2023-1 인터넷 보안
특강

Term Project: DNS signing

Team 4

2023-21943 장진화
2022-20267 이수현
2022-22025 송지원

Overview

DNS maps domain name to IP address
→ Provides IP address for a domain name

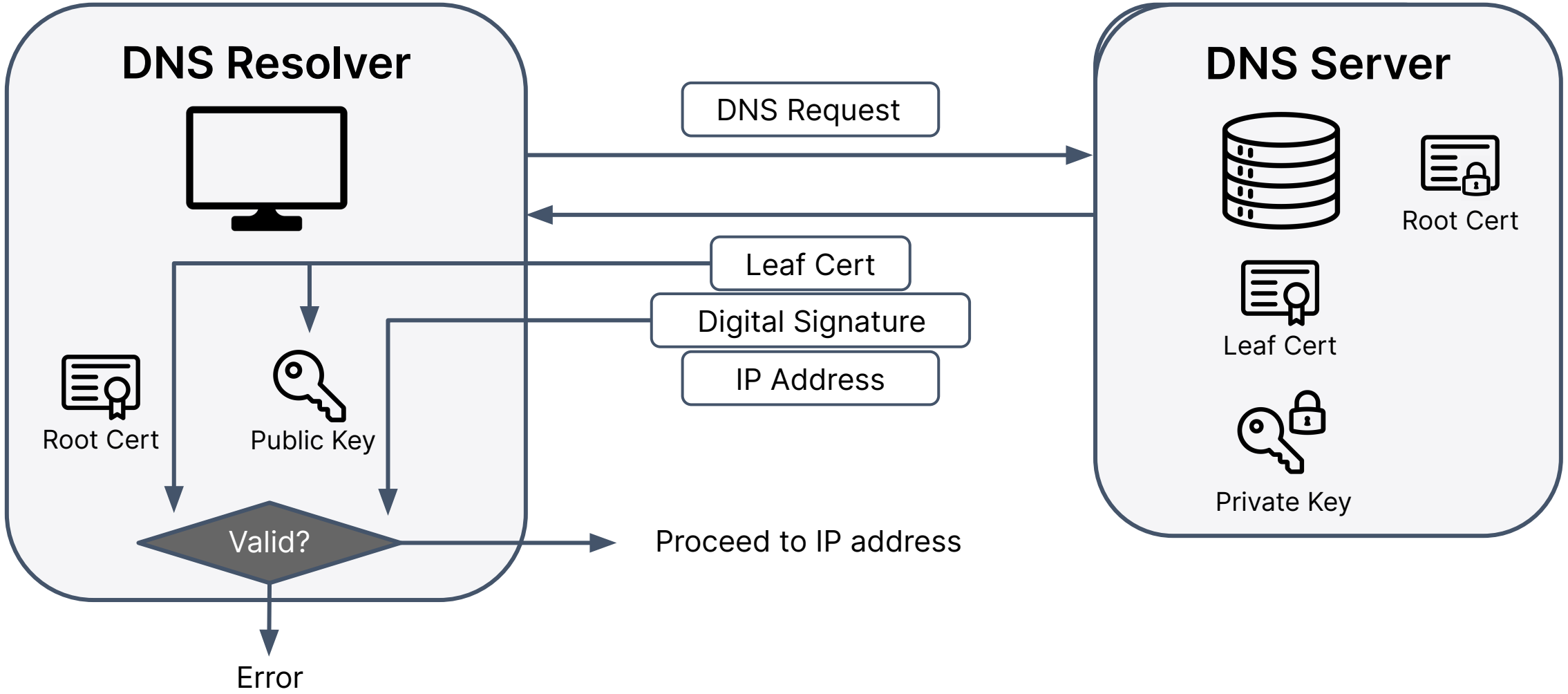
.Components

- Client App
  - Requesting host

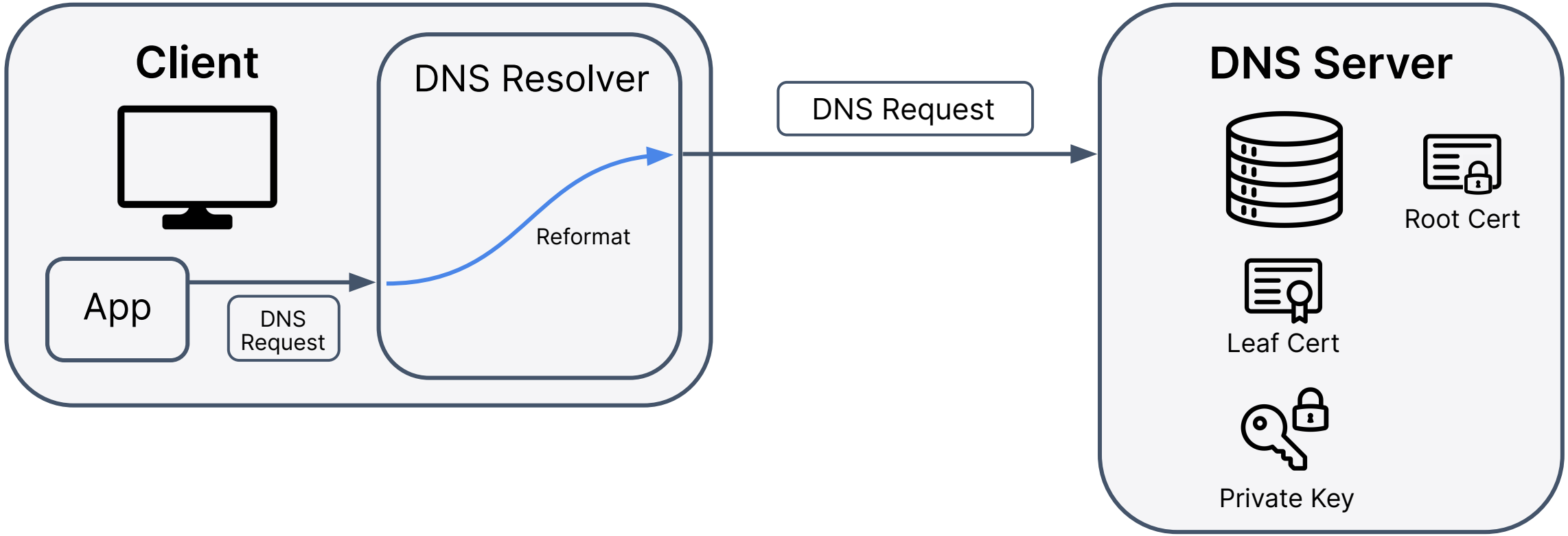
- Local DNS Resolver
  - Works for client application
  - Reformats Client app's DNS request
  - Reformats DNS server's response
  - Performs Signing & Certificate Verification on DNS server responses

- (Authoritative) DNS Server
  - Responds with corresponding IP address
  - Adds signature to response message using a leaf private key
  - Delivers a leaf certificate

Overview

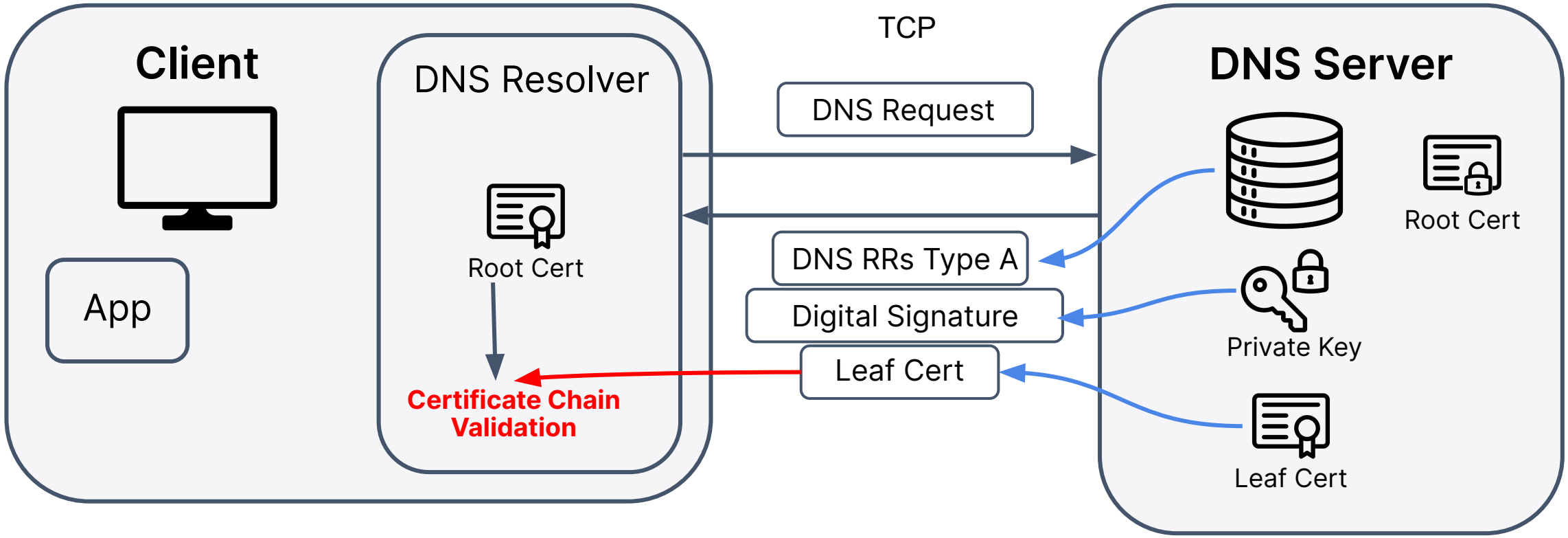

DNS Resolver
DNS Request
DNS Server
Root Cert
Leaf Cert
Digital Signature
IP Address
Leaf Cert
Root Cert
Public Key
Private Key
Valid?
Proceed to IP address
Error

DNS Request


Client
App
DNS Request
DNS Resolver
Reformat
DNS Request
DNS Server
Root Cert
Leaf Cert
Private Key

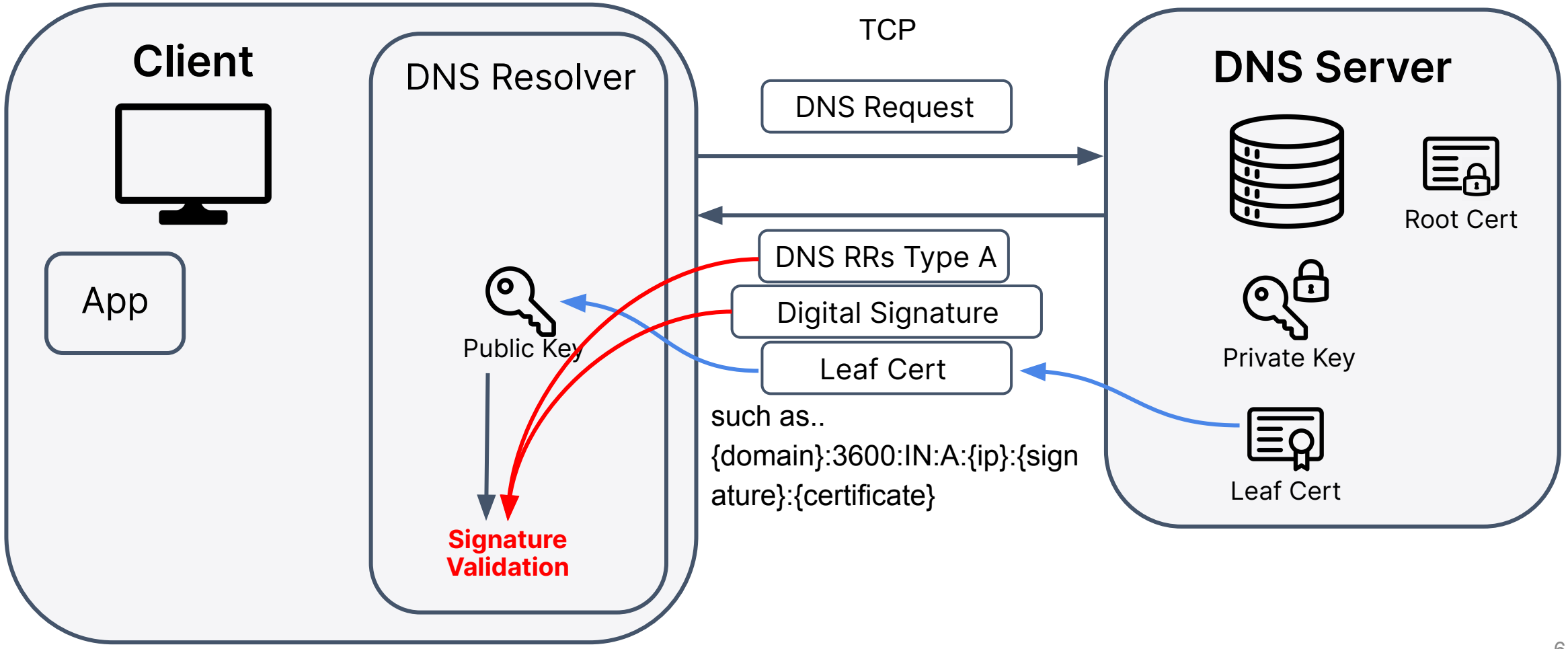
DNS Response

Certificate Chain Verification

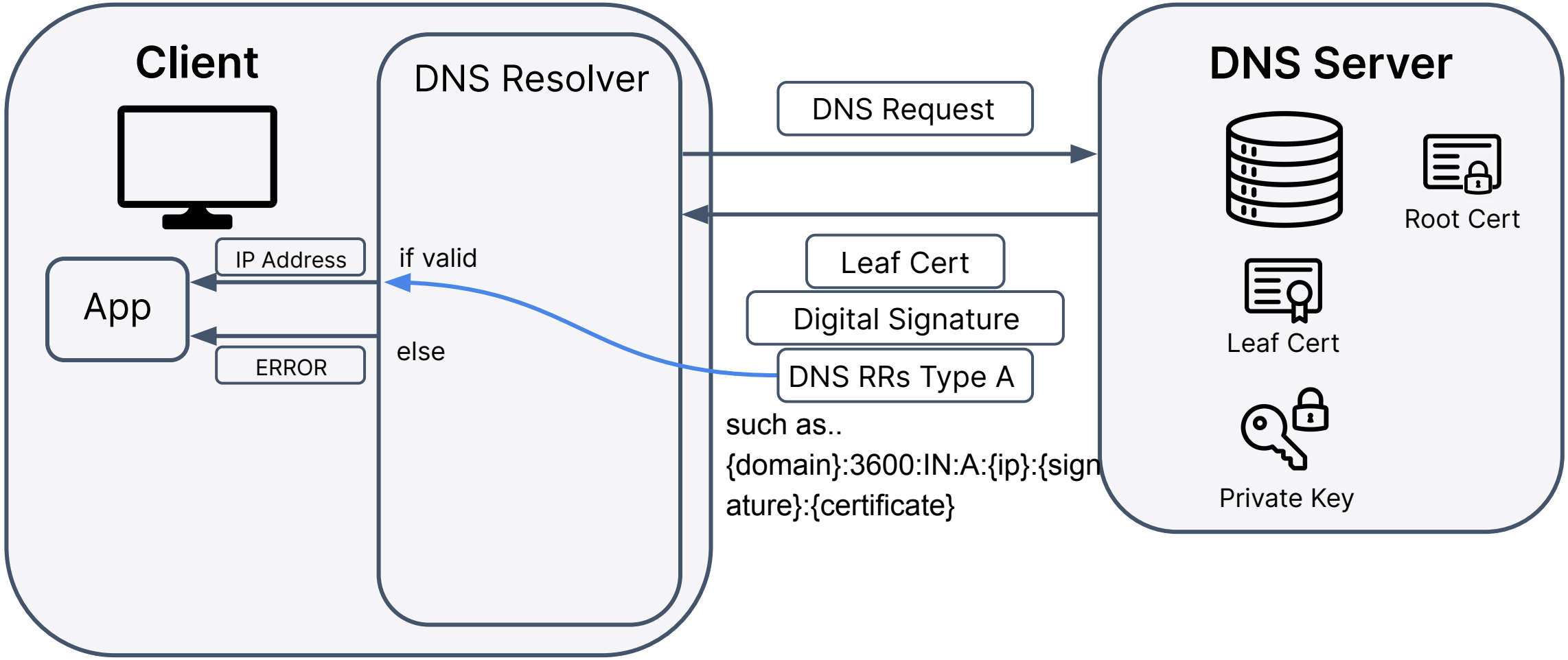


DNS Response

Signature Verification



DNS Request


Client
DNS Resolver
DNS Server
DNS Request
Root Cert
Leaf Cert
Digital Signature
DNS RRs Type A
such as..
{domain}:3600:IN:A:{ip}:{sign
ature}:{certificate}
Leaf Cert
Private Key
App
IP Address
ERROR
if valid
else

Test

Create several certificates & private keys and random assign its roles.

. A Cert & B Cert : issued by trusted Root CA.

. C Cert : issued by unknown CA.

Scenario	Message signed By	Certificate Delivered	Certificate Chain Verification	Signing Verification
1	A Cert	B Cert	Success	Fail
2	A Cert	A Cert	Success	Success
3	C Cert	C Cert	Fail	N/A

Performance - Plain text

average time : 10.21 ms

std_dev : 0.92 ms

msg_len : 39

message : “www.google.com:3600:IN:A:172.217.161.196”

NAME	TTL	CLASS	TYPE	DATA
www.google.com	3600	IN	A	172.217.161.196

Performance - vs Private Key Algorithm

hci lab
SEOUL NATIONAL UNIVERSITY

Plain Text

- average time : 10.21 ms
- std_dev : 0.92 ms
- msg_len : 39

key 1. 256 bits (ECC)

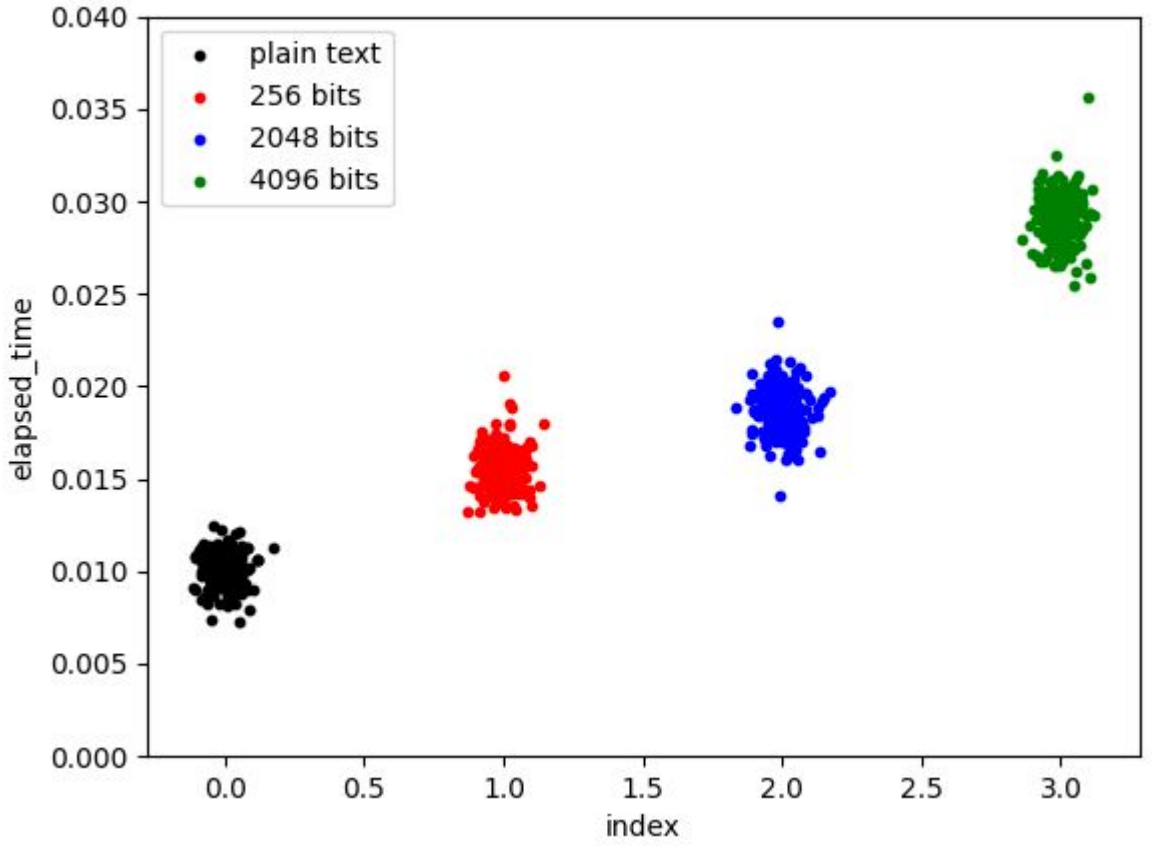
- average time : 15.59 ms
- std_dev : 1.11 ms
- msg_len : 1456

key 2. 2048 bits (RSA)

- average time : 18.66 ms
- std_dev : 1.24 ms
- msg_len : 2088

key 3. 4096 bits (RSA)

- average time : 29.20 ms
- std_dev : 1.34 ms
- msg_len : 2868



Performance - HASH

hci lab
SEOUL NATIONAL UNIVERSITY

Plain Text

- average time : 10.21 ms
- std_dev : 0.92 ms

hash 1. 160 bits (sha1)

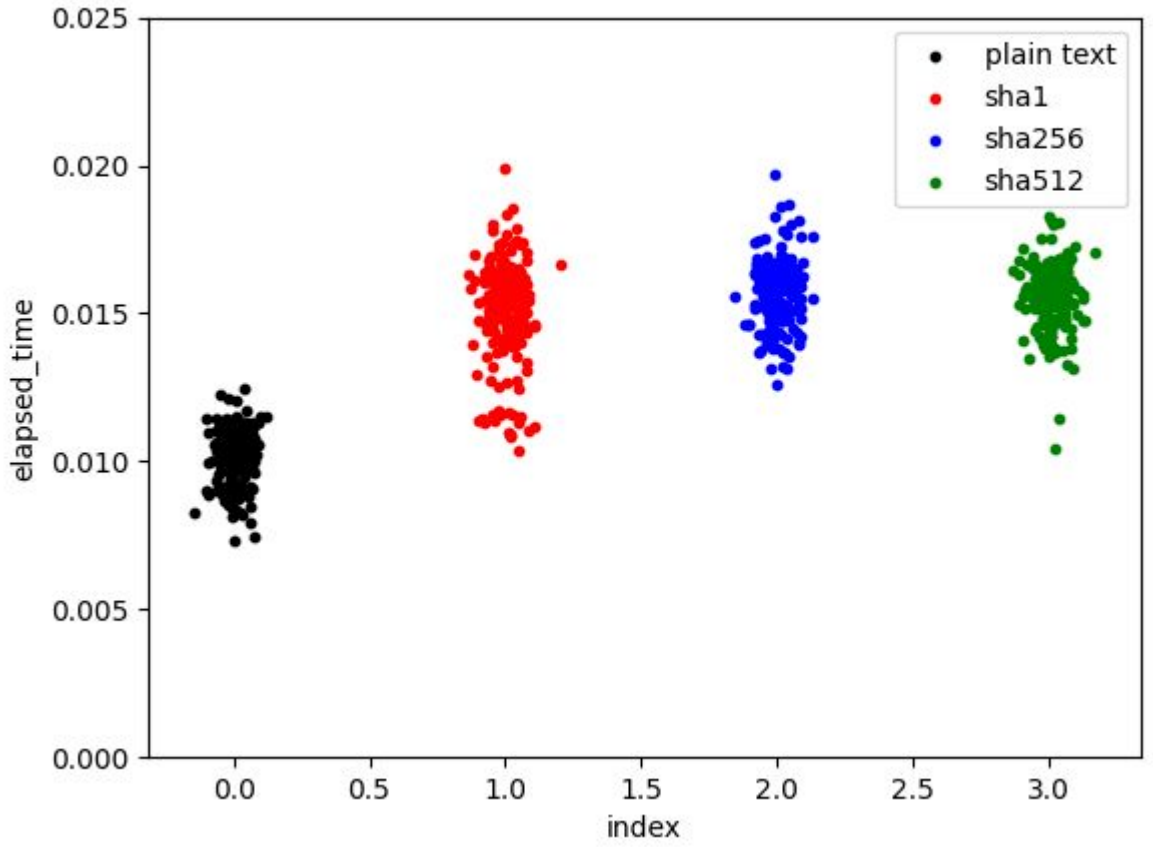
- average time : 15.12 ms
- std_dev : 1.65 ms

hash 2. 256 bits (sha256)

- average time : 15.62 ms
- std_dev : 1.13 ms

hash 3. 512 bits (sha512)

- average time : 15.64 ms
- std_dev : 1.06 ms



Github Link

hci lab
SEOUL NATIONAL UNIVERSITY

https://github.com/Sodaking/2023-insec.git