Transport Layer Security

Ensure confidentiality and authenticity of data in flight

Michael L Perry
qedcode.com
@michaellperry

pluralsight
hardcore dev and IT training

X.509

Subject

cryptofundamentals.com
Michael L Perry
Allen, TX US

Validity

March 16, 2014 through
March 16, 2015

Public Key

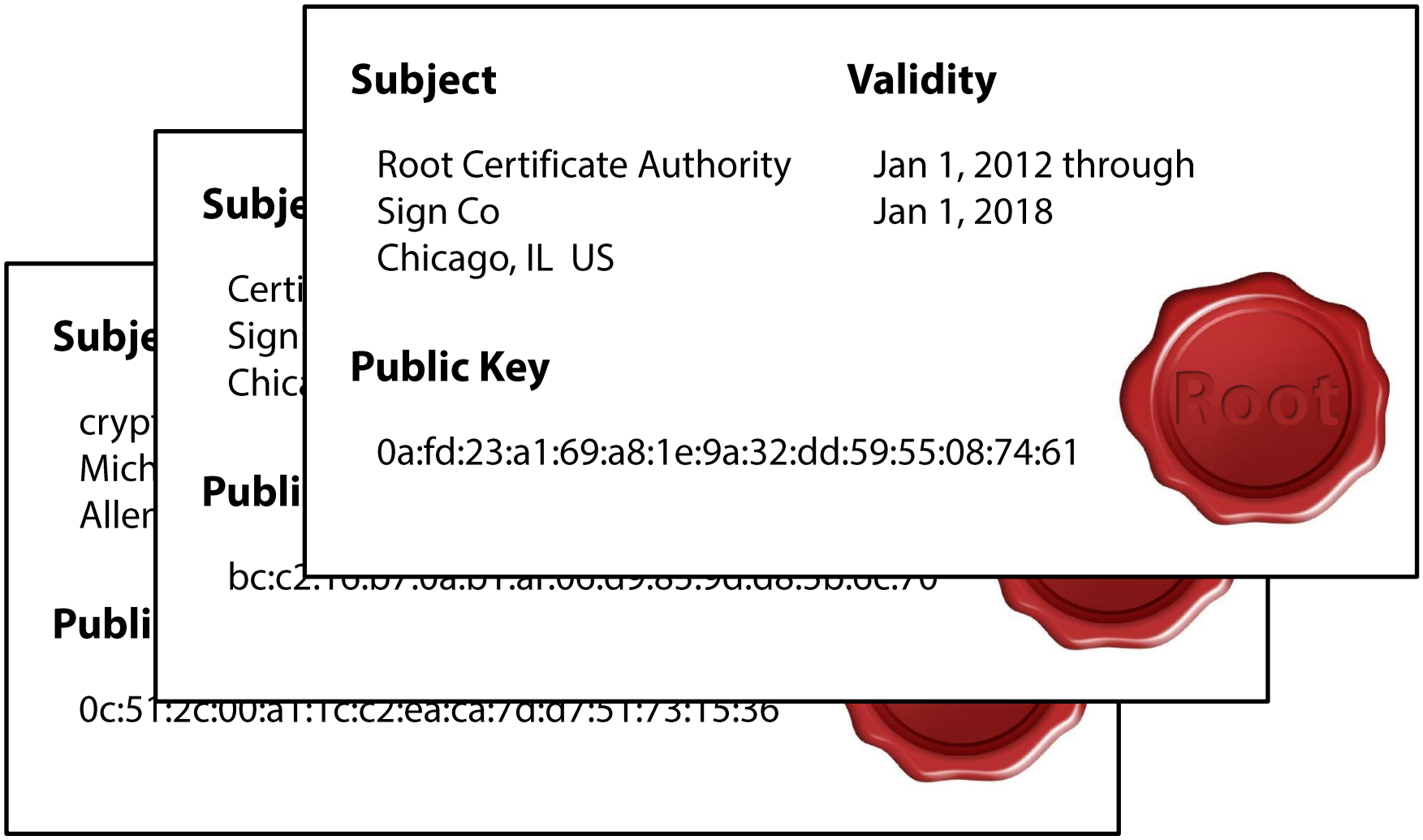
0c:51:2c:00:a1:1c:c2:ea:ca:7d:d7:51:73:15:36

Distinguished Name

- **Country (C)**
- **State (ST)**
- **Locality (L)**
- **Organization (O)**
- **Organizational Unit (OU)**
- **Common Name (CN)**

C=US, ST=Texas, L=Allen, O=Michael L Perry,
CN=www.cryptofundamentals.com

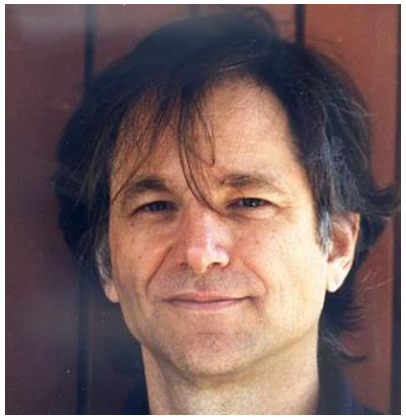
Chain of Trust



RSA Security, Inc.

Ron Rivest

Adi Shamir



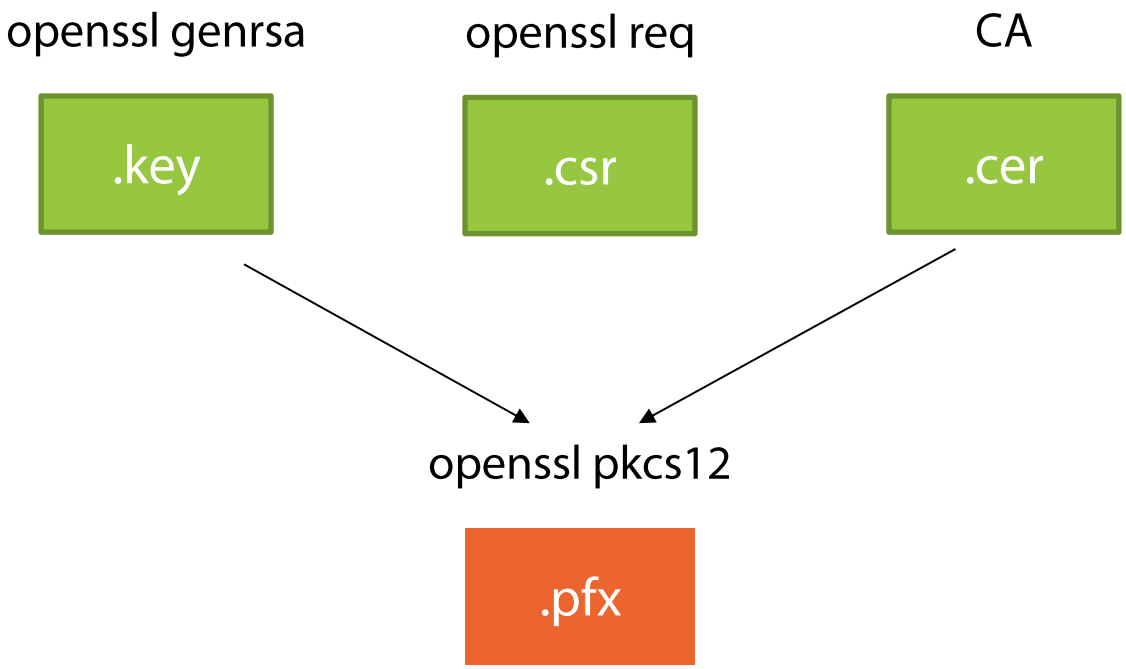
Leonard Adleman

RSA

Public Key Cryptography Standards

- **PKCS #7**
  - Cryptographic Message Syntax
  - Certificates
- **PKCS #10**
  - Certification Request
- **PKCS #12**
  - Personal Information Exchange Syntax
  - Private keys

Common File Formats



Summary

- **Certificate**
  - Subject (distinguished name)
  - Validity (date range)
  - Public key
  - Issuer's signature
- **openssl**
  - genrsa
  - req
  - x509
  - pkcs12
- **Web servers**
  - IIS
  - Tomcat
  - Apache