# Threshold Cryptography Distributed HSM

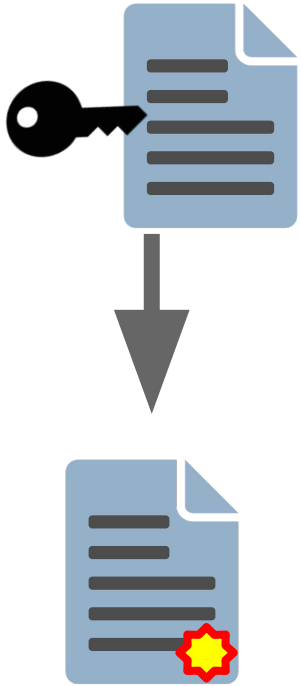
Francisco Montoto
*montoto@niclabs.cl*

frida
una iniciativa de LACNIC

NIC CHILE Research labs

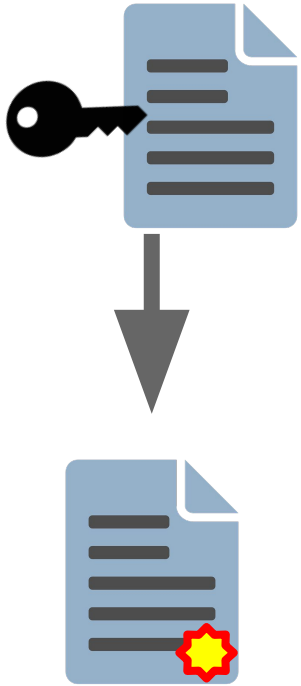
# Criptografía umbral

## Esquema tradicional de llave pública

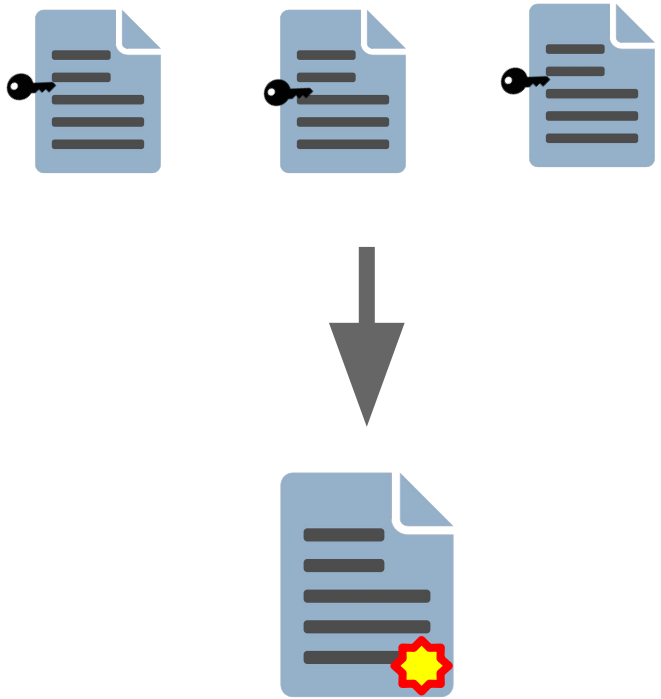


# Criptografía umbral

Esquema tradicional de llave pública

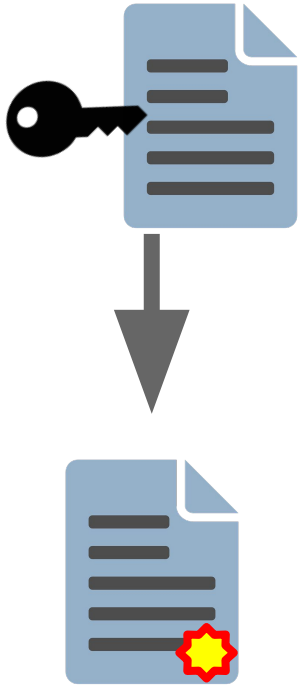


Umbral

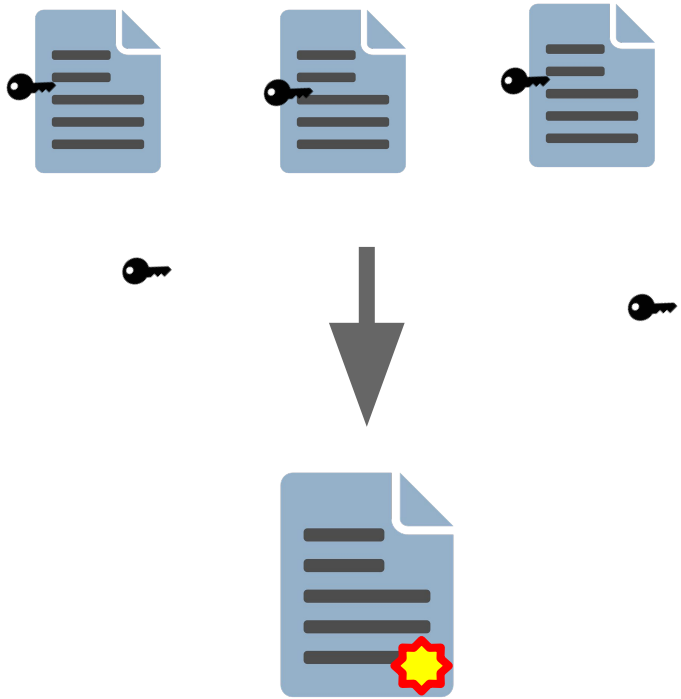


# Criptografía umbral

Esquema tradicional de llave pública



Umbral



# Hardware Security Module (HSM)

Dispositivo criptográfico basado en *hardware* que genera, almacena y protege claves criptográficas.

# TCHSM

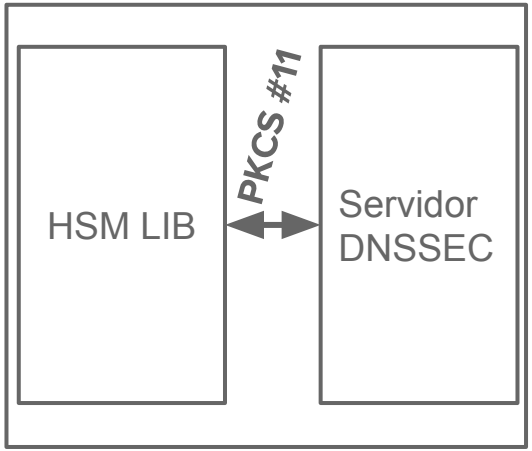
- Simular un HSM utilizando criptografía umbral, permitiendo prescindir de la adquisición de hardware dedicado manteniendo un buen nivel de seguridad.

# TCHSM

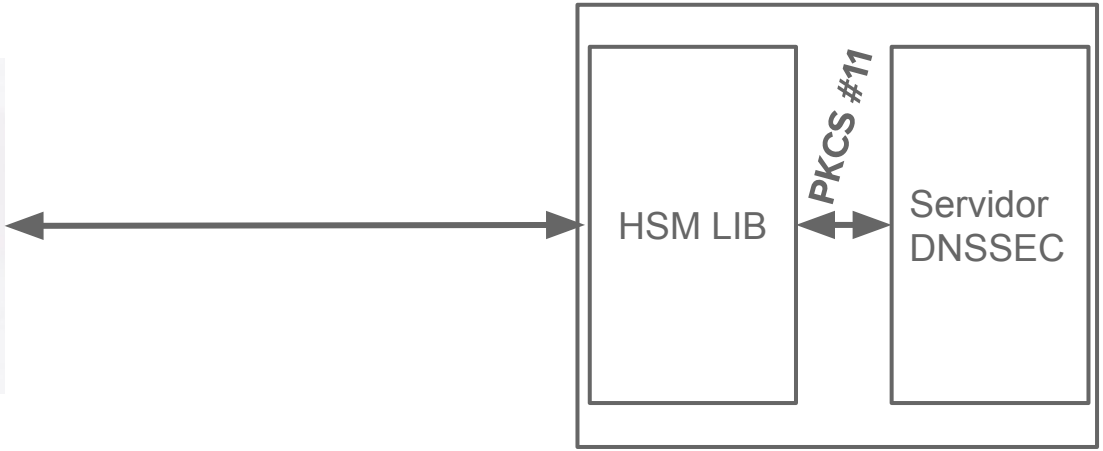
- Simular un HSM utilizando criptografía umbral, permitiendo prescindir de la adquisición de hardware dedicado manteniendo un buen nivel de seguridad.
- Idea presentada en LACNIC 22 http://www.lacnic.net/en/web/eventos/lacnic22-agenda-detallada

# Uso del HSM en un servidor DNSSEC

# Uso del HSM en un servidor DNSSEC

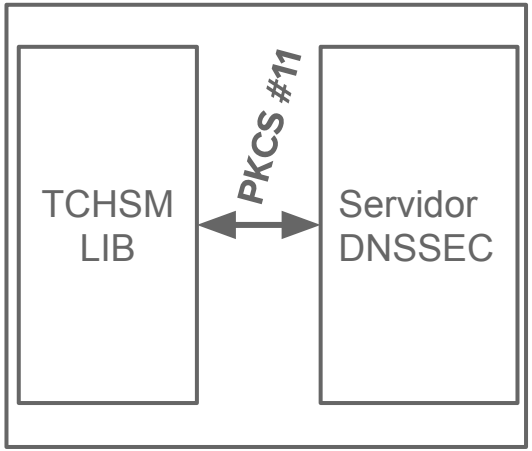


# Uso del HSM en un servidor DNSSEC

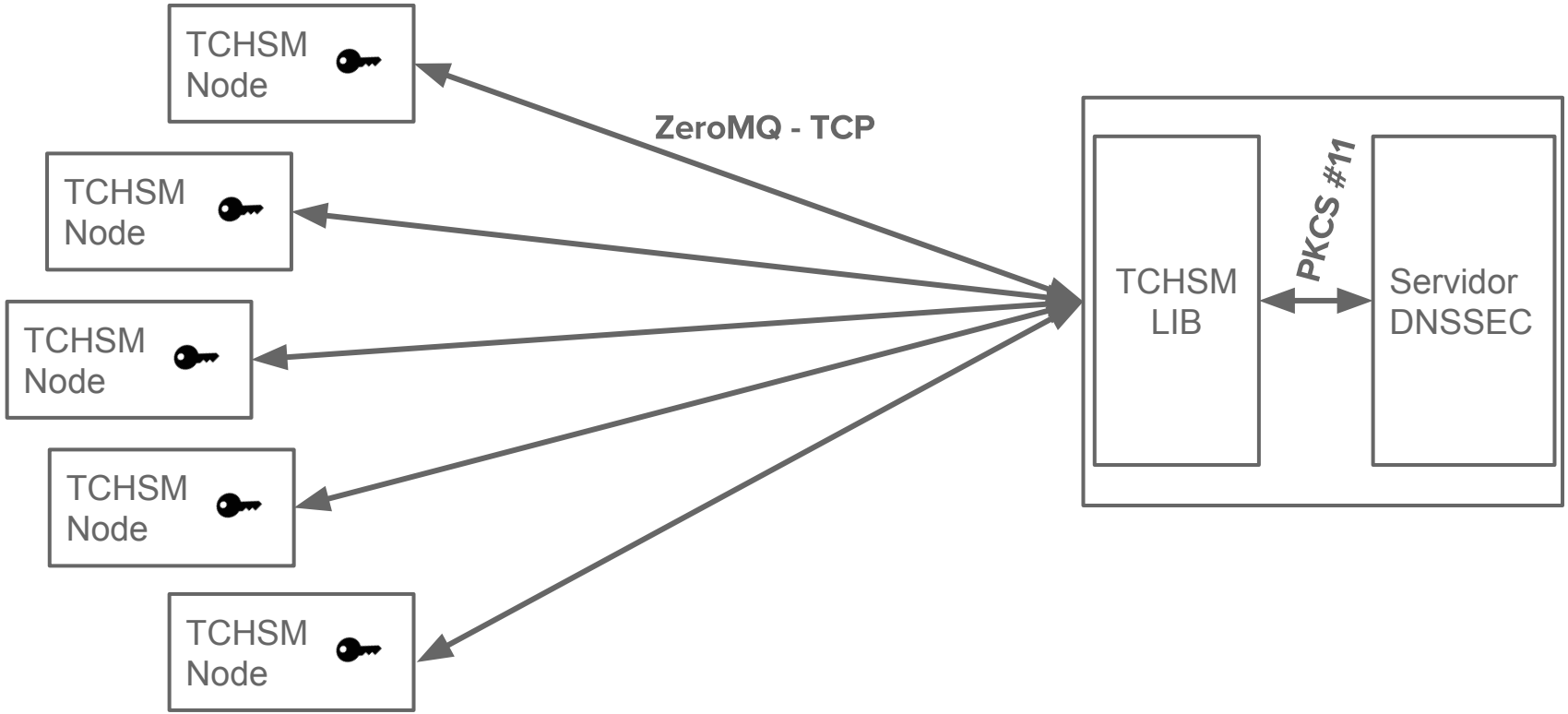



# Uso de TCHSM en un servidor DNSSEC

# Uso de TCHSM en un servidor DNSSEC

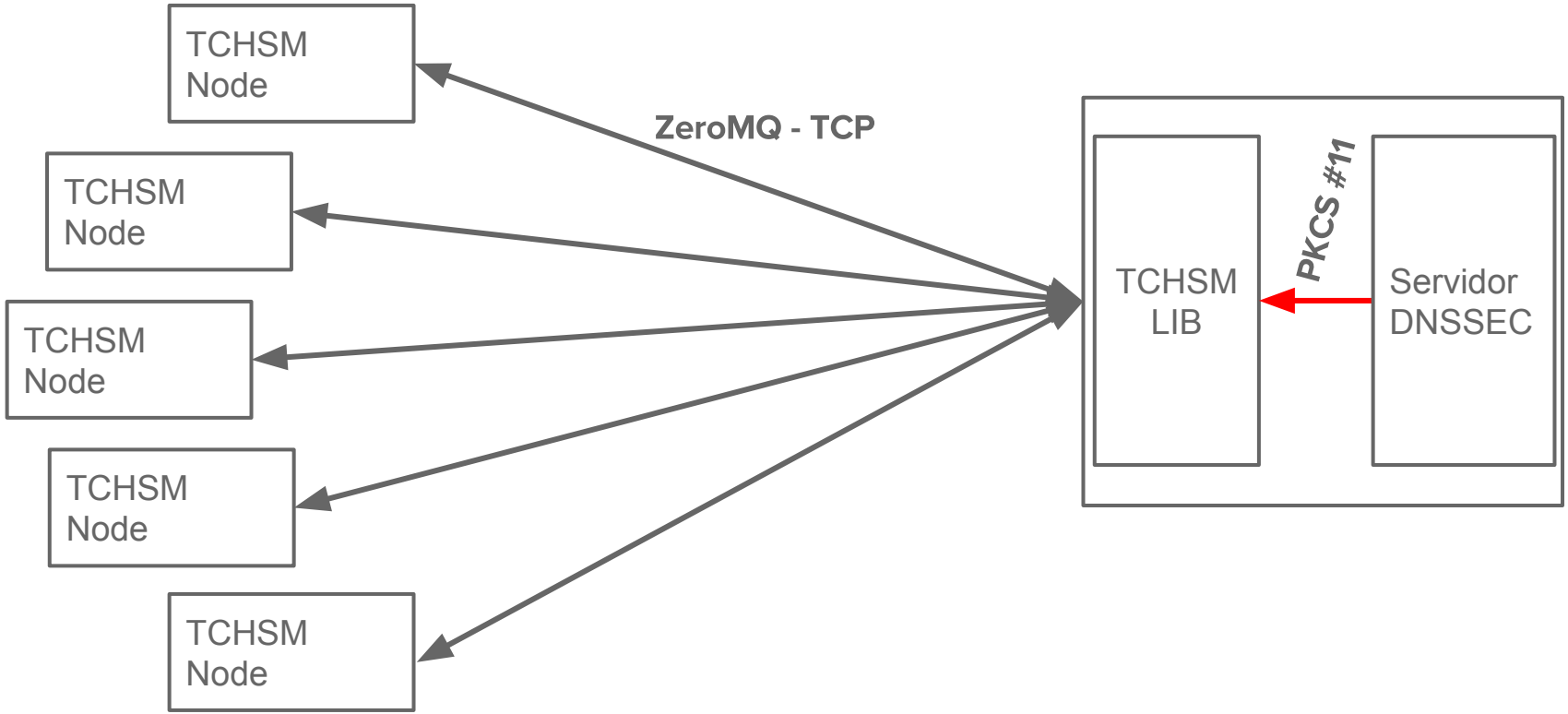


# Uso de TCHSM en un servidor DNSSEC

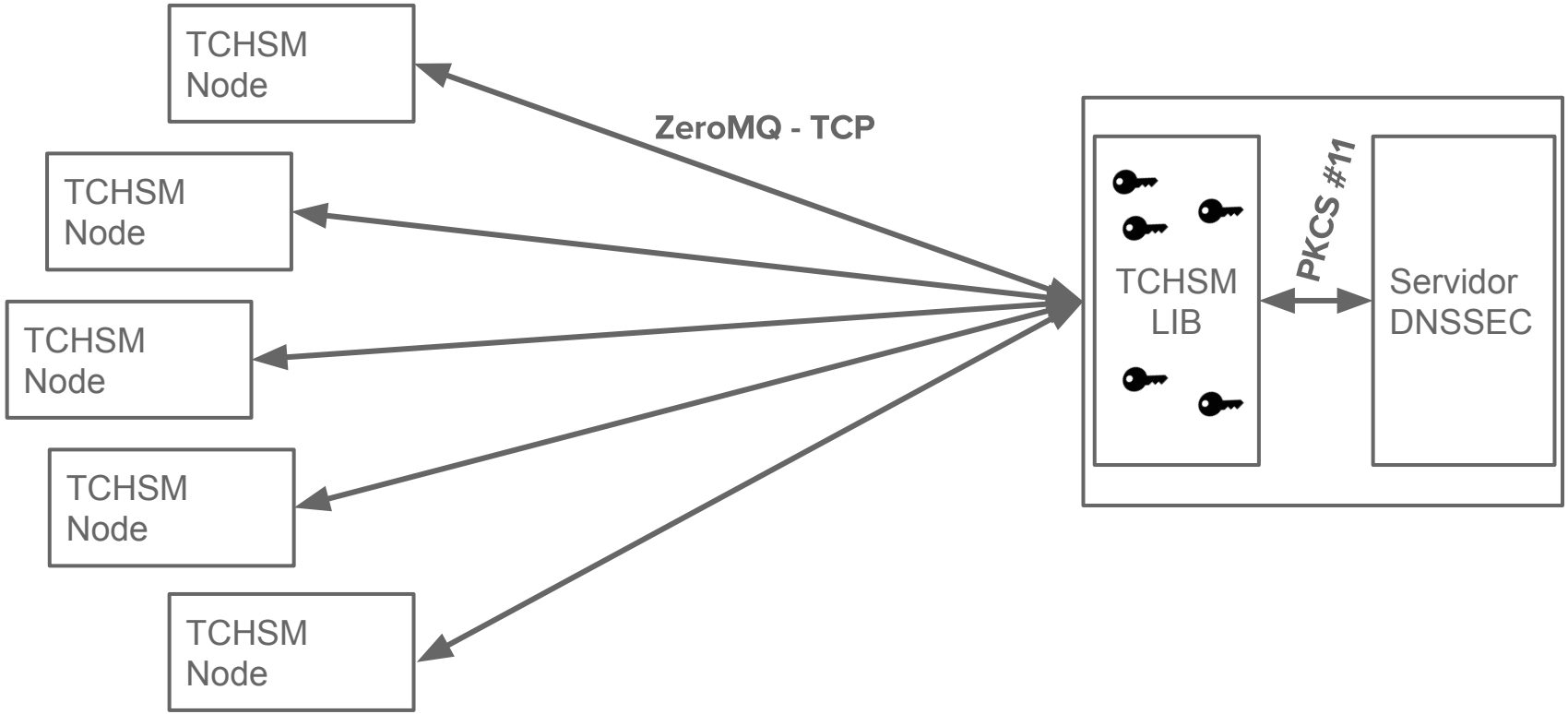


# Generación de llaves

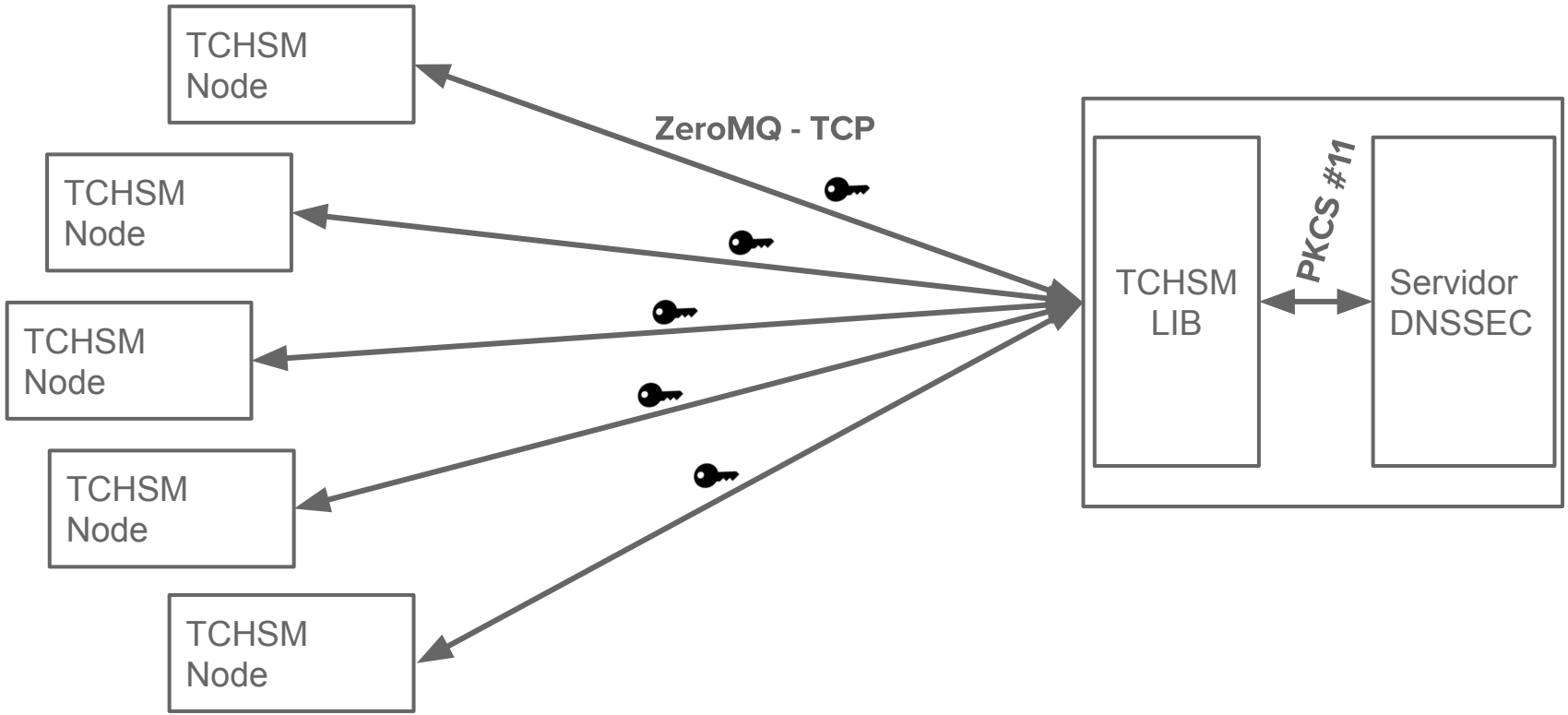
# Generación de llaves



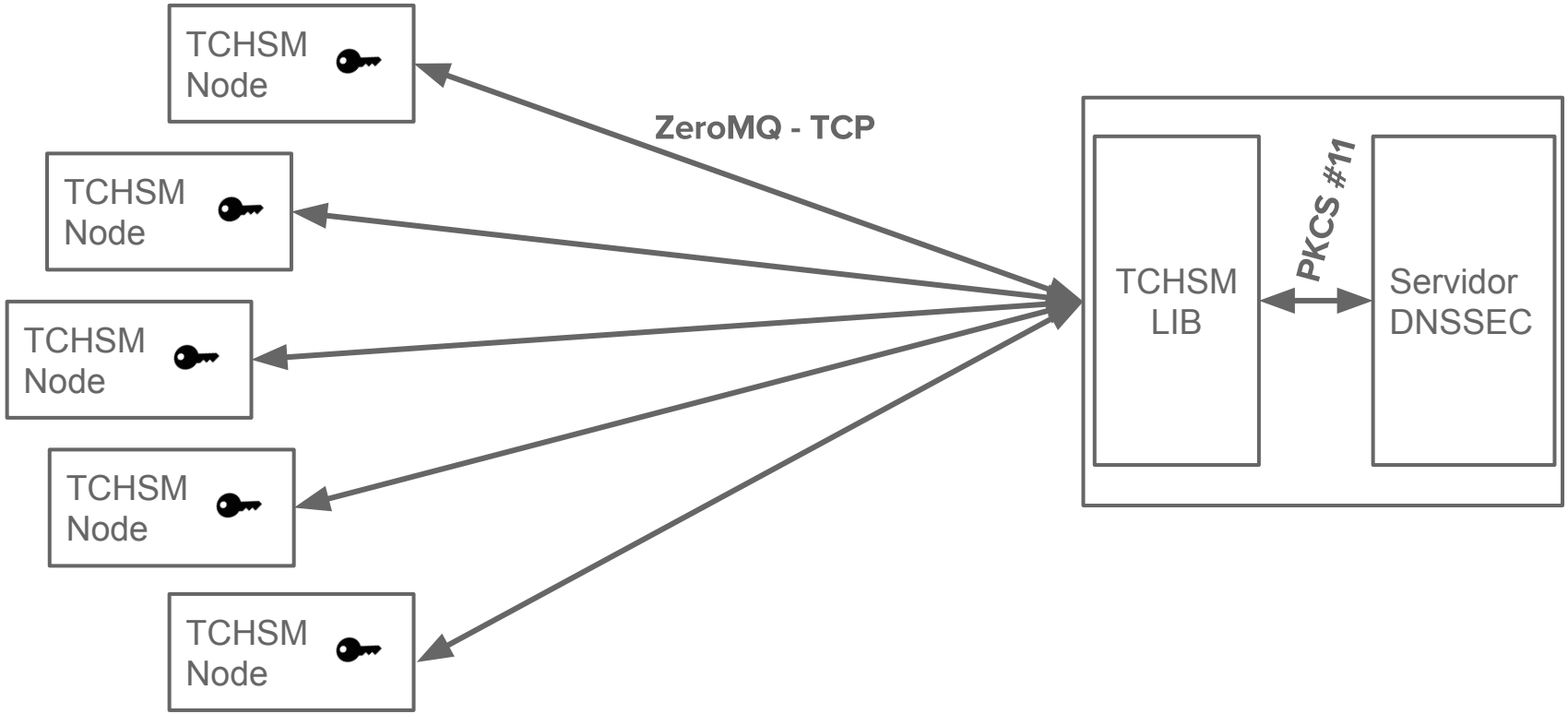
# Generación de llaves



# Generación de llaves

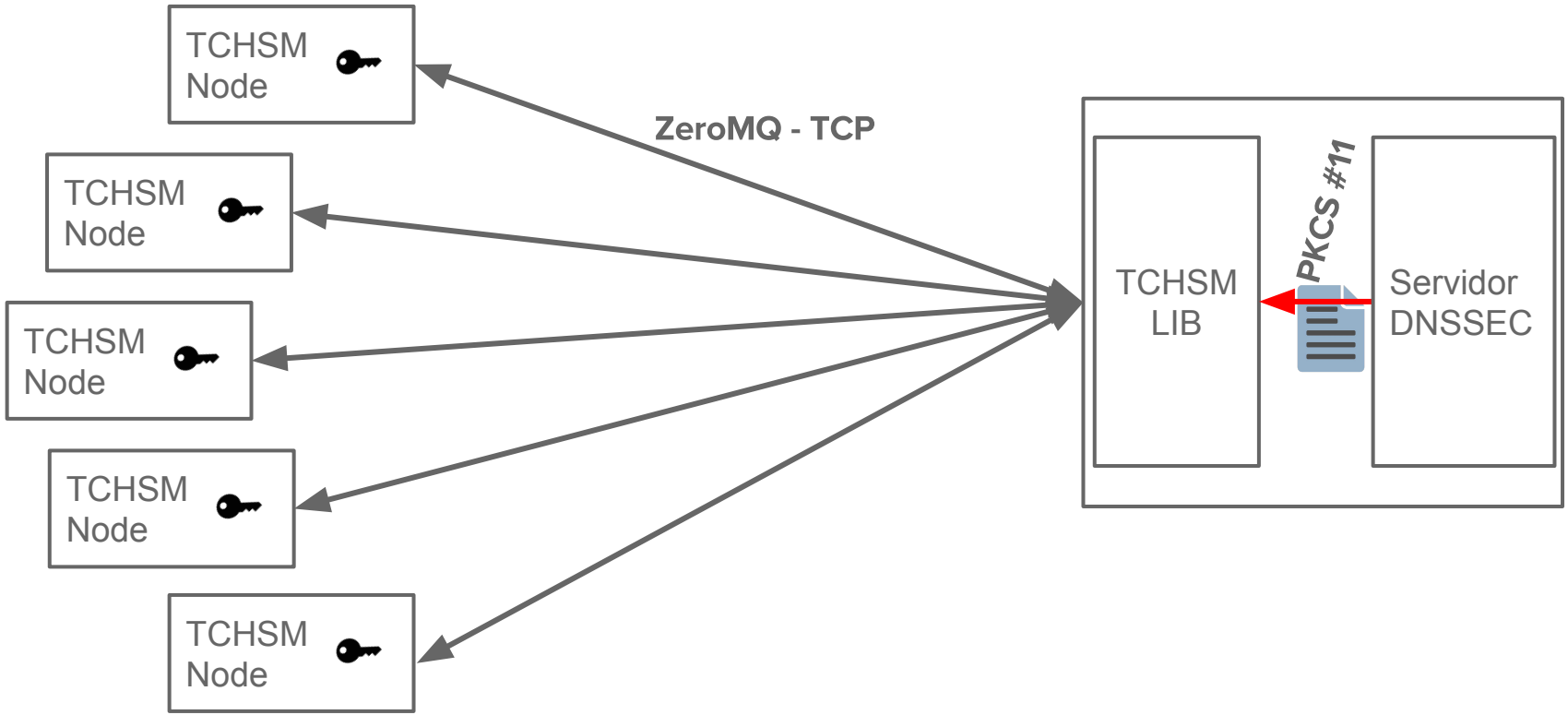


# Generación de llaves

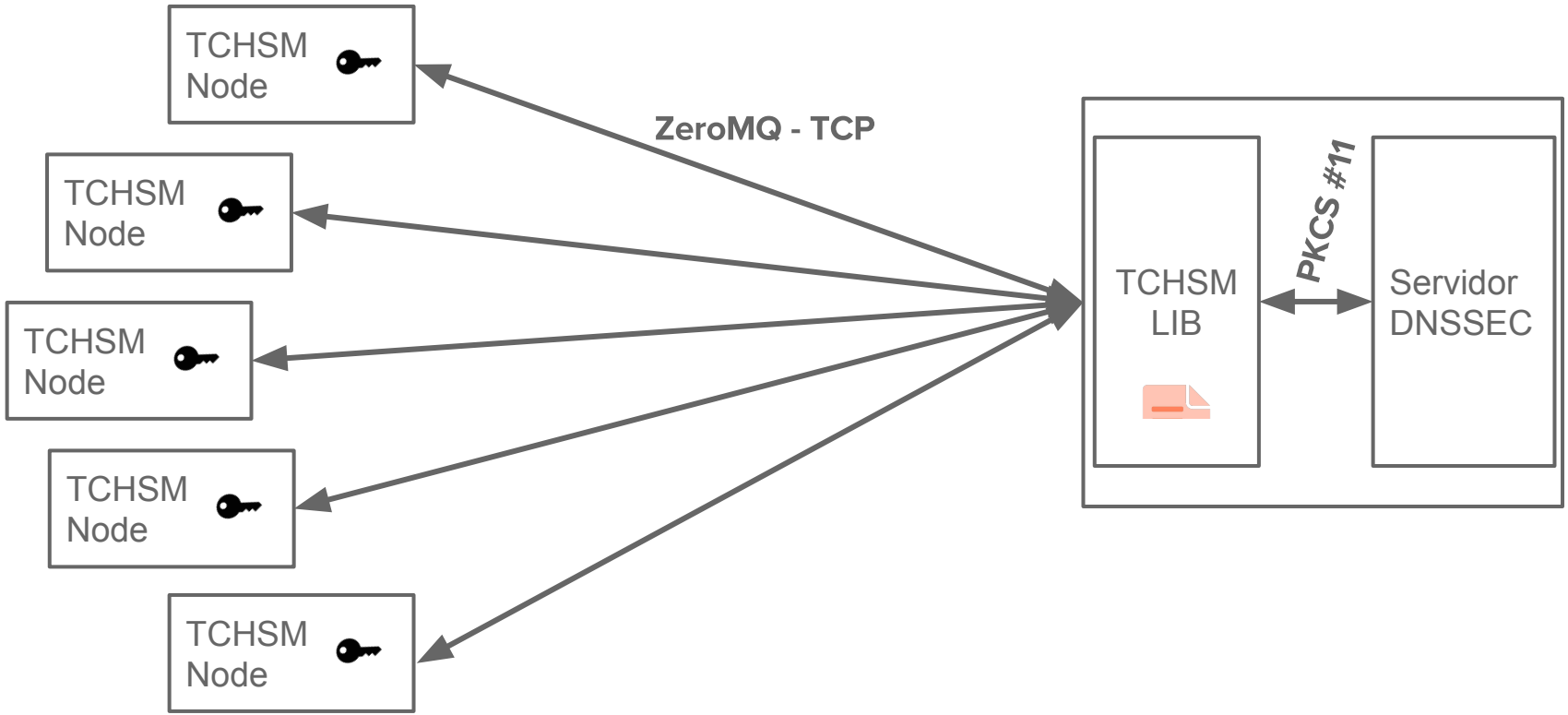


Firma

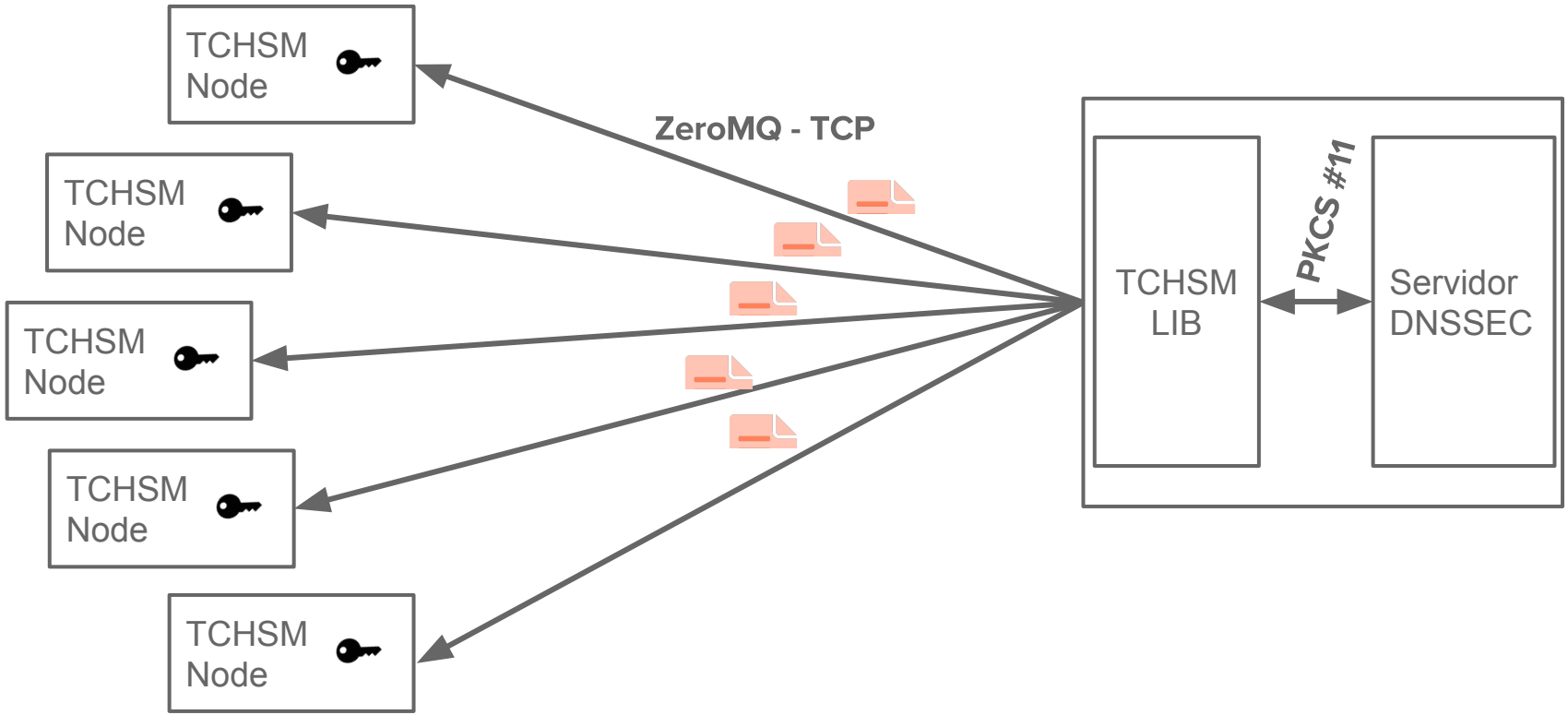
# Firma


TCHSM Node
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM Node
ZeroMQ - TCP
TCHSM LIB
PKCS #11
Servidor DNSSEC

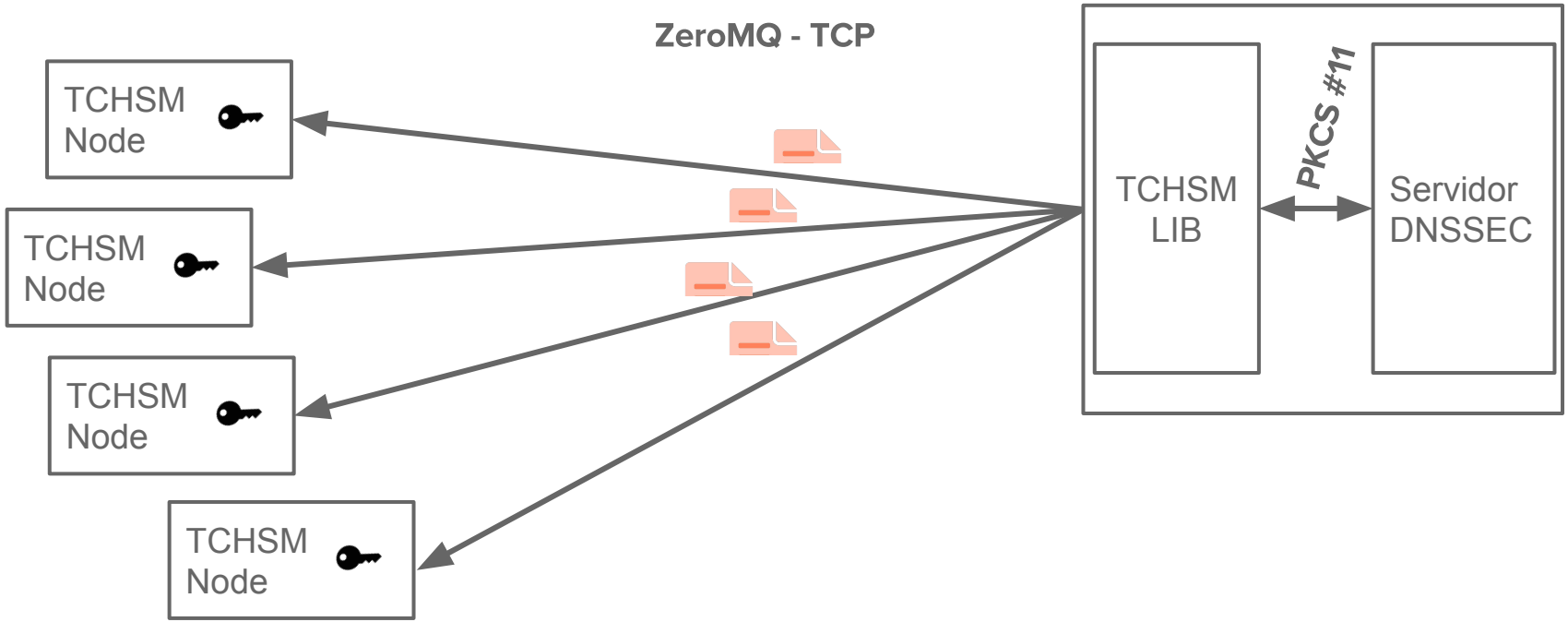
# Firma


TCHSM Node
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM Node
ZeroMQ - TCP
TCHSM LIB
PKCS #11
Servidor DNSSEC

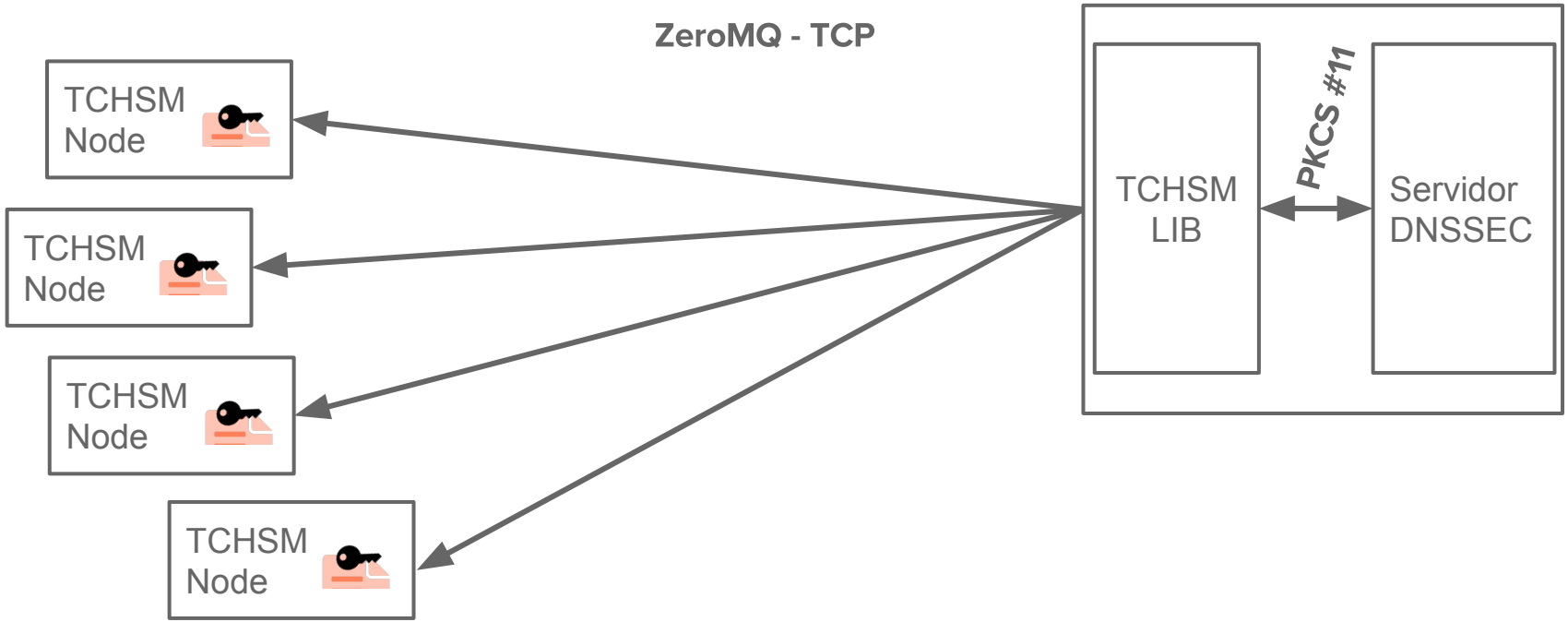
# Firma


TCHSM Node
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM Node
ZeroMQ - TCP
TCHSM LIB
PKCS #11
Servidor DNSSEC

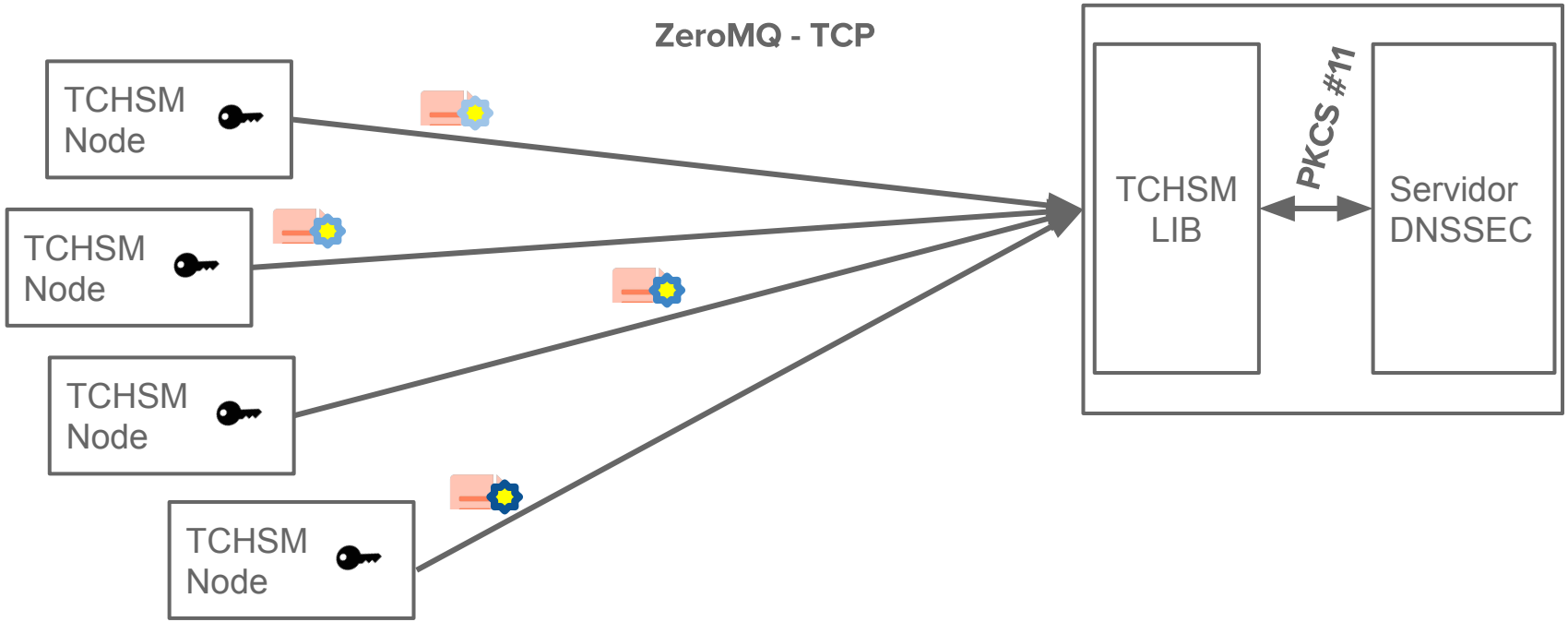
# Firma


ZeroMQ - TCP
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM LIB
PKCS #11
Servidor DNSSEC

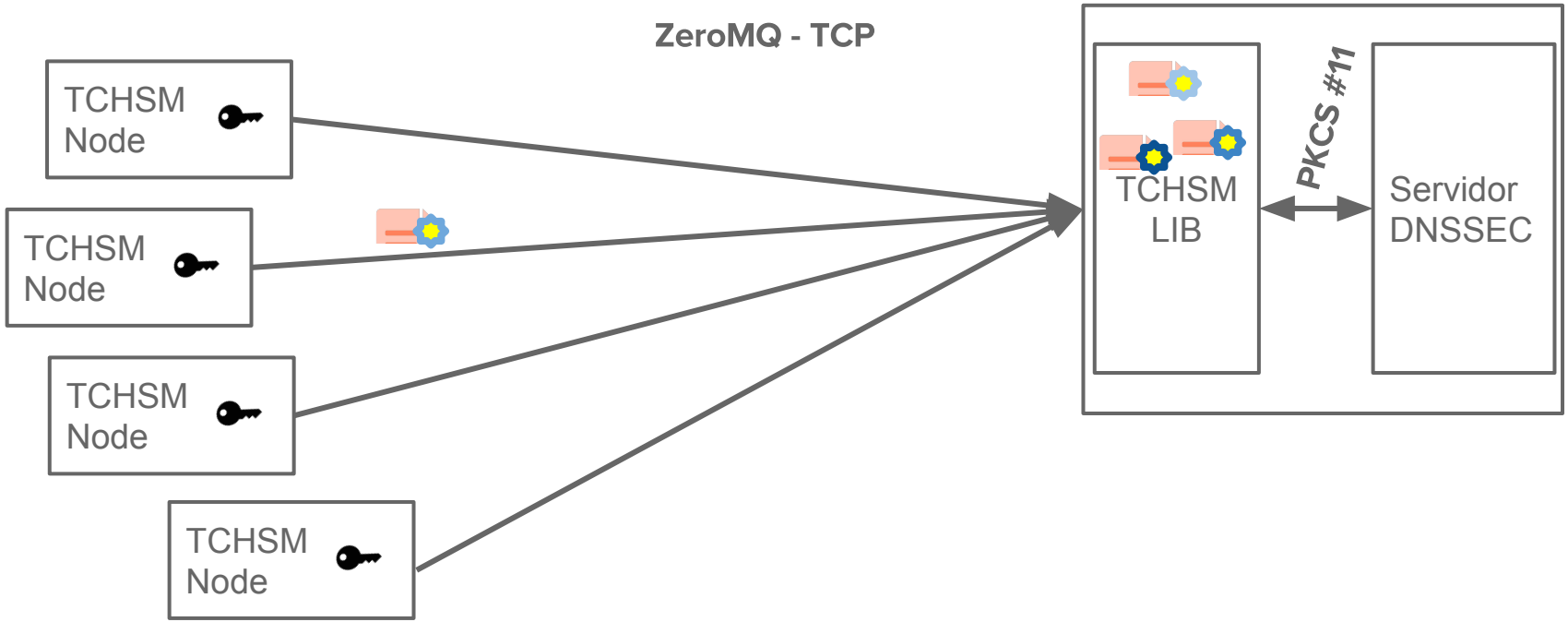
# Firma


ZeroMQ - TCP
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM LIB
PKCS #11
Servidor DNSSEC

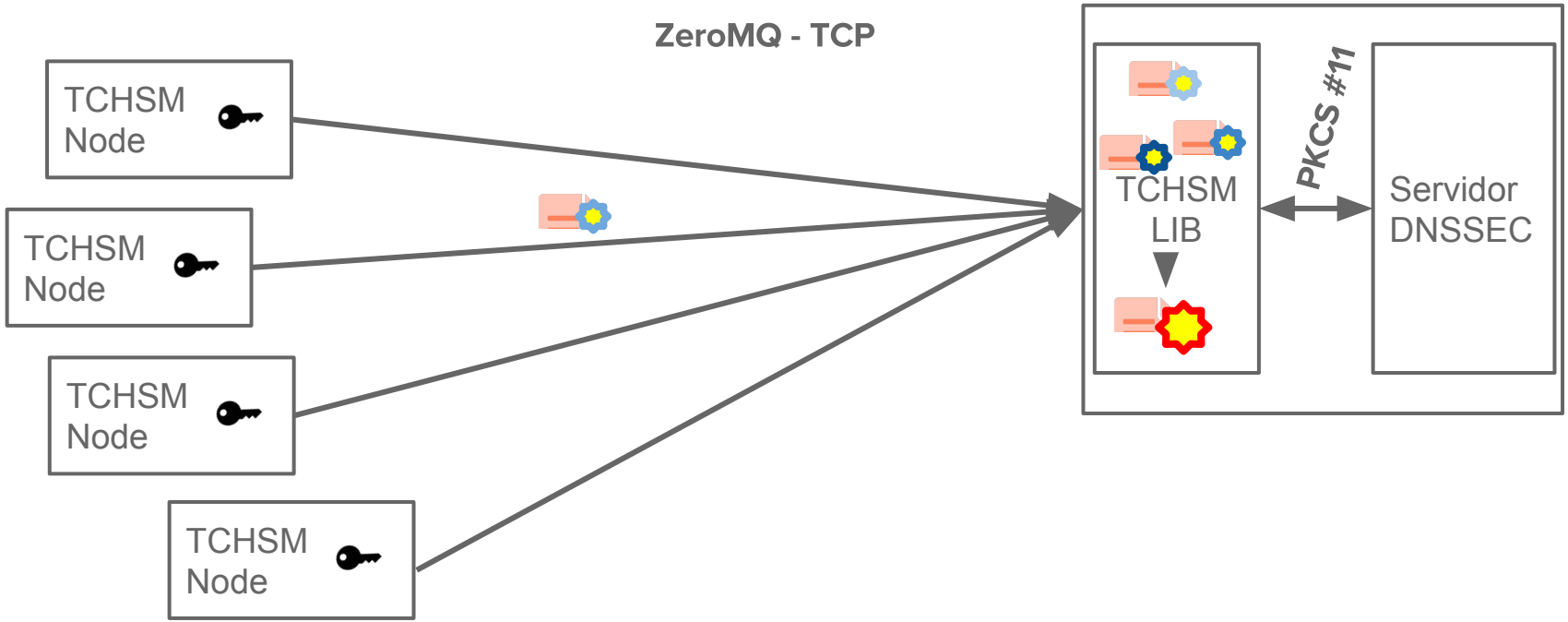
# Firma


ZeroMQ - TCP
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM LIB
PKCS #11
Servidor DNSSEC

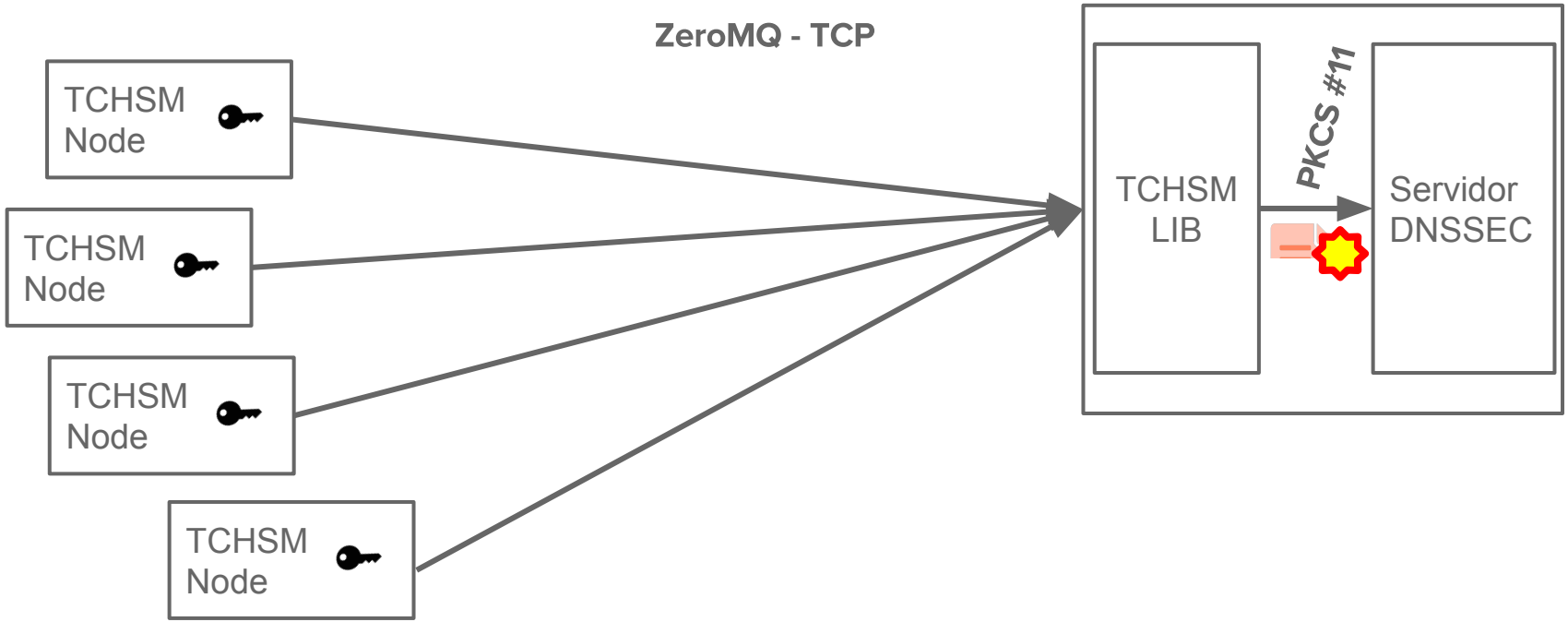
# Firma


ZeroMQ - TCP
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM LIB
PKCS #11
Servidor DNSSEC

# Firma


ZeroMQ - TCP
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM LIB
PKCS #11
Servidor DNSSEC

# Firma


ZeroMQ - TCP
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM Node
TCHSM LIB
PKCS #11
Servidor DNSSEC

# Pasos para utilizar el TCHSM

1. Generación de archivos de configuración con llaves
    - Herramienta para generar configuración en scripts/create_config.py

# Pasos para utilizar el TCHSM

1. Generación de archivos de configuración con llaves
    - Herramienta para generar configuración en scripts/create_config.py
2. Distribución offline de las llaves de comunicación que permiten autenticación y encriptación de la comunicación
    - Las llaves deben ser distribuidas de forma manual

# Pasos para utilizar el TCHSM

1. Generación de archivos de configuración con llaves
    - Herramienta para generar configuración en scripts/create_config.py
2. Distribución offline de las llaves de comunicación que permiten autenticación y encriptación de la comunicación
    - Las llaves deben ser distribuidas de forma manual
3. Ejecución de los nodos

# Estado actual

- Versión estable, soporte ofrecido por niclabs.

# Estado actual

- Versión estable, soporte ofrecido por niclabs.
- Integración y pruebas en dos de los servidores DNS más utilizados: Bind y Knot.

# Estado actual

- Versión estable, soporte ofrecido por niclabs.
- Integración y pruebas en dos de los servidores DNS más utilizados: Bind y Knot.
- niclabs.cl firmado y operando utilizando el software.

# Desempeño

- Pruebas realizadas en un computador de escritorio con Intel® Core™ i5-2400 CPU @ 3.10GHz × 4. Con un container de docker para cada participante en el esquema.
- Firmas: ~75/s
- Firma de 250k dominios, en un archivo de zona con 500k líneas toma 2h50m.

# Trabajo futuro

- Generación distribuida de llaves

# Trabajo futuro

- Generación distribuida de llaves
- Auditoría de seguridad

# Trabajo futuro

- Generación distribuida de llaves
- Auditoría de seguridad
- Patente pendiente. Solicitud 3766-2015, INAPI

# Threshold Cryptography Distributed HSM

Francisco Montoto
*montoto@niclabs.cl*

frida
una iniciativa de LACNIC

**Source:** https://github.com/niclabs/tchsm-libdtc
**Docker:** https://github.com/niclabs/docker/tree/master/tchsm

NIC CHILE Research labs