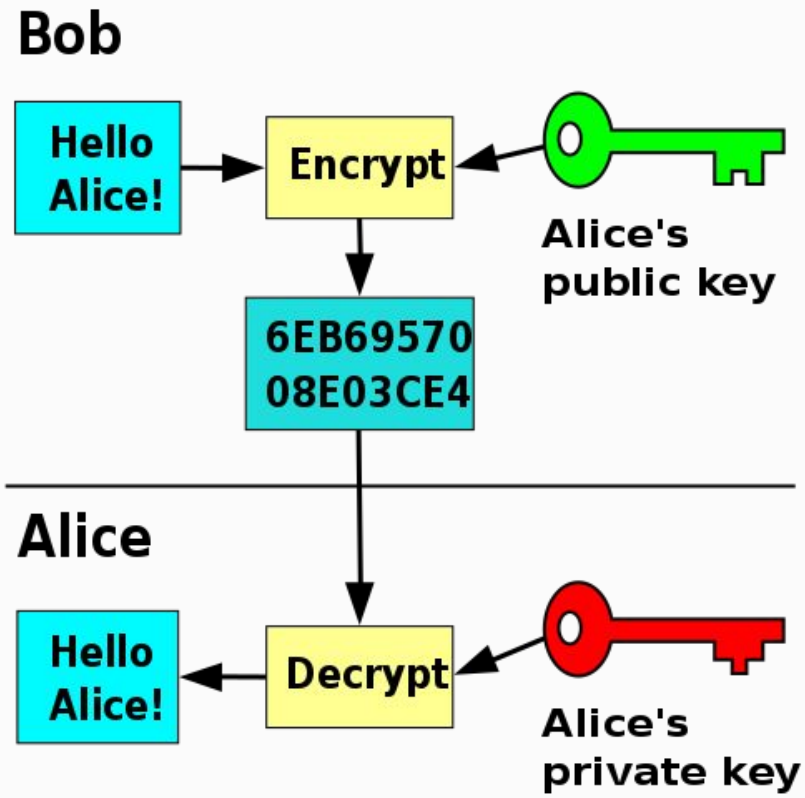
- Assuming PHP 7.2 and Symfony 4

```
composer config extra.symfony.allow-contrib true
```

```
composer install lepiaf/sapient-bundle
```

Eleven Labs

Creation of asymmetric keys

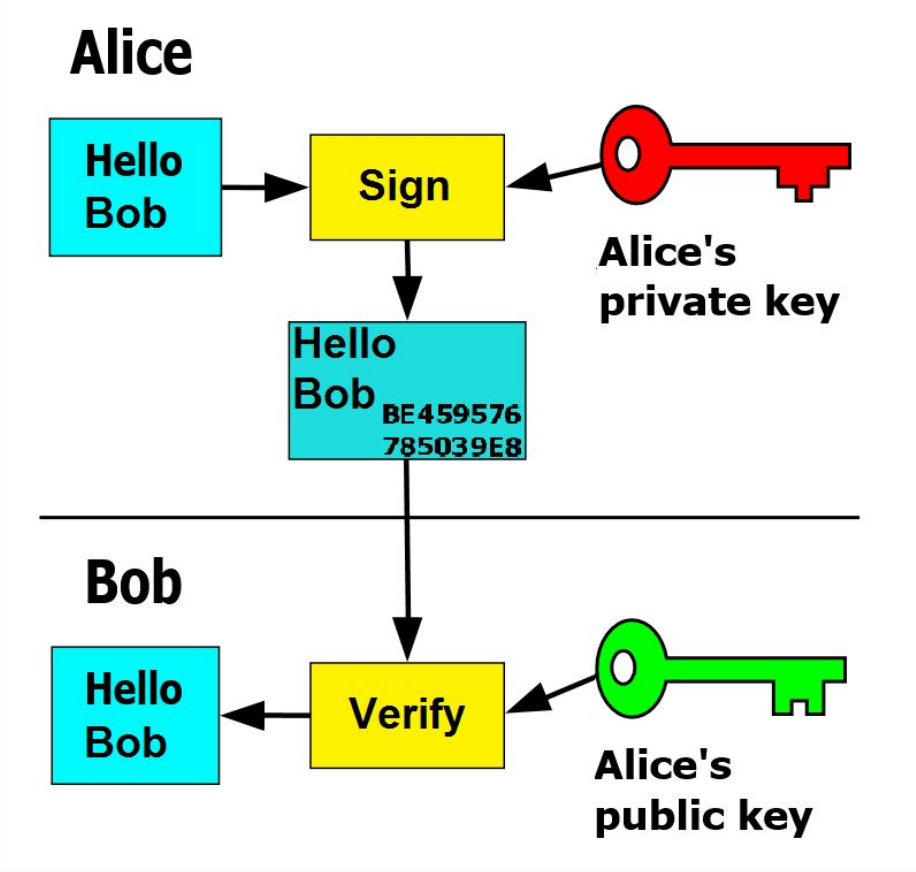



```
bin/console sapient:configure
```

```
sapient:
    sign:
        public: 'G3zo5Zub2o...'
        private: 'giP81DlS_R3JL...'
        host: 'api-alice'
        response: true
    seal:
        public: 'tquhje8C_hNdd85...'
        private: 'NoxnlCvhxl8...'
        response: true
    sealing_public_keys: ~
    verifying_public_keys: ~
```

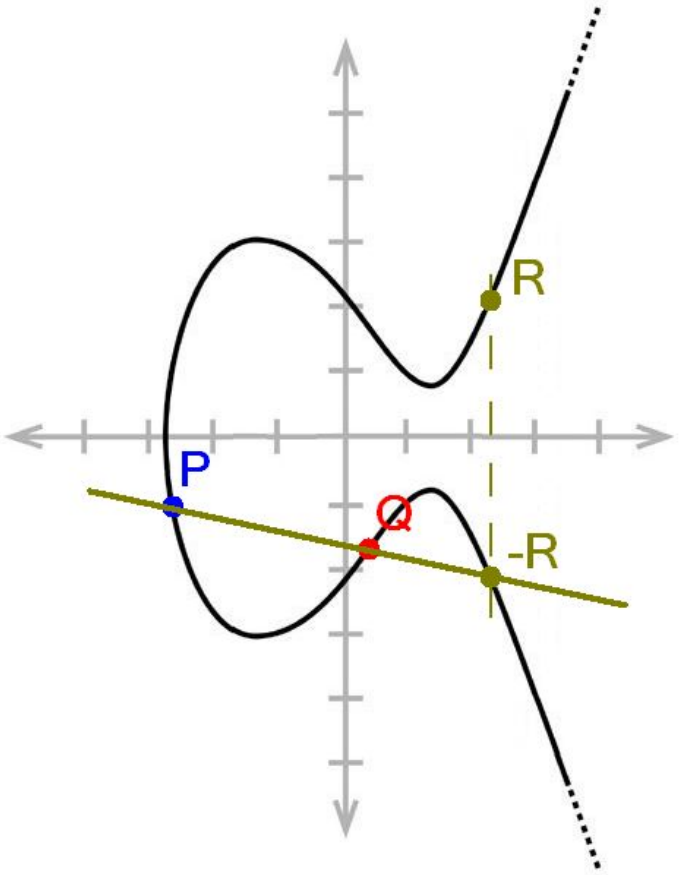
Eleven Labs

Signing message



Eleven Labs

Elliptic curve



Curve25519

- X25519
- Ed25519

$y^2 = x^3 + 486662x^2$

Eleven Labs

Demo time !

Eleven Labs

Sign all response

- Enable configuration
- All done automatically in Symfony

Eleven Labs

Encrypt response

- Enable a configuration

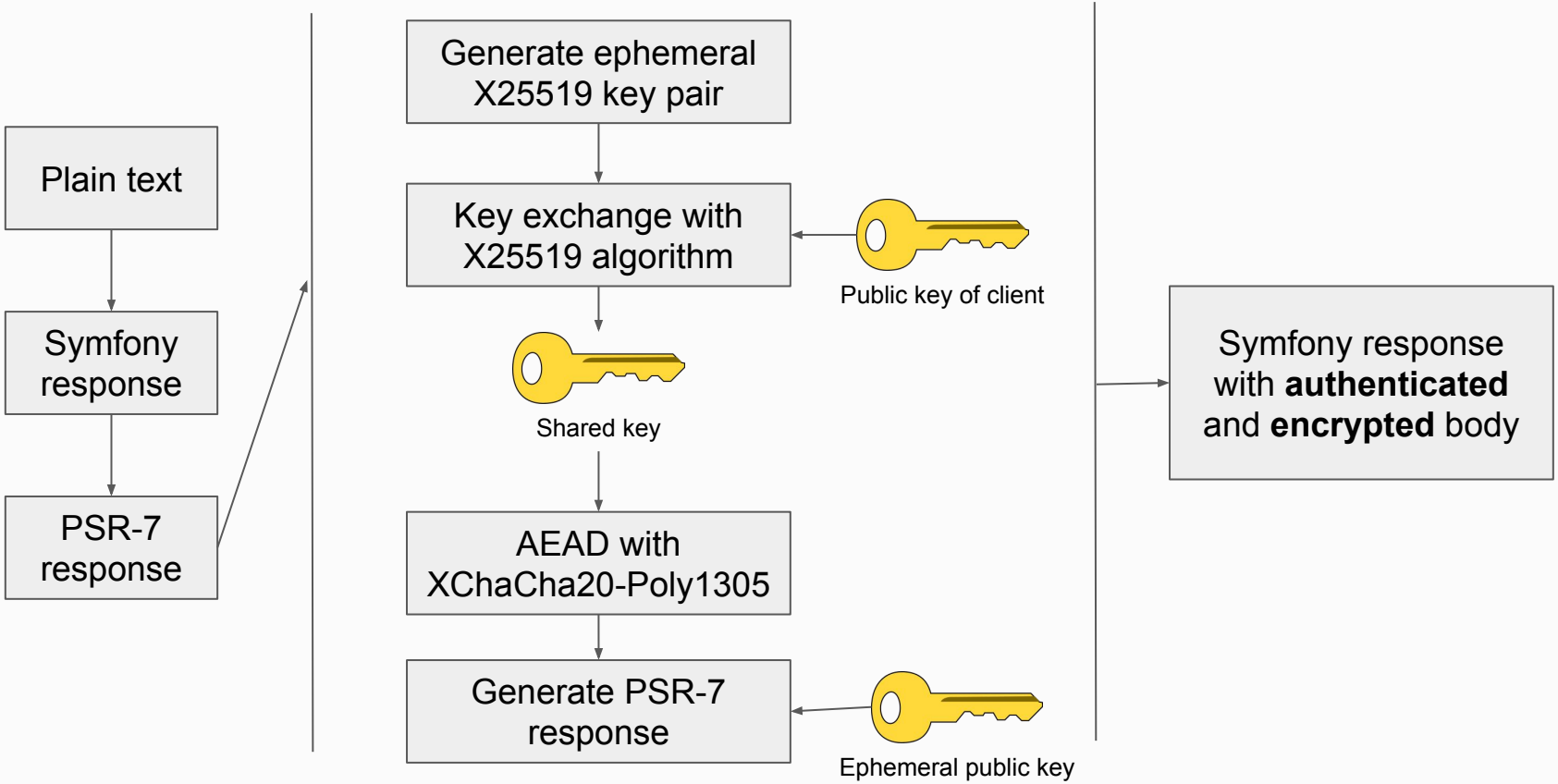
Eleven Labs

Encrypt request

- Visit documentation
  - http://sapient-bundle.readthedocs.io/
- Visit blog post
  - https://blog.eleven-labs.com/fr/renforcer-confidentialite-api-sapient-bundle/

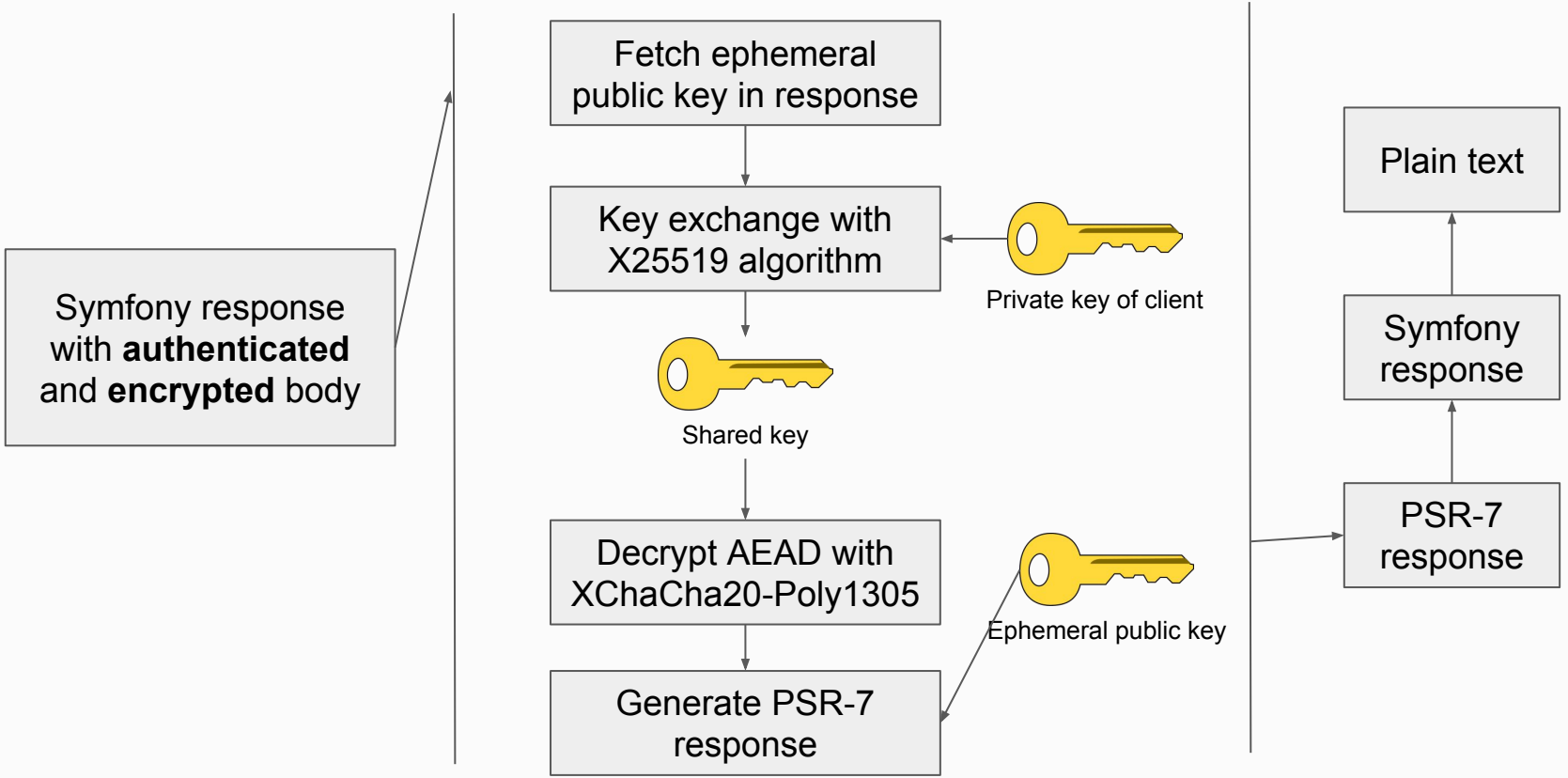
Eleven Labs

Under the hood



Eleven Labs

Under the hood



Eleven Labs

Conclusion

- Niche problematic
- Security low priority
- Elegant and modern solution exist
- libsodium can do more

Eleven Labs

Eleven Labs

Resources

- http://wiki.cacert.org/Risk/History#C0m0d0
- https://security.googleblog.com/2013/12/further-improving-digital-certificate.html
- https://www.theregister.co.uk/2018/03/01/trustico_digicert_symantec_spat/
- https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/
- https://safecurves.cr.yp.to/
- https://commons.wikimedia.org/wiki/File:Adding_P,Q.PNG
- http://www.bortzmeyer.org/7539.html
- https://blog.eleven-labs.com/fr/renforcer-confidentialite-api-sapient-bundle/