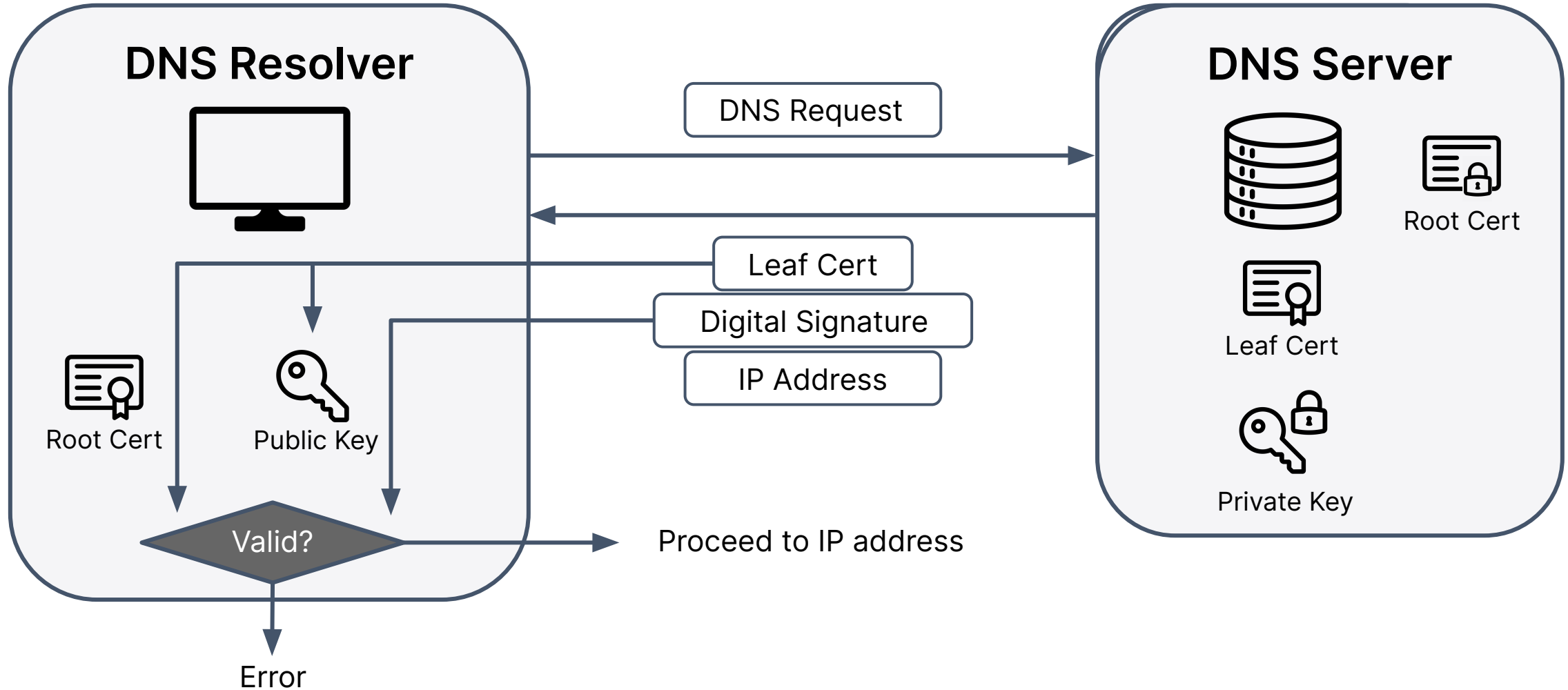


2023-1 인터넷 보안
특강

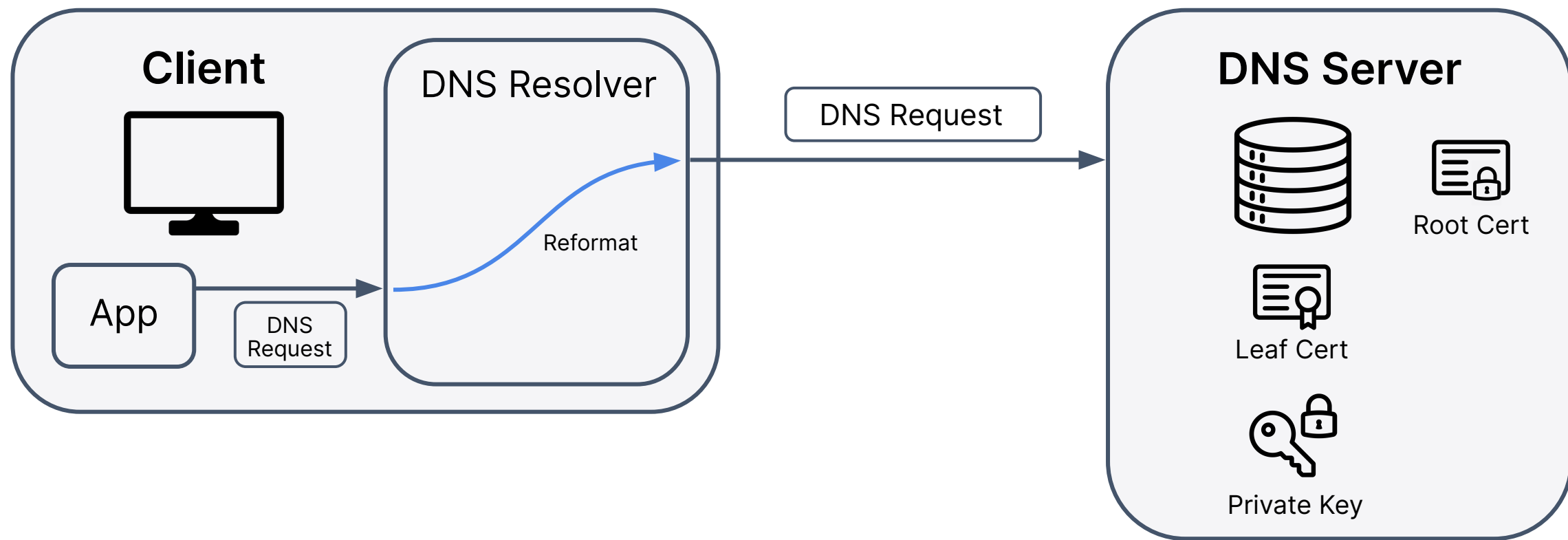
Term Project: DNS signing

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

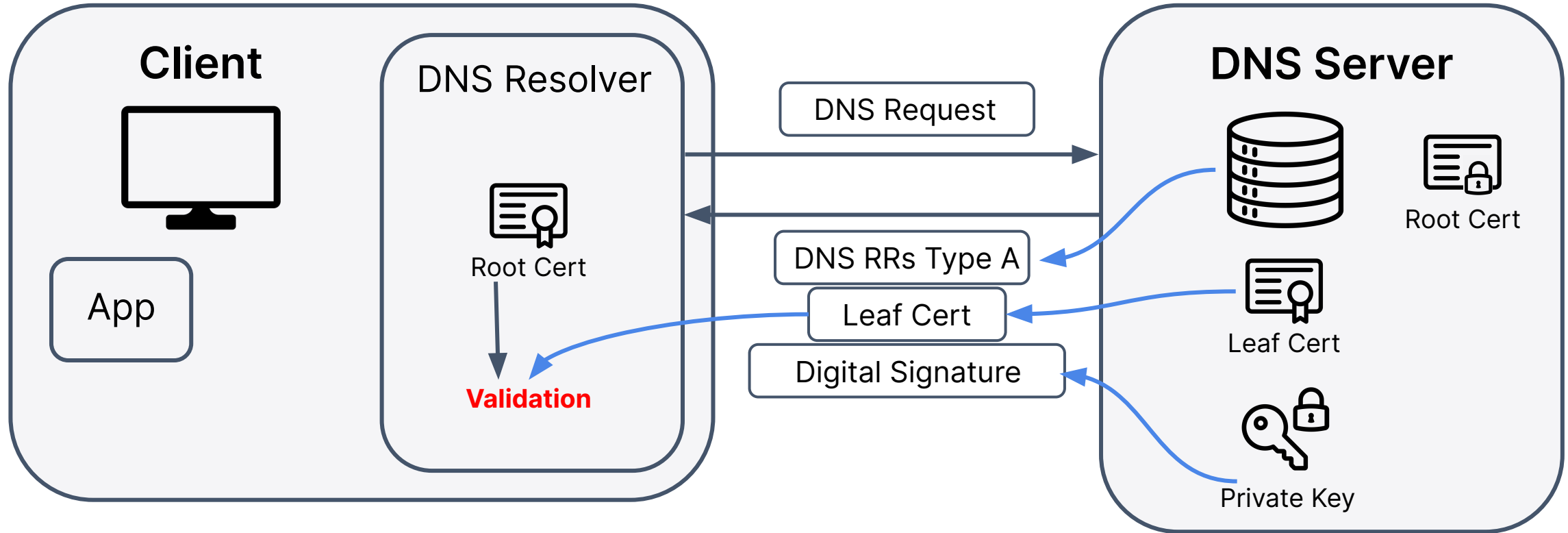
Overview



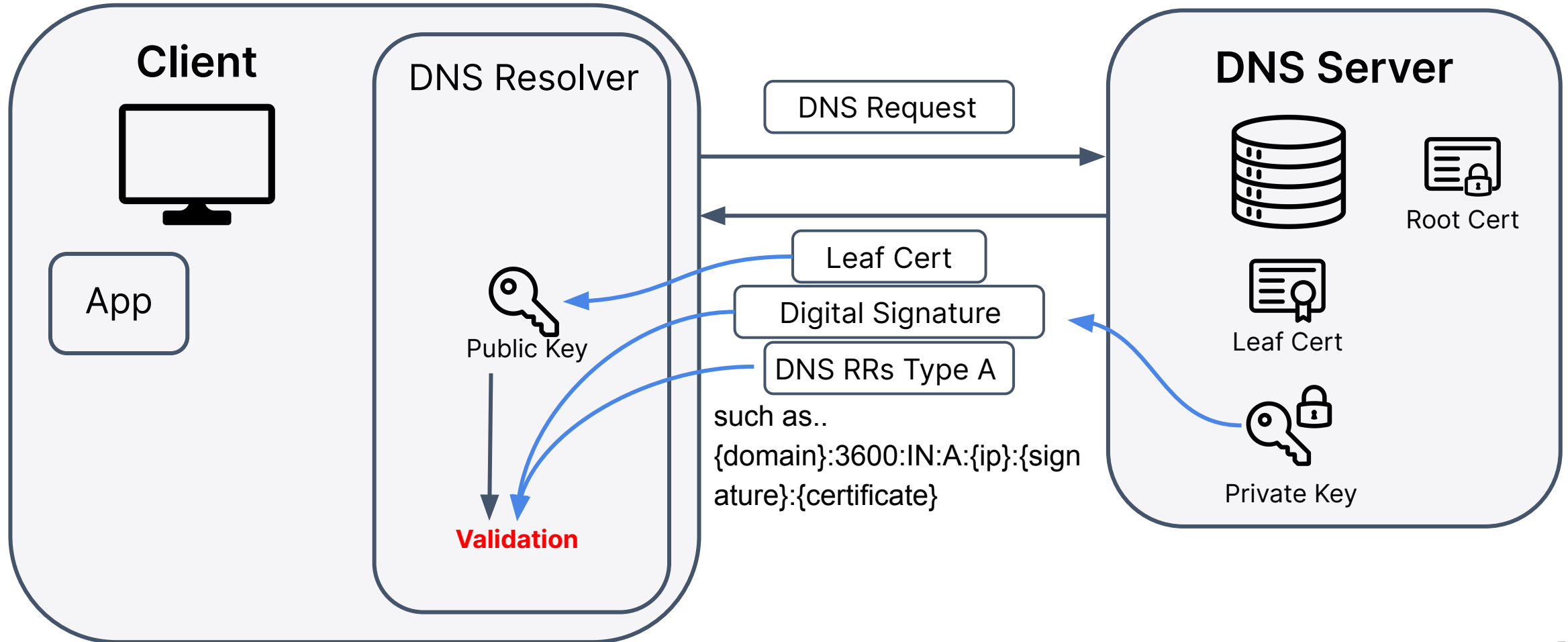
DNS Request



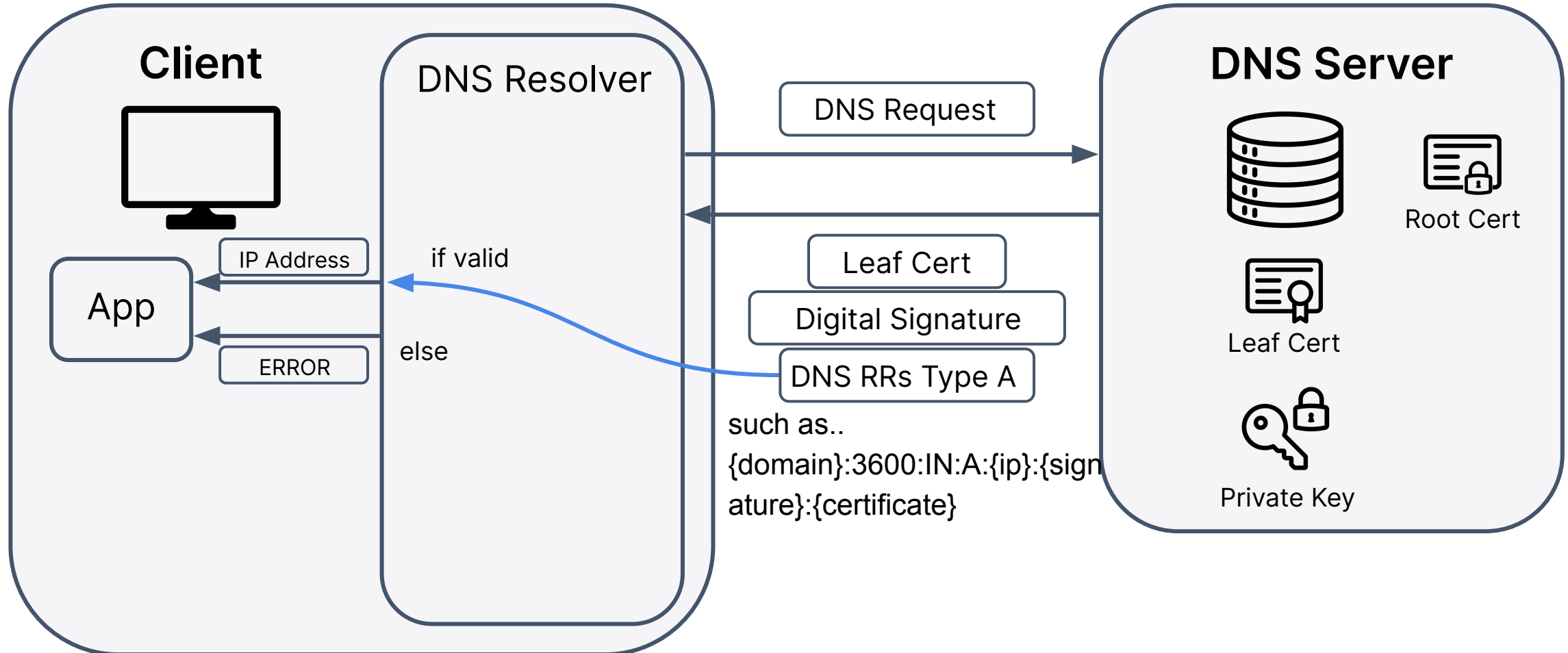
DNS Response



DNS Response



DNS Request



Plain text

average time : 0.773 ms

std_dev : 0.202 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

Private Key algorithm

key 1. 256 bits (ECC)

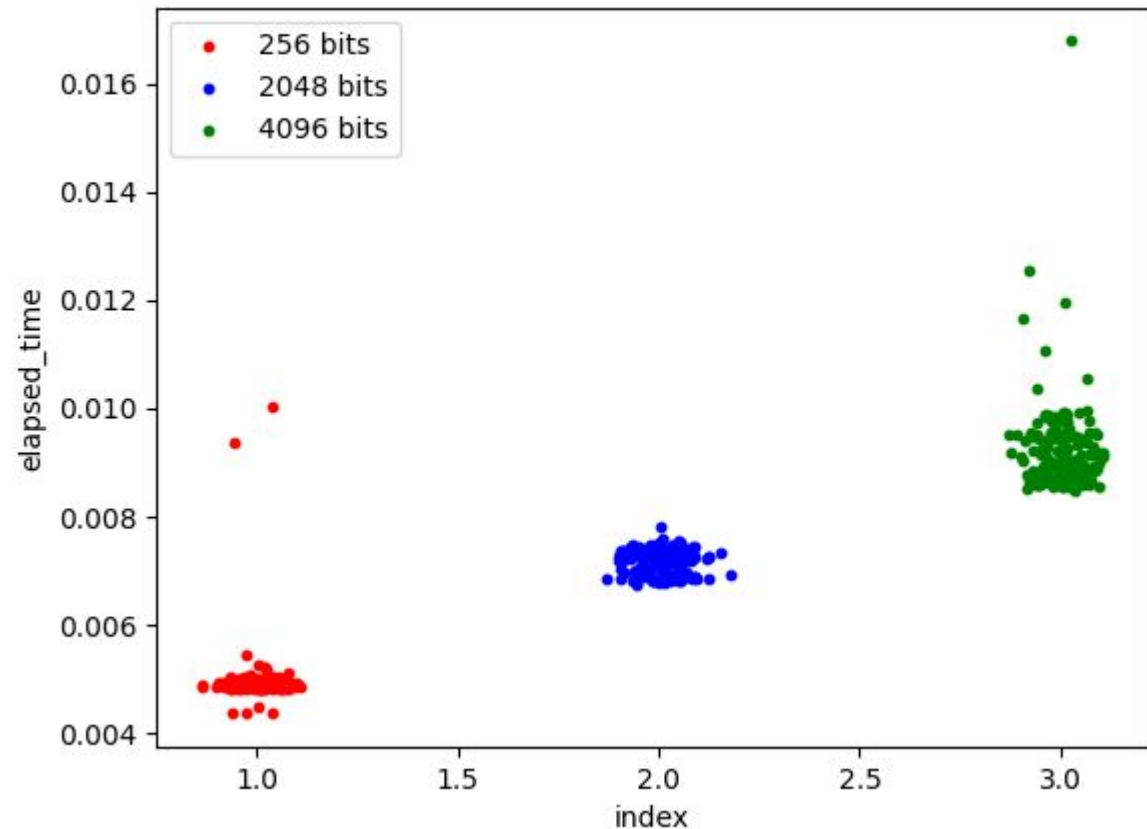
- average time : 4.96 ms
- std_dev : 0.489 ms
- msg_len : 1456

key 2. 2048 bits (RSA)

- average time : 7.19 ms
- std_dev : 0.221 ms
- msg_len : 2088

key 3. 4096 bits (RSA)

- average time : 9.21 ms
- std_dev : 0.788 ms
- msg_len : 2868



HASH Algorithm

“sha1” 160 bits

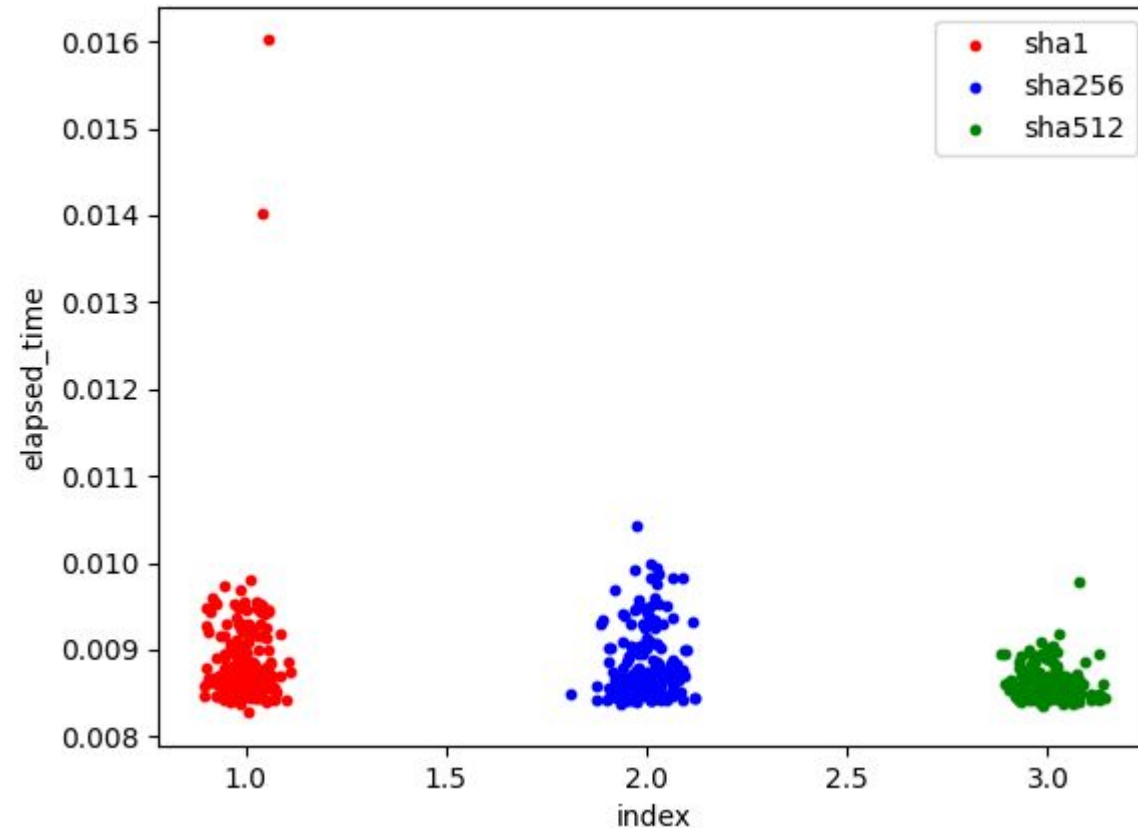
- average time : 8.88 ms
- std_dev : 0.711 ms

“sha256” 256 bits

- average time : 8.79 ms
- std_dev : 0.398 ms

“sha512” 512 bits

- average time : 8.58 ms
- std_dev : 0.185 ms



Github Link

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