



UNIVERSIDADE FEDERAL
DE SANTA CATARINA

Optimized Certificates – A New Proposal for Efficient Electronic Document Signature Validation

Martín Augusto G. Vigil

Ricardo Felipe Custódio

Joni da Silva Fraga

Juliano Romani

Fernando Carlos Pereira

Federal University of Santa Catarina/Brazil

EuroPKI'08

Fifth European PKI Workshop

Outline

- About the speaker
- Signed documents issues
- Solutions approaches
- Optimized Certificate's approach
- Optimized PKI
- Optimized Certificate Format
- Considerations
- Future work
- Questions

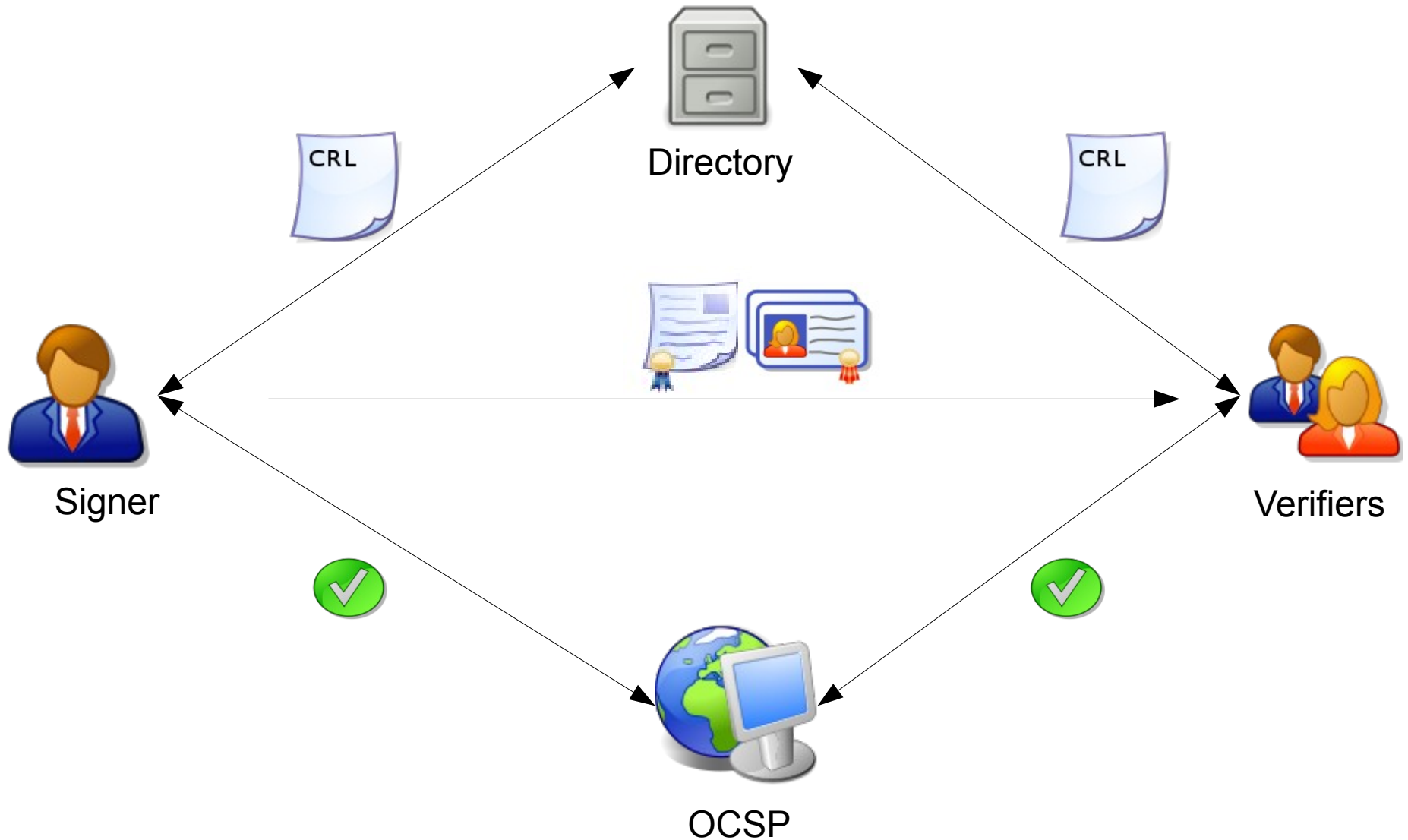
About the speaker

- Martín Augusto Gagliotti Vigil
 - MSc student at Federal University of Santa Catarina - Brazil
- Computer Security Lab (aka LabSEC)
 - *João de Barro*: development of a hardware (HSM) and software solution to support the federal Brazilian PKI (*aka ICP-Brasil*)
 - *Electronic documents management*
 - *ICPEDU*: development of a PKI for universities and research centers
 - *Optimized Certificate Certification Authority*

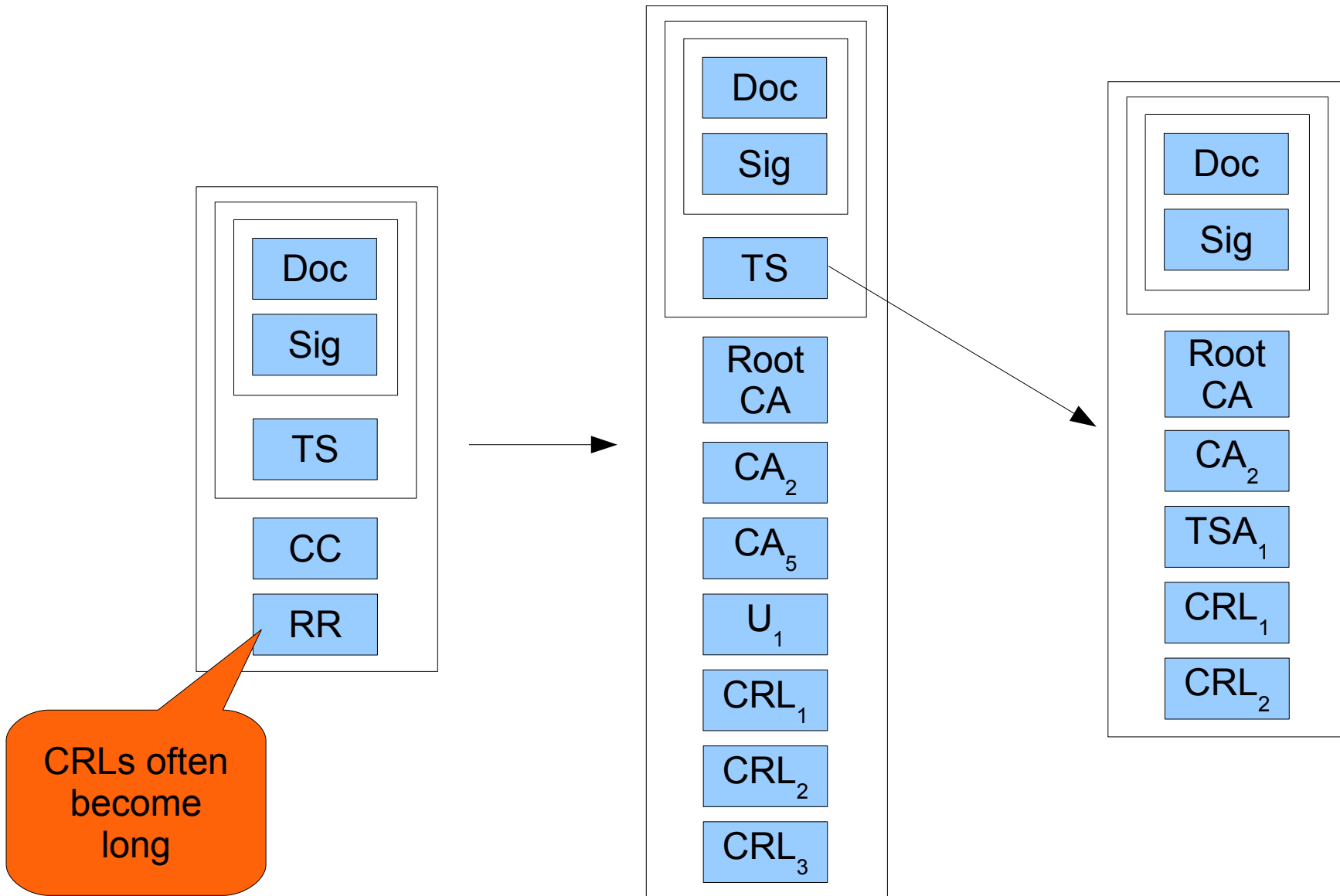
Signed documents issues

- What information will be included in a signed document in order to validate it?
 - As little as possible and performing external queries to acquire missing data when validating a signature
 - All necessary data to validate a signature
- What else is required?
 - Trusted Root CA Certificate

Using external queries approach



Embedding everything



Solution Approaches

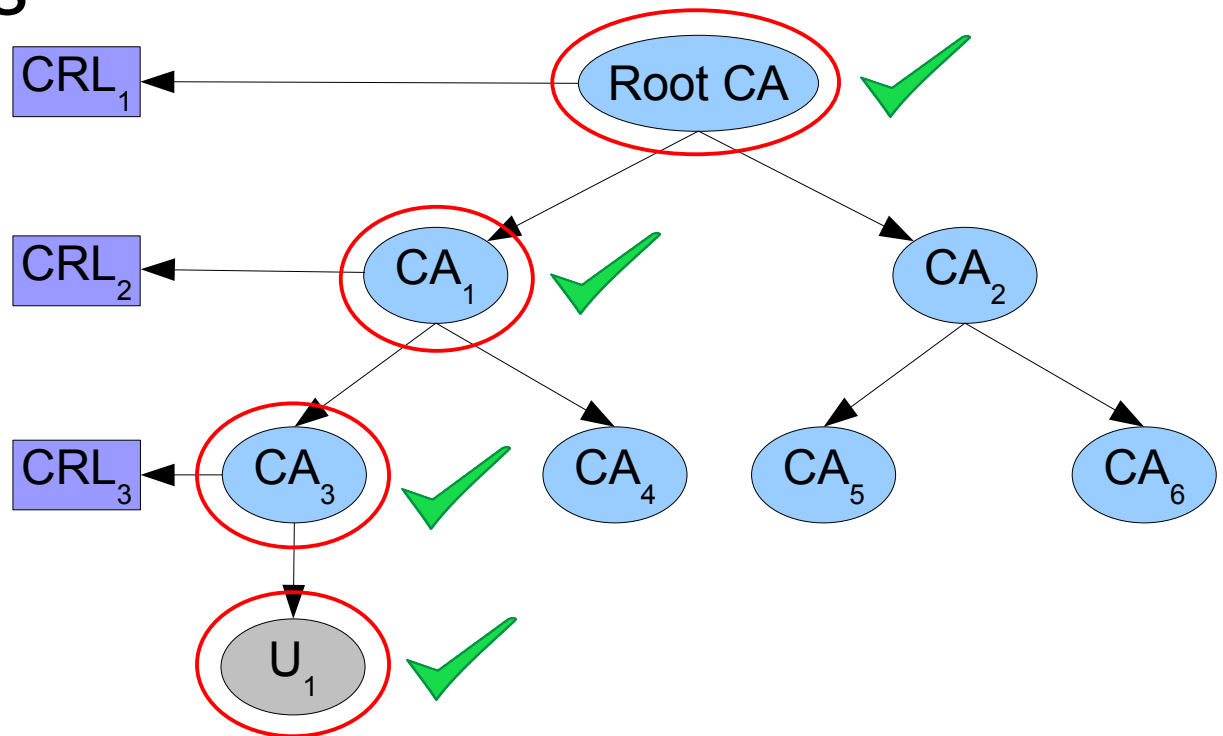
- One could use short term certificates (Rivest 1998)
 - Certificates do not need to be revoked
 - CRLs are dismissed
- Drawback in this approach
 - Overhead in renewing users certificates
 - Generation of a cryptographic key pair
 - Generation of a X509 certificate

Optimized Certificate (OC)

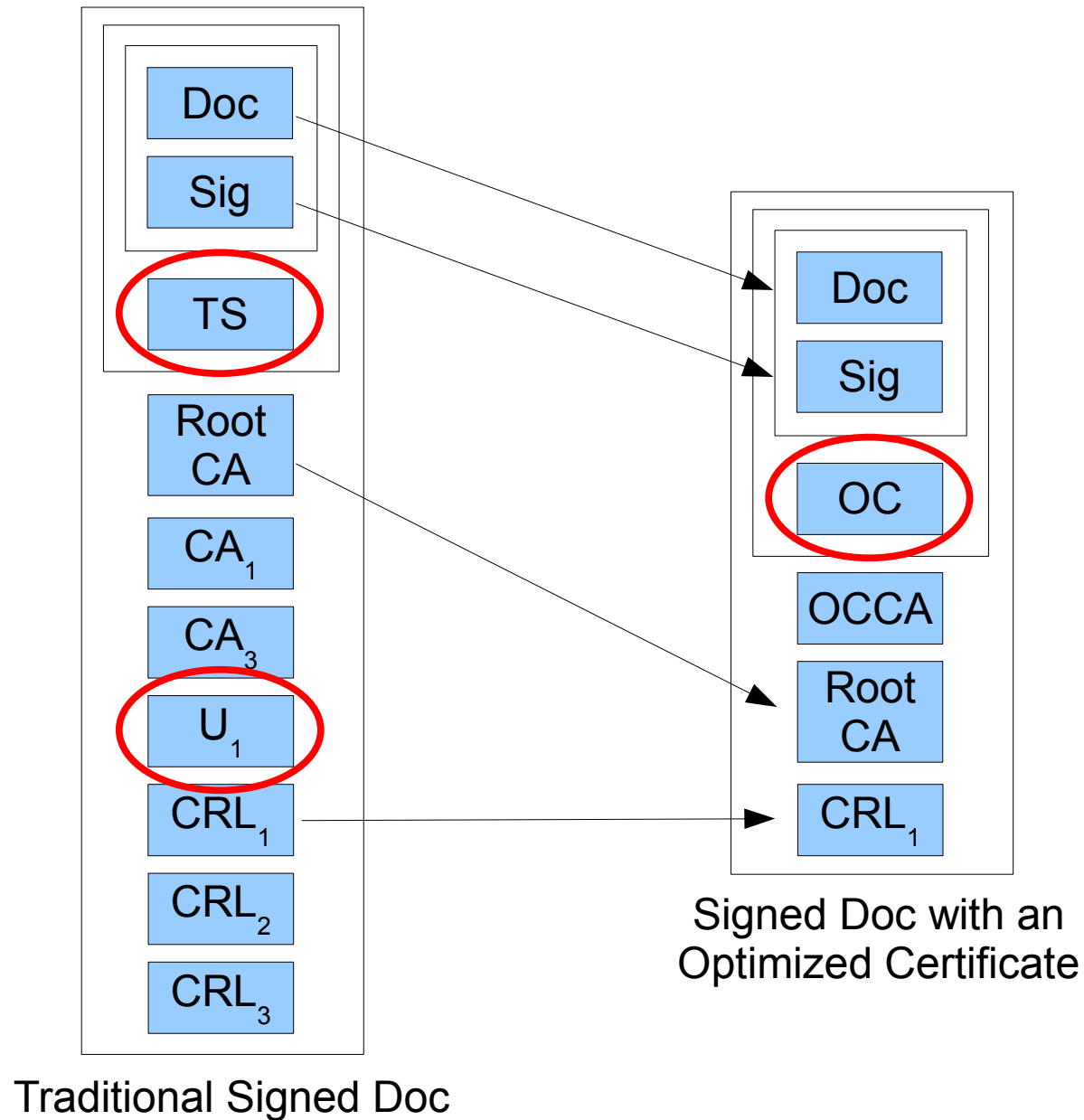
- Aiming at reducing embedded data in a signed document
 - Short term certificate: issuance and expiration date are equal
 - CRL checking for OC is dismissed
 - Signed document's time-stamp is dismissed
 - Micali's Novomodo validity proof into OCs
 - CRL checking for OC's issuer is dismissed
 - Fast revocation checking: hash evaluation

Validation Effort

- Finding out a certification path
- Validating each certificate
 - High cost: revocation status checking
- Checking policies



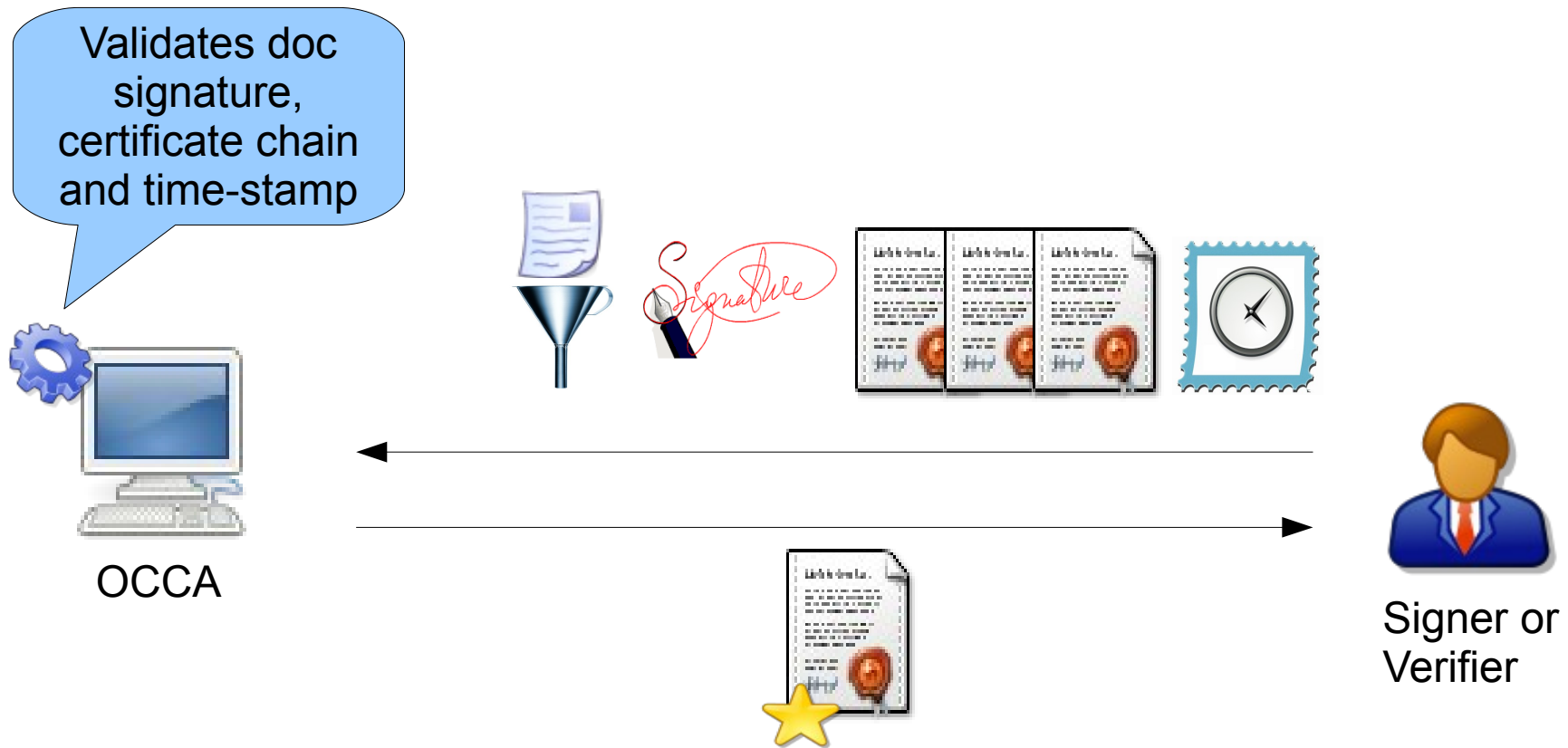
Optimized Certificate (OC)



OC and Signed Documents

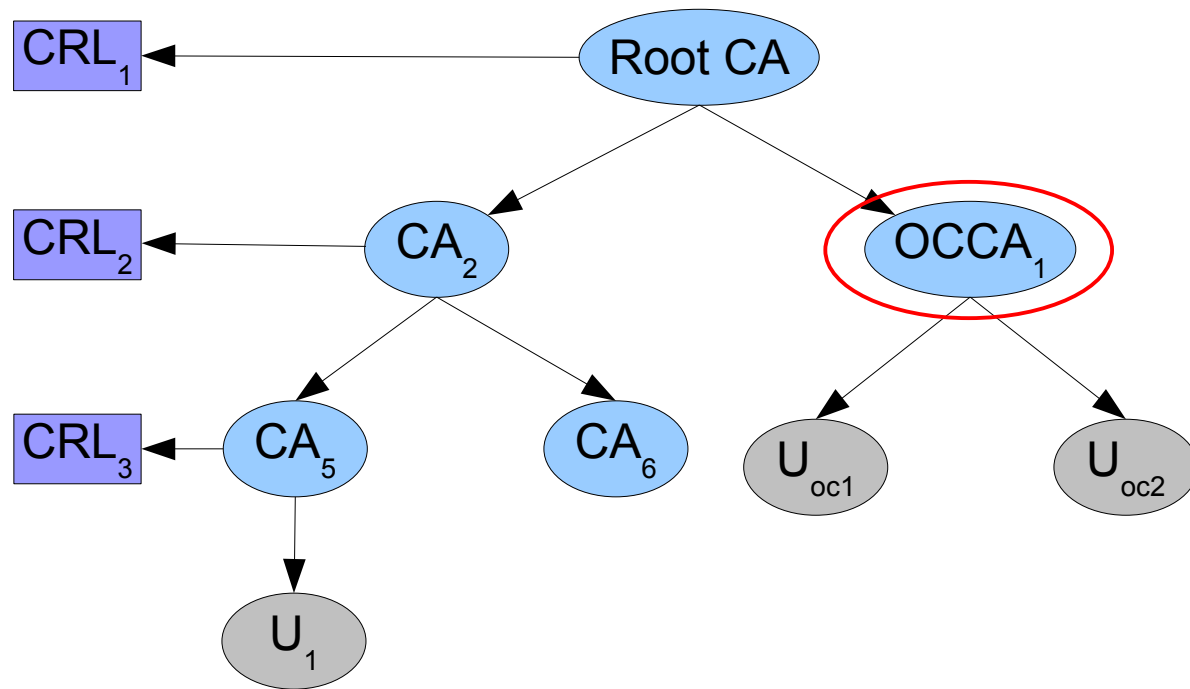
- OC carries traditional certificate's information and some extra extensions
- Optimized certificate issued for a document
 - OC linked to a document's hash code
 - OC can work as a document time-stamp
- Implemented using a X509 extension
 - Digest algorithm OID and hash value

OC Certification Authority (OCCA)



OCCA and its PKI level

- Aiming validation performance
 - Short certification path



OC and its Validation

- Short term certificate
 - Beginning and ending of validity are equal
 - X509 standard is not changed
- Revocation is not needed for an OC

OCCA's certificate and its Validation

- OCCA certificate validation engages Micali's Novomodo
 - Novomodo's proof of OCCA validity embedded in issued OCs deploying a X509 extension
 - X509 standard is not changed
 - High performance: hash function evaluations

Optimized PKI Security

- OCCA requests its validity proofs to Root CA
- OCCA issues OCs until its validity proof expires
- In order to issue OCs an attacker needs OCCA's private key and novomodo secret values owned by Root CA
- Root CA is supposed to be offline

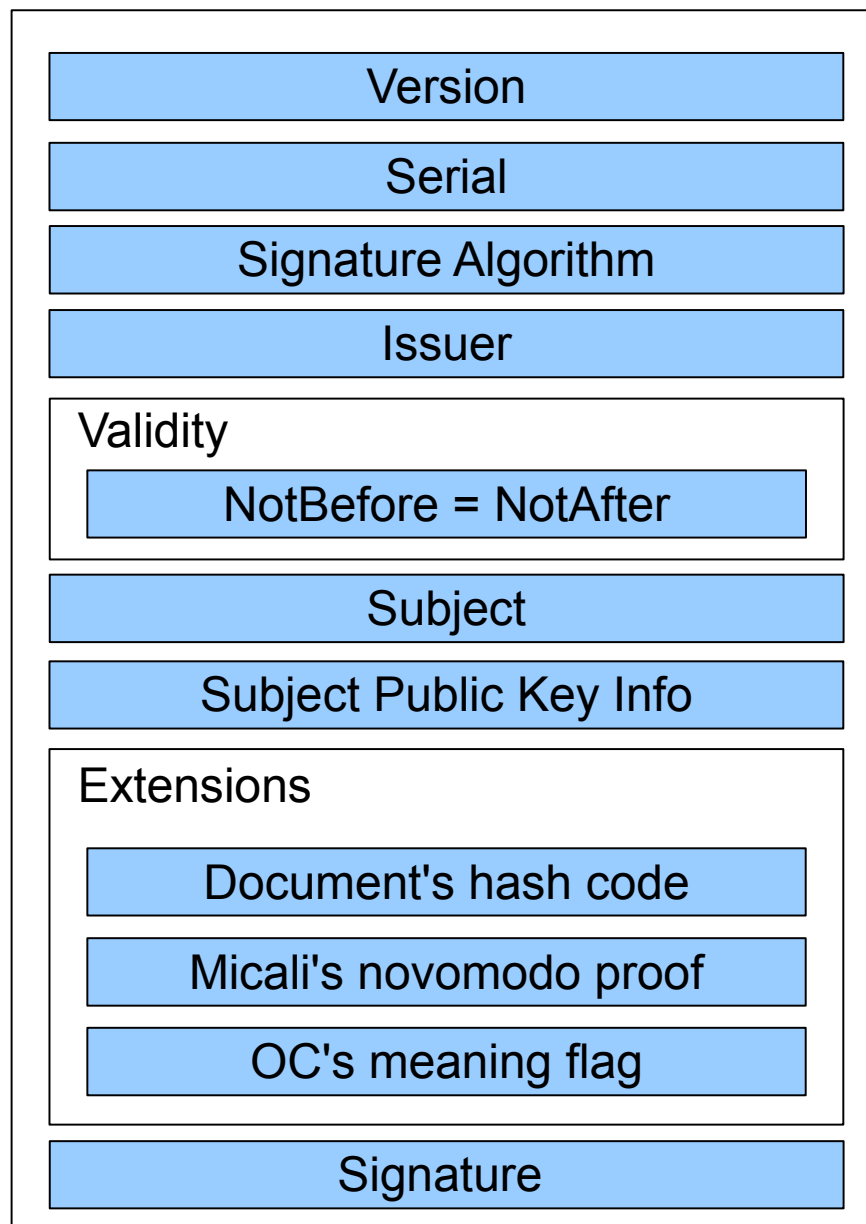
OC Interpretation

- Signer can request an OC for a signed document
 - OC date and time should be understood as the time when the signature was created
 - OC date and time can be accepted as proof of document's existence at that time
 - OCCA asks signer key ownership proof

OC Interpretation

- Also a verifier can request an OC for a third-party signed document
 - OC's date and time is the moment of OC's request
 - OC's date and time is defined by verifier
 - OC's date and time correspond to document's signature time-stamp
- Interpretation flags are embedded in issued OCs deploying a X509 extension

OC and X509

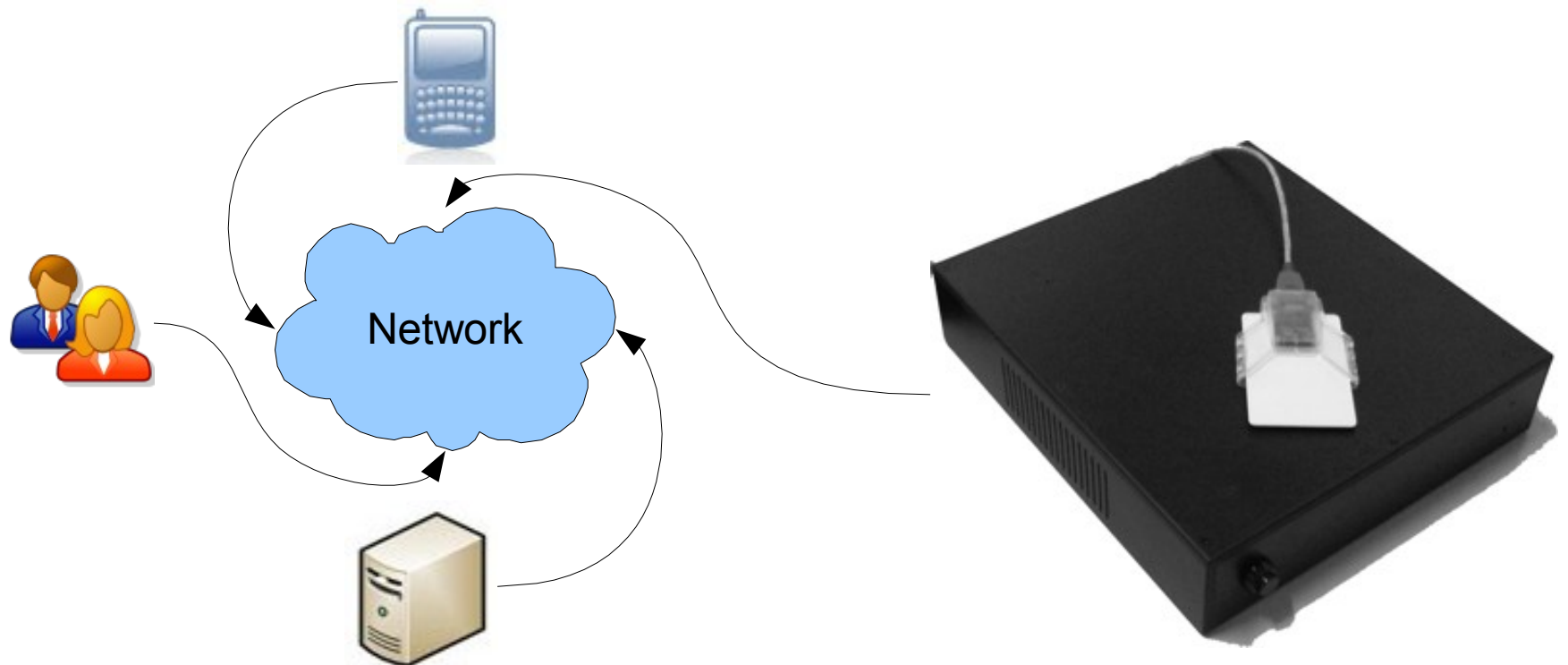


Considerations

- Optimal document representation
- No external consult needed to validate an OC
- Low costs of certificate validation and storage
- Suitable to environments of limited in energy, bandwidth and memory
- Improve the efficiency of mass on-line transactions
- Overhead in traditional certificate validation by OCCA

Future Work

- Formal analysis of OCCA's protocols
- Design and implement a prototype of an OCCA
 - Embedding OCCA in our HSM



Questions?

- Ricardo Felipe Custódio - custodio@inf.ufsc.br
- Martín Augusto G. Vigil - vigil@inf.ufsc.br

Further information

- OCCA's project website
 - <https://projetos.labsec.ufsc.br/ac-otimizadora-i>
- LabSEC's related projects
 - <https://projetos.labsec.ufsc.br>