Managing SSH Access Without Managing SSH Keys

Niall Sheridan
niall@intercom.com
Intercom Production Systems

"Many organizations don't even know how many SSH keys they have configured to grant access to their information systems or who has copies of those keys"

- *NIST IR 7966 Security of Interactive and Automated Access Management Using Secure Shell (SSH)*

Delete id_rsa
[redacted] on GitHub 6 hours ago

Delete id_rsa
[redacted] on GitHub a day ago

Delete id_rsa jenkins
[redacted] on GitHub 5 days ago

Delete id_rsa
[redacted] on GitHub 6 days ago

Delete id_rsa
[redacted] on GitHub 13 days ago

Delete id_rsa
[redacted] on GitHub 17 days ago

Delete id_rsa
[redacted] on GitHub 20 days ago

Delete id_rsa

master

[redacted] committed on GitHub 23 hours ago

Showing 1 changed file with 0 additions and 27 deletions.

27 [redacted] .ssh/id_rsa

```
...  @@ -1,27 +0,0 @@
1   -----BEGIN RSA PRIVATE KEY-----
2   -MIIEpAIBAAKCAQEA06gbxIXHQtlqwERWRTz/zRb+N2CVQFhBt9r+gpbG5FdjKKyX
3   -triLg7RYHluMdEuP8C14S9Ba9hhLfyQkgxoSPR57jlbe0acW2zckdWF5nsOqLSvu
4   -j3rV4ORhVdxngyF+NUT+LtY73OZL7bunwLc+aqiZSNjGq0olqJwtZZQAv9rb9v9y
5   -Lg4E8vy6BbnjaQ9IrZk9hOrQBf4v70zubXPt1InEtDcnnQG+K61pBlygvNspvaOu
6   -O+A4DNJ+BPGt9toXbmaFRlHx7Kn+ylT38yyDgbie6Qw+kQu9zISehD8+wFD3Gcb/
7   -2slL4r48bJ1oCHn9g9DNQo85zBAQlsYDYfTq0wIDAQABAoIBAAScoR5DG/hk7GKM
8   -GqUfkyNQ4PEr9ZSVV7k92FXYGzVWgh6cxCGDG+cewtzGeeT+0IAXPYvJWnIKTXrT
9   -usfwhX03cNHFKs2+qkzUgsLcAN5ovQiG8IfH0Wk5ELXiO48r56gZfMBggqVpjzX6
10  -5MjaNU31poFj19BbqT5nSMXx16JWhFY7+kcfRxJ05CgfIOvLV3LIfGeLB32LxTrG
11  -2tsUHoWPlrlf0uiCZuHZacSjiONiqinWee3AVswelVG+8EIe9AeaDDsR6HMYVYxw
12  -wFUzDZInMKFqbcCJVrpy/QJfqgIlZzEC8CHvad+g33e4mpo6angigtnbeemHpBaZ
13  -sq2/SgECgYEA8GRDpf3SCoEG/zzrUxRBBbtxKRVhN6KWfAIGmwEXFbxdAh0uofeB
14  -6maA7JMBw0DcC6Ias3Qnr605hOhm9/RKmQ7RoDKo8mdZImiBPUPPjZ7LToqjfmMh
15  -VTuudYX6yu76h7y1EzB/cjXJyayDVE5avr7ofDz86ccAOk63q/aMfkECgYEA4WY3
16  -wwcU3LvTjtxL3fhBIZQ63qYjOaE1AlmKKA0sgy1PIRKh7ZB4DGAC9rRgU/9NuDDu
17  -2QlJSTAFtl0IjxjuewwG8REgHuSMQ4D3cejXFfBqThvjhZBRzP71zxz7PbYxn7FN
18  -9GWHjdYNtVU+O2BNuxXDNbTXMbjFr9/CGdl8jBMCgYEA6A/ChmFq/JzmRktm2QK6
```

Security

16

Hackers break into FreeBSD with stolen SSH key

JUN
16
2017

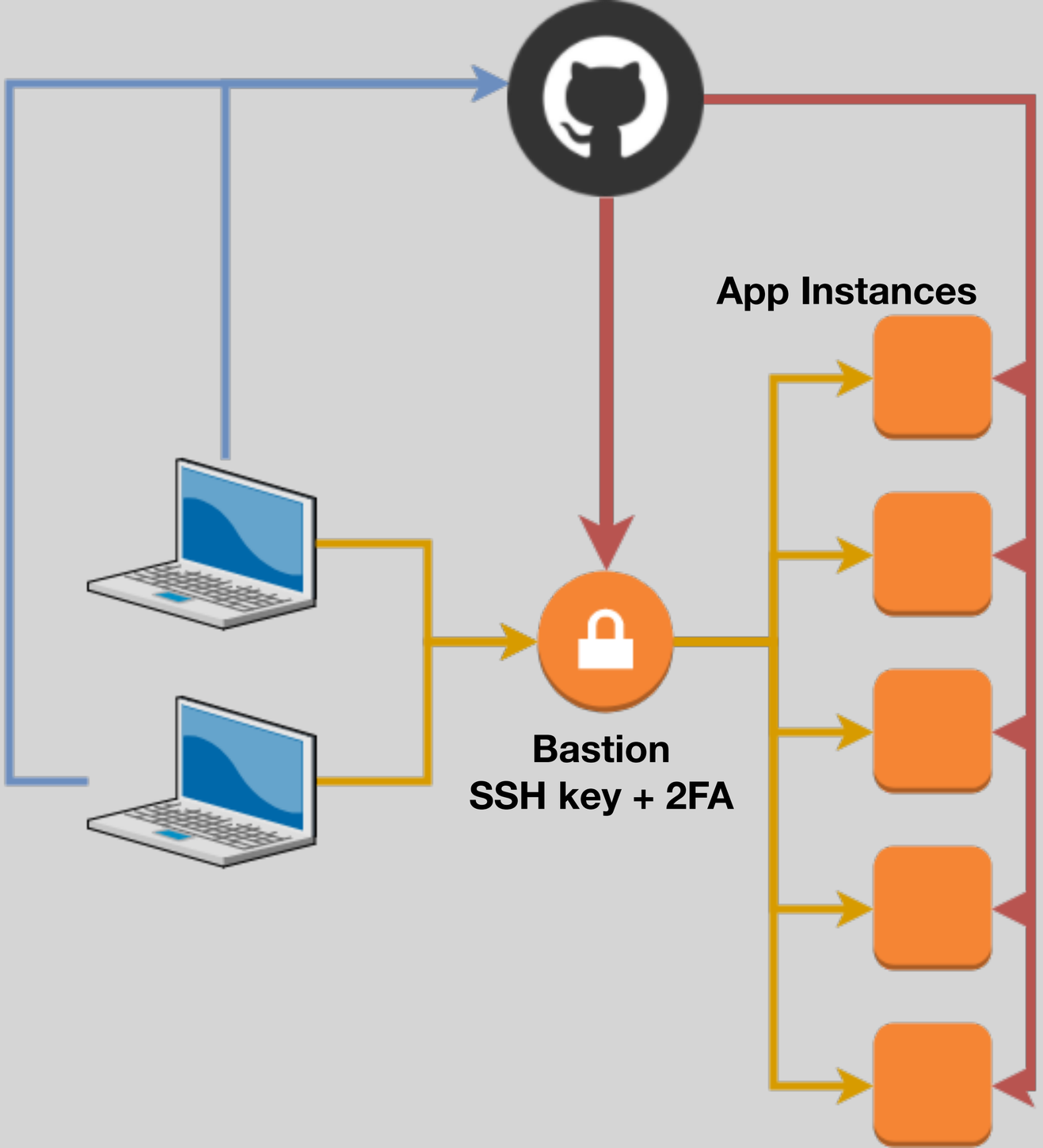
A Multi-billion Dollar Defense Firm Fails to Protect Private SSH Keys

Chris Vickery, a cyber risk analyst from UpGuard, successfully retrieved a cache of 60,000 documents related to a United States military project for the National Geospatial-Intelligence Agency (NGA). The sensitive files (close to 28 GB) linked to the U.S. intelligence agency were left unsecured (without a password) on a public Amazon server for anyone to access. Some of these files included the private SSH keys of a Booz Allen – one of country's top defense contractors – employee, and various plain text passwords belonging to contractors with Top Secret Facility clearance.

CIA Malware Can Steal SSH Credentials, Session Traffic


SECURE
LEVER

HOPE IS NOT A STRATEGY

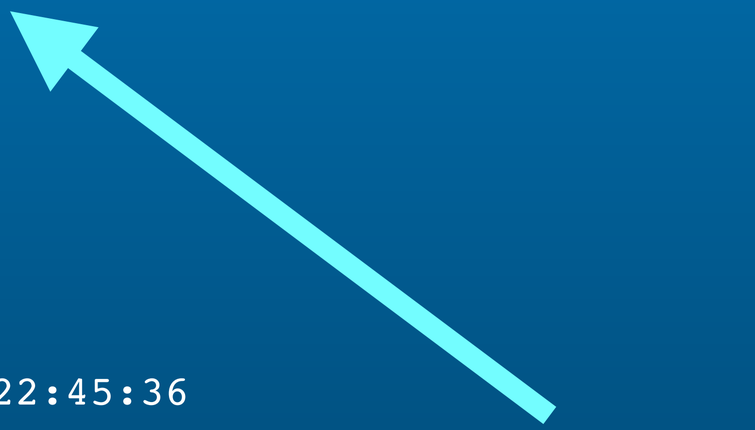

App Instances
Bastion
SSH key + 2FA

SSH Certificates

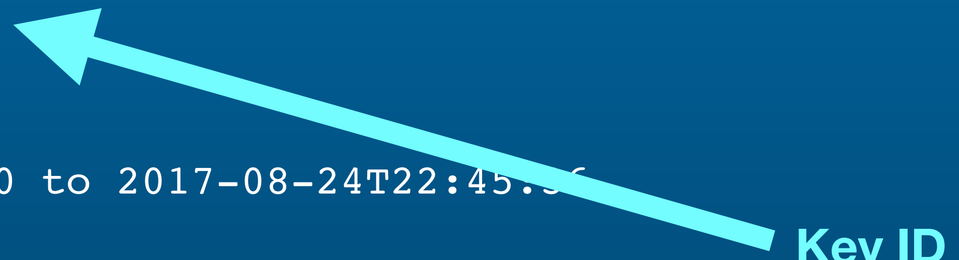
- Composed of: ssh key + signature + signing key + metadata
- Only need to distribute 1 public key to machines - the signing key
- Metadata allows for some nice properties to be set

```
Type: ssh-ed25519-cert-v01@openssh.com user certificate
Public key: ED25519-CERT SHA256:WHATEVER
Signing CA: ED25519 SHA256:WHATEVER
Key ID: "some identity string"
Serial: 0
Valid: from 2017-08-23T22:40:40 to 2017-08-24T22:45:36
Principals:
        prod-user
Critical Options:
        force-command /bin/date
        source-address 12.34.56.78/29
Extensions:
        permit-pty
        permit-port-forwarding
        permit-x11-forwarding
```

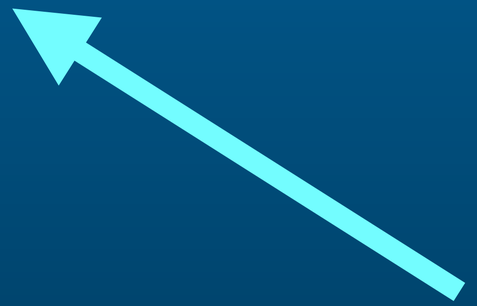
```
Type: ssh-ed25519-cert-v01@openssh.com user certificate
Public key: ED25519-CERT SHA256:WHATEVER
Signing CA: ED25519 SHA256:WHATEVER
Key ID: "some identity string"
Serial: 0
Valid: from 2017-08-23T22:40:40 to 2017-08-24T22:45:36
Principals:
        prod-user
Critical Options:
        force-command /bin/date
        source-address 12.34.56.78/29
Extensions:
        permit-pty
        permit-port-forwarding
        permit-x11-forwarding
```



```
Type: ssh-ed25519-cert-v01@openssh.com user certificate
Public key: ED25519-CERT SHA256:WHATEVER
Signing CA: ED25519 SHA256:WHATEVER
Key ID: "some identity string"
Serial: 0
Valid: from 2017-08-23T22:40:40 to 2017-08-24T22:45:
Principals:
        prod-user
Critical Options:
        force-command /bin/date
        source-address 12.34.56.78/29
Extensions:
        permit-pty
        permit-port-forwarding
        permit-x11-forwarding
```

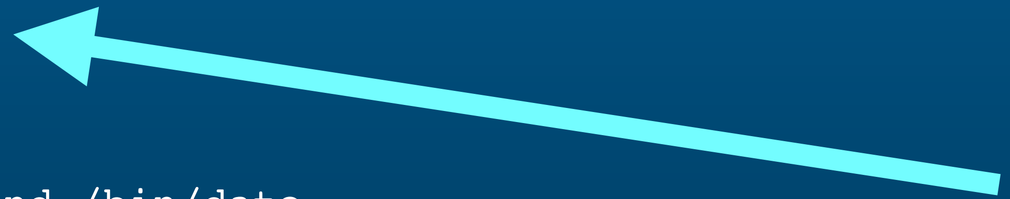


```
Type: ssh-ed25519-cert-v01@openssh.com user certificate
Public key: ED25519-CERT SHA256:WHATEVER
Signing CA: ED25519 SHA256:WHATEVER
Key ID: "some identity string"
Serial: 0
Valid: from 2017-08-23T22:40:40 to 2017-08-24T22:45:36
Principals:
        prod-user
Critical Options:
        force-command /bin/date
        source-address 12.34.56.78/29
Extensions:
        permit-pty
        permit-port-forwarding
        permit-x11-forwarding
```



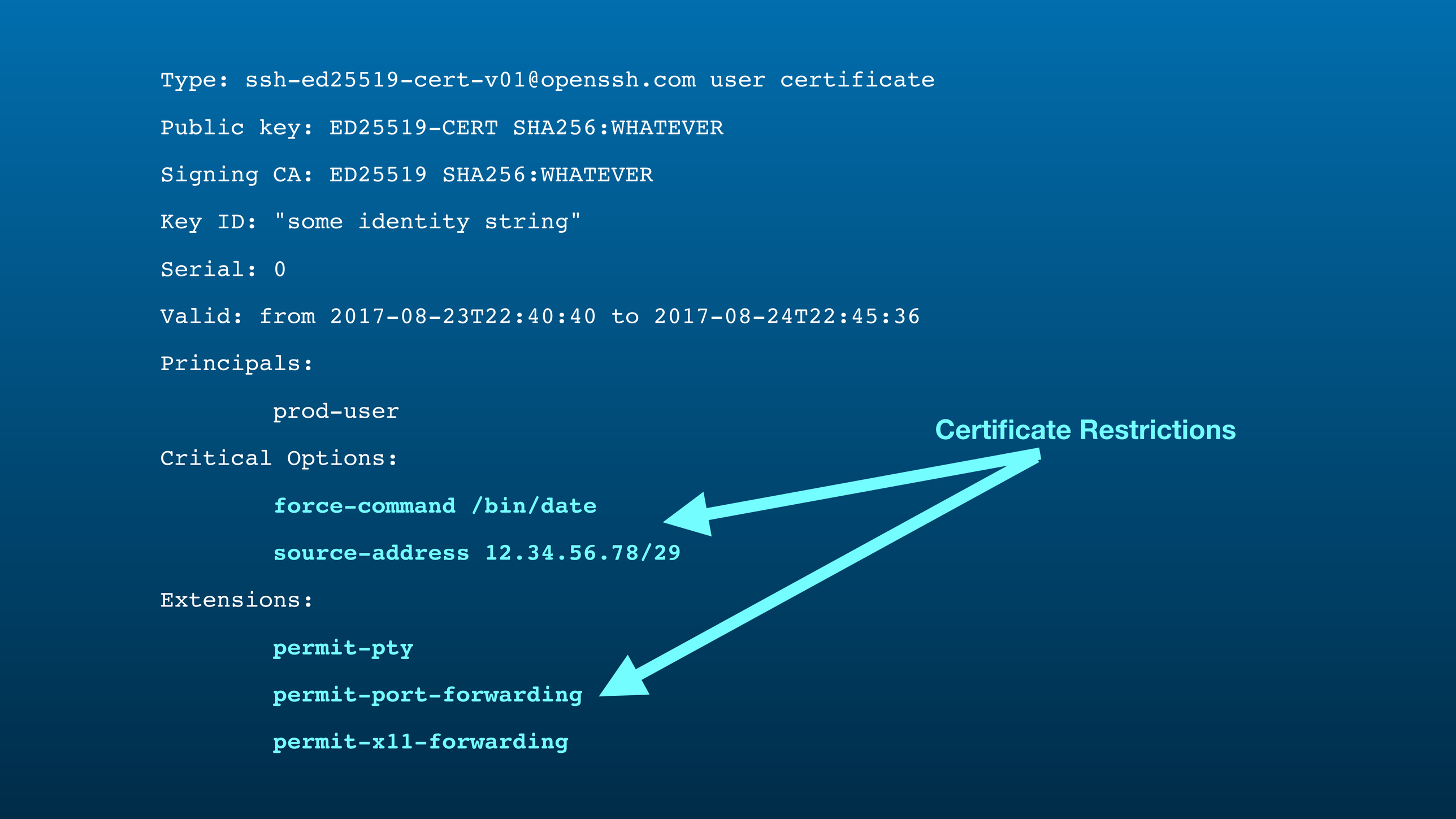
Certificate Lifetime

```
Type: ssh-ed25519-cert-v01@openssh.com user certificate
Public key: ED25519-CERT SHA256:WHATEVER
Signing CA: ED25519 SHA256:WHATEVER
Key ID: "some identity string"
Serial: 0
Valid: from 2017-08-23T22:40:40 to 2017-08-24T22:45:36
Principals:
        prod-user
Critical Options:
        force-command /bin/date
        source-address 12.34.56.78/29
Extensions:
        permit-pty
        permit-port-forwarding
        permit-x11-forwarding
```



Username(s)

```
Type: ssh-ed25519-cert-v01@openssh.com user certificate
Public key: ED25519-CERT SHA256:WHATEVER
Signing CA: ED25519 SHA256:WHATEVER
Key ID: "some identity string"
Serial: 0
Valid: from 2017-08-23T22:40:40 to 2017-08-24T22:45:36
Principals:
        prod-user
Critical Options:
        force-command /bin/date
        source-address 12.34.56.78/29
Extensions:
        permit-pty
        permit-port-forwarding
        permit-x11-forwarding
```

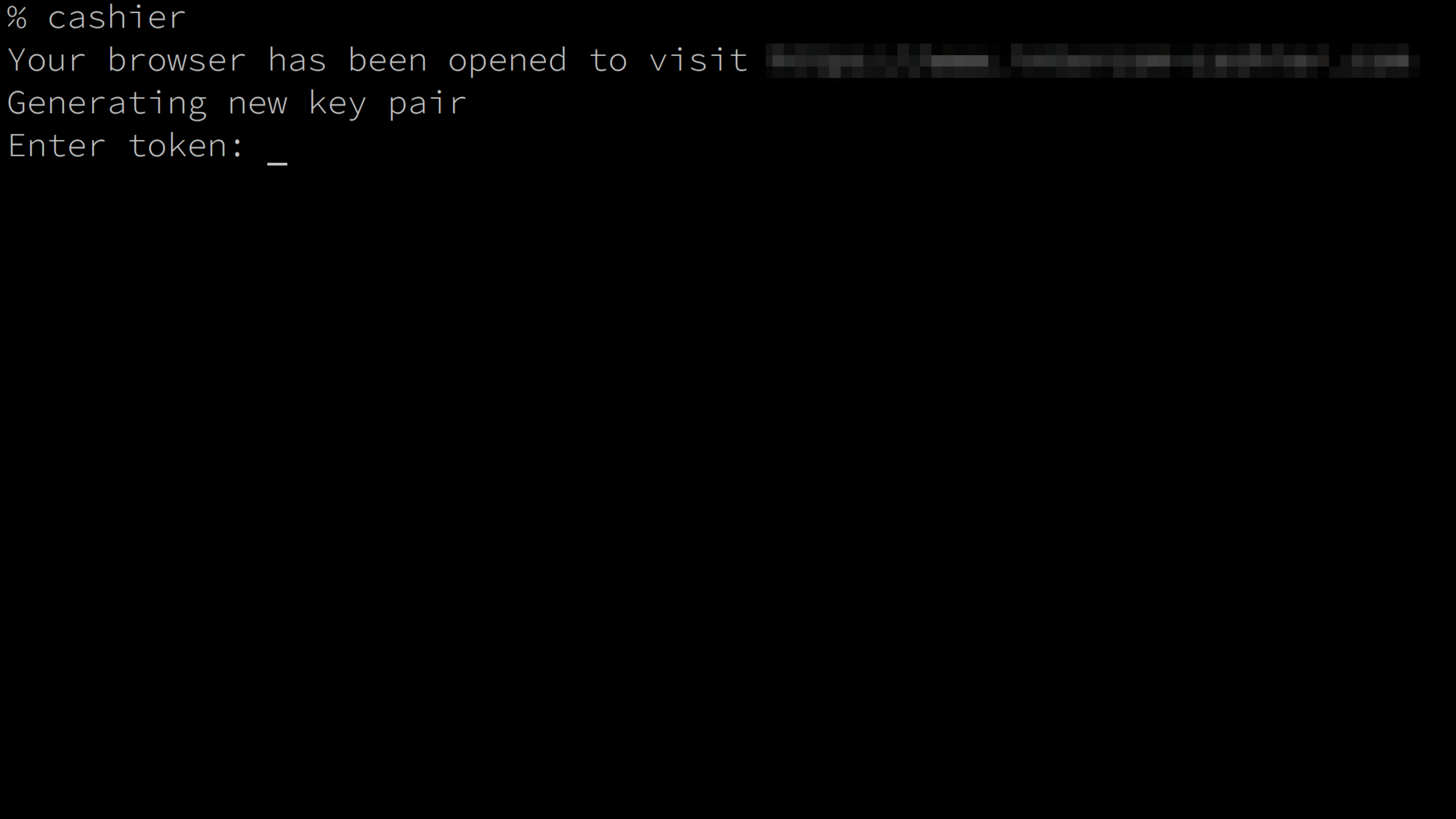


/etc/ssh/sshd_config:

```
TrustedUserCAKeys /etc/ssh/ca.pub
```

/etc/ssh/ca.pub:

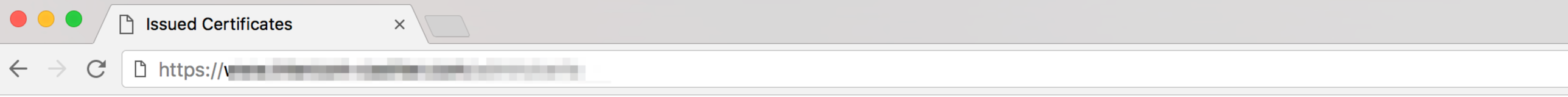
```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDAYZL32Emt4Ap.....
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDGmvJaFt37ZTz.....
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDWmdffJK0YR8z.....
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOBL2PHBRyIa7ok.....
```


% cashier
Your browser has been opened to visit
Generating new key pair
Enter token: _

Access Token

[redacted]

```
% cashier
Your browser has been opened to visit [redacted]
Generating new key pair
Enter token: [redacted]
Credentials added.
% ssh-add -l
256 SHA256:CIxATG78JkHH1AF+bk6vumRtP3z22wpRP+Y6hoMK9v4 niall_1503934975 [Expires
2017-09-04 16:42:54 +0100 IST] (ED25519-CERT)
256 SHA256:CIxATG78JkHH1AF+bk6vumRtP3z22wpRP+Y6hoMK9v4 niall_1503934975 [Expires
2017-09-04 16:42:54 +0100 IST] (ED25519)
% _
```



Issued SSH Certificates

Search

SHOW EXPIRED

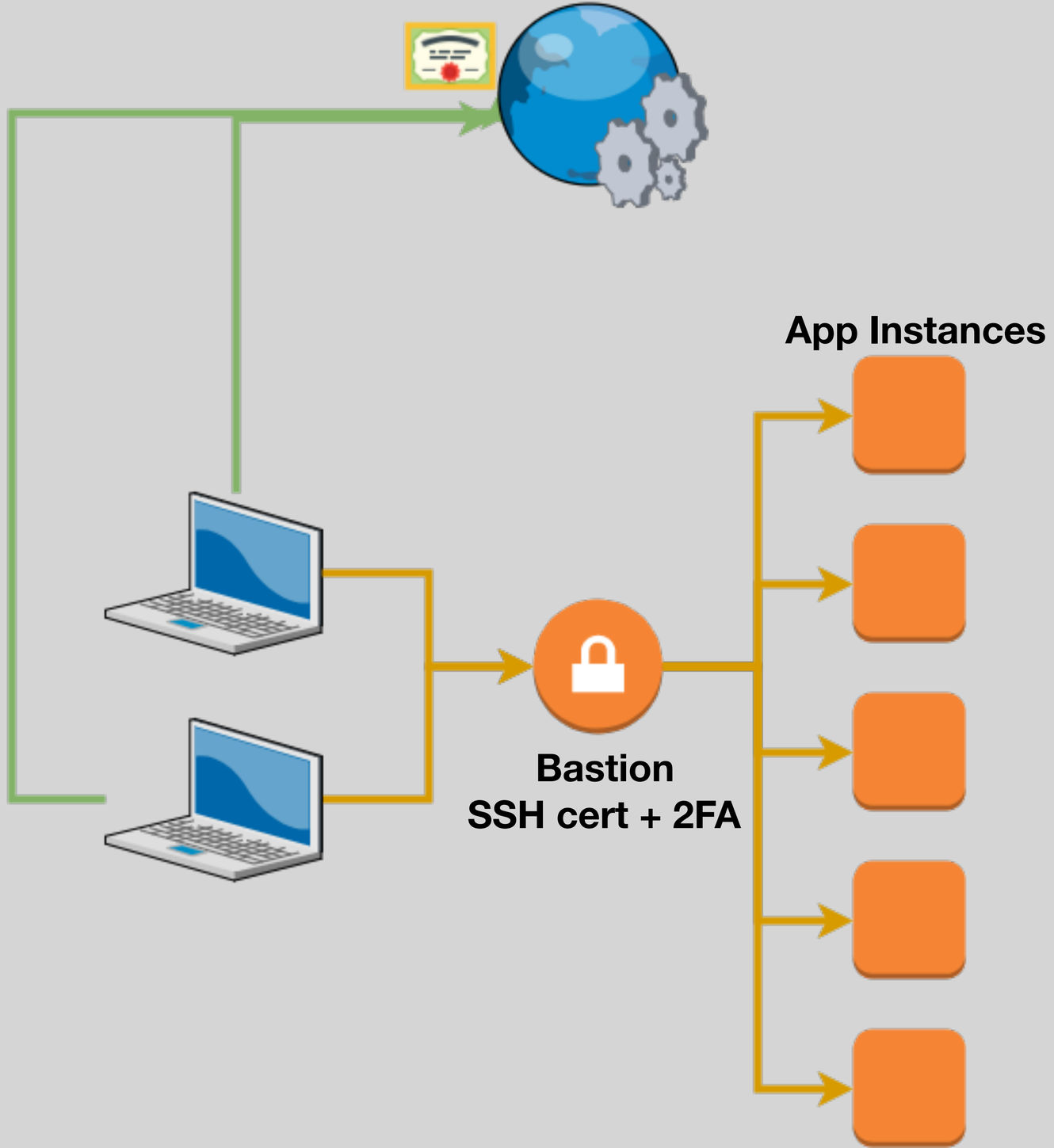
ID	Created	Expires	Principals	Revoked	Revoke
[redacted]	[redacted]	[redacted]	[redacted]	false	☐
[redacted]	[redacted]	[redacted]	[redacted]	false	☐
[redacted]	[redacted]	[redacted]	[redacted]	false	☐
niall_1503934975	2017-08-28 15:37:55 +0000	2017-09-04 15:42:54 +0000	niall,prod-user	false	☐
[redacted]	[redacted]	[redacted]	[redacted]	false	☐
[redacted]	[redacted]	[redacted]	[redacted]	false	☐
[redacted]	[redacted]	[redacted]	[redacted]	false	☐

SSH Key:

```
sshd[6382]: Accepted publickey for prod-user from
10.0.0.167 port 49562 ssh2: RSA bb:86:14:02:cf:
37:91:b9:4f:09:76:8f:e0:bc:52:77
```

SSH Certificate:

```
sshd[6382]: Accepted publickey for prod-user from
10.0.0.167 port 33984 ssh2: ED25519-CERT ID
niall_1503934975 (serial 0) CA ED25519 bd:0b:55:9f:
84:be:ad:e9:eb:ac:7e:8c:83:ed:4d:cb
```


App Instances
Bastion
SSH cert + 2FA

Questions?

https://github.com/nsheridan/cashier

Niall Sheridan
niall@intercom.com