海联金汇 HYUNION HOLDINGS
股票代码：002537

UMF 联动优势 UNION MOBILE FINANCIAL TECHNOLOGY
海联金汇旗下企业

科技赋能普惠金融

自我主权的数字身份（SSI）到底有什么

王宇

MAKE FINTECH EVERYWHERE

目录

从网络传输安全开始

TLS

Transport Layer Security (TLS)

TLS handshake

客户端

服务端

$g^x \ \% \ n = A$

$B = g^y \ \% \ n$

$$
\begin{aligned}
Key &= (g^x \ \% \ n)^y \ \% \ n \\
&= (g^x)^y \ \% \ n \\
&= (g^y)^x \ \% \ n \\
&= B^x \ \% \ n
\end{aligned}
$$

$$
\begin{aligned}
Key &= (g^x \ \% \ n)^y \ \% \ n \\
&= (g^x)^y \ \% \ n \\
&= A^y \ \% \ n
\end{aligned}
$$

$(g^x)^y \ != \ g^x g^y$

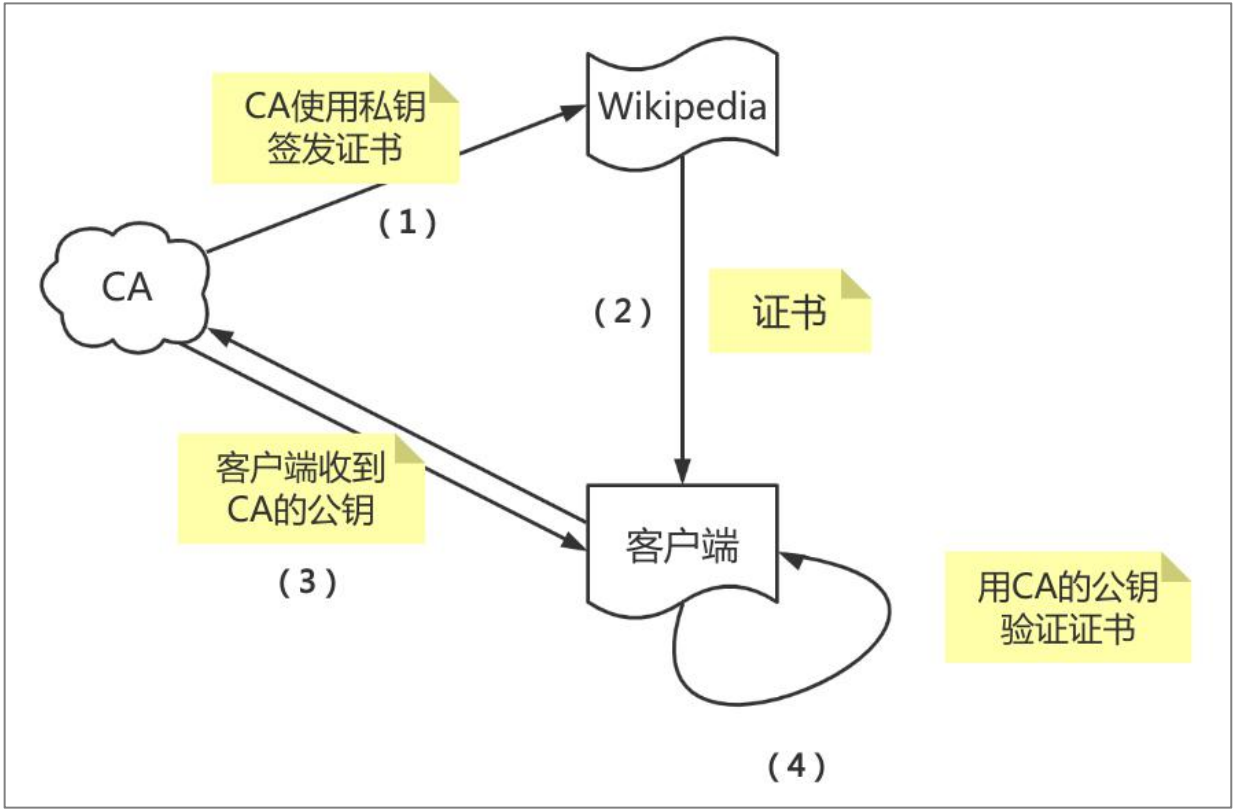
TLS

TLS 保证了通信双方一旦建立连接，通信将是安全的

CA

Certificate authority (CA)

The process of CA



CA 是可信任的第三方；

CA 签发的证书叫

Public key cerificate

(digital cerificate)

CA

CA 确认了通信方的身份

HTTPS

HTTPS

(HTTP over TLS)

问题

可以利用 CA，达到在建立连接的时候网站就知道用户身份的效果吗？

目录

关于某类 VPN

Shadowsocks

Shadowsocks is a secure split proxy loosely based on SOCKS5.

```
client <---> ss-local <--[encrypted]--> ss-remote <---> target
```

```
SS-URI = "ss://" userinfo "@" hostname ":" port ["/"] ["?"plugin] ["#" tag]
userinfo = websafe-base64-encode-utf8(method ":" password)
```

The last / should be appended if plugin is present, but is optional if only tag is present. For example:

```
ss://YmYtY2ZiOnRlc3Q@192.168.100.1:8888/
    ?plugin=url-encoded-plugin-argument-value
    &unsupported-arguments=should-be-ignored
    #Dummy+profile+name.
```

V2Ray

- 多协议支持: V2Ray 可同时开启多个协议支持，包括 Socks、HTTP、Shadowsocks、VMess 等。每个协议可单独设置传输载体，比如 TCP、mKCP、WebSocket 等。

VMess

动态端口指令

1 字节	2 字节	16 字节	2 字节	1 字节	1 字节
保留	端口 Port	用户 ID	AlterID	用户等级	有效时间 T

Trojan

When a trojan client connects to a server, it first performs a **real** `TLS` handshake. If the handshake succeeds, all subsequent traffic will be protected by `TLS`; otherwise, the server will close the connection immediately as any `HTTPS` server would. (Trojan now also supports nginx-like response to plain HTTP requests.) Then the client sends the following structure:

```
+-----------------------+---------+----------------+---------+----------+
| hex(SHA224(password)) |  CRLF   | Trojan Request |  CRLF   | Payload  |
+-----------------------+---------+----------------+---------+----------+
|          56           | X'0D0A' |    Variable    | X'0D0A' | Variable |
+-----------------------+---------+----------------+---------+----------+

where Trojan Request is a SOCKS5-like request:

+-----+------+----------+----------+
| CMD | ATYP | DST.ADDR | DST.PORT |
+-----+------+----------+----------+
|  1  |  1   | Variable |    2     |
+-----+------+----------+----------+
```

方案

可以利用 CA，达到在建立连接的时候网站就知道用户身份的效果吗？

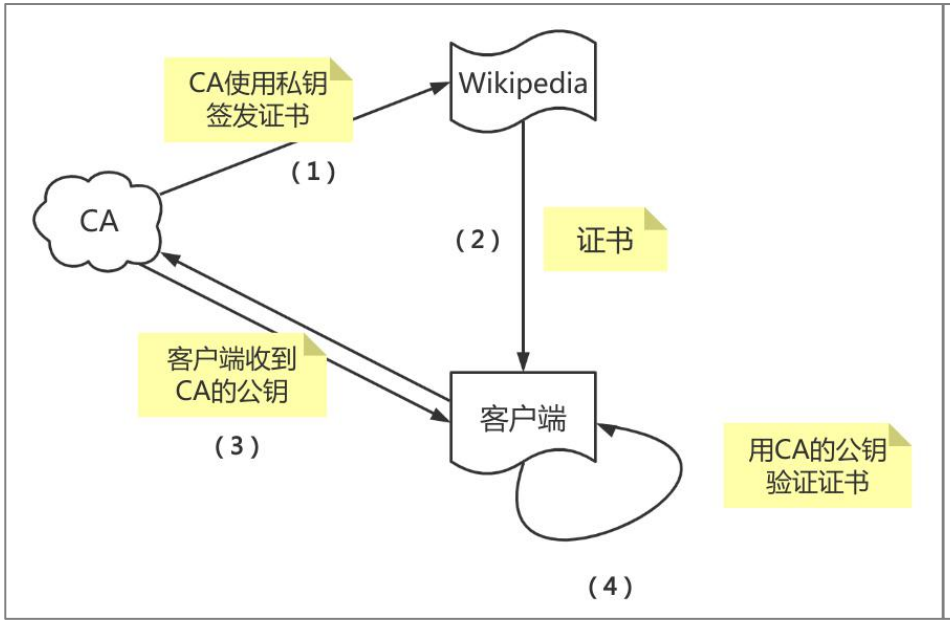
HTTPS VS ？

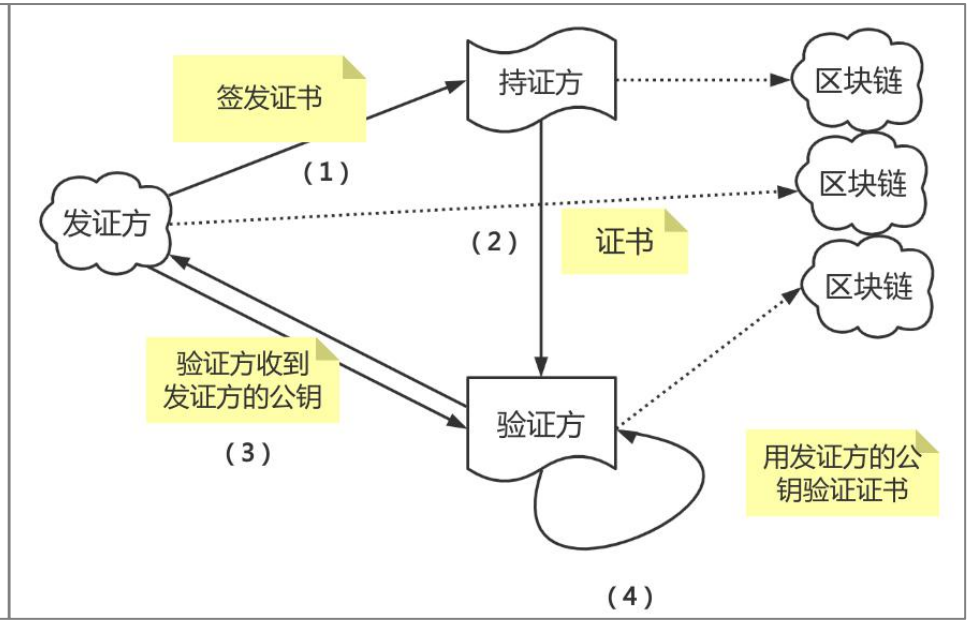
目录

回到 SSI

?

HTTPS VS SSI


CA使用私钥
签发证书
Wikipedia
（1）
CA
（2）
证书
客户端收到
CA的公钥
客户端
（3）
用CA的公钥
验证证书
（4）


签发证书
持证方
区块链
（1）
区块链
发证方
（2）
证书
区块链
验证方收到
发证方的公钥
验证方
（3）
用发证方的公
钥验证证书
（4）

?

Public key certificate VS Verifiable Credentials

证书查看者：*.w3.org

基本信息(G) 详细信息(D)

此证书已通过验证，具有以下用法：

SSL 服务器证书

颁发对象

公用名 (CN)	*.w3.org
组织 (O)	<未包含在证书中>
组织单位 (OU)	Domain Control Validated

颁发者

公用名 (CN)	Gandi Standard SSL CA 2
组织 (O)	Gandi
组织单位 (OU)	<未包含在证书中>

有效期

颁发日期	2019年5月23日星期四上午8:00:00
截止日期	2021年6月2日星期三上午7:59:59

指纹

SHA-256 指纹	2C 64 3F BE 90 2D 53 EE E1 E5 94 79 7F F7 49 BD 6D EA 40 11 8B F1 9D 3E DD 97 4A 3D 7C BC 3E 3C
SHA-1 指纹	40 AF 00 6B EC 90 22 41 8E A3 AD FA 1A E8 25 41 1D 1A 54 B3

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "NameAndAddress"],
  "issuer": "https://example.edu/issuers/14",
  "holder": {
    "type": "LawEnforcement",
    "id": "did:example:ebfeb1276e12ec21f712ebc6f1c"
  },
  "issuanceDate": "2010-01-01T19:73:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "name": "Mr John Doe",
    "address": "10 Some Street, Anytown, ThisLocal, Country X"
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2018-06-17T10:03:48Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://example.edu/issuers/14/keys/234",
    "jws": "pY9...Cky6Ed = "
  }
}
```

目录

SSI 到底有什么？

SSI

SSI 在技术上并没有革命性创新；

SSI 是一种给予数字身份主权的理念，去中心化的身份标识和机器可验证的证明可以助力实现这一理念；

W3C 提供了开放和正确的去中心化的身份标识规范（DIDs）和可验证证明规范（VCs）。

感谢聆听　敬请指正