A Distributed Online Certificate Status Protocol

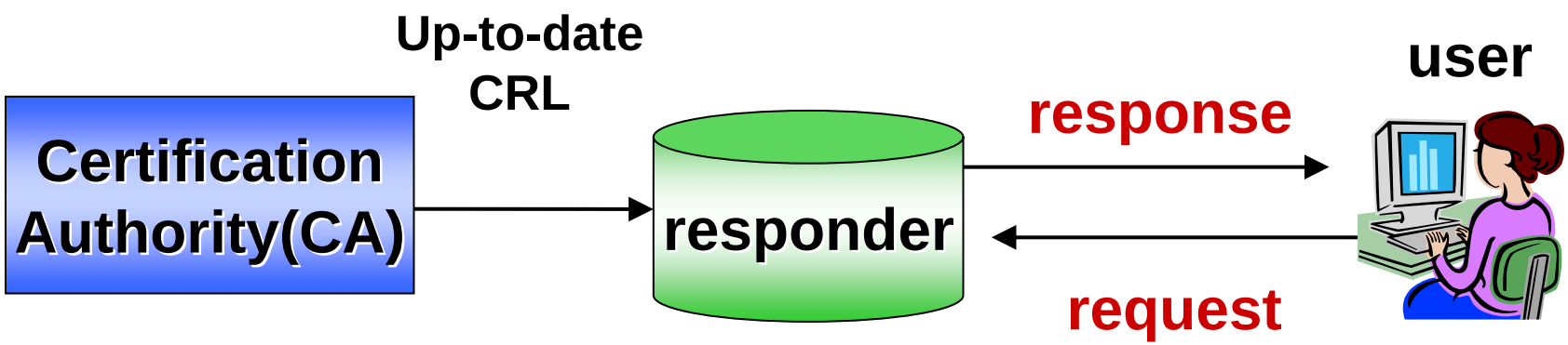
Satoshi Koga, Kouichi Sakurai
Kyushu University, Japan

Background

- Certificate Revocation Problem
  - The certificate should be revoked in case that:
    - User's private key is compromised
    - User's personal information is changed
  - The user should check whether the certificate has been revoked or not
- Online Certificate Status Protocol (OCSP)

OCSP

- The standard protocol of online revocation system
  1. The client requests to OCSP responder
     - Is this certificate valid or not ?
  2. The OCSP responder responses to the user
     - OCSP responder digitally signs the response



Problems

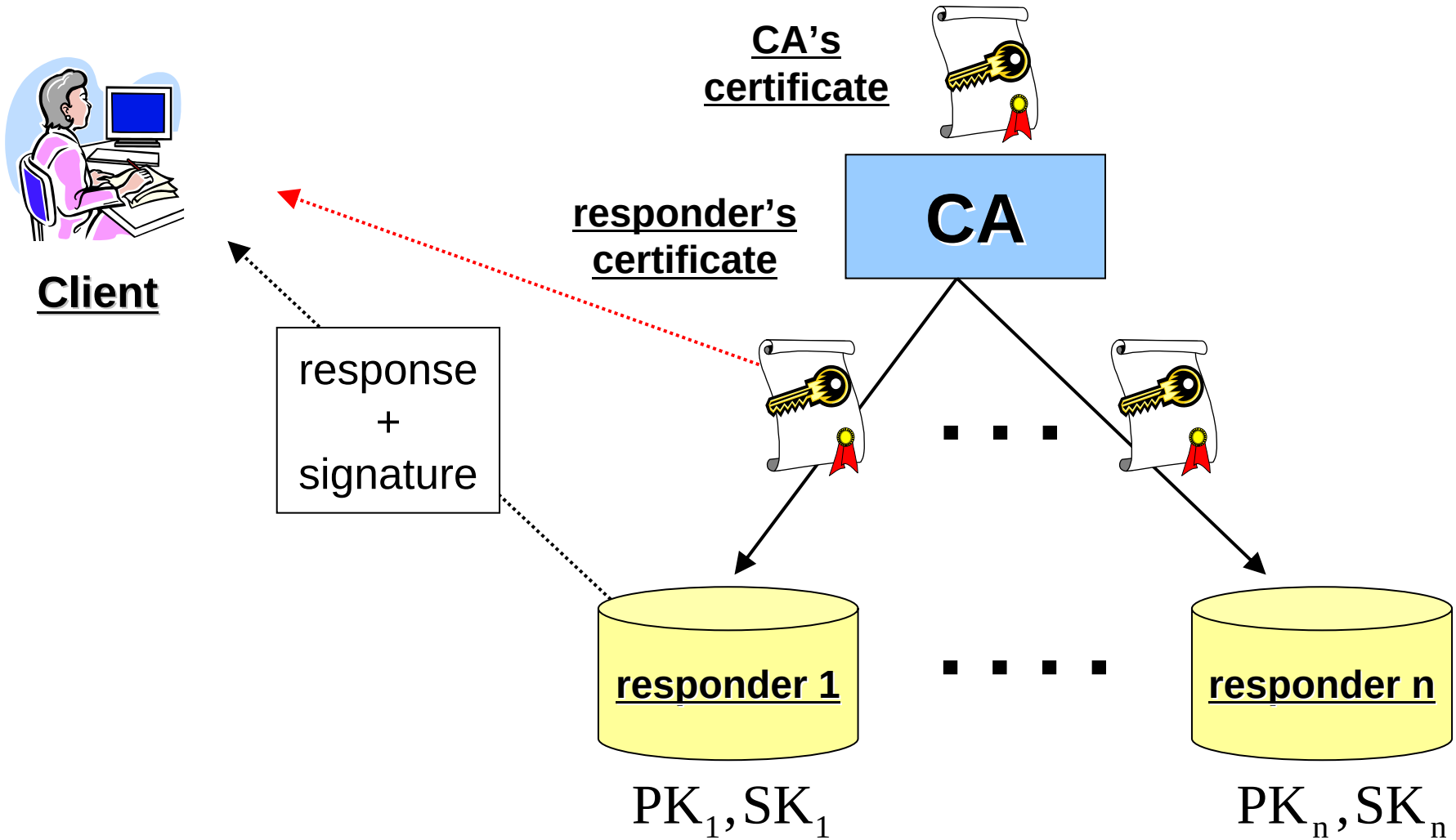
- If responder is centralized, it's vulnerable to Denial of Service (DoS) attacks
- Compromise of responder's private key is affected the entire system

Distributed OCSP

- Private key exposures appear to be unavoidable
  - Minimizing the damage caused by responder's key exposures is important

- A Distributed OCSP (D-OCSP) composed of the multiple responders
  - Each responder has own private key
  - If the responder's private key is compromised, the others are not affected

D-OCSP


CA's certificate
CA
responder's certificate
Client
response + signature
responder 1
responder n
PK_1, SK_1
PK_n, SK_n

Motivation

- General D-OCSP
  - Every time the client receives the response, he should download responder's certificate
  - The client needs to obtain the different responder's certificates

[Goals]

- Minimize the damage caused by responder's private key exposures
- Reduce the load of users

Our Method

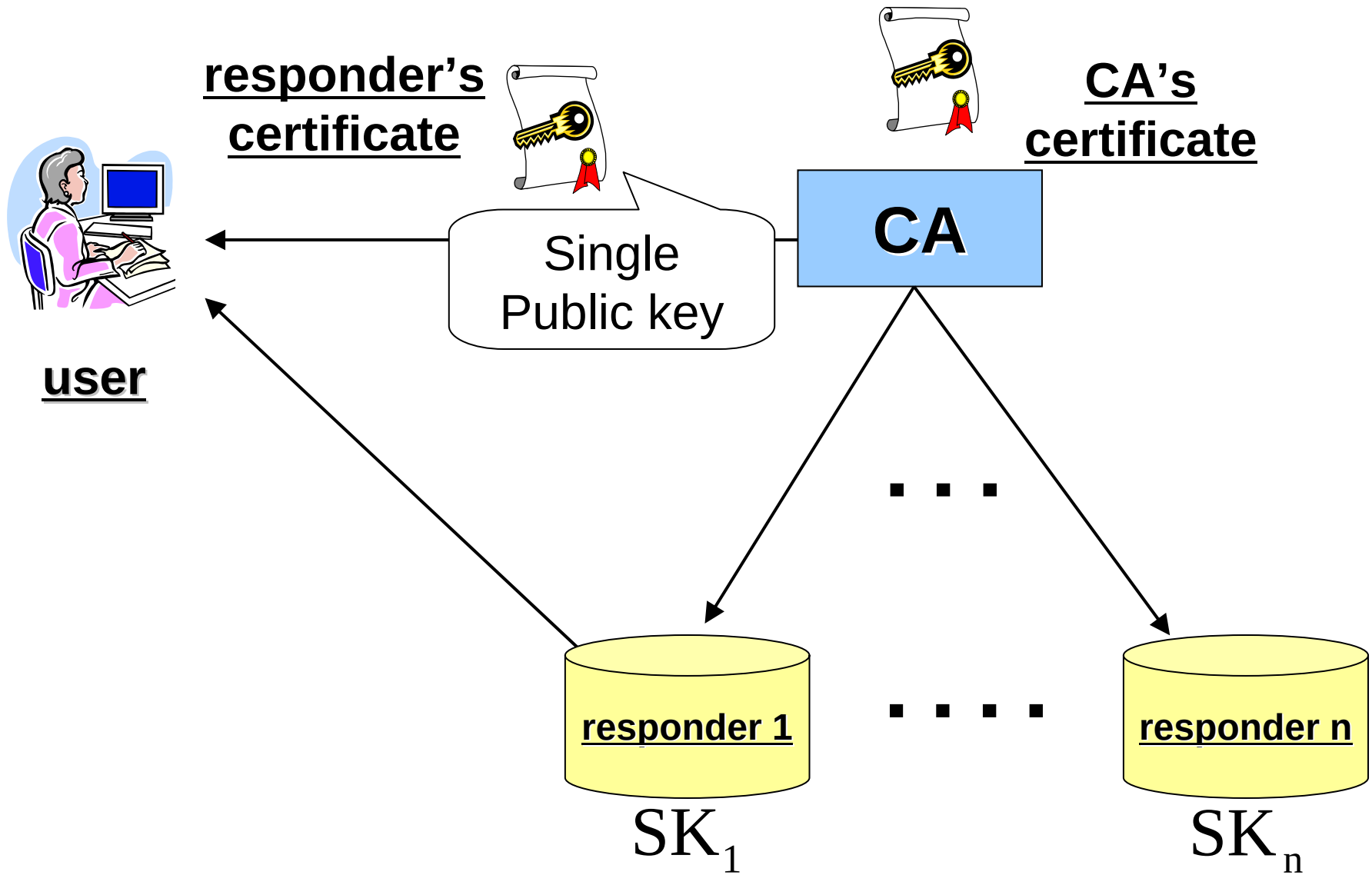
- Key-Insulated Signature Scheme [D03]
  - The private key can be changed frequently, but the corresponding public key remains fixed

[Our Method]

- The multiple private keys are generated and assigned each responder
  - The user can verify any responses using a single public key !!

[D03] Y.Dodis et al. , "Strong Key-Insulated Signature Schemes", PKC 2003

Proposed D-OCSP



Thank you !!

satoshi@itslab.csce.kyushu-u.ac.jp