Network Security: Attack and Defense

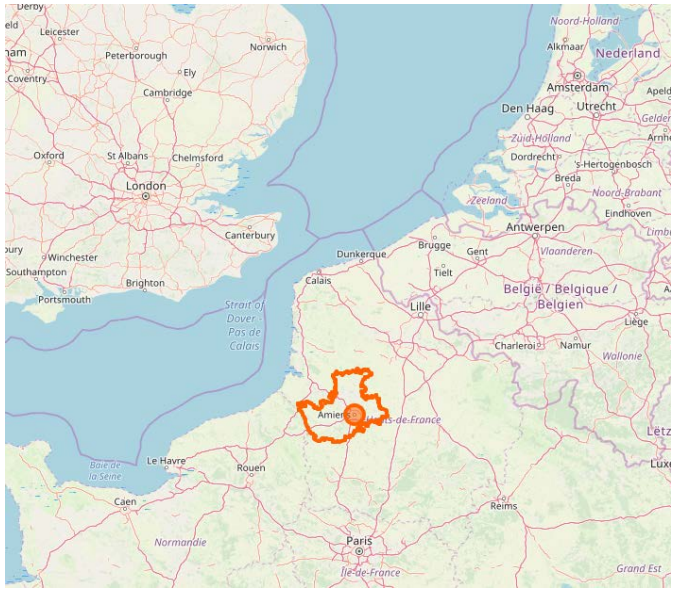
A comprehensive guide focused on Encryption and Endpoint Authentication

Aristide Bouix
09/11/2020

Agenda

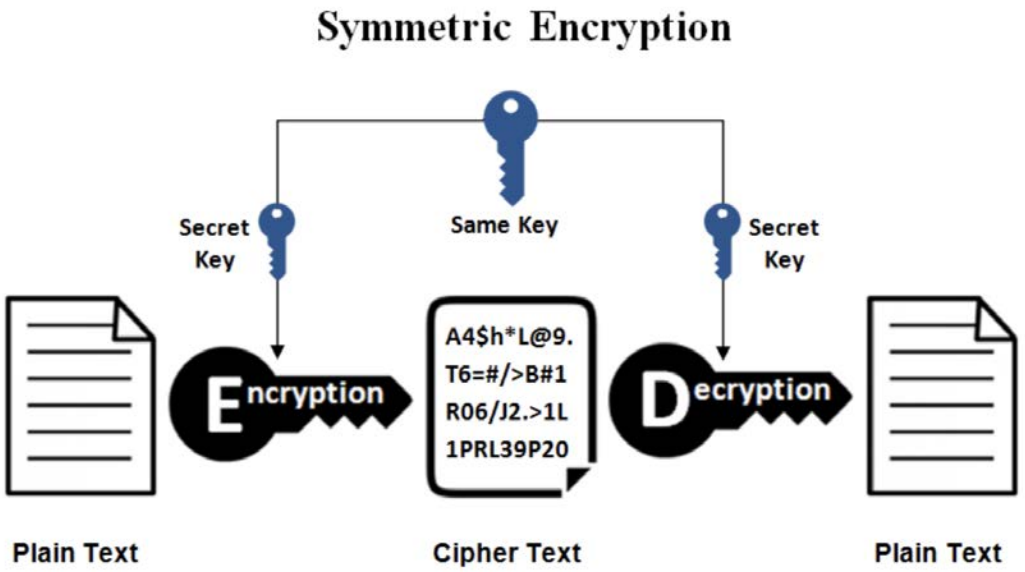
1. About me
2. Introduction to encryption: basic concepts
3. The fortress model
4. What are we fighting?
5. Introduction to PKI
6. A Zero Trust Architecture study case: Google BeyondCorp
7. Exercise: Set-up TLS mutual authentication

About me

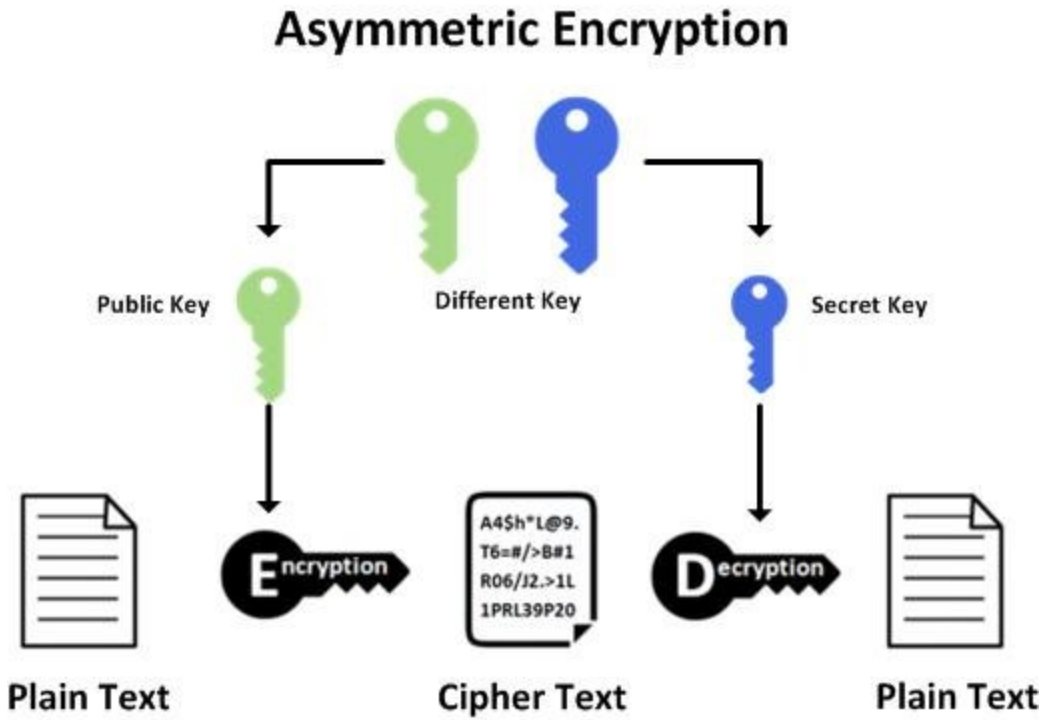


- Senior Consultant, Cybersecurity, DevSecOps lead
  - Certification: 5 AWS, 2 MSFT, 1 SNOW, CCSKv4, Itilv3
- Focus on security operations and secure IT architecture
  - Actively working on Cloud security automation and DevOps security
- Prior worked at an MSSP at Atos and consulting at Devoteam/D2SI
  - MSC in Telecommunication Engineering, major in Network and System security
  - BSC in Electrical Engineering
- Like: Korean food, Metal, Hiking, HomeLabs, Gaming, …
- Dislike: Parsley, Writing security policies, …

Introduction to encryption: Symmetric vs Assymmetric

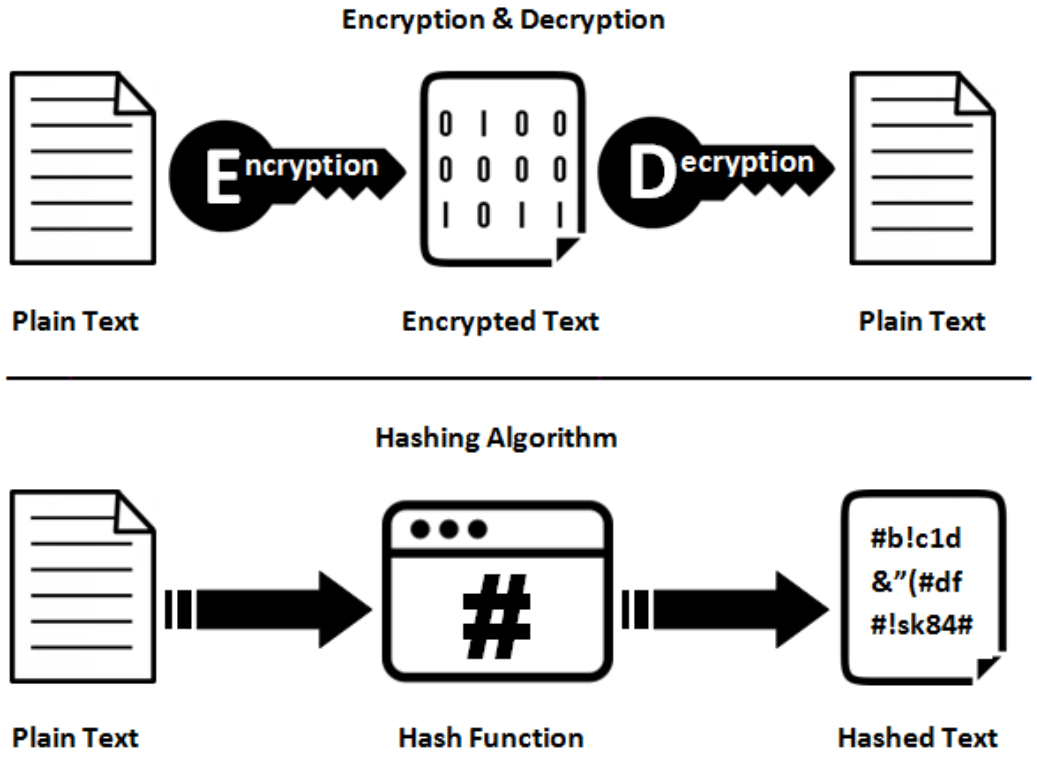


Source: https://medium.com/@emilywilliams_43022/cryptography-101-symmetric-encryption-444aac6bb7a3

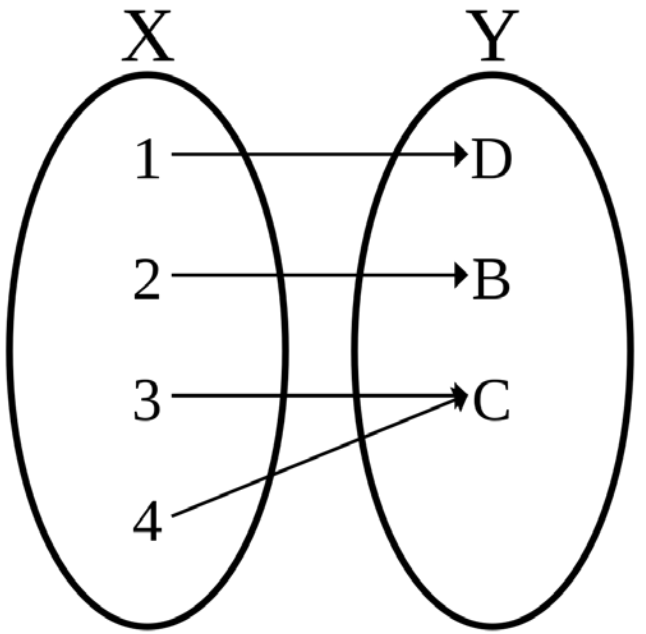


Source: https://www.researchgate.net/figure/Asymmetric-encryption-primitive_fig2_321123382

Introduction to encryption: Hashing



Source: https://www.ssl2buy.com/wiki/difference-between-hashing-and-encryption



Surjection

Introduction to encryption: Collision

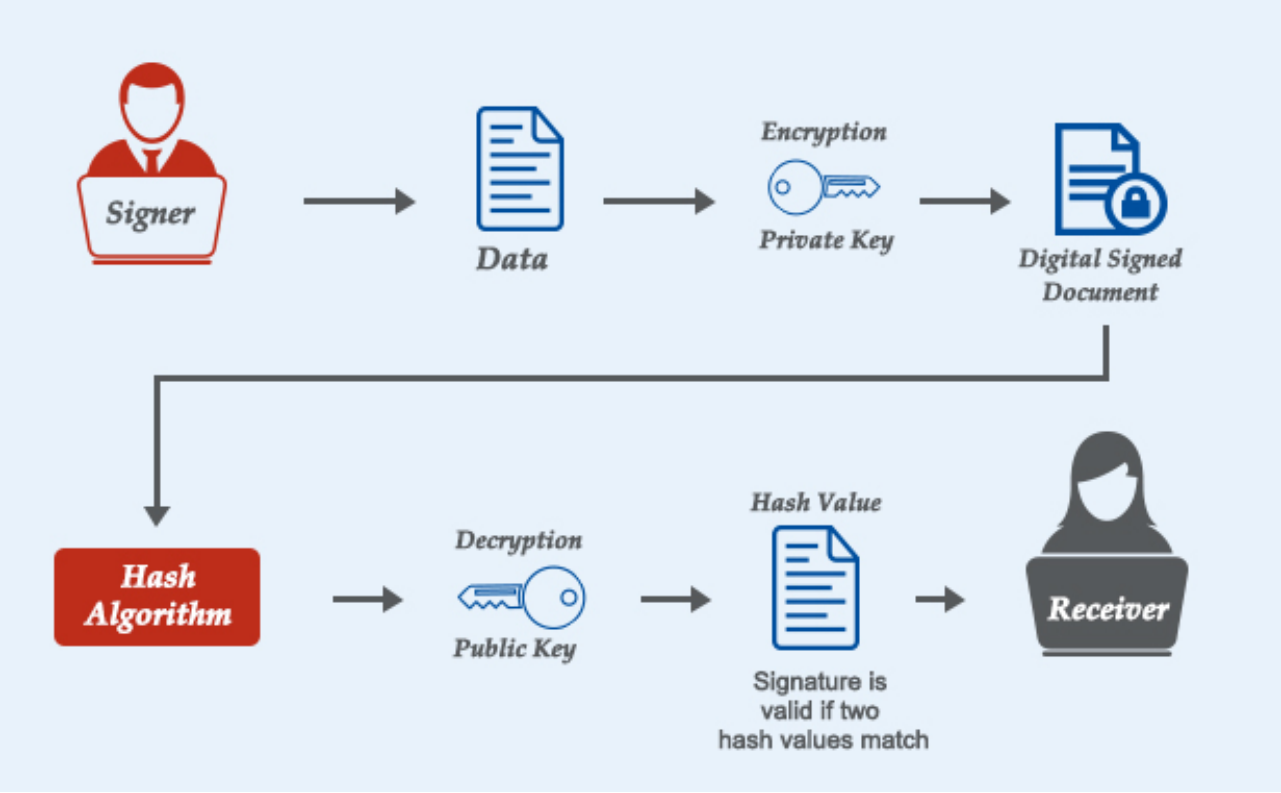
d131dd02c5e6eec4693d9a0698aff95c
2fcab50712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325f1415a
085125e8f7cdc99fd91dbd7280373c5b
d8823e3156348f5bae6dacd436c919c6
dd53e23487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080280d1e
c69821bcb6a8839396f965ab6ff72a70

d131dd02c5e6eec4693d9a0698aff95c
2fcab58712467eab4004583eb8fb7f89
55ad340609f4b30283e4888325 71415a
085125e8f7cdc99fd91dbdf280373c5b
d8823e3156348f5bae6dacd436c919c6
dd53e2b487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080a80d1e
c69821bcb6a8839396f9652b6ff72a70

Let's play: https://gchq.github.io/CyberChef/

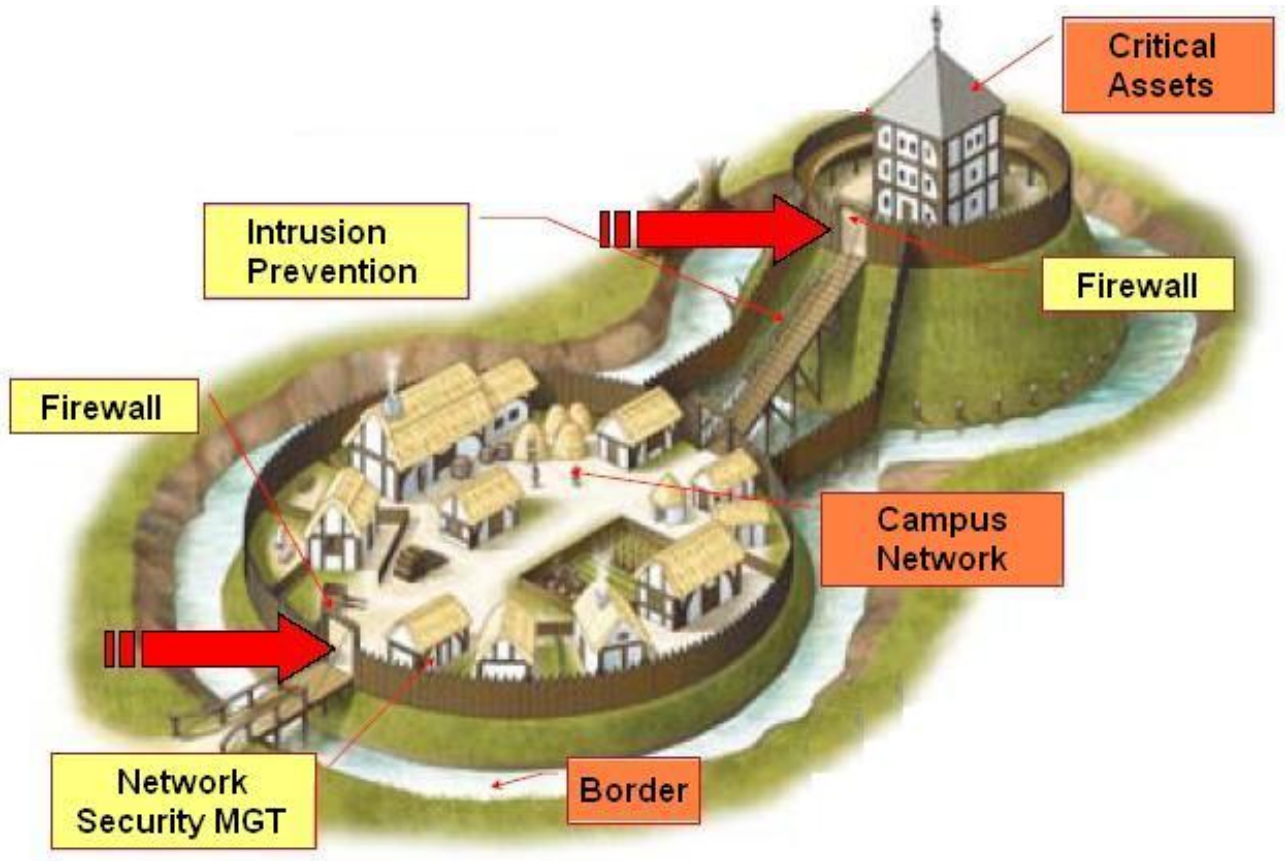
More on: https://www.mathstat.dal.ca/~selinger/md5collision/

Introduction to encryption: Signing



Source: https://comodosslstore.com/blog/what-is-digital-signature-how-does-it-work.html

The fortress model: Perimeter Security



Source: https://nigesecurityguy.wordpress.com/2013/06/

How is the fortress model challenged?

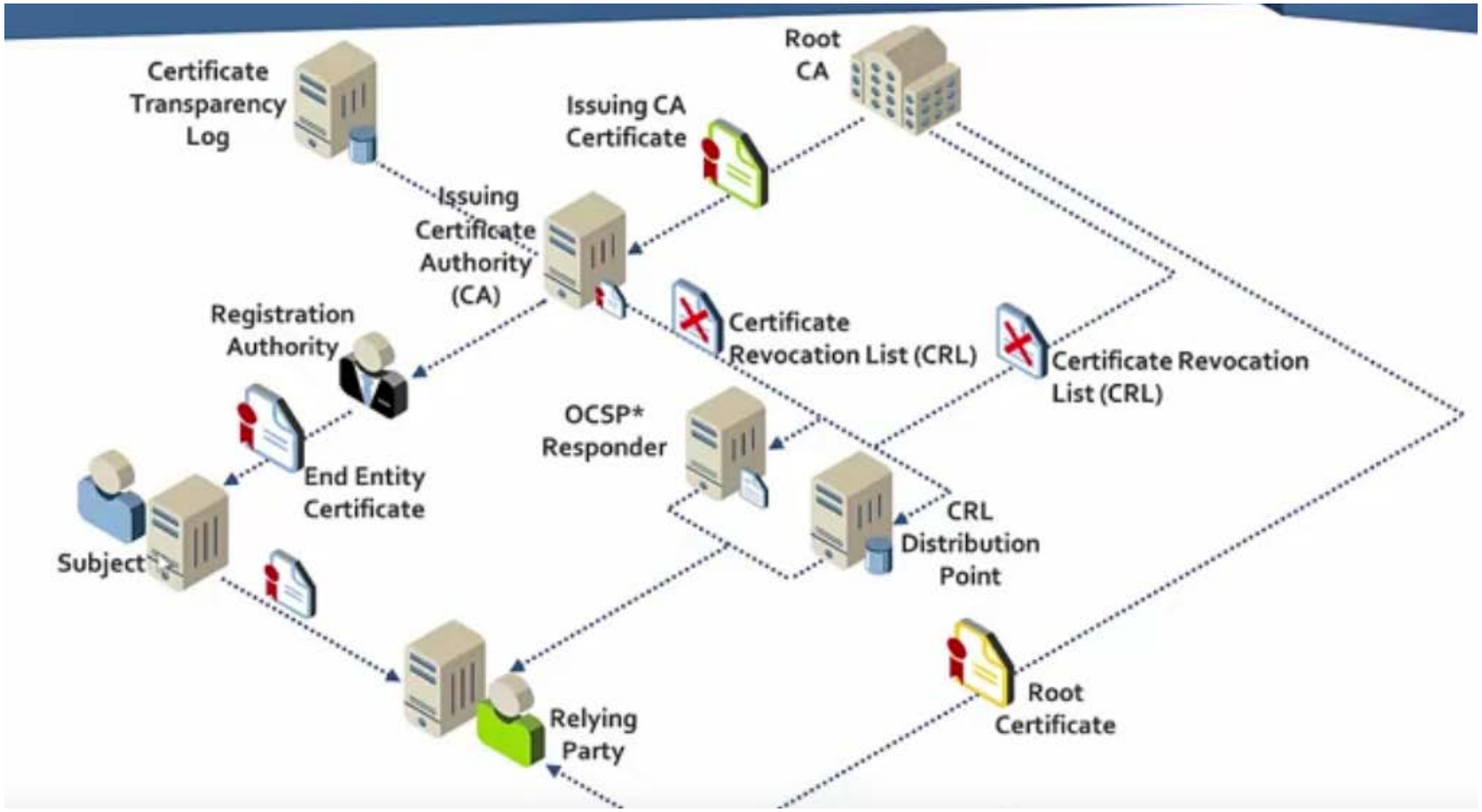
- Social engineering
  - Mobile devices
  - Phishing
- Unsecured networks (MITM)
  - Work from home
  - Public Wi-Fi
- Unmanaged devices
  - BYOD
  - Shadow IT

Users, Networks and Endpoints can no longer be trusted !

<u>Impact of a security incident</u>:

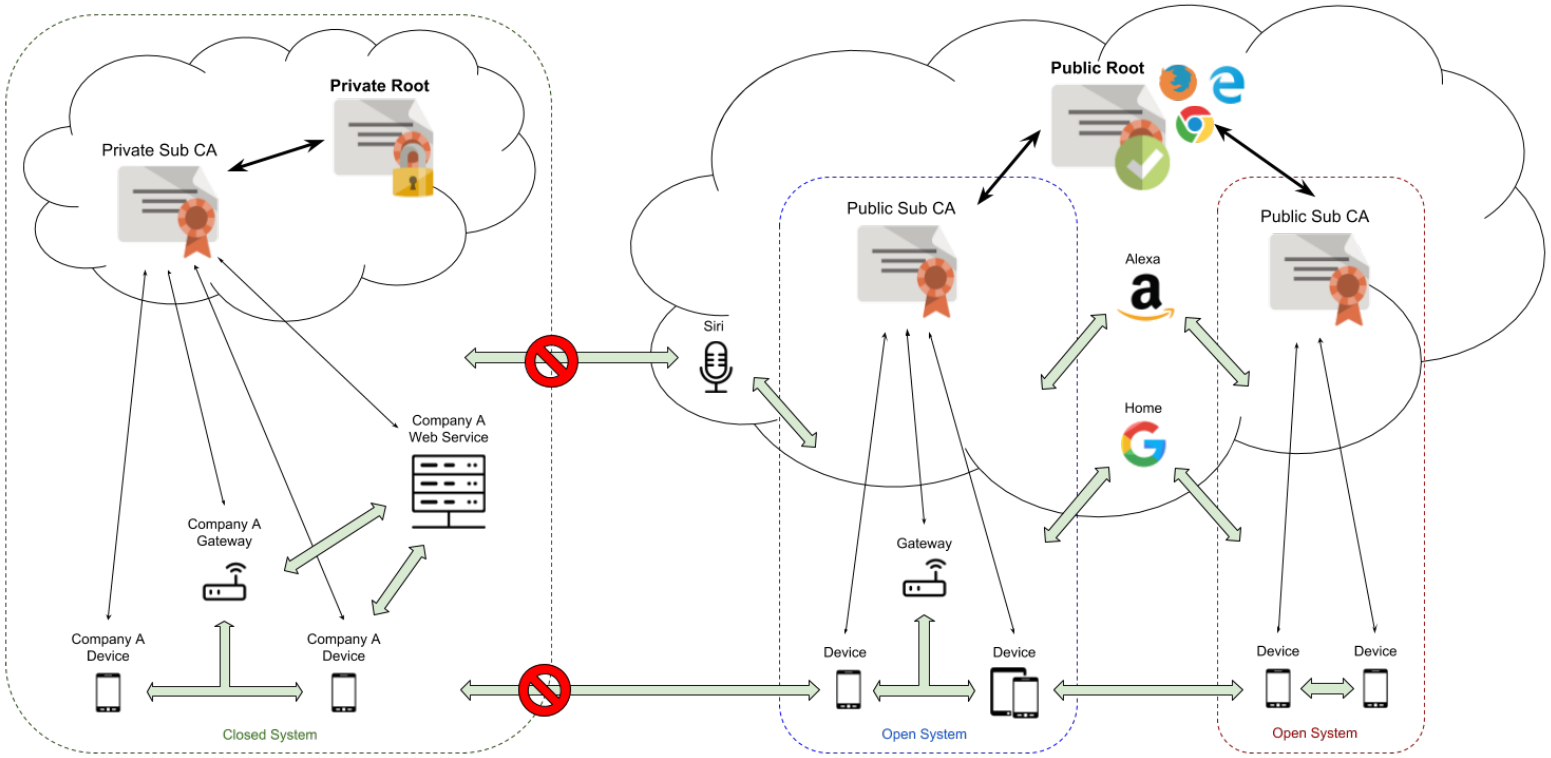
- Loss of critical data
- GDPR legal fine
- Damage to reputation

Introduction to PKI: Public PKI

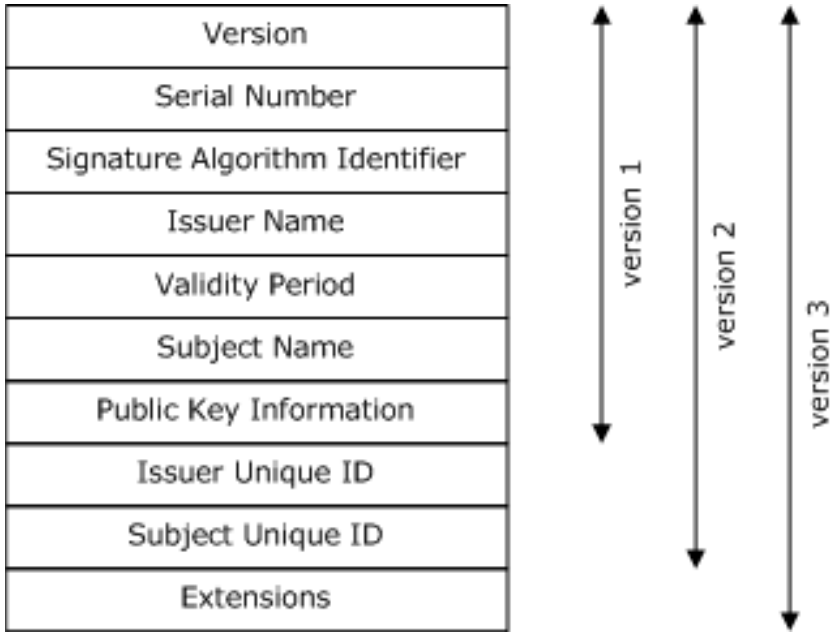


Source: https://www.youtube.com/watch?v=5OqgYSXWYQM

Introduction to PKI: private PKI and Certificates

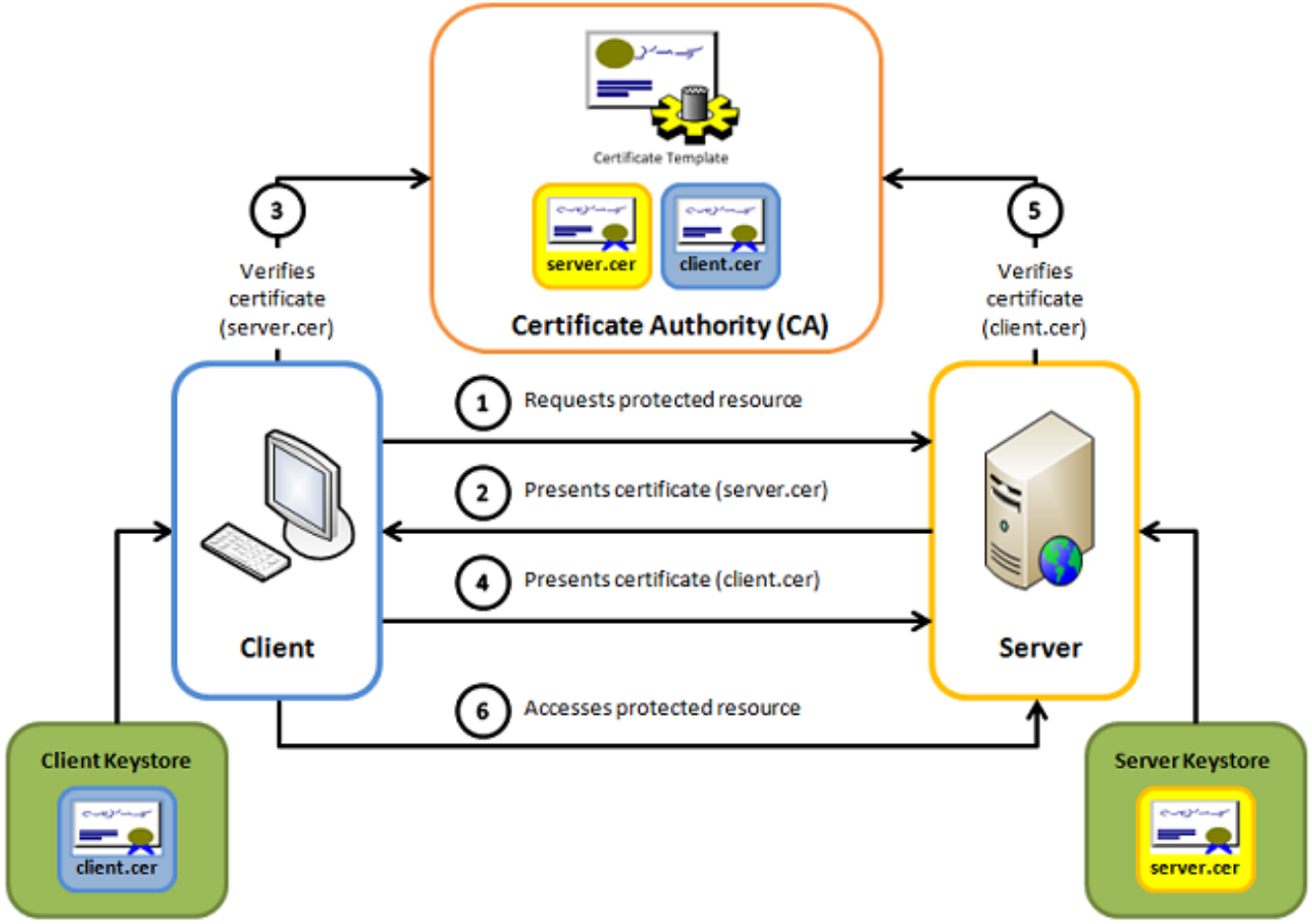


Source: https://www.ssl.com/article/private-vs-public-pki-building-an-effective-plan/



Source: https://docs.microsoft.com/en-us/windows/win32/seccertenroll/about-x-509-public-key-certificates

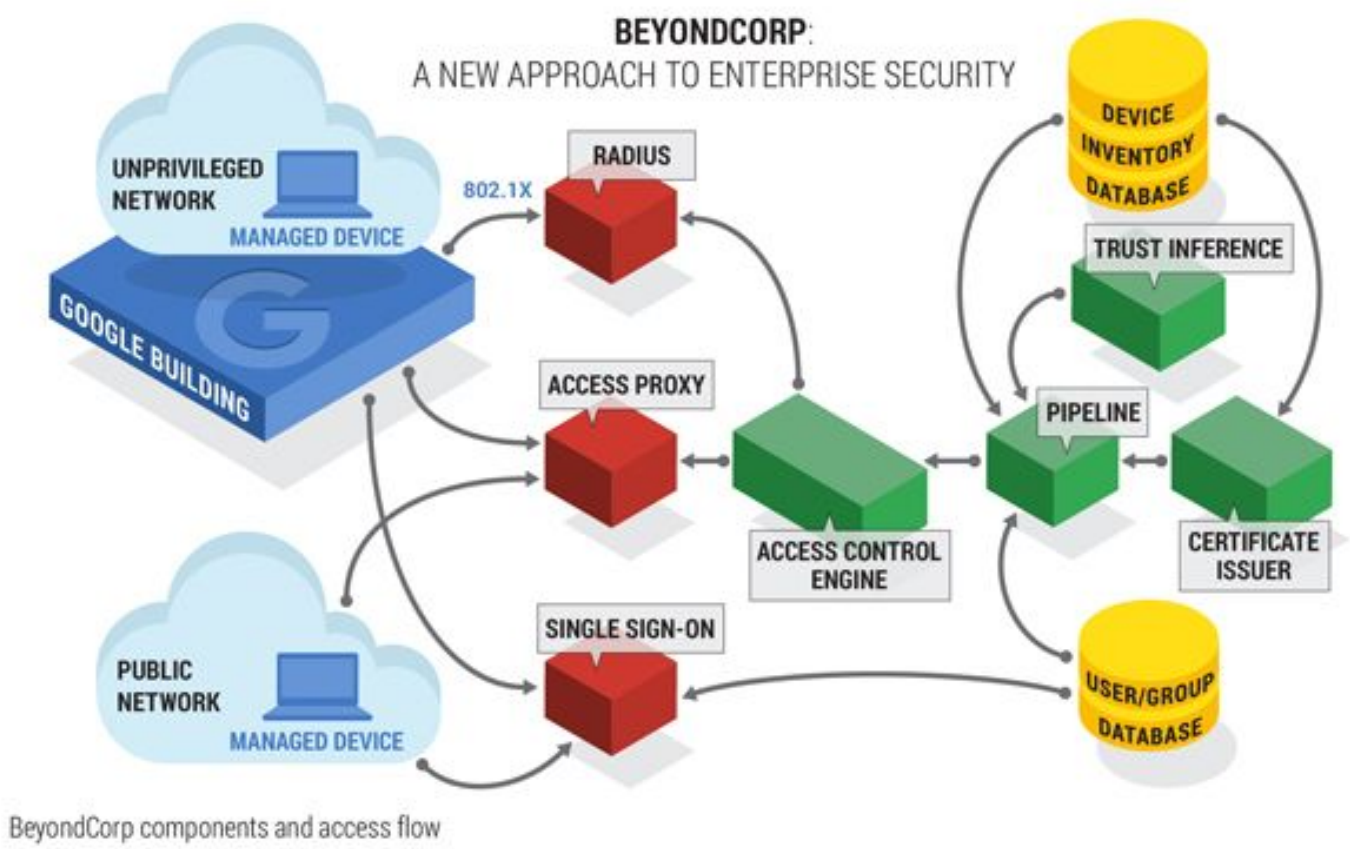
Introduction to PKI: TLS



Mutual SSL authentication / Certificate based mutual authentication

Source: https://www.codeproject.com/Articles/326574/An-Introduction-to-Mutual-SSL-Authentication

The new World: Zero Trust Architecture



BeyondCorp components and access flow

- All IT moved to the Cloud
- Location Agnostic without VPN
- **Full Authentication, Full Authorization, Full Encryption**

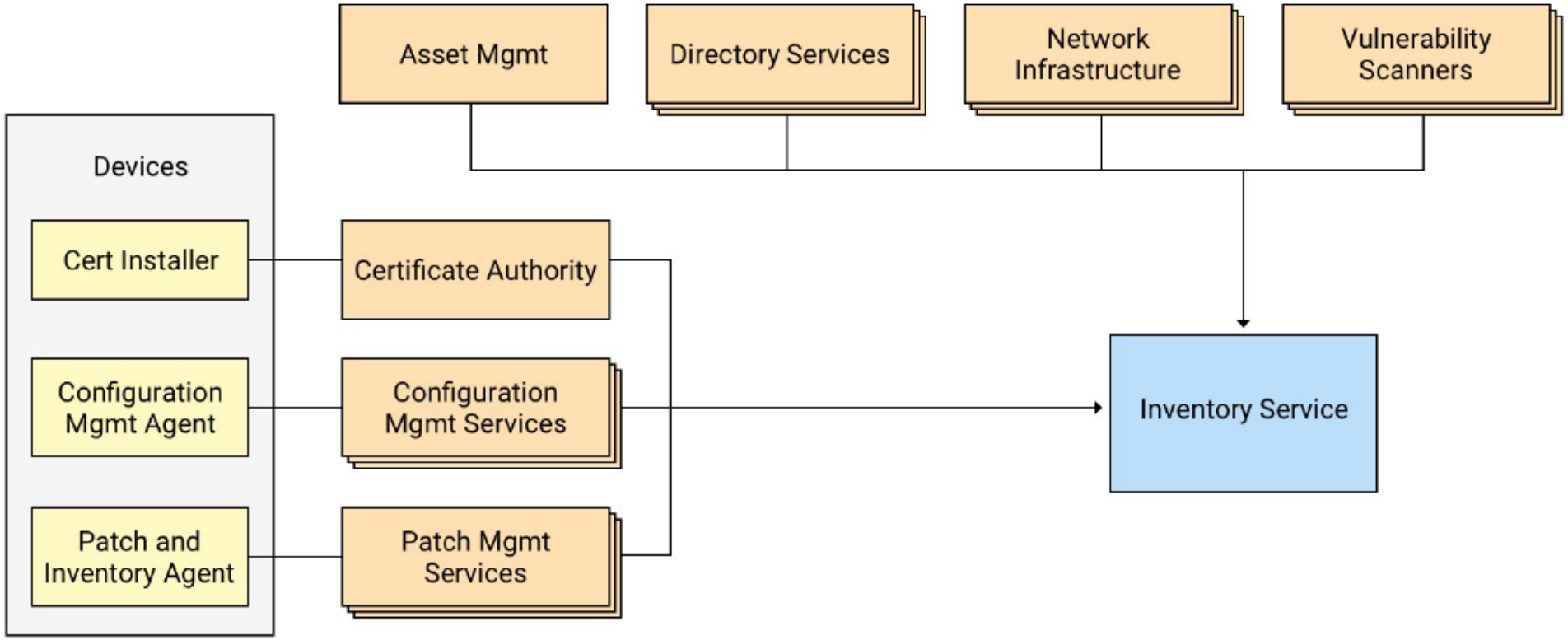
- Identify Devices
- Identify Users
- Inventory based access
- Unified Access Control Engine

Where our PKI can be used?

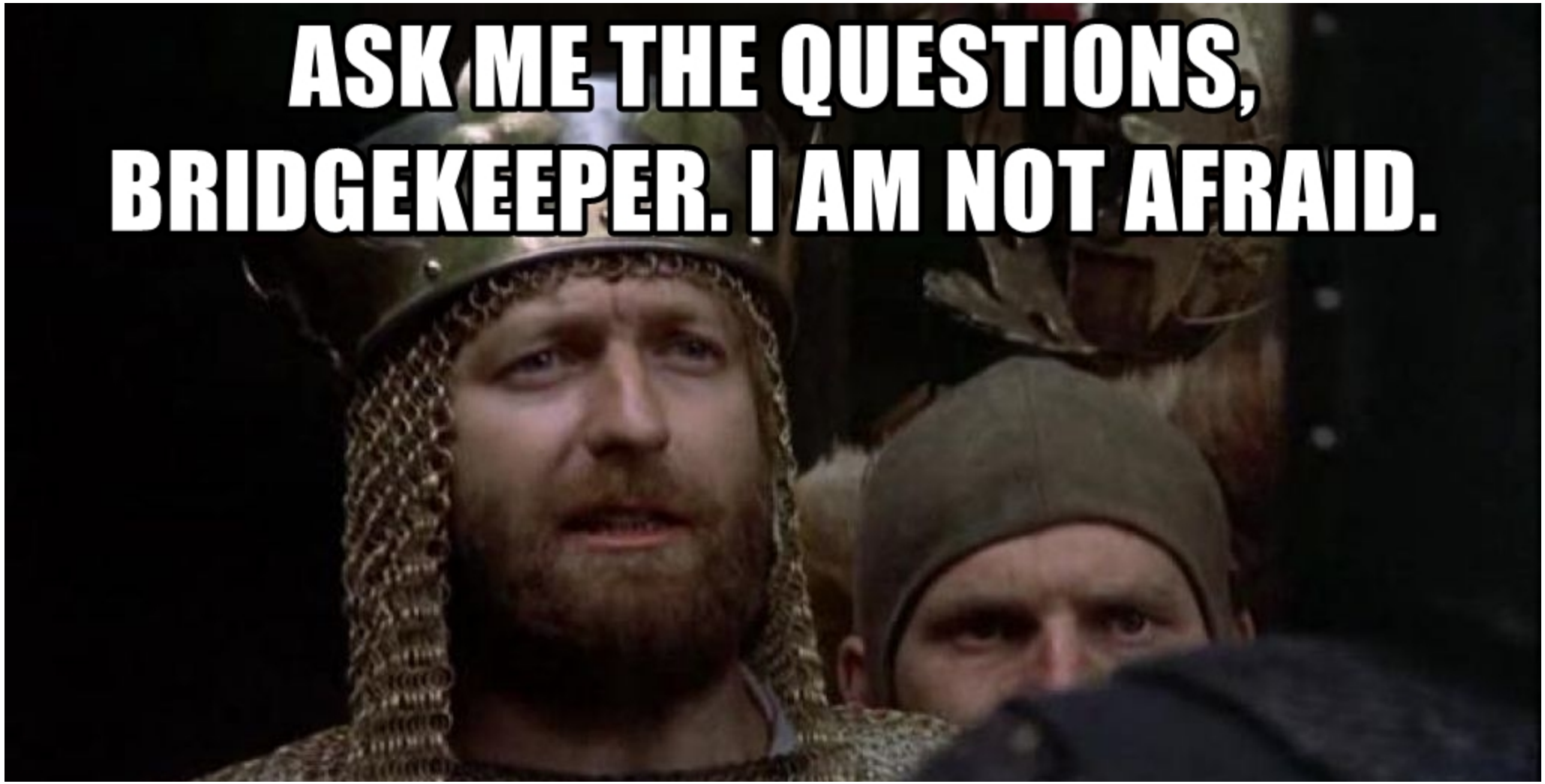
- Seemless Single-Sign-On experience:
  - Wi-Fi Authentication:

  - Web Application Authentication

BeyondCorp Device Inventory Service



Source: BeyondCorp Device Inventory Service


ASK ME THE QUESTIONS,
BRIDGEKEEPER. I AM NOT AFRAID.

Exercise: Set-up TLS mutual authentication

1. Install Nginx and an /admin administration website (RubyOnRail,Django,Flask …)
2. Create a private CA authority certificate with Openssl
3. Create a Certificate Signing Request (CSR)
4. Create server certificate
5. Create client certificate
6. Configure an Nginx website to use the server certificate on /admin
7. Install the CA certificate in your browser
8. Install the client certificate
9. Access the webserver url /admin

Guide: https://rollout.io/blog/how-to-set-up-mutual-tls-authentication/

Sent me an encrypted email with the screenshot of the TLS connection at: aristide.bouix@gmail.com (pgp.mit.edu) : Deface the webpage with you name to prove you've made it

Exercise: Bonus

Could you propose me a way of automating the generation, signing and delivery of X509 certificates between the CA/Servers and Clients?

Additional information

Install nginx on Windows: http://nginx.org/en/docs/windows.html

Set and configure Ruby on Rails with Nginx: https://www.linode.com/docs/guides/use-unicorn-and-nginx-on-ubuntu-14-04/

Access your home directory in Linux: cd ~/

Unicorn.socks file location: /home/username/example/shared/sockets

Install Active Admin: https://activeadmin.info/documentation.html

Ruby application default config file: /home/username/example/config/example.rb

Thank You!