Security in the distributed IT systems

A.Kryukov
(kryukov@theory.sinp.msu.ru)
A.Demichev
(demichev@theory.sinp.msu.ru)

SINP MSU, Moscow

The work was supported by Ministry of Science and Education of Russia.
Agreement 14.604.21.0146

Outline

- Problem
- Current status
- Possible solution
- Conclusion

- We will not consider
  - the encryption algorithms itself
  - The protection communication links
- We will consider the only logistics of requests submition in distributed IT system from security point of view.

Problem (1/2)

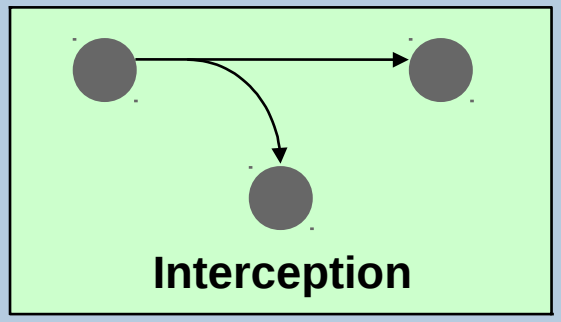
- Security infrastructute of distributed IT (DIT) system is very important part of any them.
  - Authentication ---> Certificate
  - Authorization ---> Proxy with noncritial extensions (VO information)
  - Delegation ---> Secondary proxies
- (Main) requirements for security infrastructure of DIT systems
  - Reliability
  - Convenience
- These requirements should be applied for users and administrators.
- Currently the PKI infrastructure with proxy certificate is used.
- This approach is not so convenience especially for non-IT specialists.

So, the problem of simplification of using security infrastructure by users and convenience for system administrators and programmers is very important.

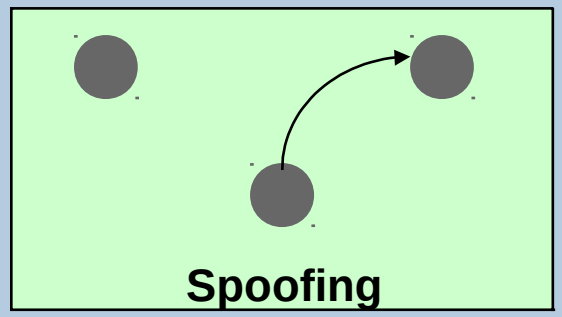
Problem (2/2)

Possible security threats

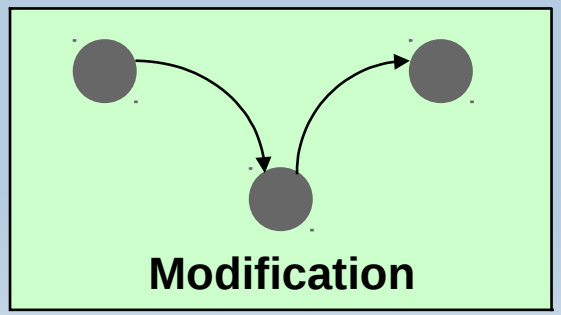
Privacy



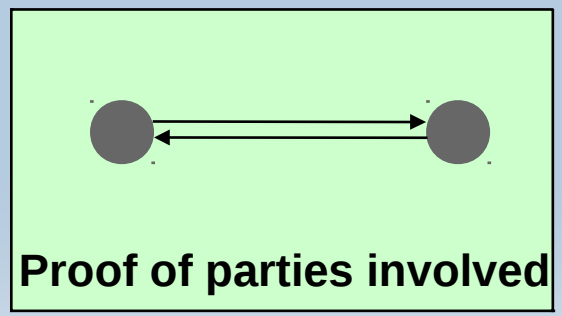
Authentication



Integrity



Non-repudiation

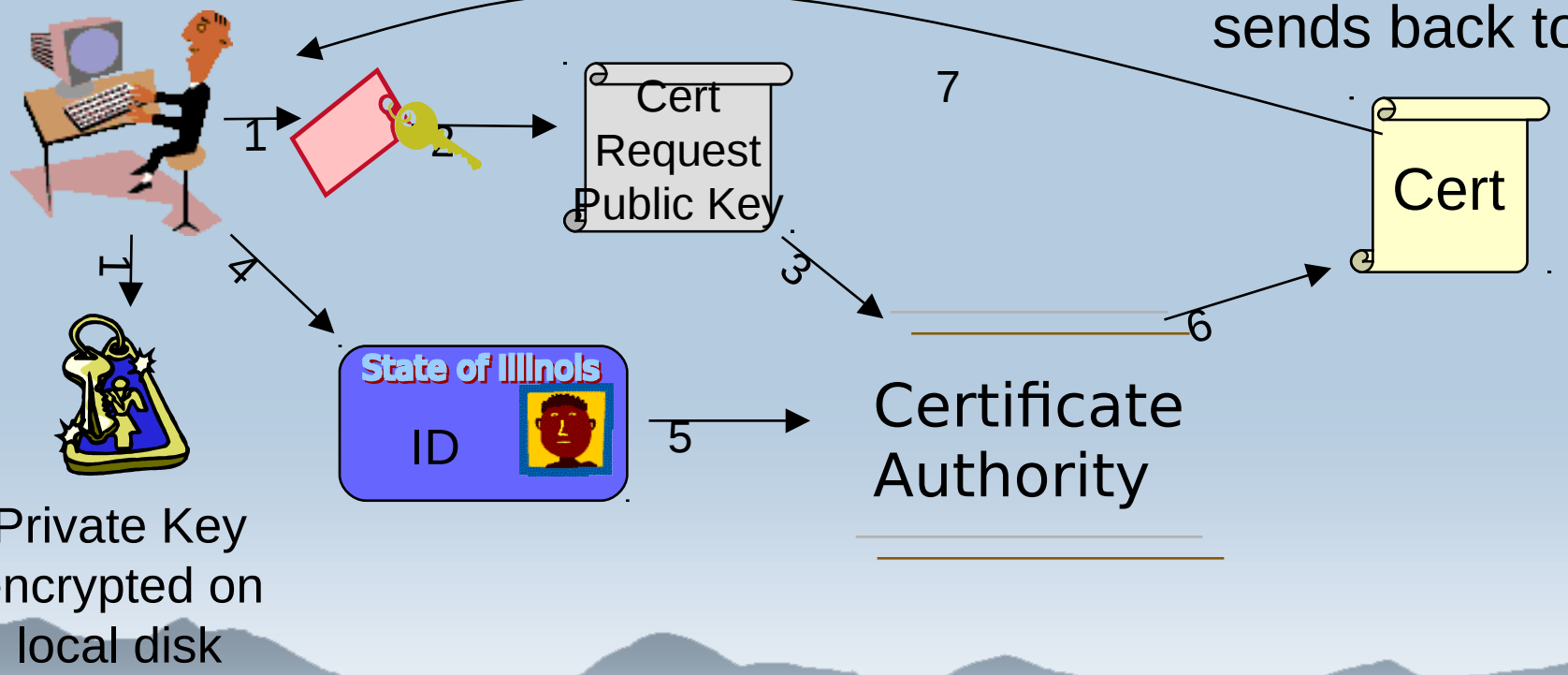


Certificate Request

User generates public/private key pair.

User send public key to CA along with proof of identity.

CA confirms identity, signs certificate and sends back to user.



Certificate request in reality

- Generate private and public keys (not for nervous people)
- Send public key to Registration Authority to confirm certificate request
  - Signed special form
  - Approve the form in Organization Authority
  - Send the form to RA and goes to RA personally
- RA confirm request and send confirmation to Certificate Authority
- CA confirm request
  - Signed public key
  - Send certificate to requestor
- That's all?! - No, you need proxy!

The usual way

- Fill the web-form and press button “I am agree”
- Why we can not use so simple scheme?
  - Your rights have to be approved by verified manner

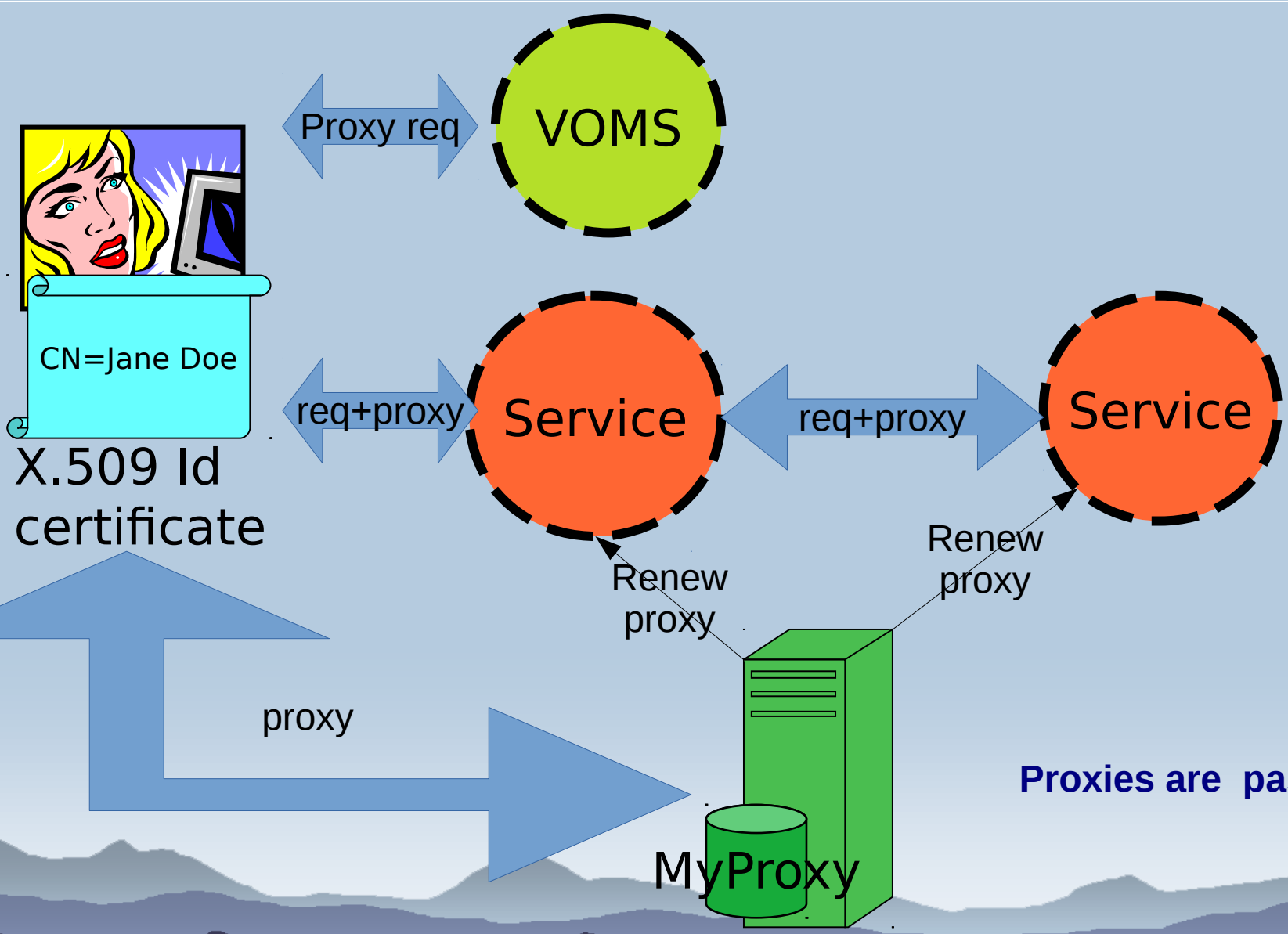
Proxy certificate

- Why you need proxies?
  - Authorization (your rights and roles)
  - Short time living certificate for security reason
- Your rights and roles in VO have to attached to certificate from VO management service.
- Proxies are short time living certificate (for security reason), but we can not predict how much time do you need to process request.
  - There is special services to support prolongation of proxy life time

Proposal solution

- The main idea is using well tested PKI infrastructure for service-to-service interaction without proxies.
- Use pair login/password for user authentication.
  - Multifactor authentication for strong security if necessary
- Using just in time approving right via special service
- Signing each request by individual certificate which is non limited in time
  - No problem with renew proxies

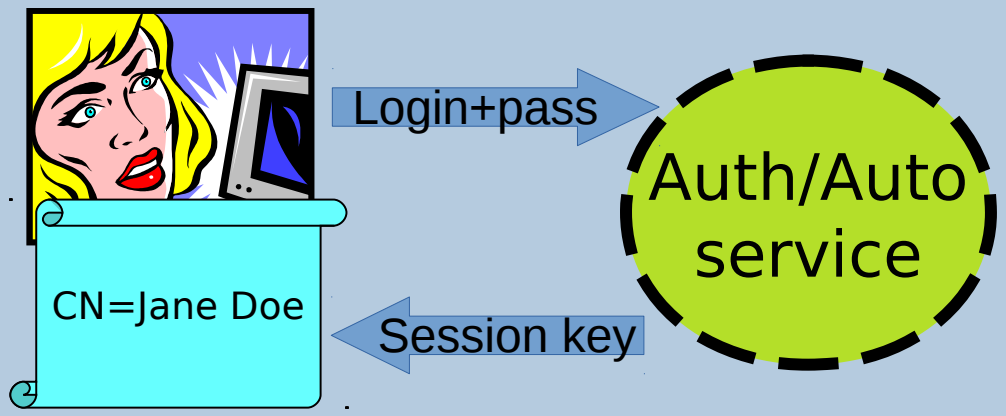
Proxy certificate



Proxies are passwordless

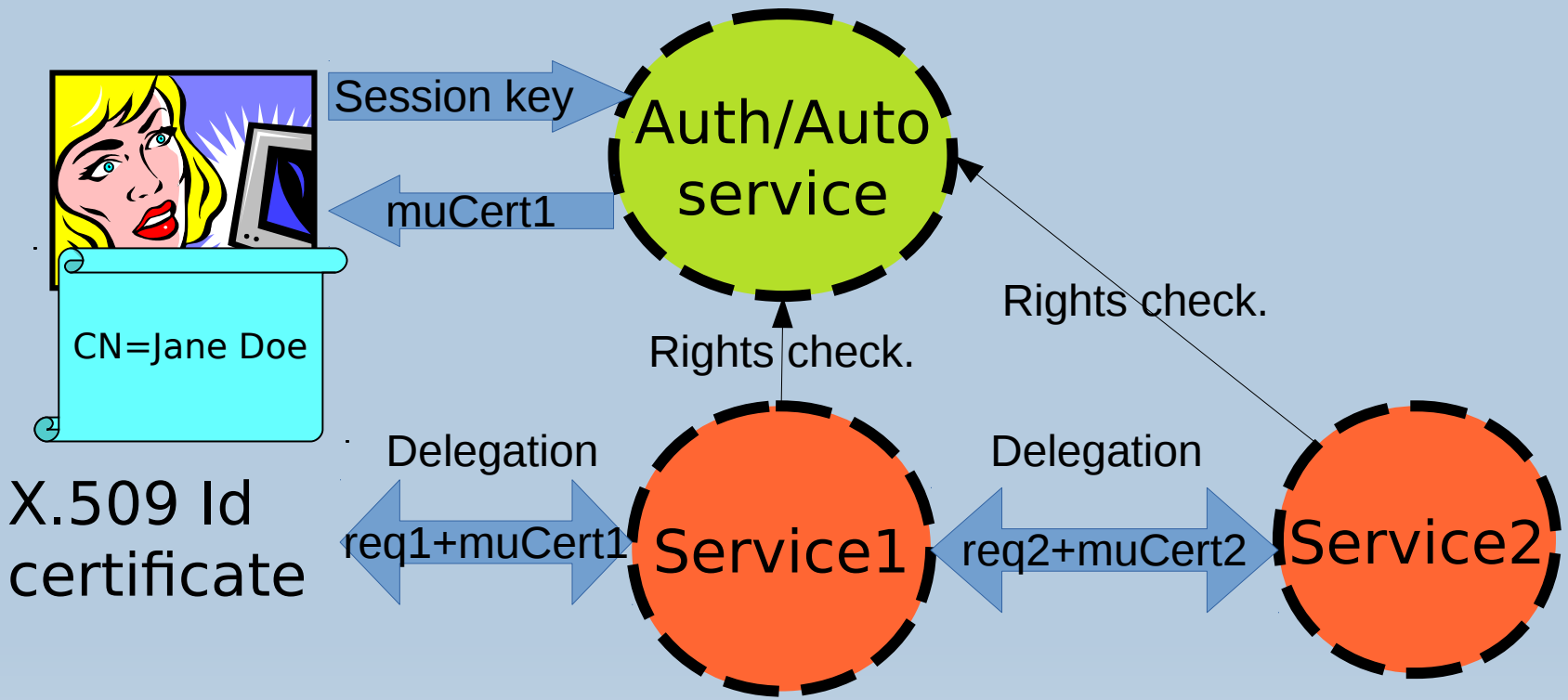
Life without proxies

- Authentication
- On-line authorization



X.509 Id certificate

Life without proxy



muCerts are passwordless and non limit lifetime

Conclusion

- The proposal approach should significantly simplify the using of distributed IT system
  - In particular by rejecting of proxies
- Save high level of security which characterized the PKI
- We guarantee the immutability of request during processing of it

THANK YOU FOR ATTENSION