Design and Analyze Secure Networked Systems 3

Prof. Edward Chow @ Colorado Univ.

Note by waegaein@github.com

Principle of Least Privileges

- Every program and user of the system should operate using the lest set of privileges necessary to complete the job.
- Unintentional, unwanted, or improper uses of privileges are less likely to occur.
- It limits the damage from error, accident, or break-in.

E.g.

- User's home directory
  - drwx------.
  - Only owner can access.
- Sharing documents with read-only permission
  - -rw-r--r--.
  - Only owner can write.
- Append-only permission for log file
  - drwxr-sr-x+
  - Logs cannot be overwritten.
  - Plus means extended access control like append-only.

Principle of Adequate Protection

- Computer items must be protected only until they lose their value.
- PII (Personally Identifiable Information) never lose their values, thus they need to be encrypted in storage and in transmission.

Certificate Signing and Installation

1. Service provider requests server certificate to certificate authority (e.g. Symantec) for signing.
2. Certificate authority hashes the certificate content to generate message digest. (e.g. SHA-256)
3. Certificate authority encrypts the digest using its private key to generate signature.
4. Certificate authority append the signature along with certificate content to form a digital certificate.
5. Certificate authority sends the digital certificate back to the service provider.
6. Service provider installs the digital certificate on its web servers.

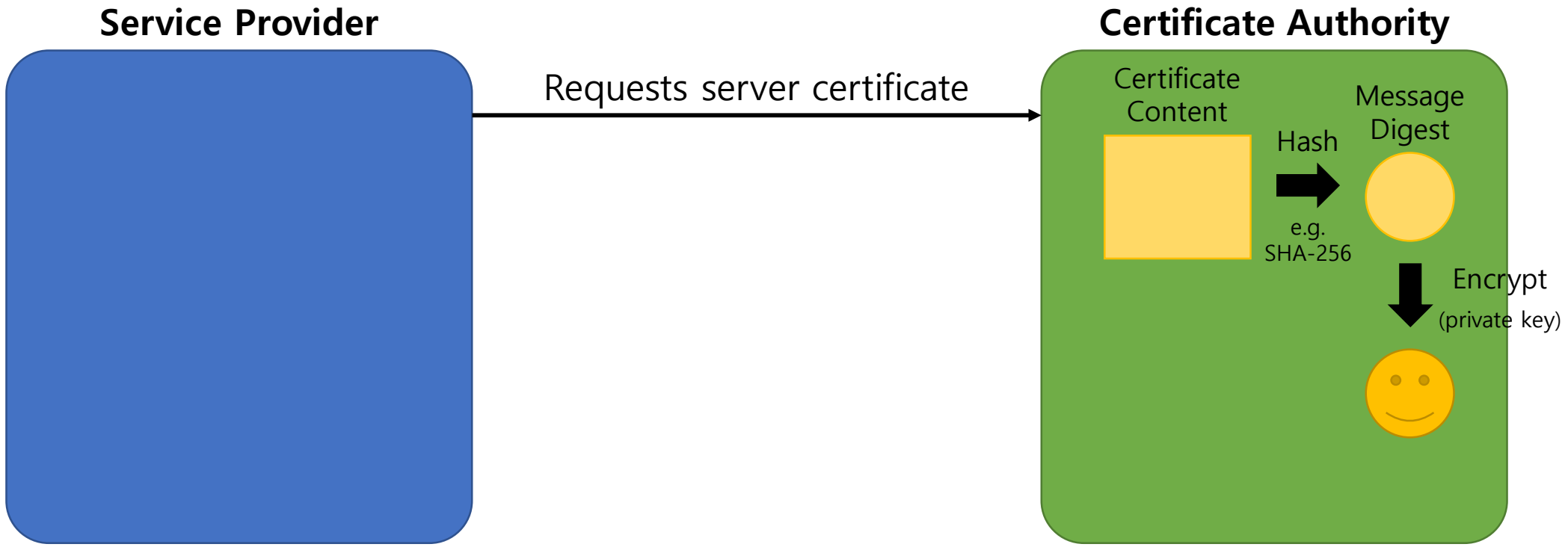
Certificate Signing and Installation

Certificate Signing and Installation

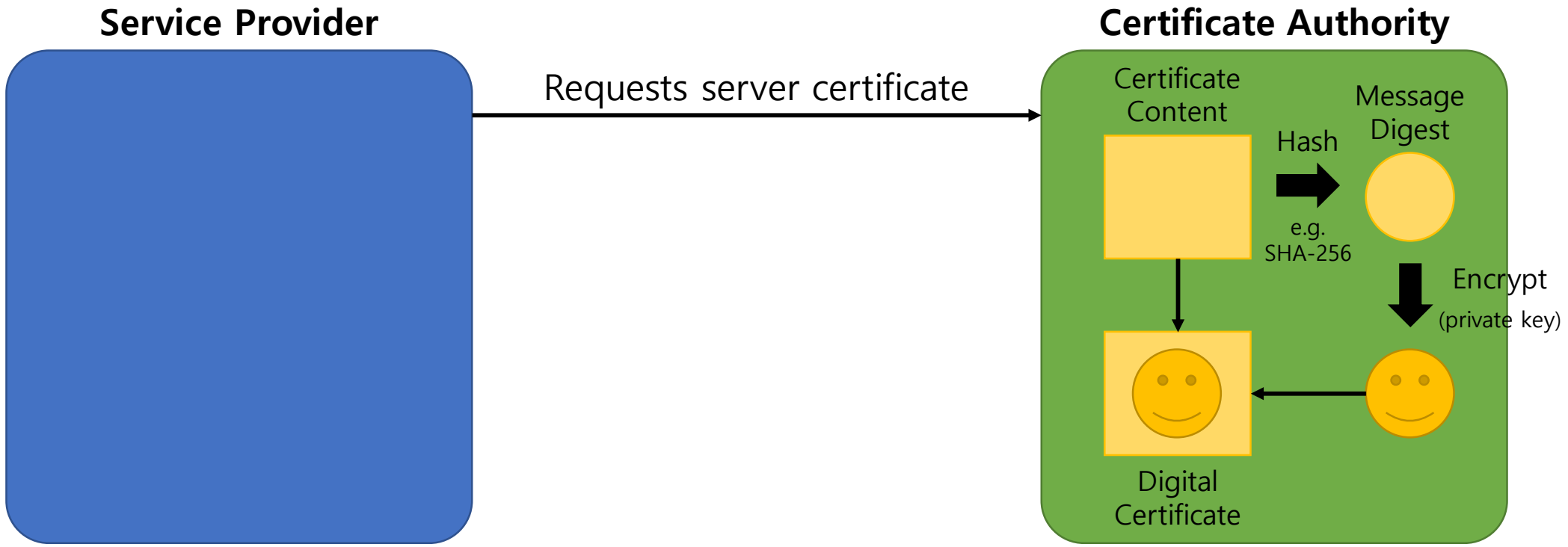
Certificate Signing and Installation

Certificate Signing and Installation

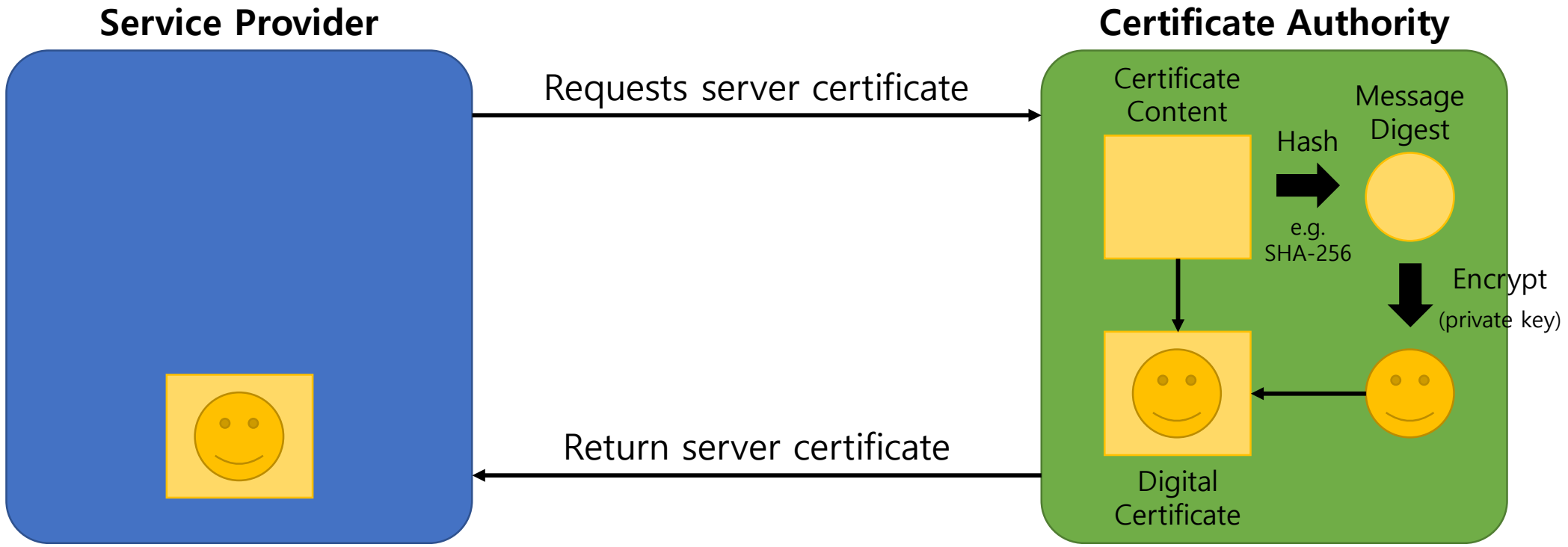
Certificate Signing and Installation



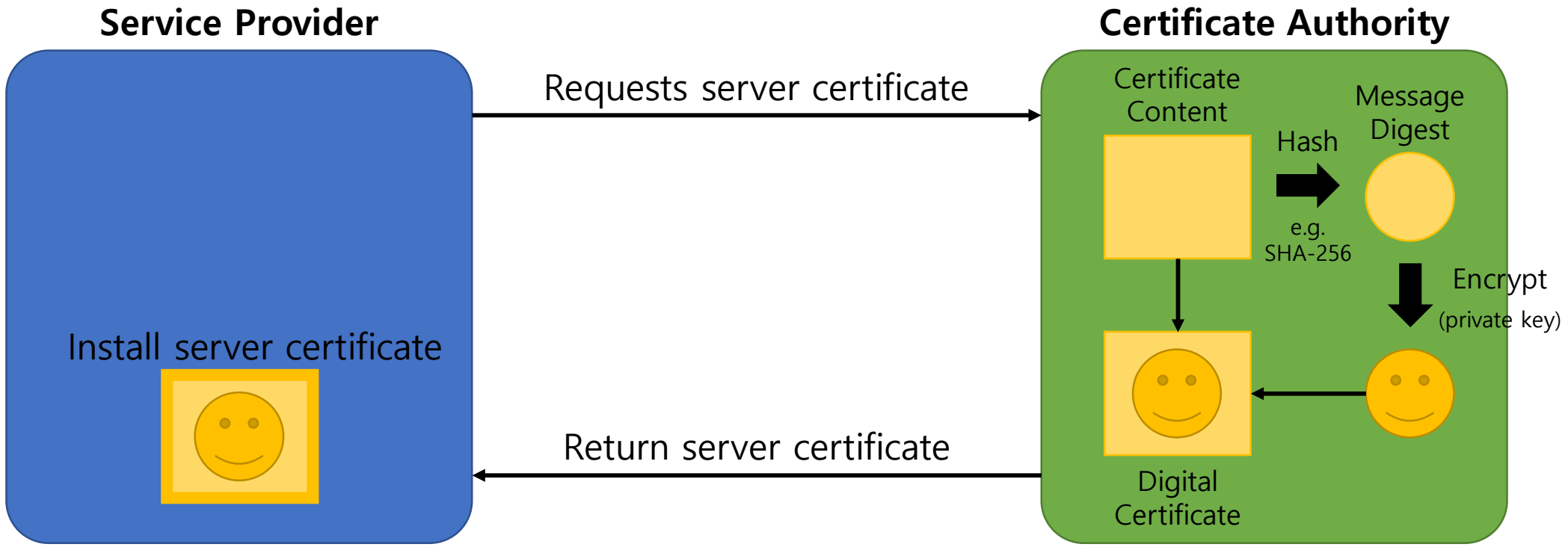
Certificate Signing and Installation



Certificate Signing and Installation



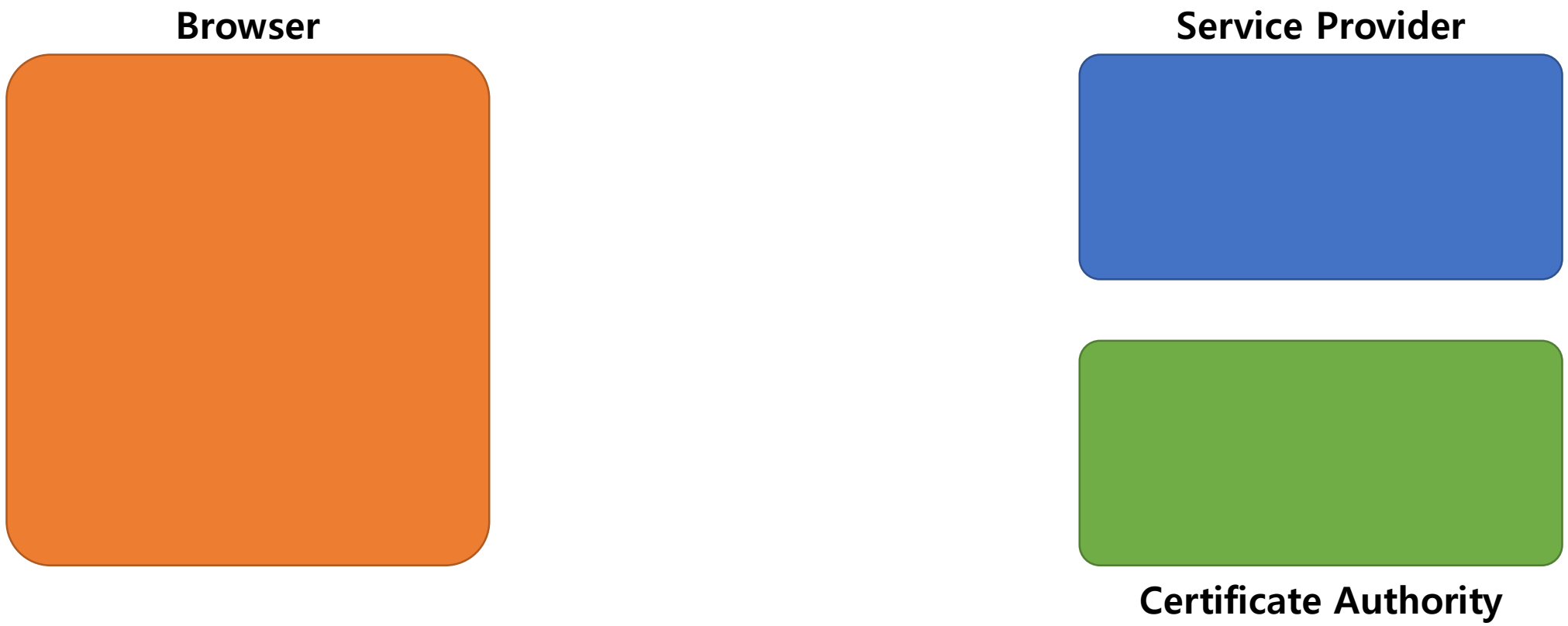
Certificate Signing and Installation



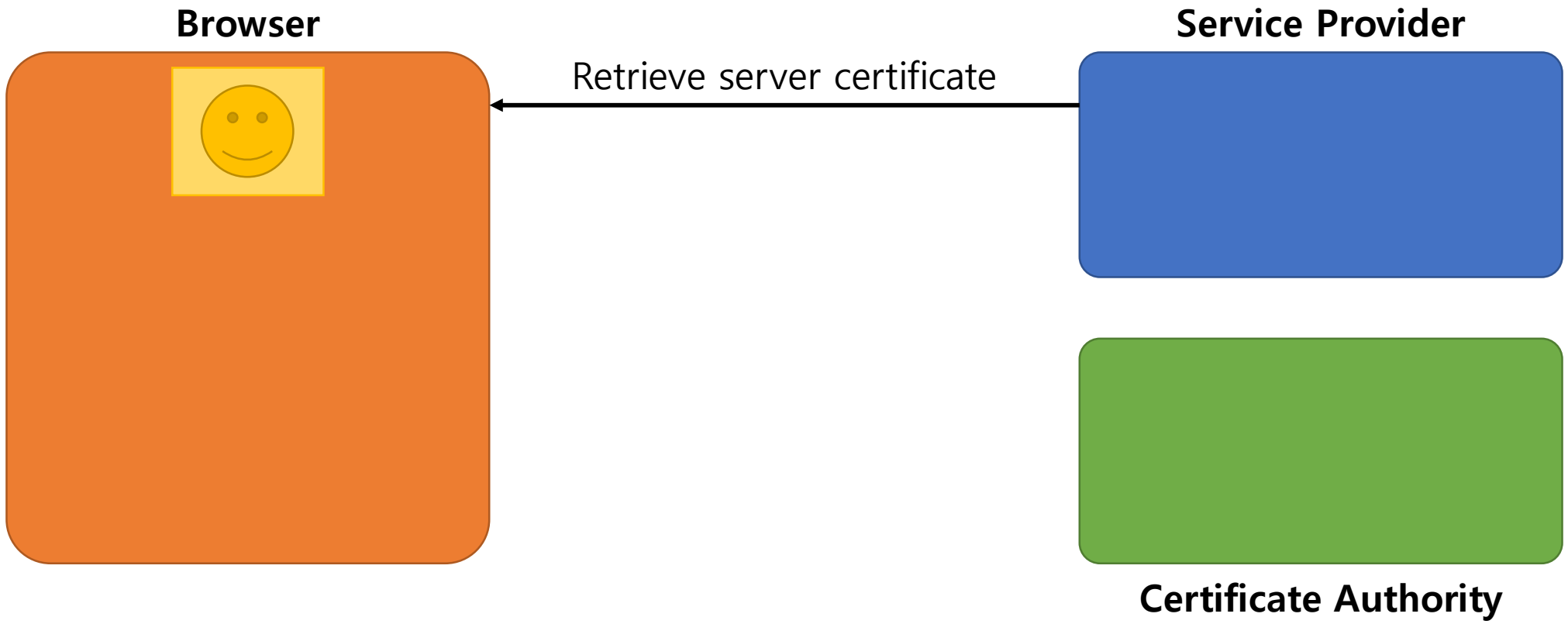
Certificate Verification

1. Browser retrieves digital certificate from web server.
2. Browser extracts signature from the digital certificate.
3. Browser retrieves public key of certificate authority based on issue field in certificate.
4. Browser decrypts the signature to restore the message digest.
5. Meanwhile, the browser hashes certificate content to generate a message digest.
6. If the two digests are identical, the server is verified and good to go.
7. If those are different, it is considered to be altered.

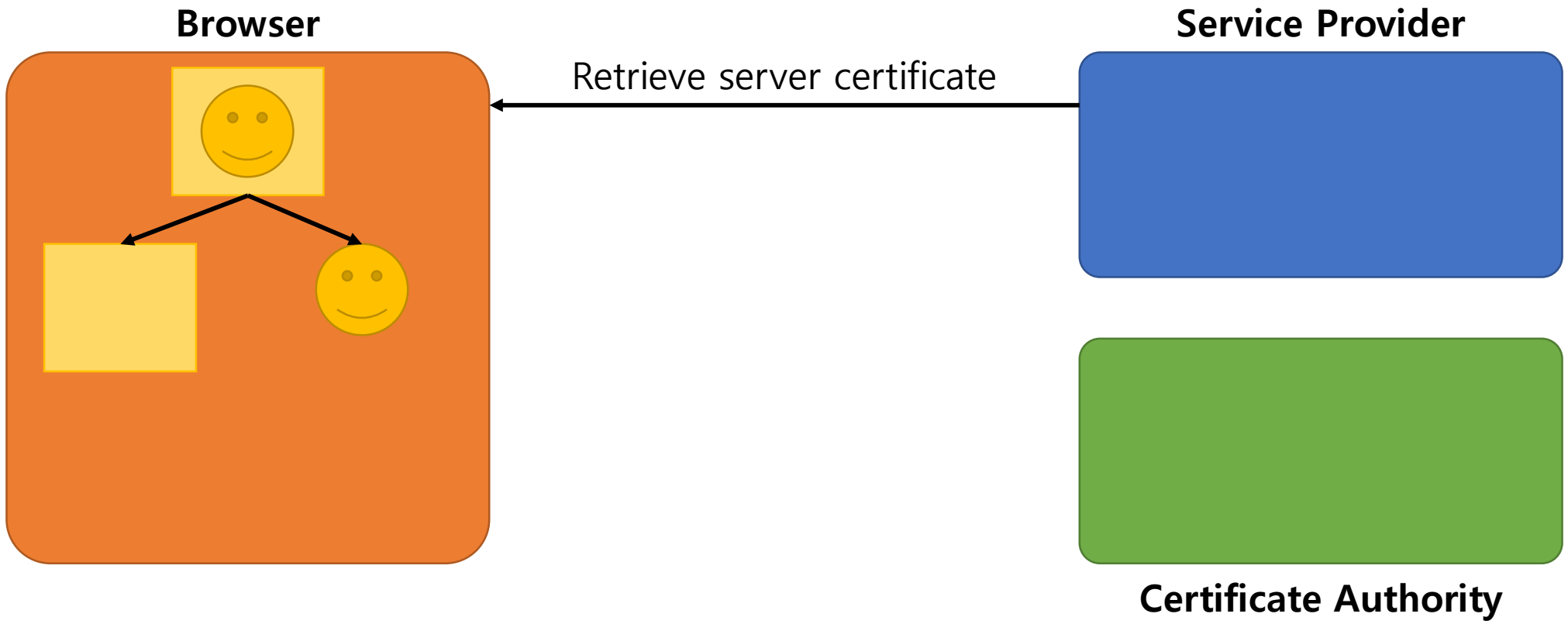
Certificate Verification



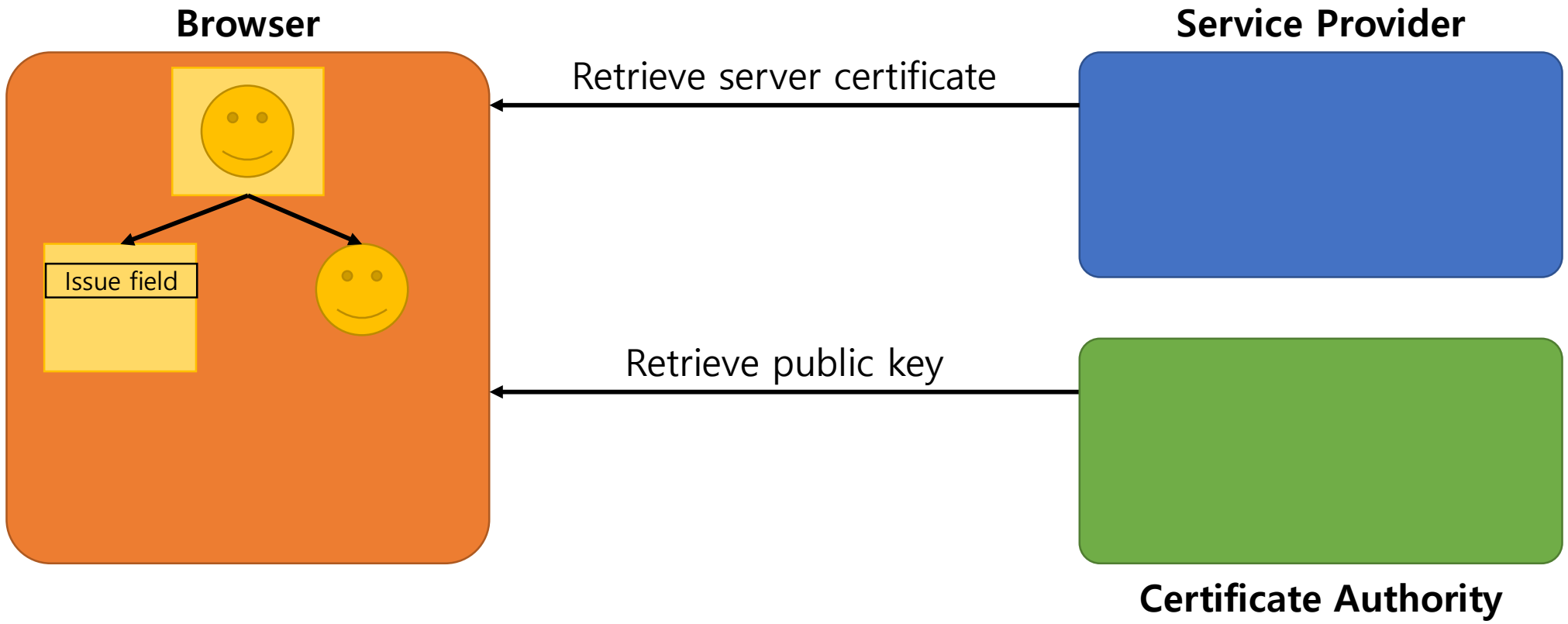
Certificate Verification



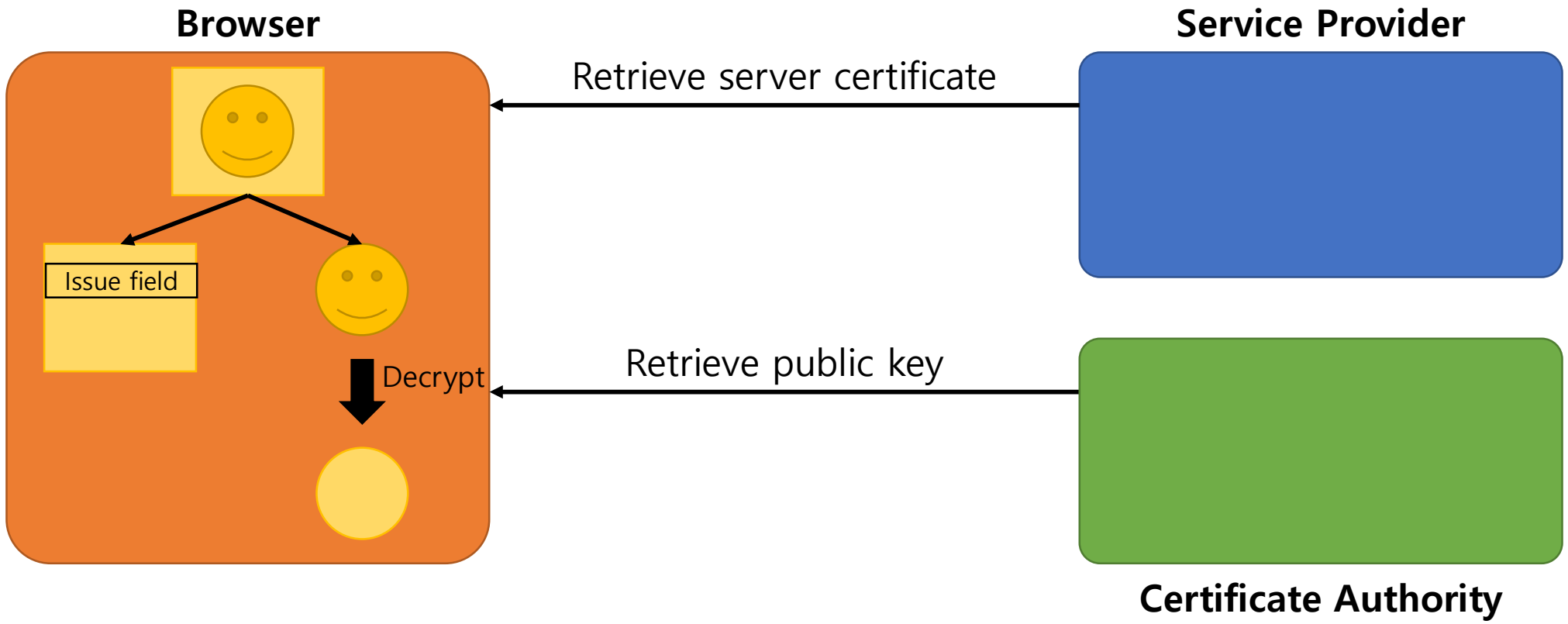
Certificate Verification



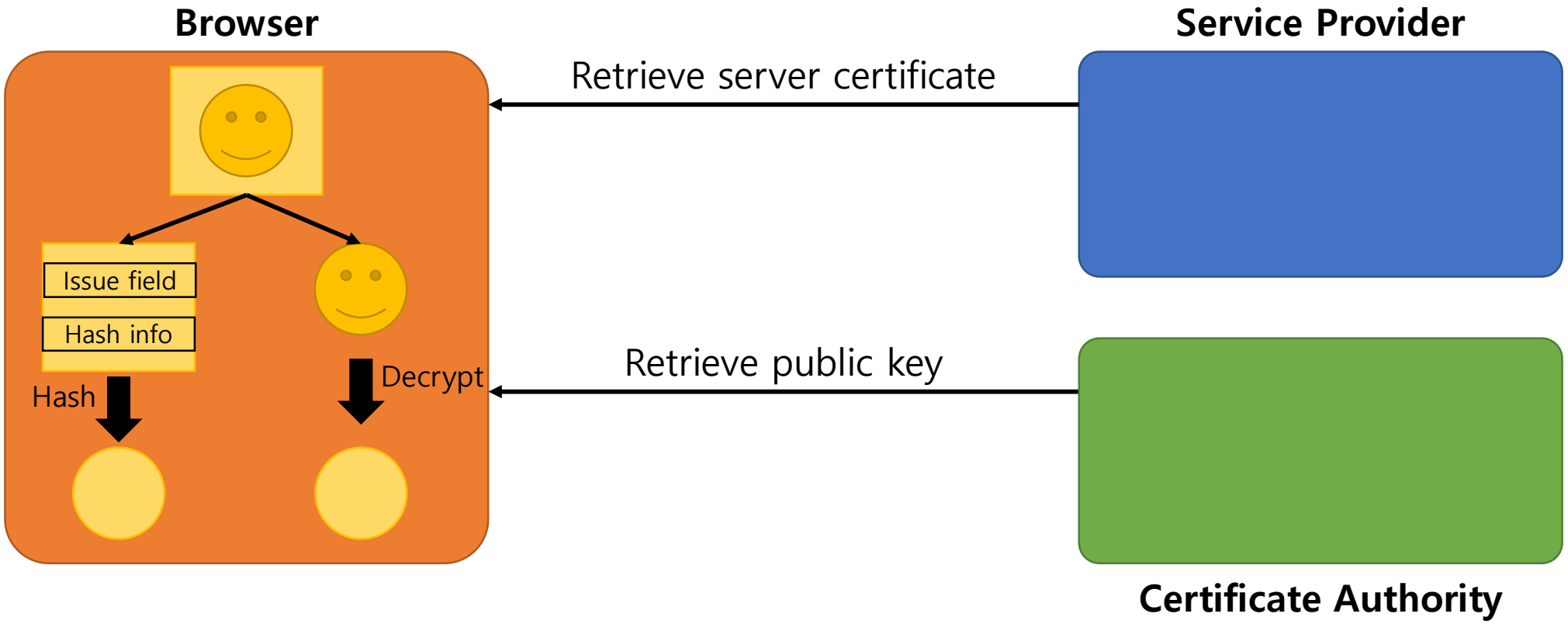
Certificate Verification



Certificate Verification



Certificate Verification



Certificate Verification