Week 8: Applications of Cryptography II

Dr. Qublai Ali Mirza

University of Gloucestershire

qalimirza@glos.ac.uk

UNIVERSITY OF GLOUCESTERSHIRE

Overview

Overview

- A digital certificate provides a level of assurance, validated by a trusted third party of the stated owner of the public key and their identity.
- A digital certificate contains the owners public key, essential owner information, and validity time period.
- This information signed by a certification authority using their private key.

Example Digital Certificate

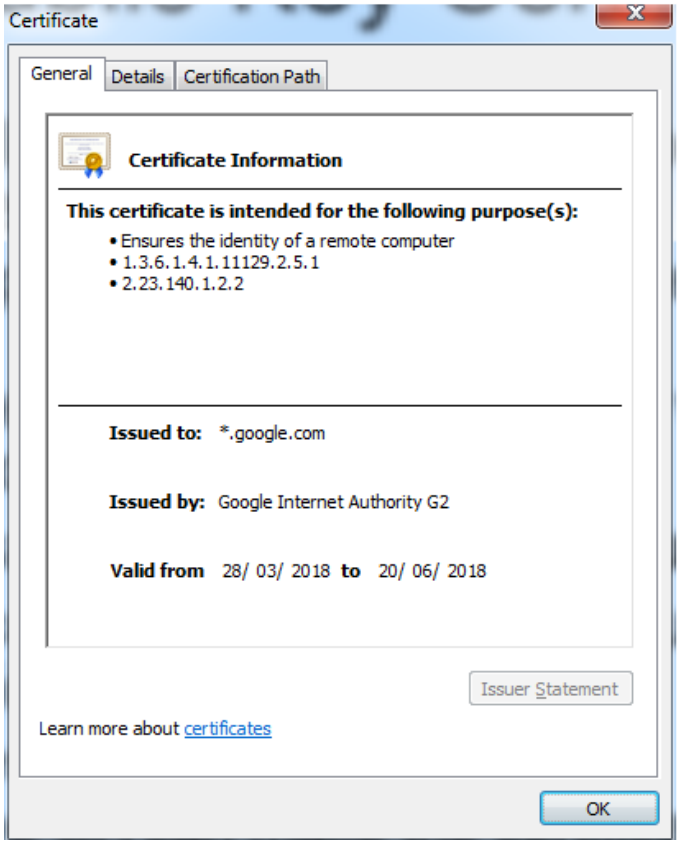

Figure: Example digital certificate

UNIVERSITY OF GLOUCESTERSHIRE

Characteristics

- Digital certificates can be used for encryption, signing, encryption and signing.
- Can also be used for signature and smartcard login. Initial login with a smart card and digitally signing data.
- Intended to prove and validate the identity of the owner of the public key.

Characteristics

- Can be stored in a central repository, providing easy access to requesting parties.
- The certificate contains verified information about the web site it secures in order to assist the user to conform the web site.
- They assert the online identities of individuals, organisations, computers and other hosts on the network.

Public Key Infrastructure (PKI)

- The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies and procedures to create, manage, distribute, implement, store and revoke digital certificates.
- The PKI is used to manage the digital certificates.
- The public key certificate creators have three important roles.
- Certificate creation, certificate revocation (certificate revocation list, CRL) and certificate trust anchor.

PKI overview

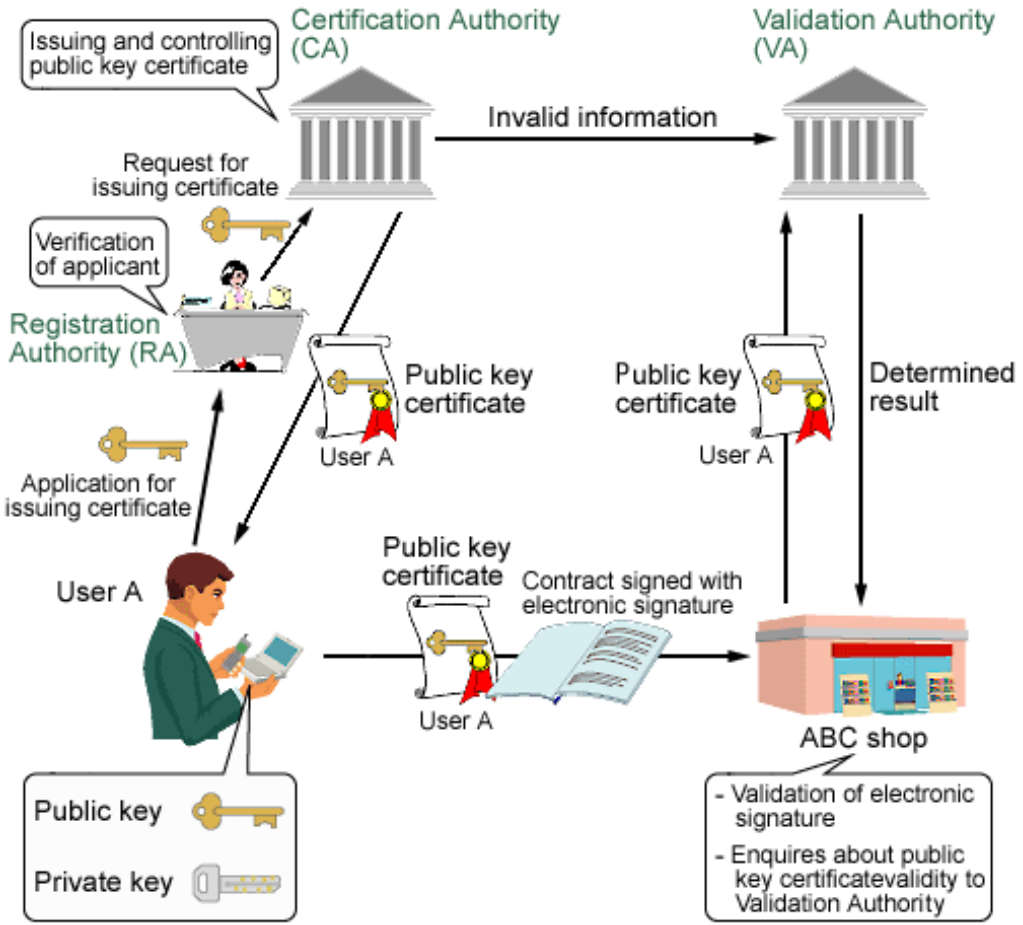

Figure: Public Key Infrastructure overview, from [**RumiPKI**]

Components

- A certificate management system, responsible for the generation, distribution, storage and the verification of certificates.
- One or more directories where the certificates and public keys are held.
- The directories need to be held in a secure location to store and index the keys.

Components

- A Certificate Authority (CA). They issue and validate digital certificates.
- A Registration Authority (RA). Verifies the subject identity.
- RAs reduce the workload on CAs due to the amount of work involved in validating the subject. The RA may also be the CA.
- A CA may also be called a trusted third party.
- The Validation Authority (VA) verifies the digital certificate of a subject (users, organisations or systems).

How PKI components work together

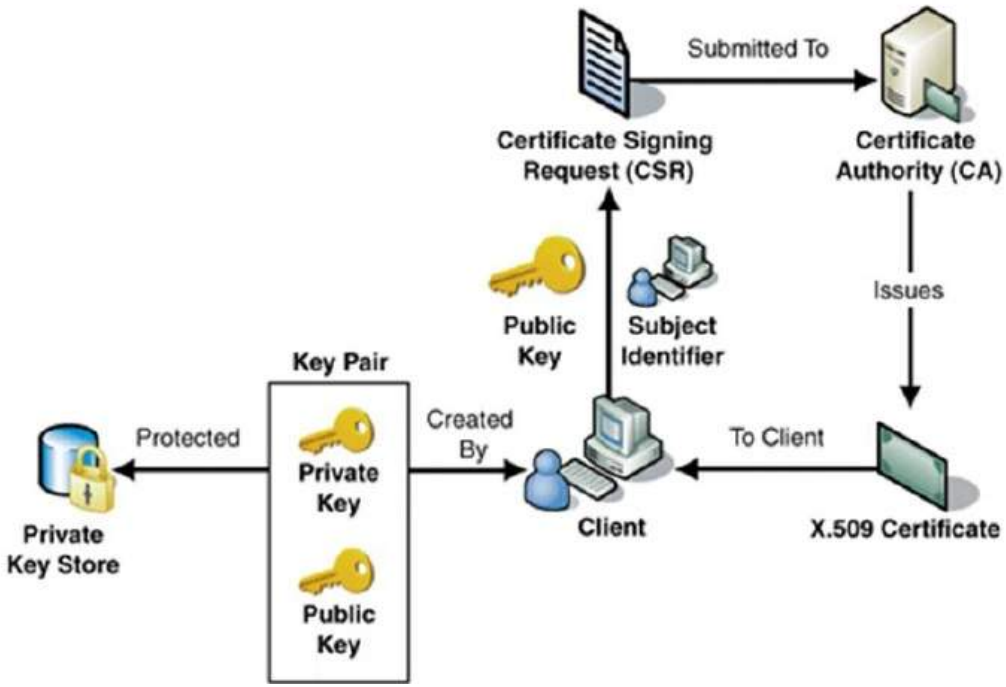

Figure: How digital certificates work in PKI, from [**RumiPKI**]

Data at rest

- Encryption can be applied to protect two main categories of data, namely:
  - Data at rest: Data which is located on a persistent storage
  - Data in transit: Data which is transmitted from one device to the next
- For our lecture this week, we will be looking at *data at rest*

Examples of data at rest

- Typical examples of data at rest include:
  - Database files
  - Access control list (ACL)
  - Files on a server
  - Etc

Key considerations

- Trust
  - Asymmetric encryption used
  - Required for key access and management (*why?*)
- Data security
  - Symmetric encryption used (*why?*)
  - Decreases the risk of the key being compromised

Encryption schemes

- Encrypting data at rest can be done either through:
  - Server-side
  - Client-side

Server-side encryption

- Done at the server-side of a network
- Typically done through using:
  - Keys managed by the *service provider*
  - User-managed keys

Server-side encryption

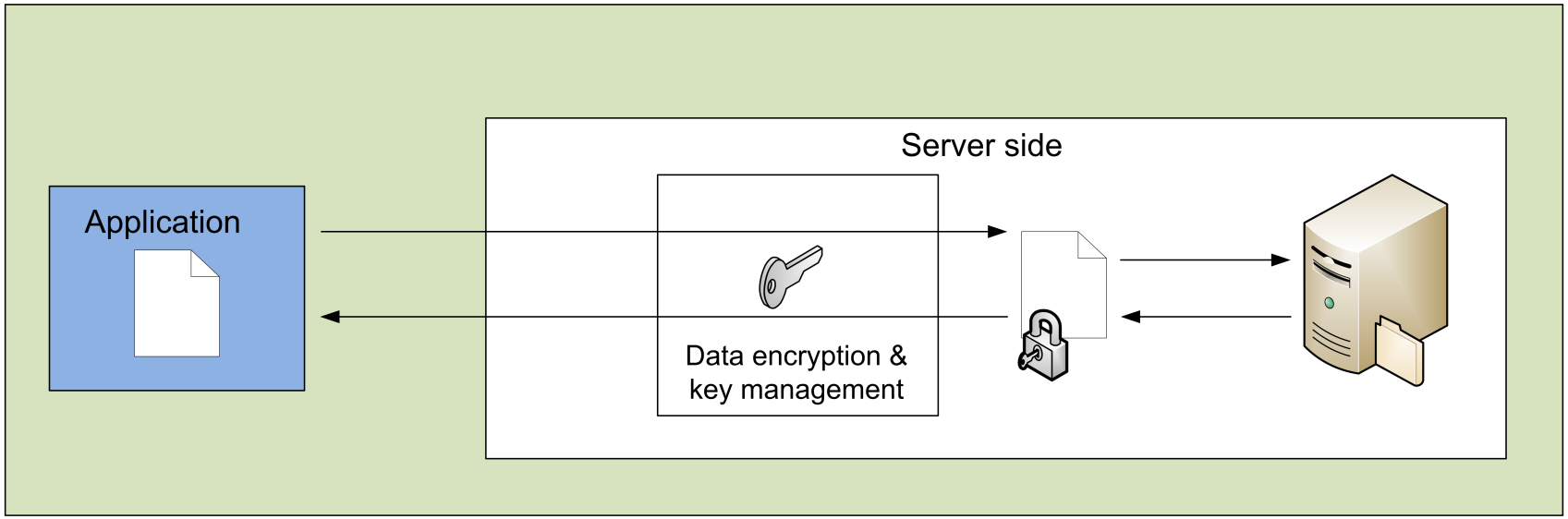

Figure: Server-side encryption

Encryption using provider-managed keys

- Data encryption provided by the *service provider*
- User identifies the resource(s) to be encrypted
- Key management and storage provided by the service provider
- Advantages
  - Easy to set up
  - Low overhead on the client side
- Disadvantages
  - Lack of user control
  - Difficult to set up in *federated* environments

User-managed keys

- User manages *all* aspects of key management
- Encryption still conducted on the server side
- User responsible for key management and lifecycle
- Advantages
  - User has complete control of the keys
  - Available support for federated services
- Disadvantages
  - Additional overhead in terms of key management
  - Requires additional back-up solutions

Client-side encryption

- Encryption/decryption done on the client-side
- The server only stores the encrypted version of the data
- *Question:* What are the:
  - Advantage (s);
  - Disadvantage (s) of this approach?

Client-side encryption

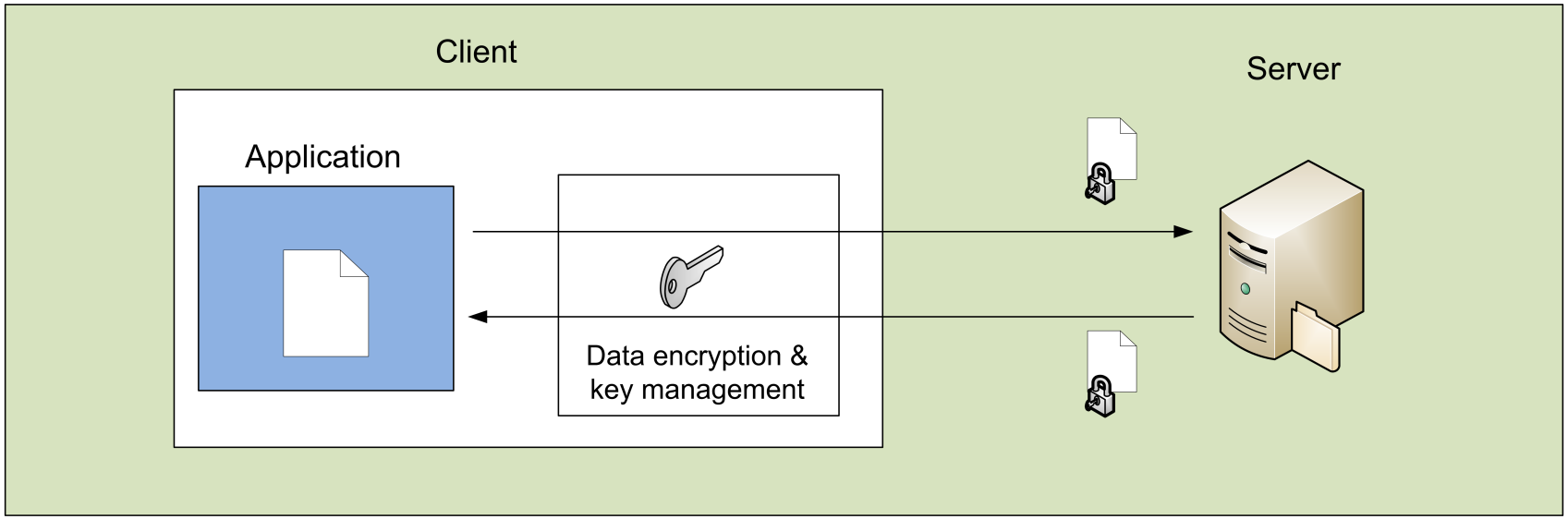

Figure: Client-side encryption

Bringing it all together

- Today we looked at *applications of cryptography*
- We looked at how digital signatures work
- We also at key management and distribution
- Next week: *Applications of Cryptography III*

References I

Q & A