Explaining Public Key Infrastructure (PKI)

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

Public Key Infrastructure (PKI)

A security architecture developed to increase the confidentiality of information exchanged over an insecure internet.

PKI is asymmetric

PKI Components

Certificate Management System (CMS)

Digital Certificates

Validation Authority (VA)

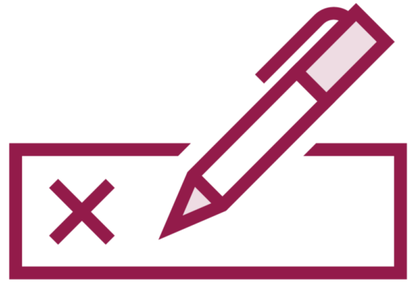
Certification Authority

Registration Authority (RA)

End User

Digital Certificates

A digitally signed statement with a public key and the subject (user, company, or system) name in it.



How Does PKI Work?

How Does PKI Work?

Public Key

Private Key

How Does PKI Work?

Public Key

Private Key

How Does PKI Work?

Public Key

Public Key

Private Key

How Does PKI Work?

Public Key

Public Key

Private Key

How Does PKI Work?

Public Key

Public Key

Private Key

How Does PKI Work?

Public Key

Public Key

Private Key

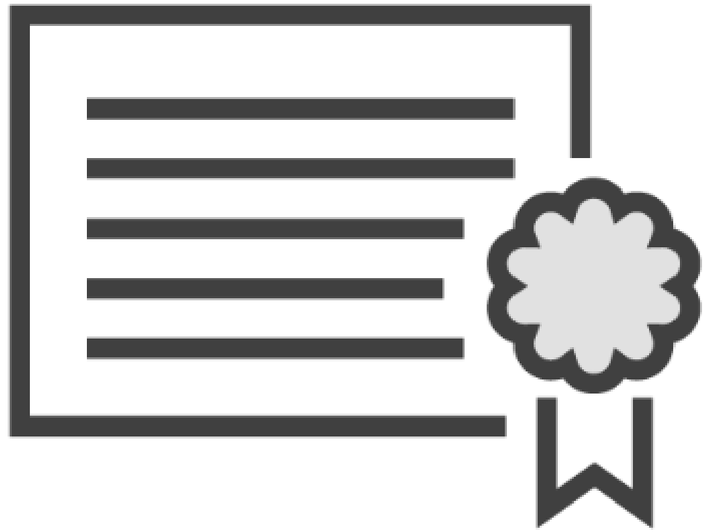
Who to Trust?

Who Do You Trust?

CA (Certificate Authority)

Who Do You Trust?

CA (Certificate Authority)



Who Do You Trust?

Verisign

thawte

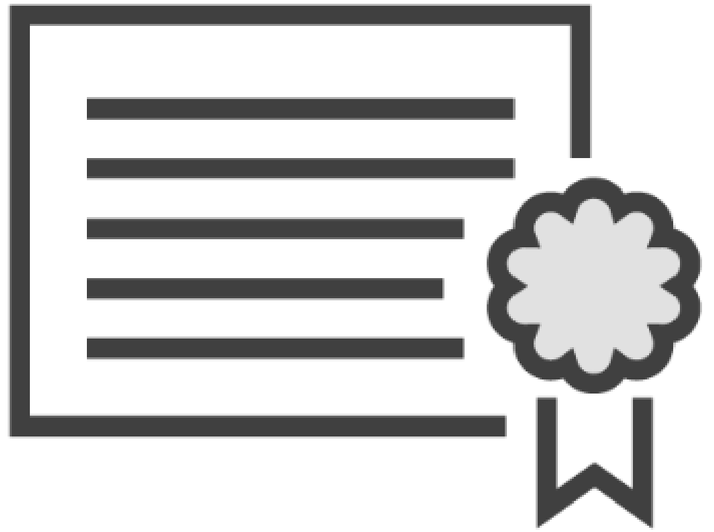
Entrust

GoDaddy

DigiCert

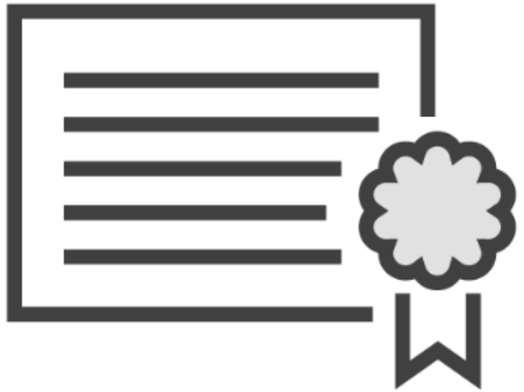
Who Do You Trust?

CA (Certificate Authority)



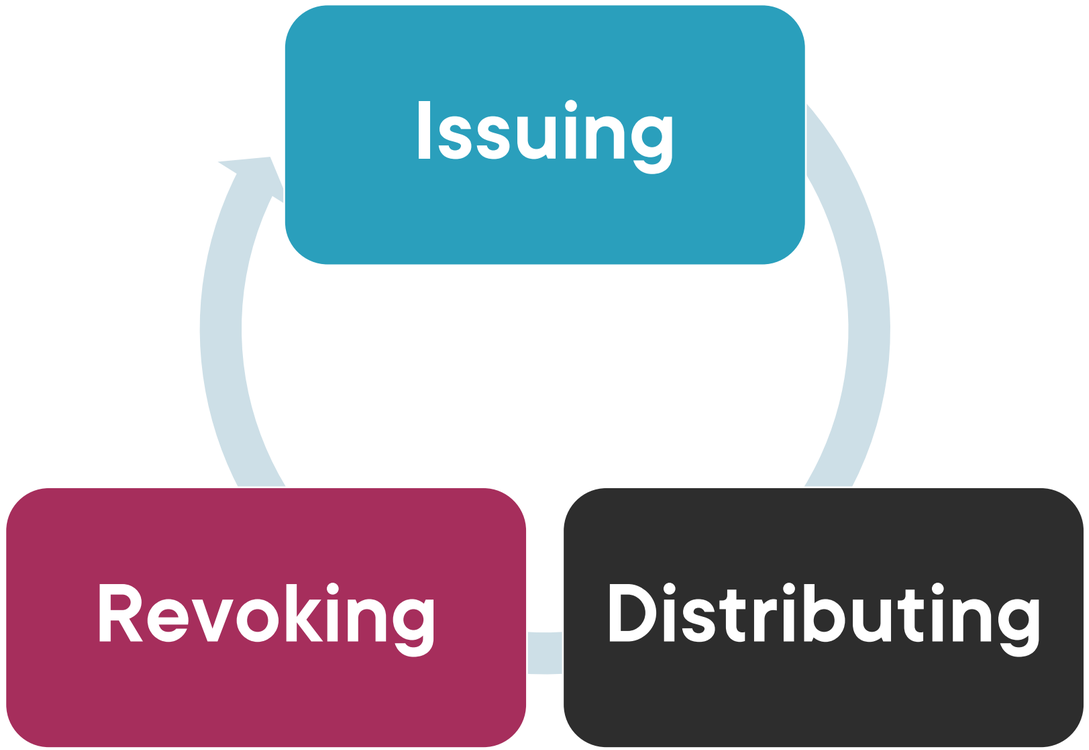
Who Do You Trust?

CA (Certificate Authority)



Who Do You Trust?

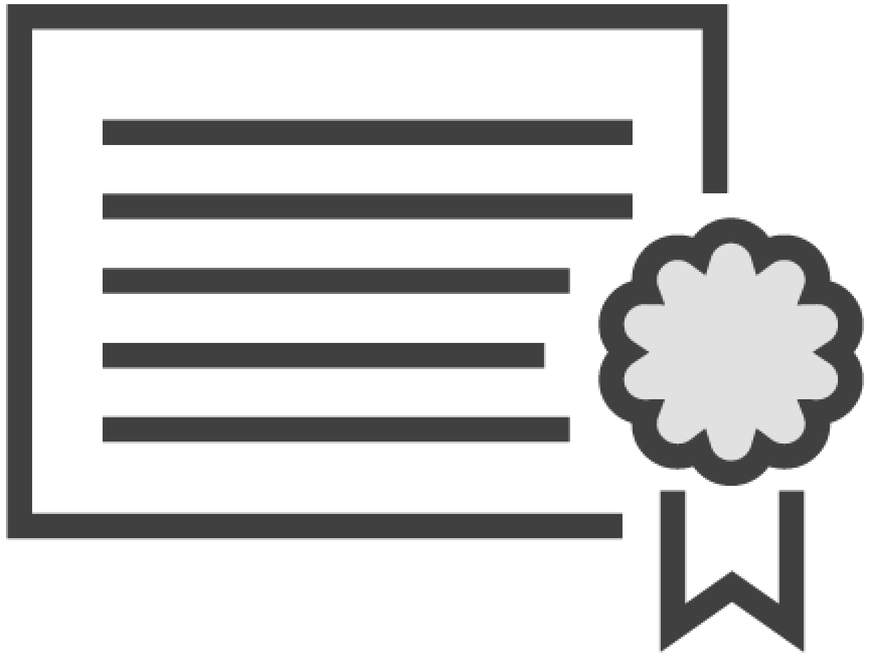
CA (Certificate Authority)



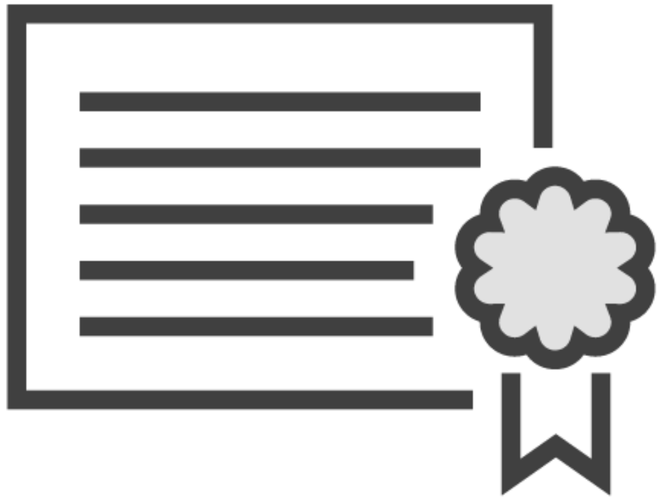
Who Do You Trust?

CA (Certificate Authority)

Your Certificate



Your Certificate



Signed

Self-Signed

Learning Check

Learning Check

- Asymmetric
- Digital certificate
- Certificate Authority
- Registration Authority
- Private key

Up Next:
Outlining Email and Disk Encryption