ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERIA EN SISTEMAS

DISEÑO Y PROTOTIPO DE UN SISTEMA DE AUDITORIA Y CONTROL ELECTORAL PARA LOS PROCESO DE ESCRUTINIOS Y PUBLICACIONES DE RESULTADOS BASADOS EN DLT

DISEÑO E IMPLEMENTACION DEL PROTOTIPO DEL SISTEMA DE SEGURIDAD

Autor: Emerson Ceracapa

Tutor: Dr. Enrique Mafla

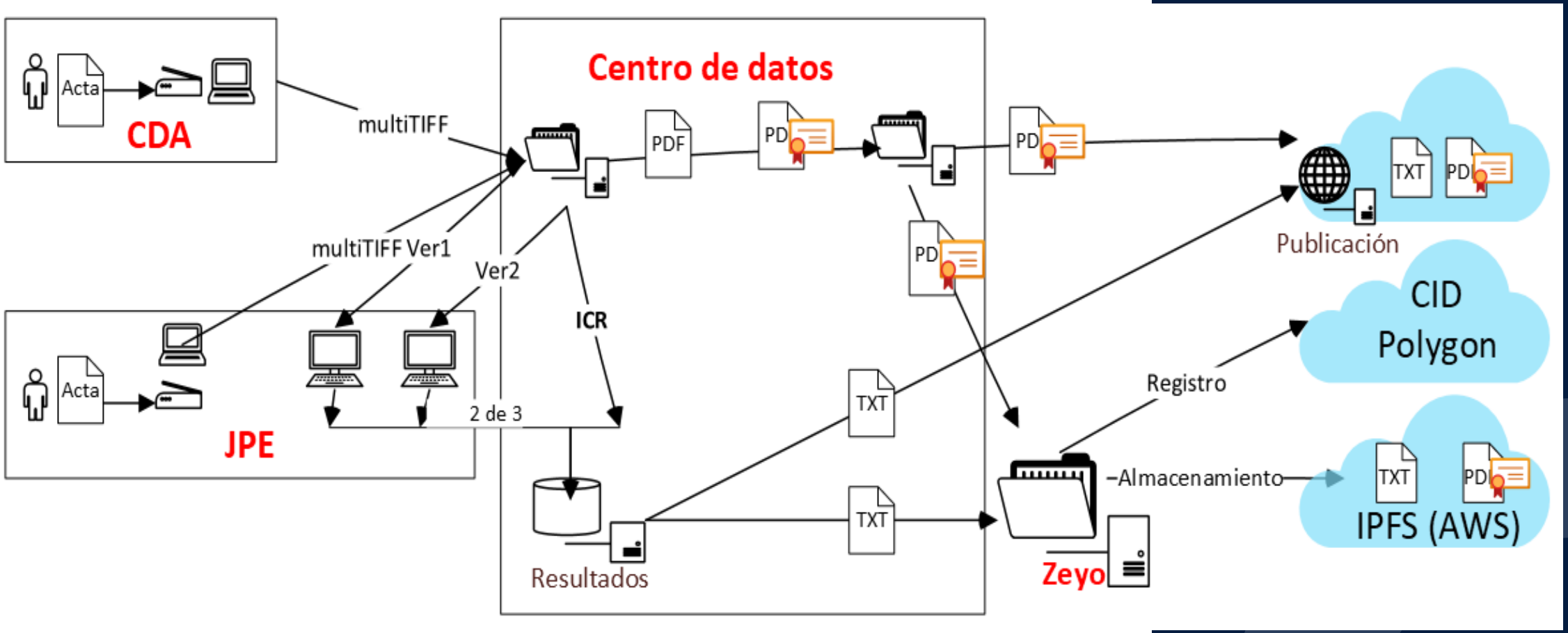
Objetivo General

Garantizar la identificación y autenticación segura y confiable de los diferentes componentes de la red blockchain, así como la integridad y confidencialidad de las comunicaciones entre dichos elementos. Esto se logrará mediante el diseño de una robusta infraestructura de llave pública (PKI).

Objetivos Específicos

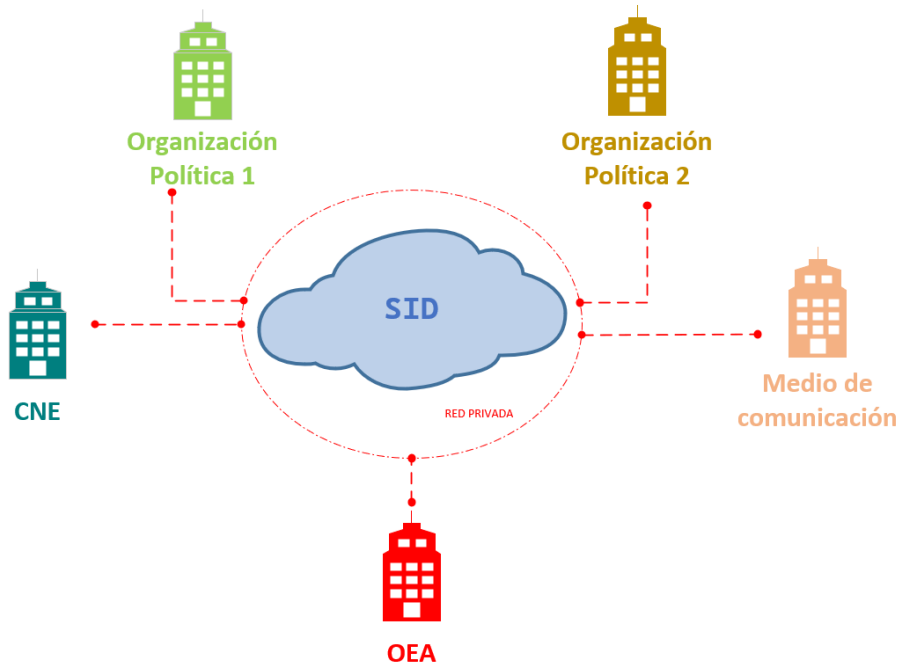
1. Analizar los problemas de seguridad y transparencia en el proceso actual de escrutinios y publicación de resultados.
2. Revisar las soluciones existentes para una PKI.
3. Diseñar un sistema de seguridad basado en una PKI.
4. Implementar un prototipo PKI para validar el diseño.

Análisis de la Situación Actual



Descentralización y Red

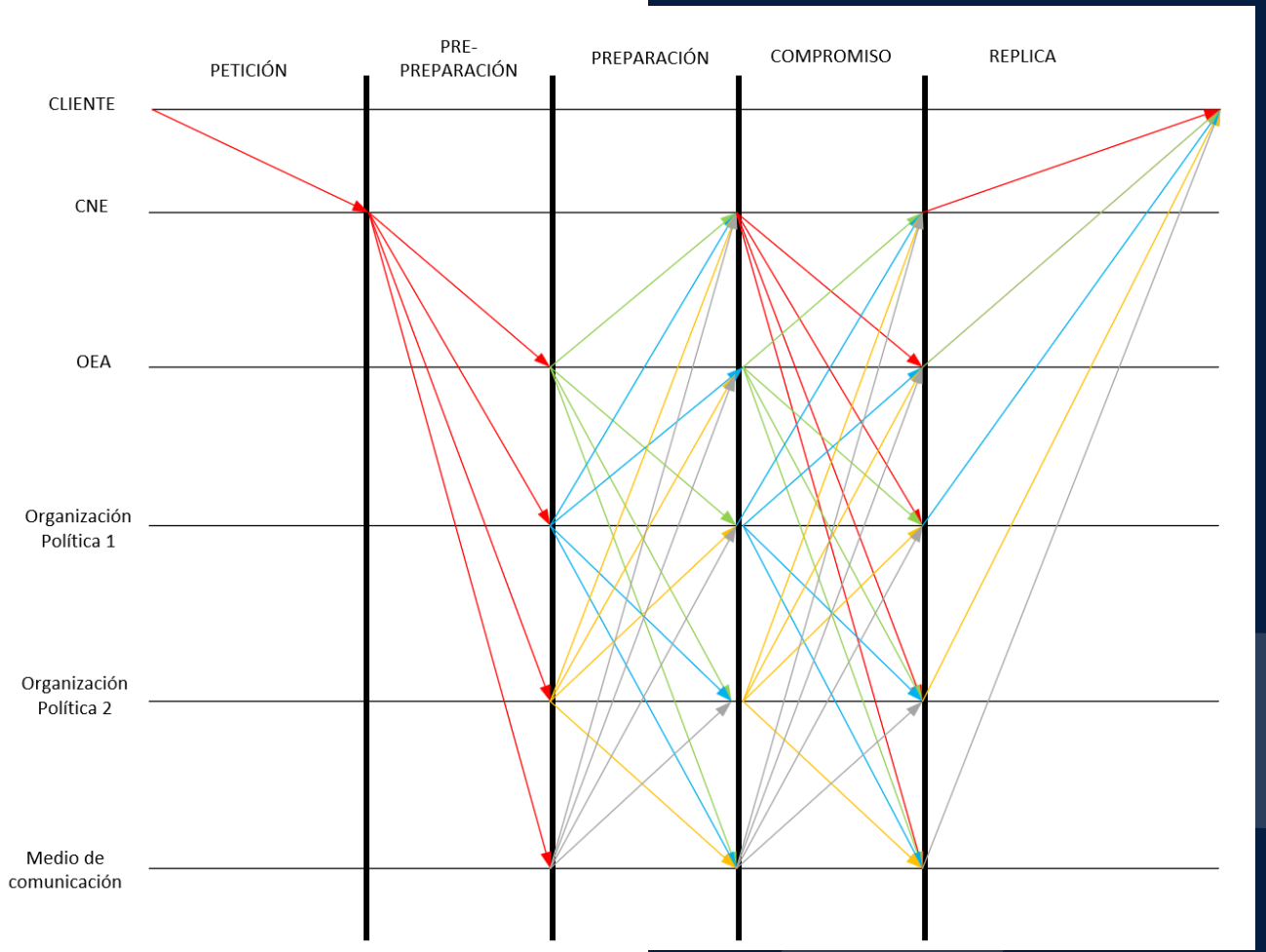
- Para solventar el problema de descentralización, el diseño plantea implementar un SID, en el cuál participen más organizaciones.
- A su vez, también se plantea que este SID se encuentre en una red privada.



Consenso

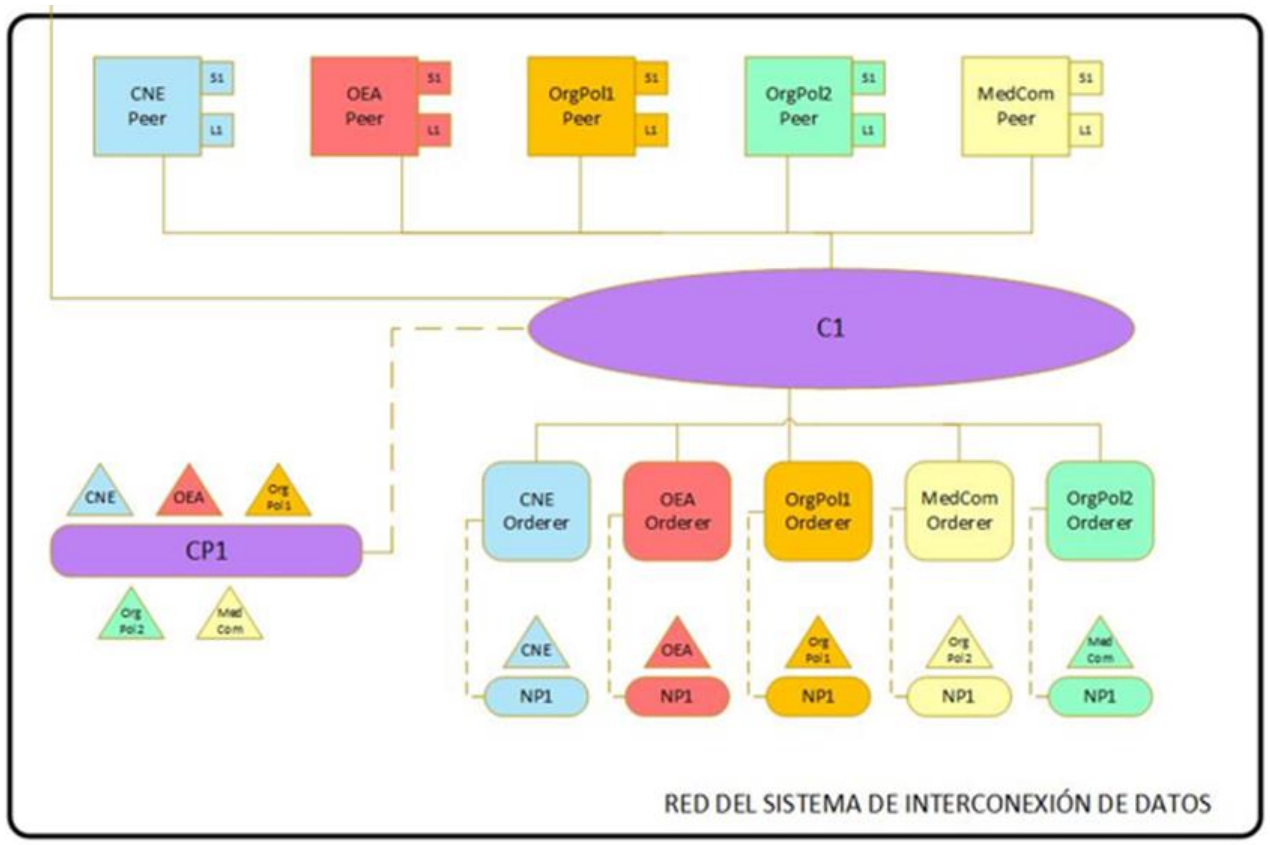
- Se hará uso de algoritmos contra fallas bizantinas (BFT), ,en específico, el algoritmo PBFT (Practical Bizantine Fault Tolerance).

- Para que una transacción sea realizada dentro del sistema todos los participantes dentro del SID deben aprobarla.



Canal

El SID deberá tener únicamente un solo canal, esto para fomentar que la comunicación entre los nodos sea transparente y eficiente.



Autoridades Certificadoras (CAs)

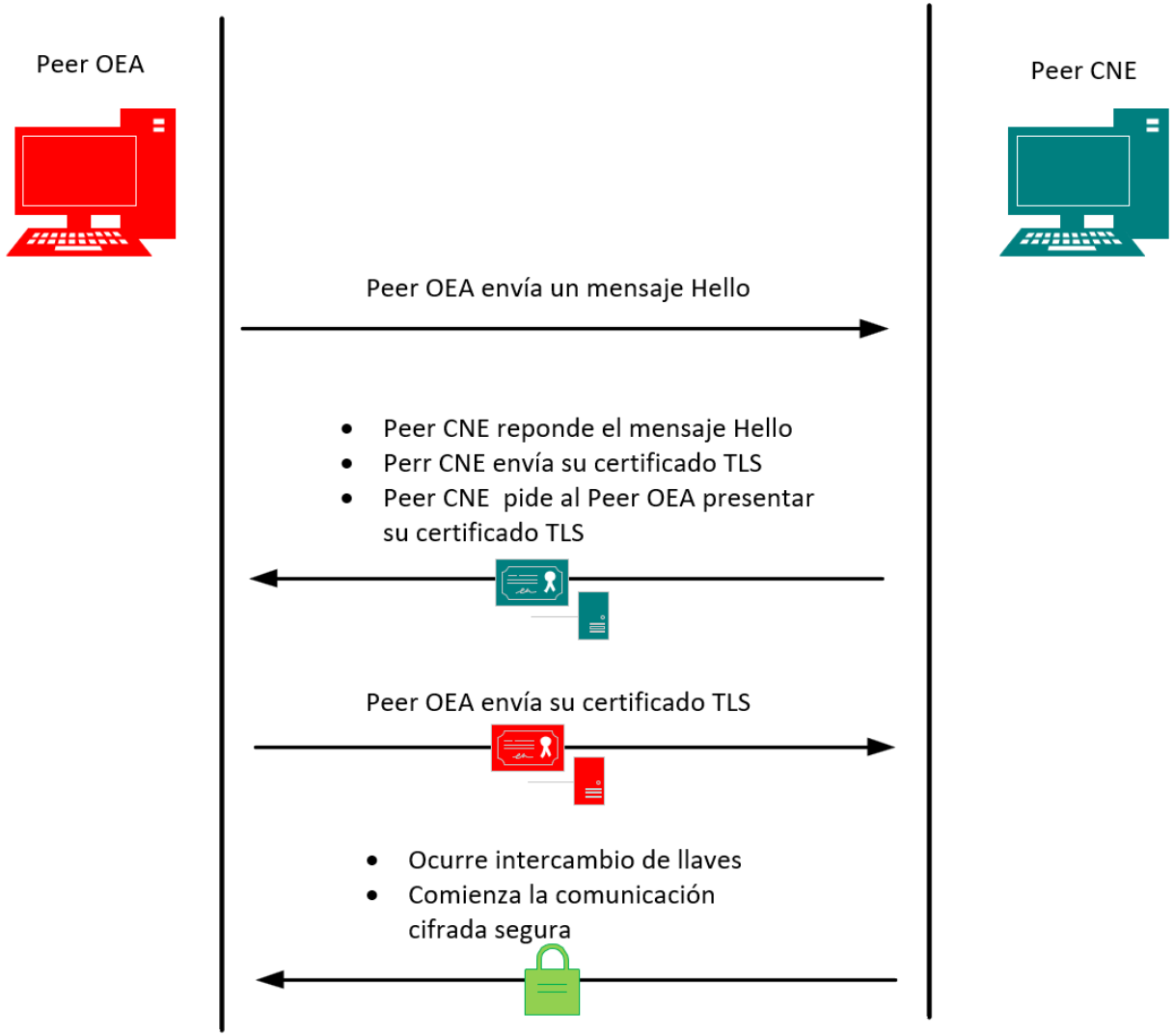
Para TLS

- CA utilizada para asegurar las comunicaciones entre las organizaciones.
- Las comunicaciones se realizan con el uso de certificados de TLS.

Para Enrollment

- CA encargada de la emisión de certificados de identidad de los usuarios, administradores y nodos participantes de la red.
- Estos certificados son usados para autenticar las identidades y autorizar operaciones dentro del SID.

Funcionamiento TLS



Proveedor de servicios de membresía (MSP)

- Cada organización tendrá su propio MSP.
- MSP especifica que certificados de las respectivas cas de las organizaciones serán válidos para actuar en nombre de dicha organización.

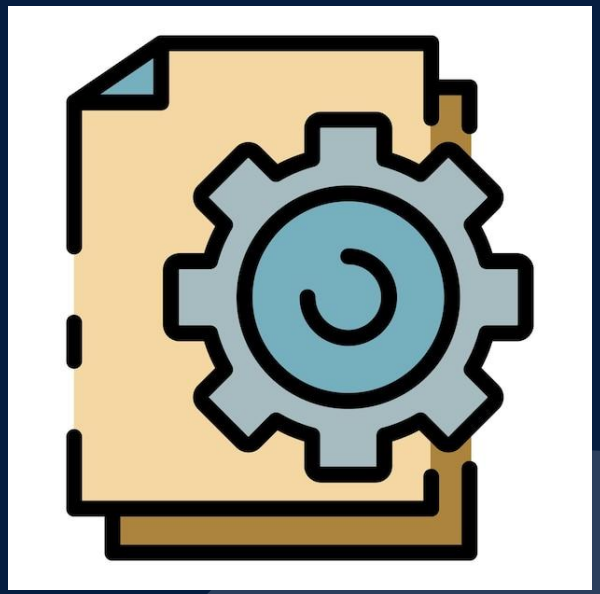
Archivos de configuración

fabric-ca-server-config

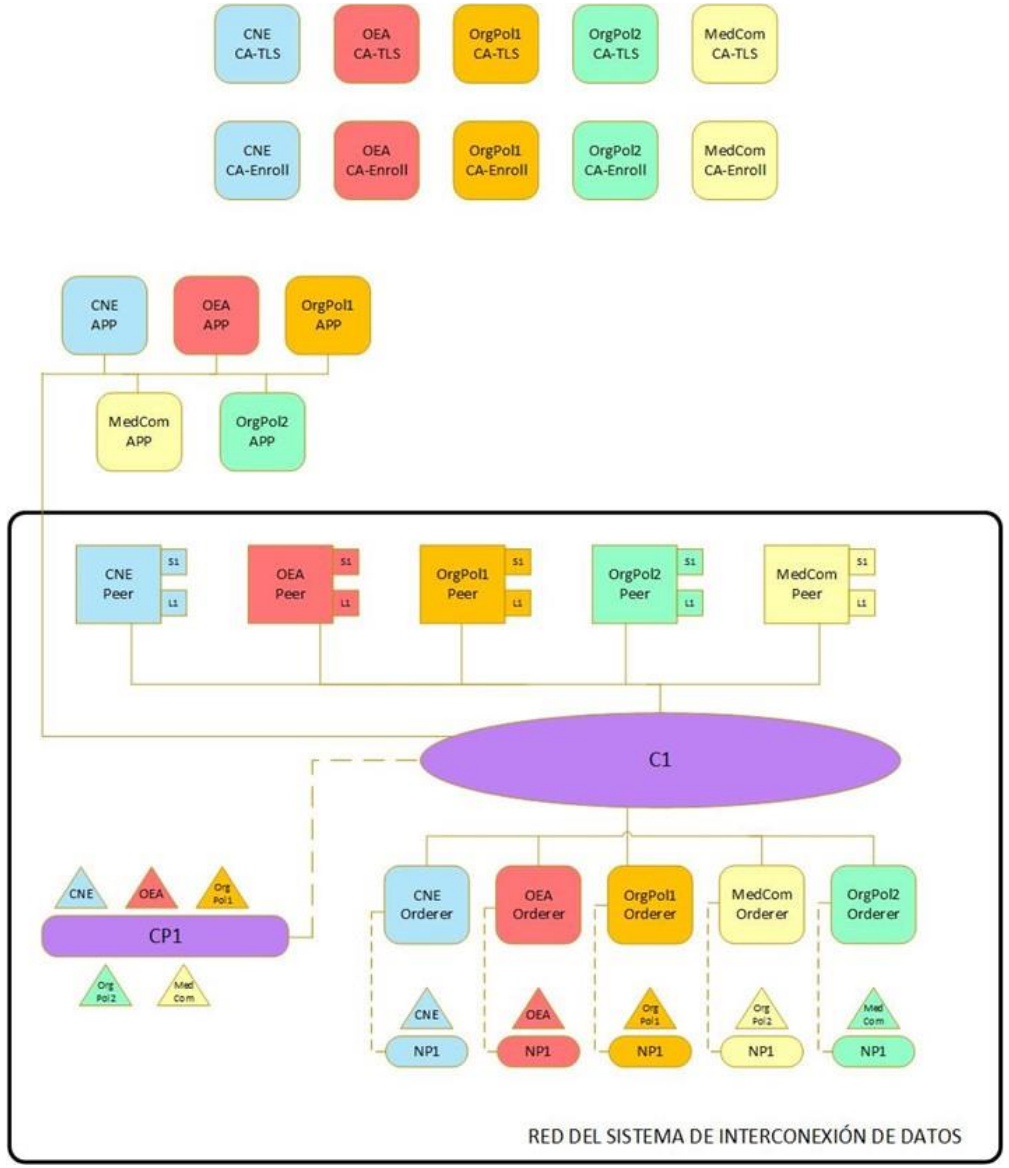
- Define los parámetros de funcionamiento de una CA.
- Todas las organizaciones participantes deberán acordar las configuraciones de sus CAs.

configtx

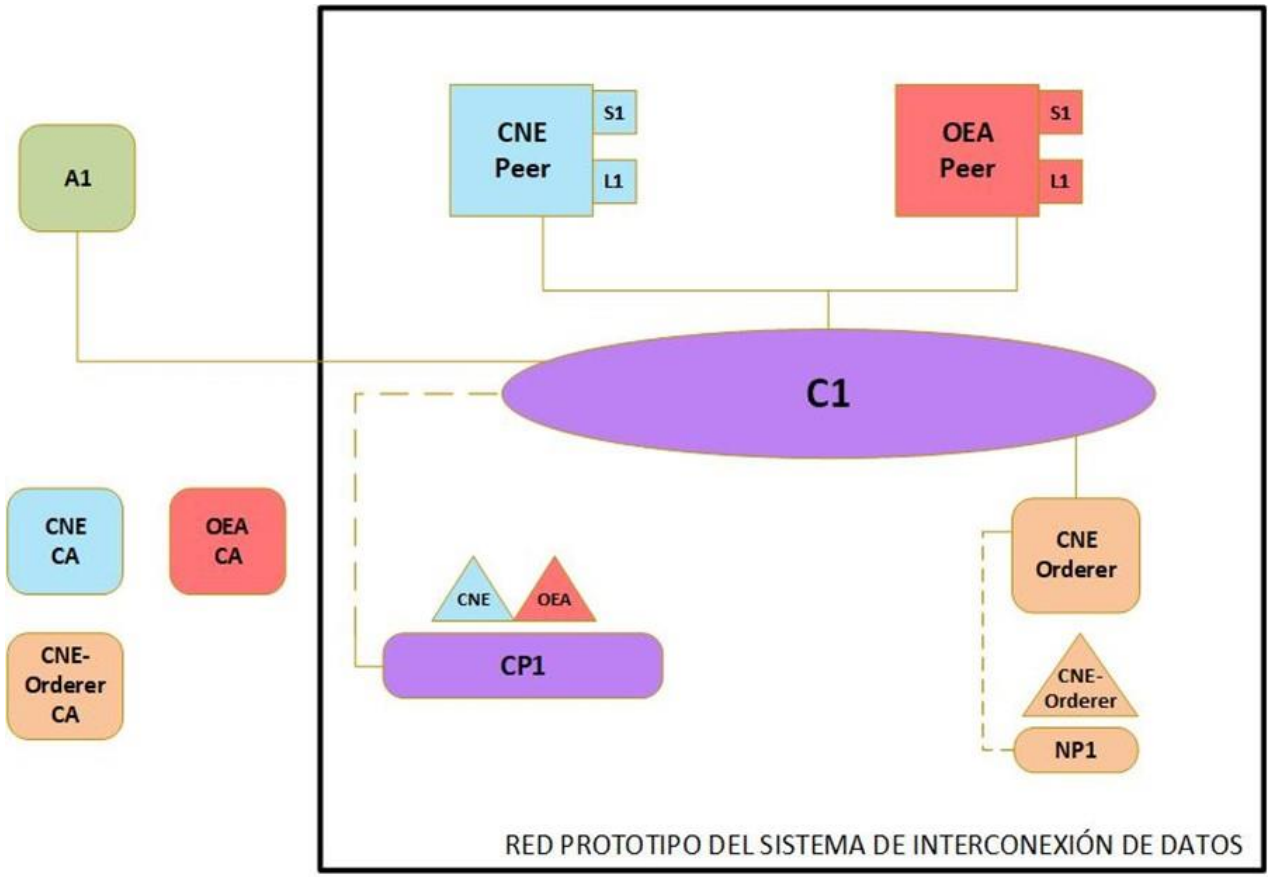
- Define aspectos claves de la red.
- Asegura que las operaciones dentro del SID sigan las mismas reglas y condiciones.
- Todas las organizaciones deben tener el mismo “configtx”.



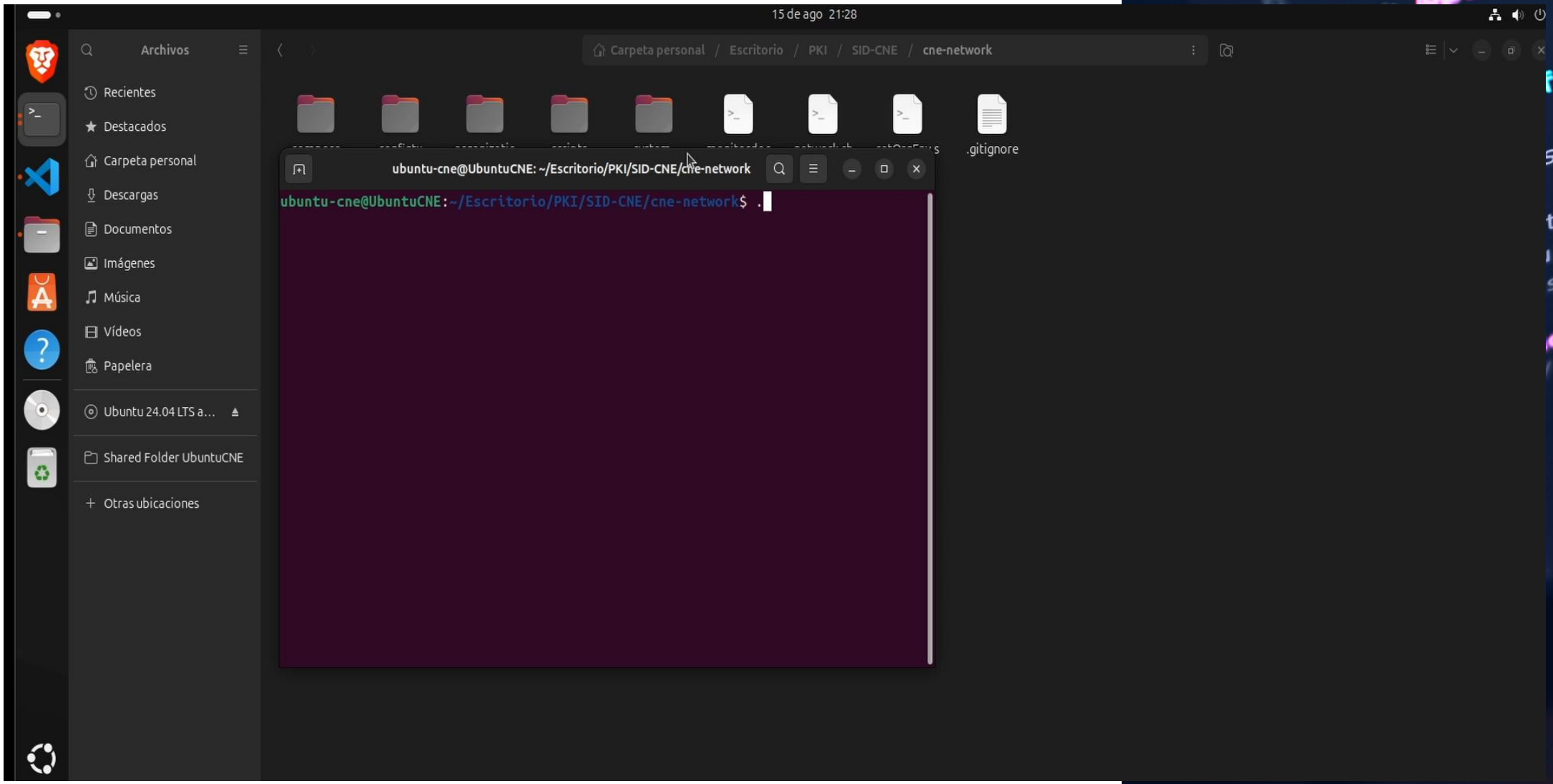
Arquitectura de la red del SID



Arquitectura de la red del SID

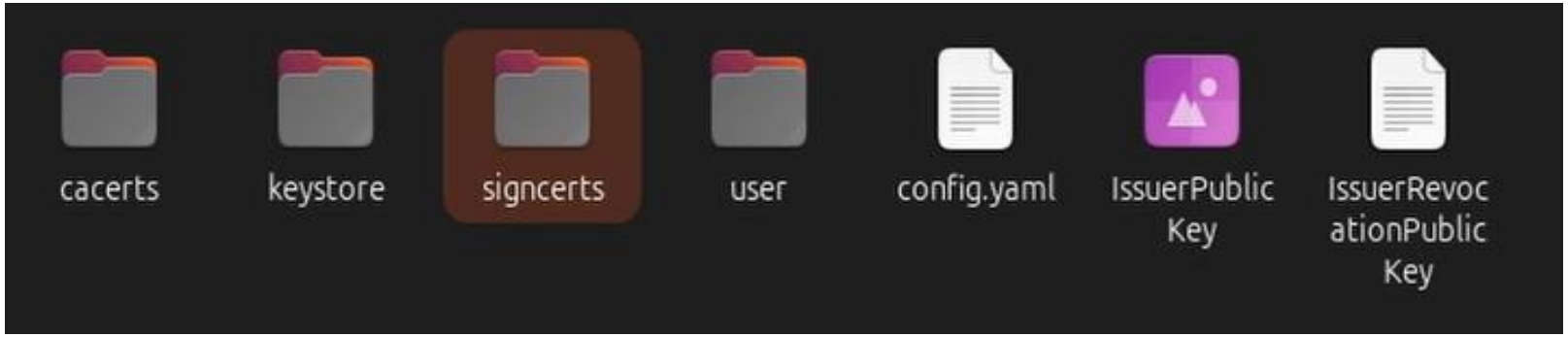


Inicio Contenedores

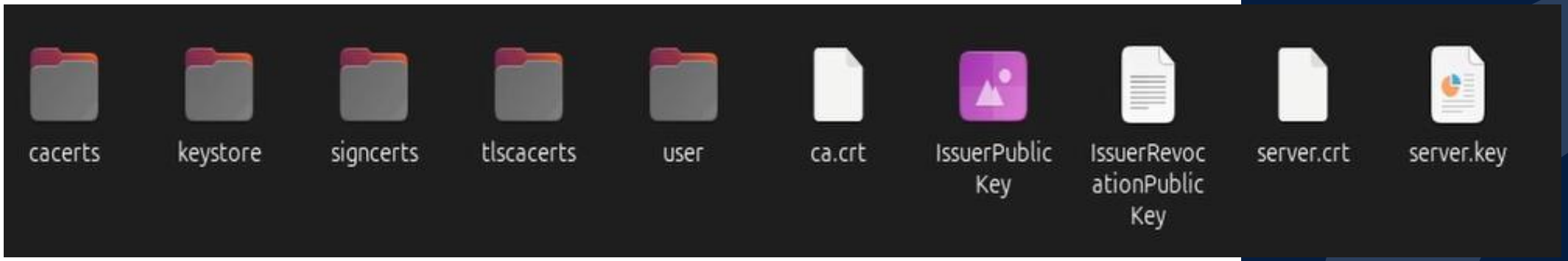


Certificados

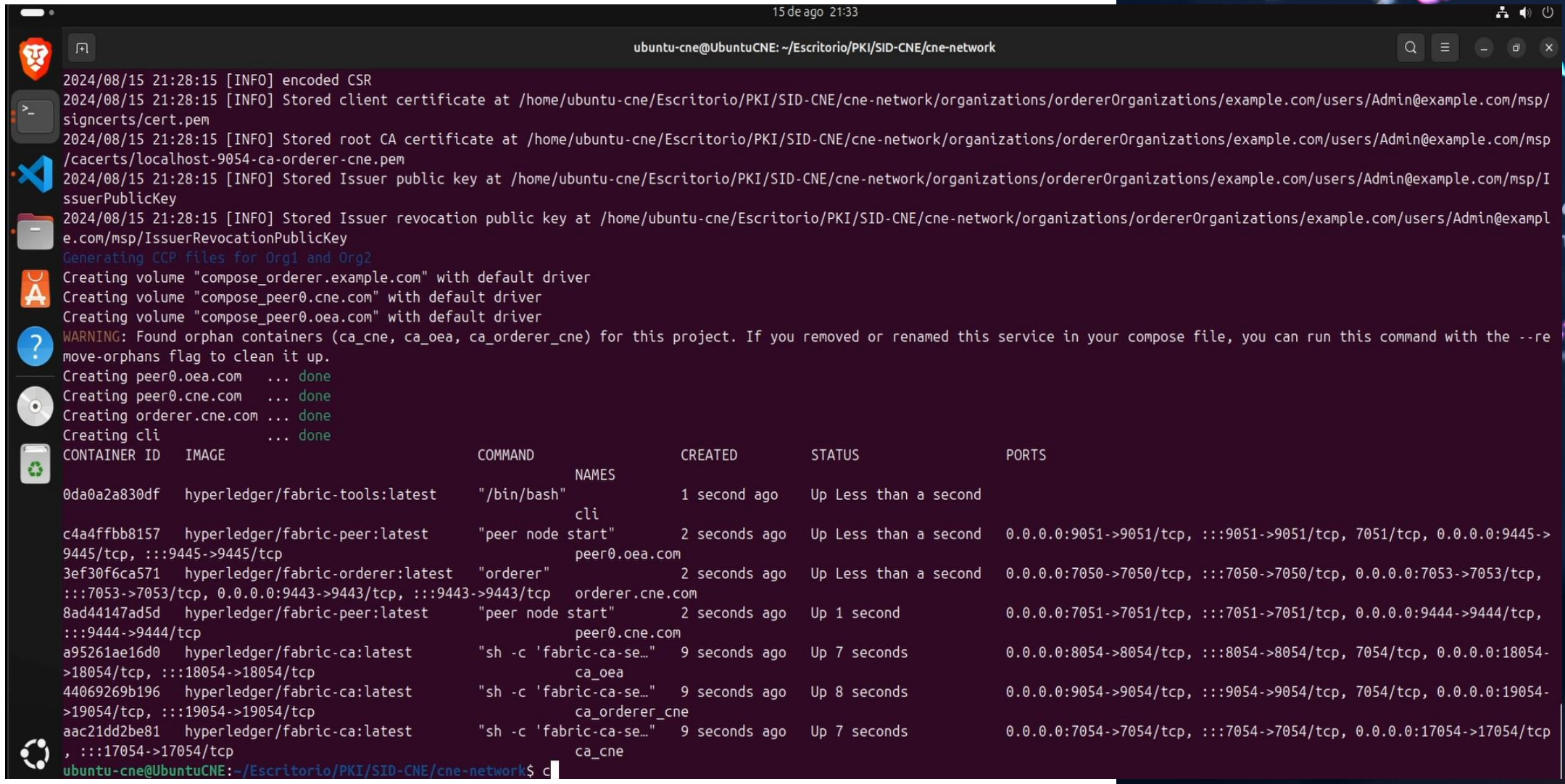
MSP



TLS

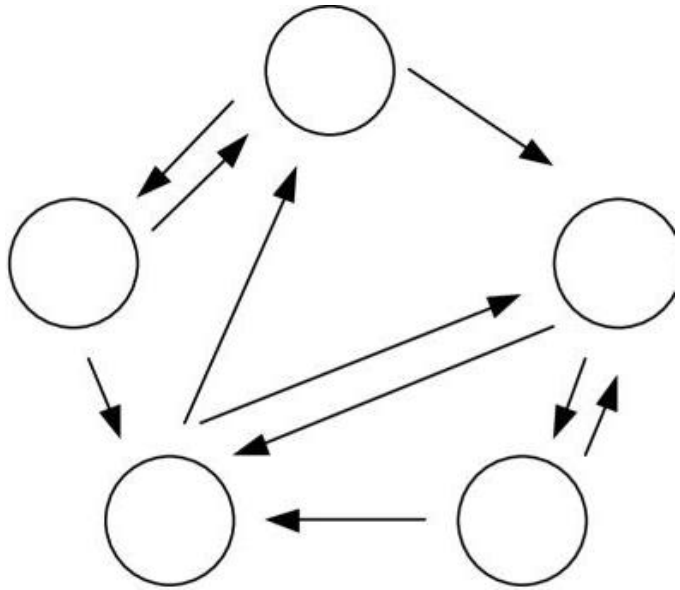


Creación Canal

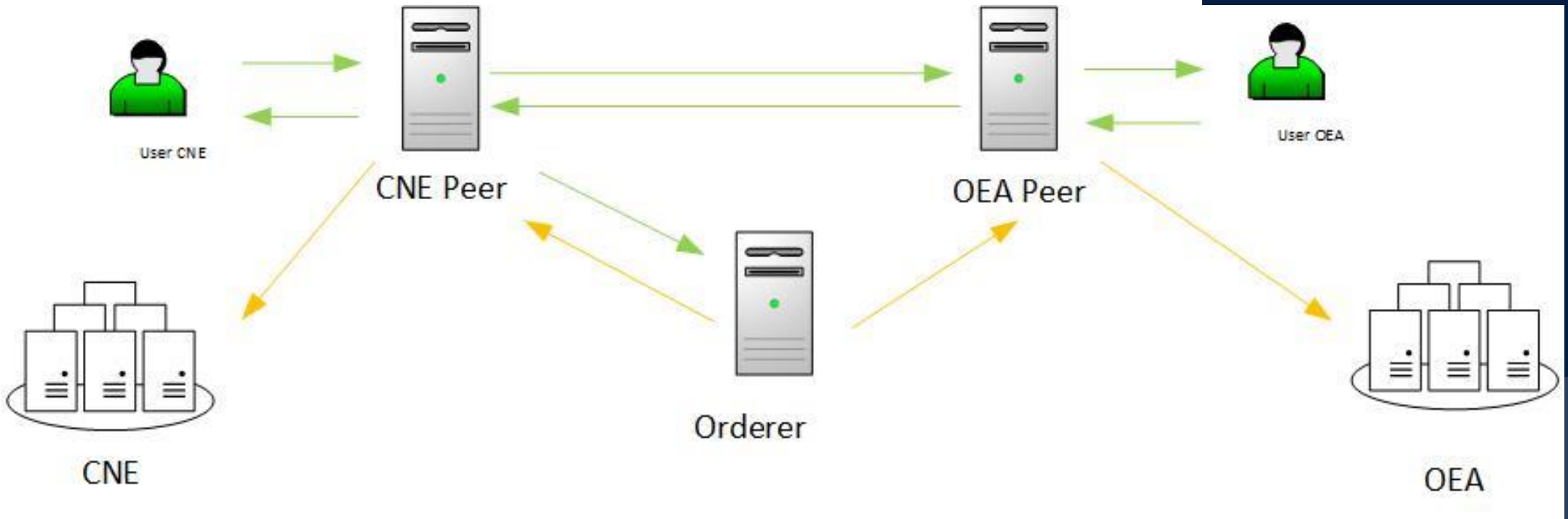


Comunicaciones

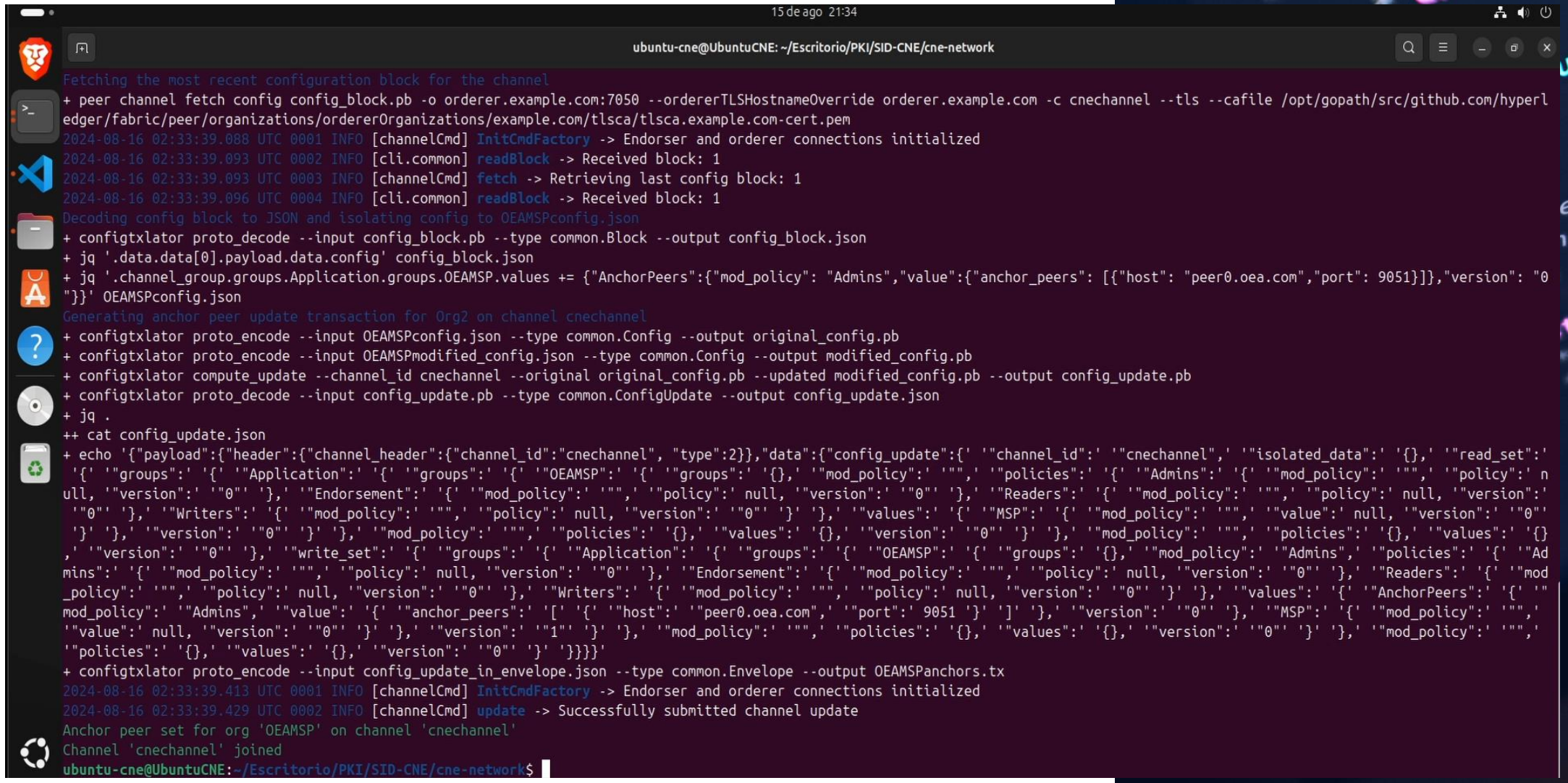
Dentro de Hyperledger Fabric, las comunicaciones se realizan mediante el protocolo Gossip.



Comunicaciones



Instalación Chaincode



Conclusiones

- Se demostró que la implementación de una infraestructura de llave pública (PKI) en la red blockchain fue efectiva para garantizar la identificación y autenticación segura de los diferentes componentes.

- El análisis de los problemas de seguridad y transparencia en el proceso actual de escrutinios y publicación de resultados reveló varias vulnerabilidades, como la centralización del sistema o la posibilidad de acceso no autorizado y la manipulación de datos.

- La revisión de soluciones existentes para una PKI permitió seleccionar tecnologías adecuadas para el proyecto, como Hyperledger Fabric, que ofreció una infraestructura modular y segura para la gestión de identidades y comunicaciones.

Conclusiones

- El diseño de un sistema de seguridad basado en una PKI incluyó la configuración de autoridades certificadoras (CAs) para la emisión de certificados de TLS y Enrollment. Se diseñó un proceso de autenticación y autorización que permitió controlar el acceso y asegurar la integridad de los datos dentro de la red.

- La implementación del prototipo de una PKI en Hyperledger Fabric validó el diseño propuesto, mostrando que es posible asegurar la integridad y autenticidad de las transacciones dentro de la red blockchain.