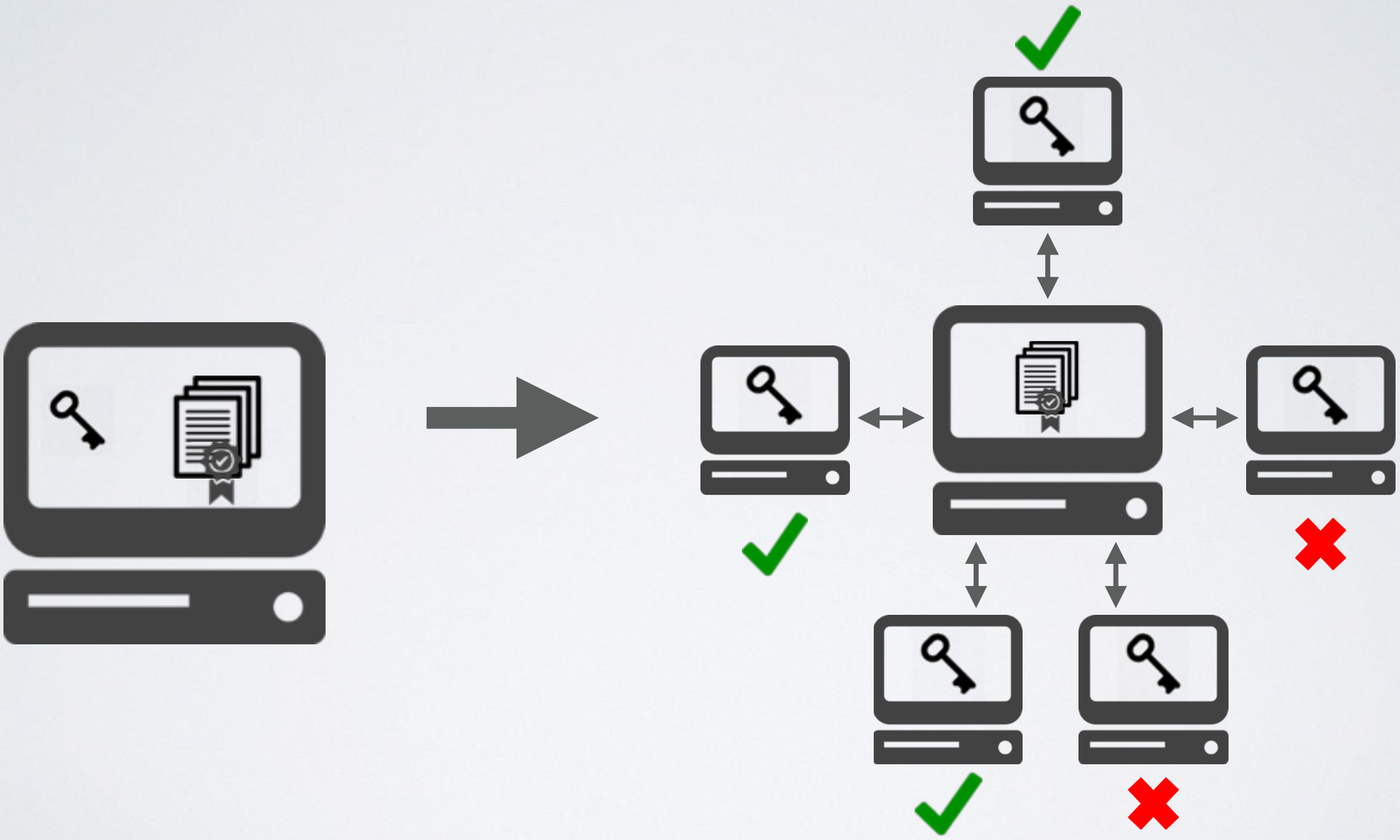
THRESHOLD-CRYPTOGRAPHY DISTRIBUTED HSM

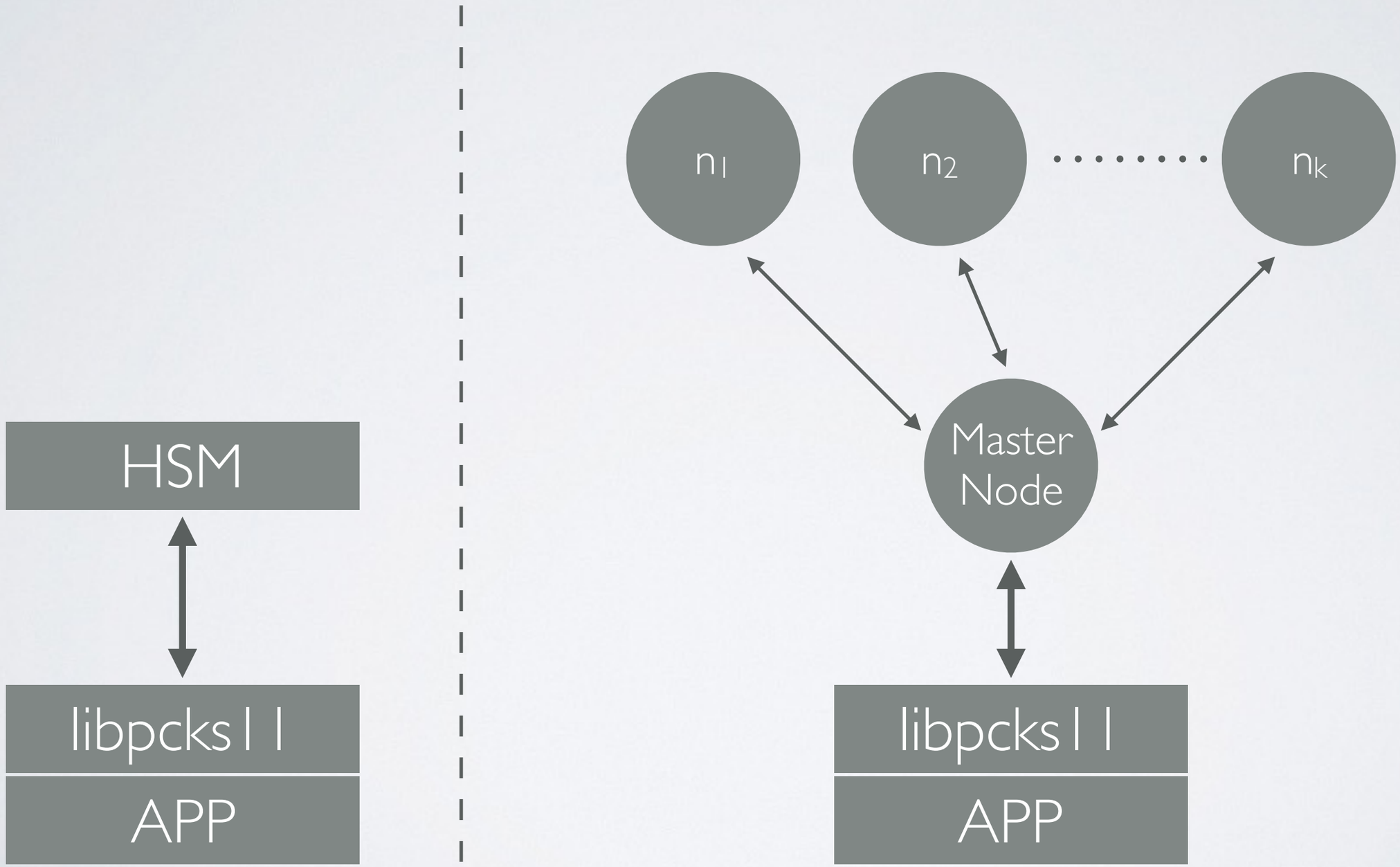
(TCHSM)

Francisco Cifuentes
francisco@niclabs.cl

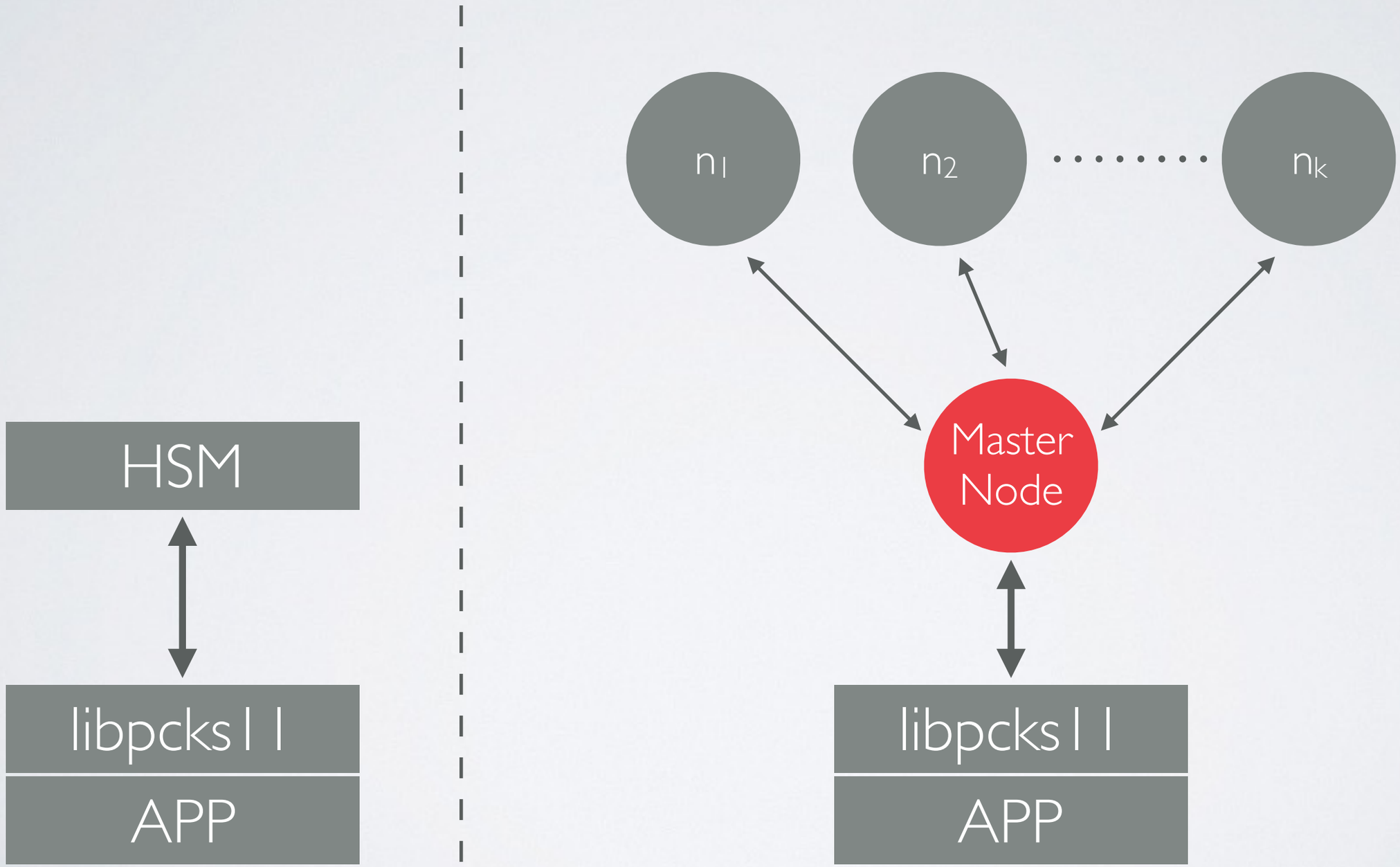
THRESHOLD CRYPTOGRAPHY



HSM BASED APPLICATIONS

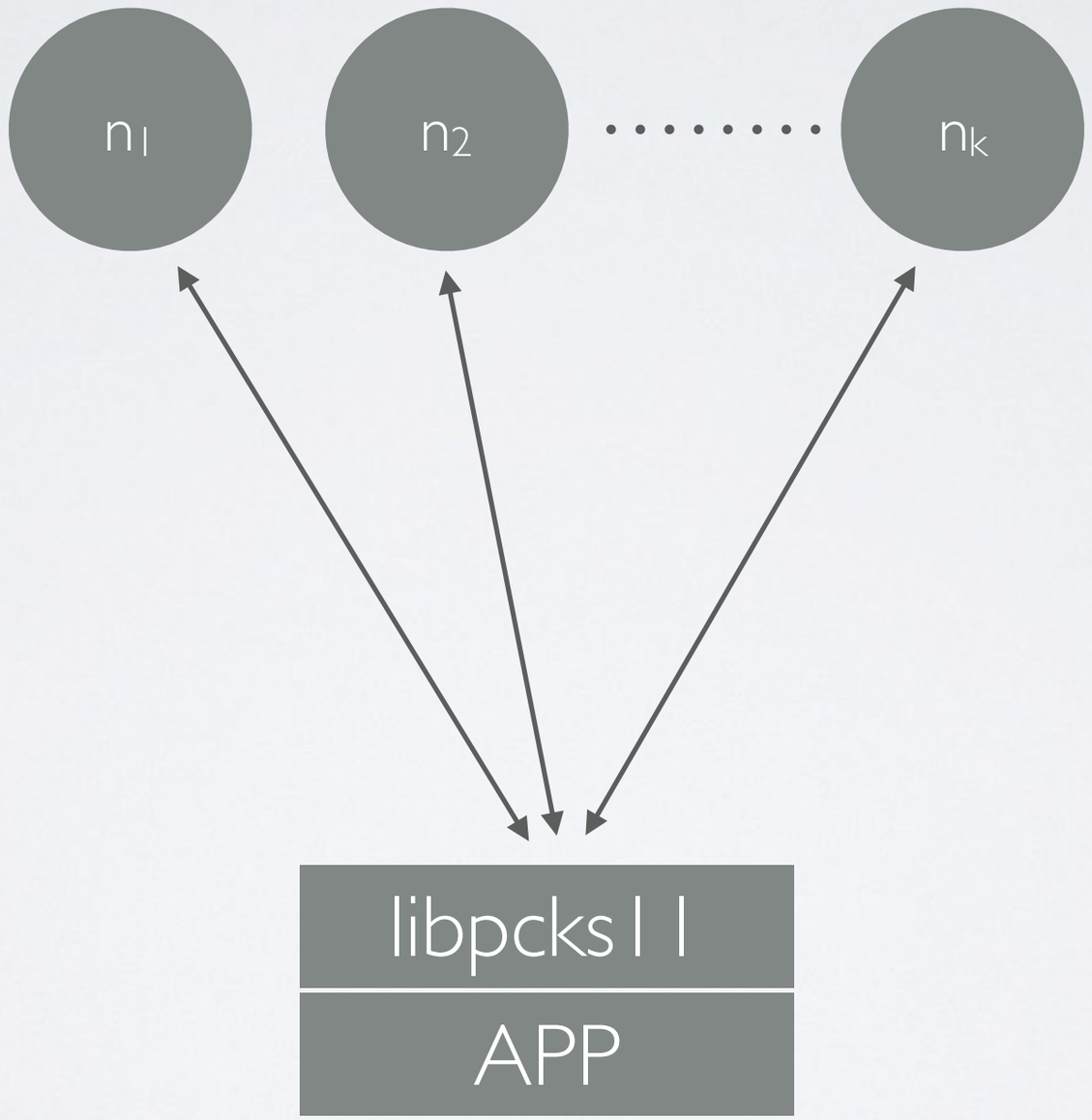


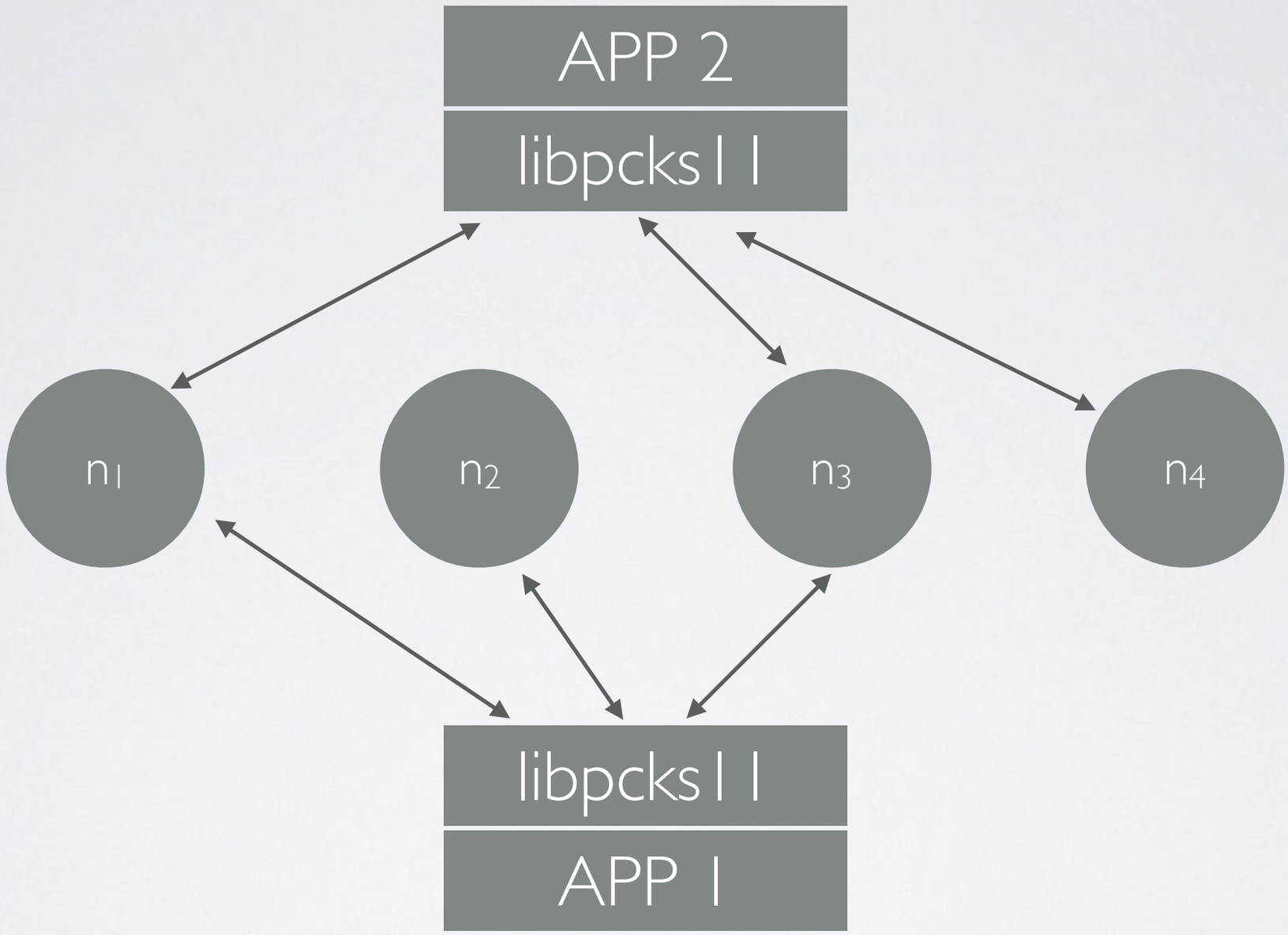
SINGLE POINT OF FAILURE



TCHSM 2014

DESIGN UPDATE




APP 2
libpcks11
n1
n2
n3
n4
libpcks11
APP 1

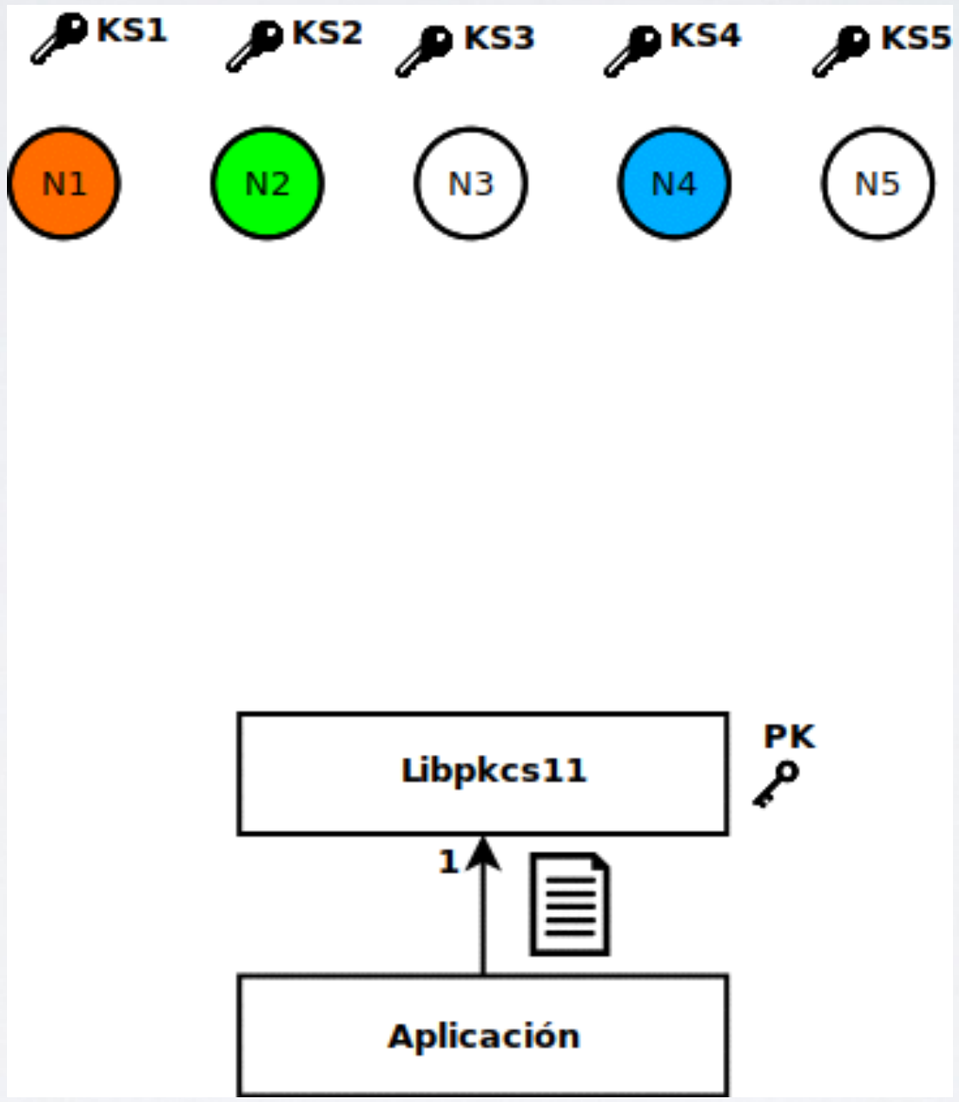
WHAT WE DID

- A Threshold Cryptography algorithms library.
- A Threshold Cryptography distributed system.
- A PKCS#11 API implementation, in order to use it with HSM compatible software*.

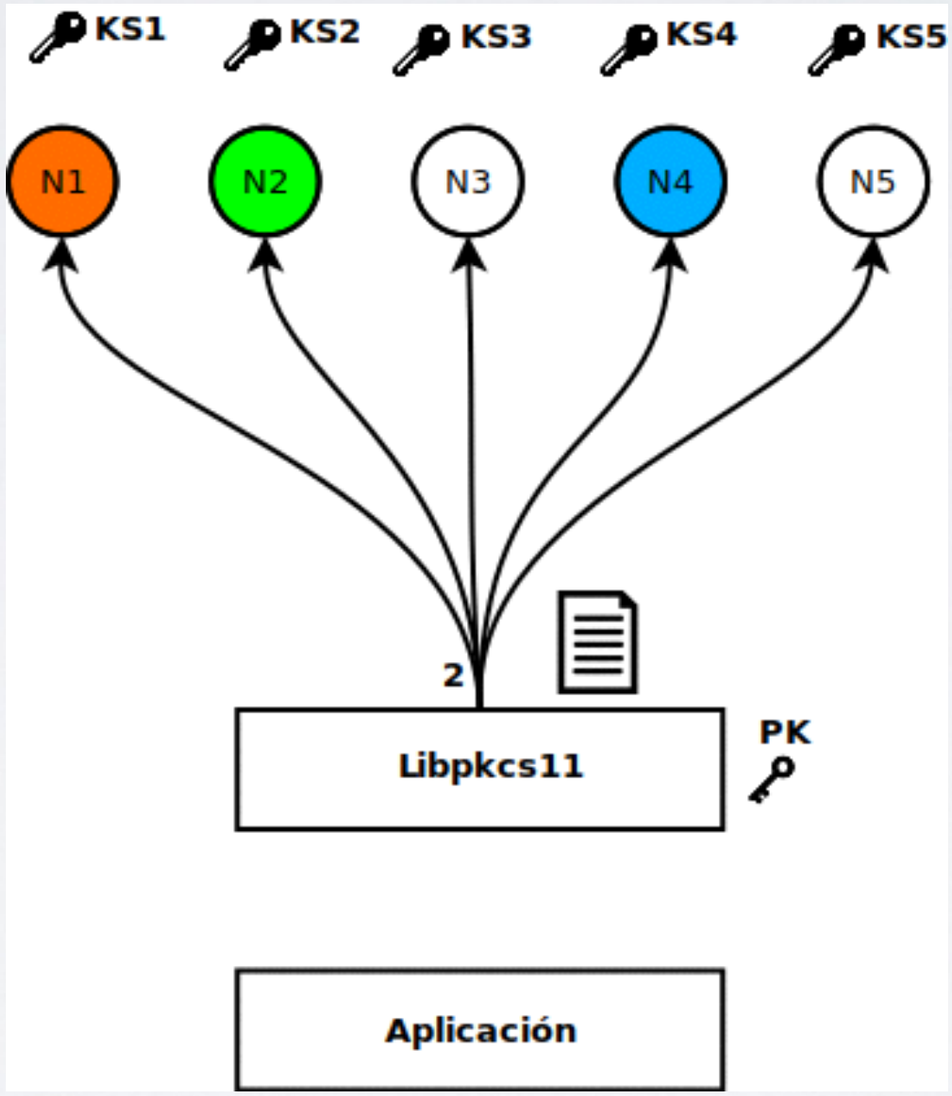
All wrote in C.

* e.g. OpenDNSSEC or KNOT

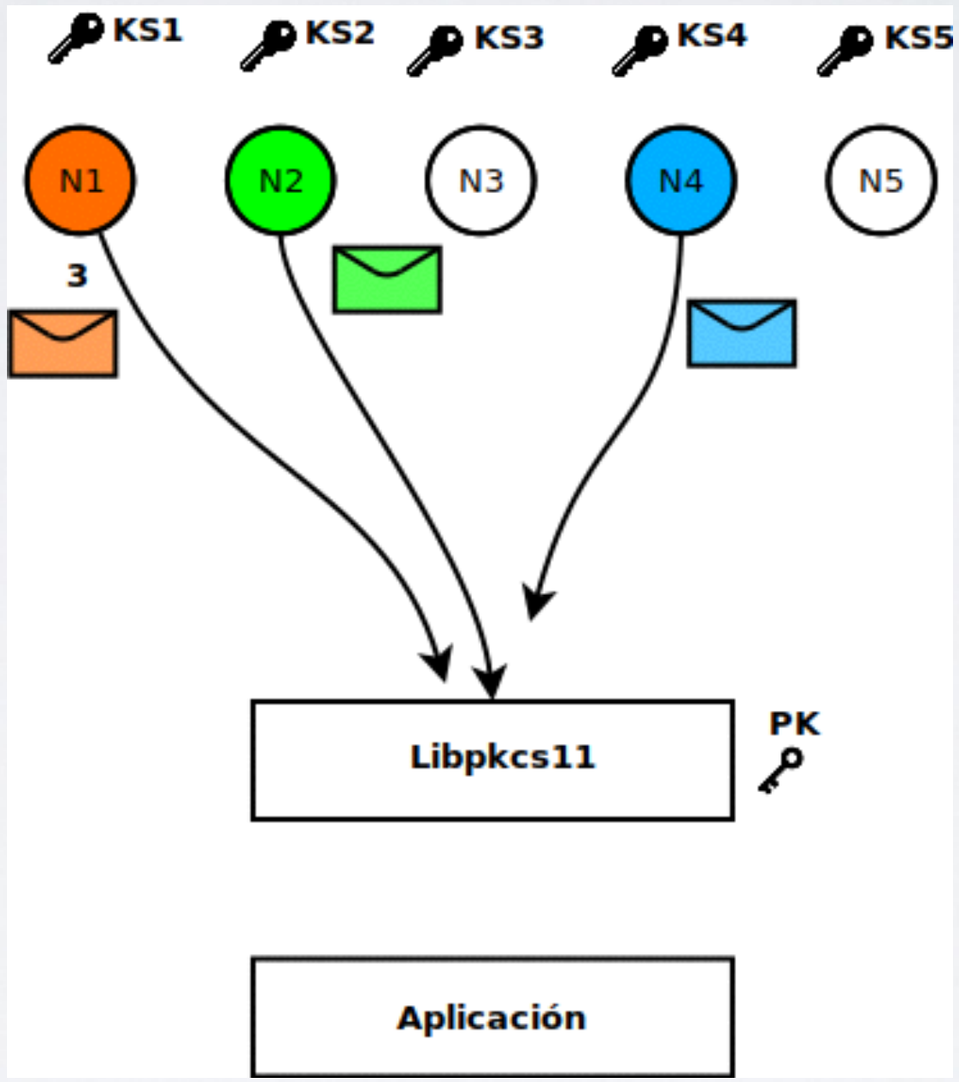
SYSTEM'S OPERATION



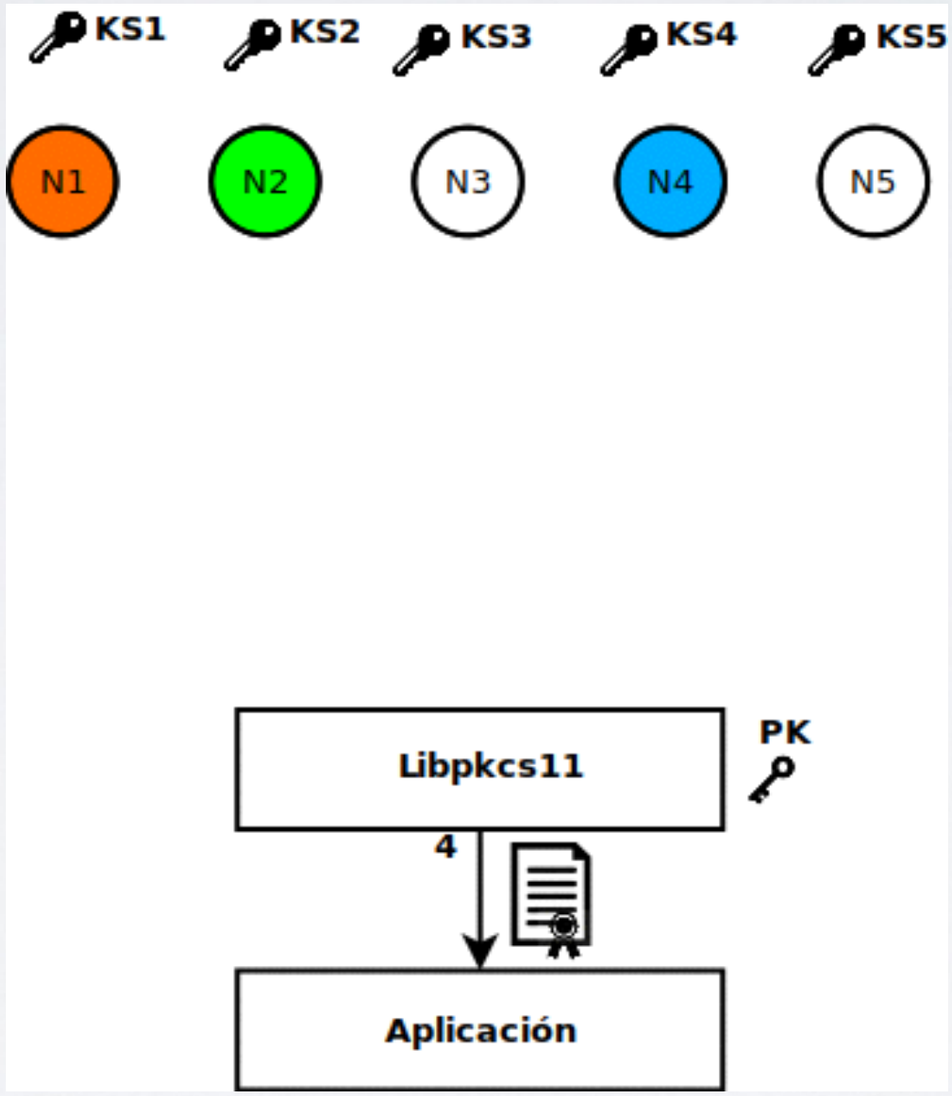
SYSTEM'S OPERATION



SYSTEM'S OPERATION

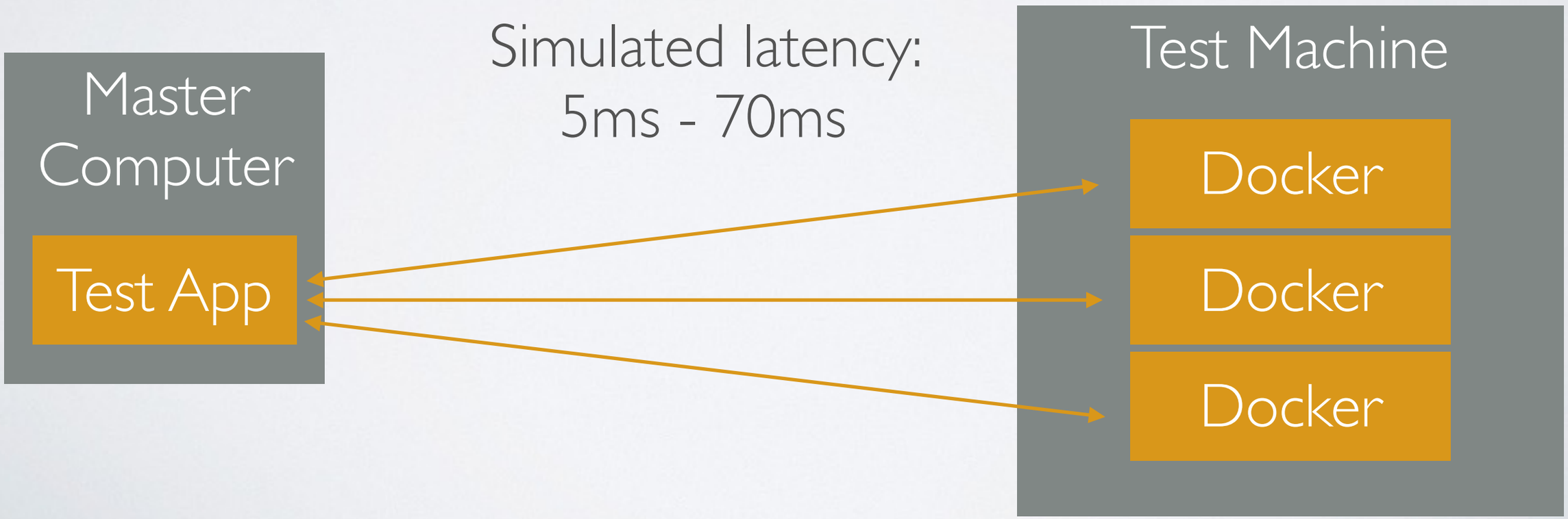


SYSTEM'S OPERATION



SYSTEM'S PERFORMANCE

- ~80 RSA Signatures / second, with a 1024 bits key.
- 1 RSA1024 bit key on ~6 seconds.



FUTURE WORK

- Fully distributed key generation.
- Test the system with more applications, possibly on fields other than DNSSEC.

THRESHOLD-CRYPTOGRAPHY DISTRIBUTED HSM

(TCHSM)

Francisco Cifuentes
francisco@niclabs.cl