



El futuro digital
es de todos

MinTIC



INTEROPERABILIDAD DE SISTEMAS DE INFORMACIÓN MEDIANTE X-ROAD

INFRAESTRUCTURA DE LLAVE PÚBLICA



Infraestructura de Llave Pública

Una Infraestructura de Llave Pública (**Public Key Infrastructure - PKI**), es un conjunto de **procedimientos y políticas** que, soportadas por complejas soluciones de software y hardware, tienen la finalidad de aportar **seguridad y garantías** a operaciones de **firma digital, identificación, autenticación y cifrado**.

El objetivo final es el **no repudio** de las transacciones. Esta característica se consigue garantizando la **identidad del interesado** y la **integridad del contenido**.

Infraestructura de Llave Pública

1



Una PKI permite a los proveedores de servicios en línea, **identificar** y **autenticar** a sus clientes electrónicamente, y además permite el uso de **firma electrónica** para transacciones en línea.

2



Una PKI es una arquitectura de seguridad que proporciona un mayor nivel de **confianza** para intercambiar información a través de Internet, mediante el uso de **pares de llaves criptográficas públicas y privadas**.

3



Una PKI aprovecha la **protección de datos**, ya que cumple con las leyes de transacciones electrónicas.



Criptografía Simétrica

Es un método criptográfico en el cual se usa **una misma llave** para **cifrar y descifrar los** los mensajes, en el emisor y en el receptor, respectivamente. Las dos partes que se comunican deben **acordar** el **esquema** de llaves a usar.

Llave Privada



Una vez que ambas partes tienen acceso a una **llave privada**, el **remitente cifra** un mensaje usándola, lo envía al **destinatario**, y éste lo **descifra** con la misma **llave**.



Criptografía Asimétrica

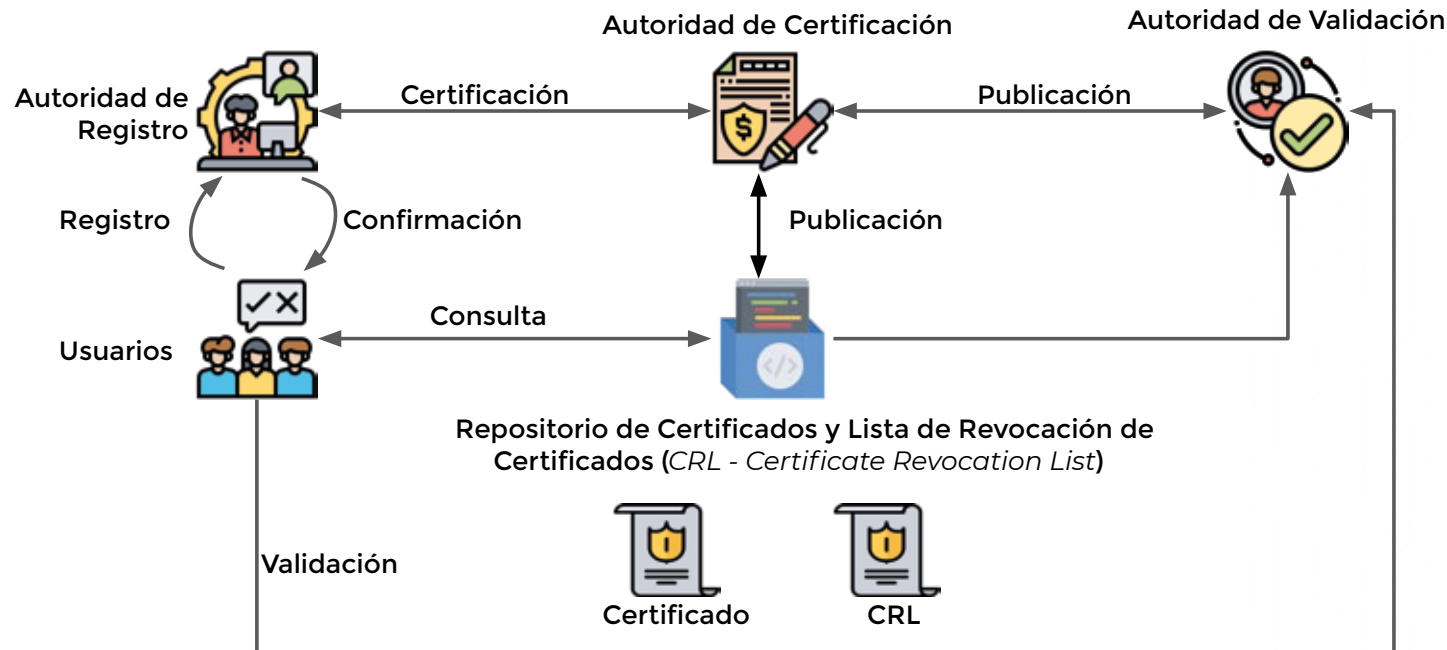
Es un método criptográfico que usa **un par de llaves** para el envío de mensajes. Una **llave es pública** y se puede entregar a **cualquier actor**, la otra **llave es privada** y el propietario debe salvaguardarla, de modo que nadie tenga acceso a ella.

Llaves Pública y Privada



Quando el emisor desea enviar un mensaje a un receptor, **cifra** la información con la **llave pública** del receptor. Este, una vez que le haya llegado el **mensaje cifrado**, procederá a **descifrarlo** con la **llave privada** que solo él posee.

Componentes de una PKI





Autoridad de Certificación

También llamado **Emisor de certificados** , se utiliza para emitir los certificados y las listas de revocación. Cada certificado de clave pública se emite a un individuo y cada certificado tiene una firma digital de la **Autoridad de Certificación emisora** .

Un **certificado** es una estructura de datos compuesta por el valor de la **clave pública** y la **información identificada** que pertenece al titular de la **clave privada** correspondiente.

Autoridad de Certificación

Representa la **fuentes de credibilidad** de la PKI.

1



Es quien **emite** los certificados, firmándolos digitalmente con su **llave privada**.

2



Da **certeza** a una entidad, de la validez de un **llave pública** asignada en un certificado..

3



Recibe y procesa peticiones de certificados de los usuarios finales.

Autoridad de Certificación

Representa la **fuentes de credibilidad** de la PKI.

4

Consulta con una **Autoridad de Registro** para determinar si acepta o rechaza la petición de un certificado.

5

Gestiona las listas de revocación de certificados.

6

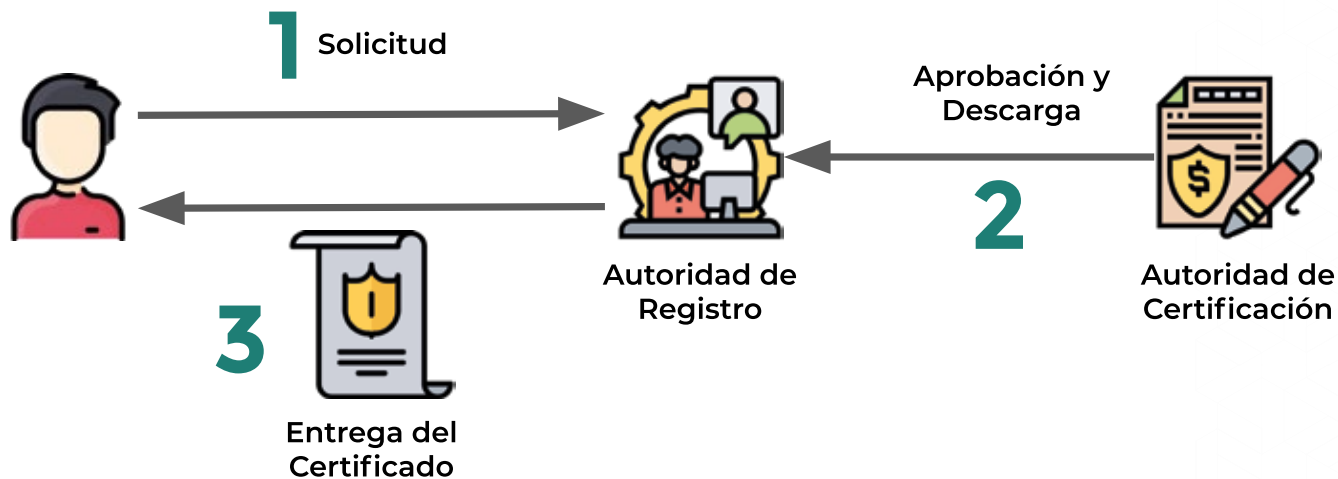
Renueva certificados.



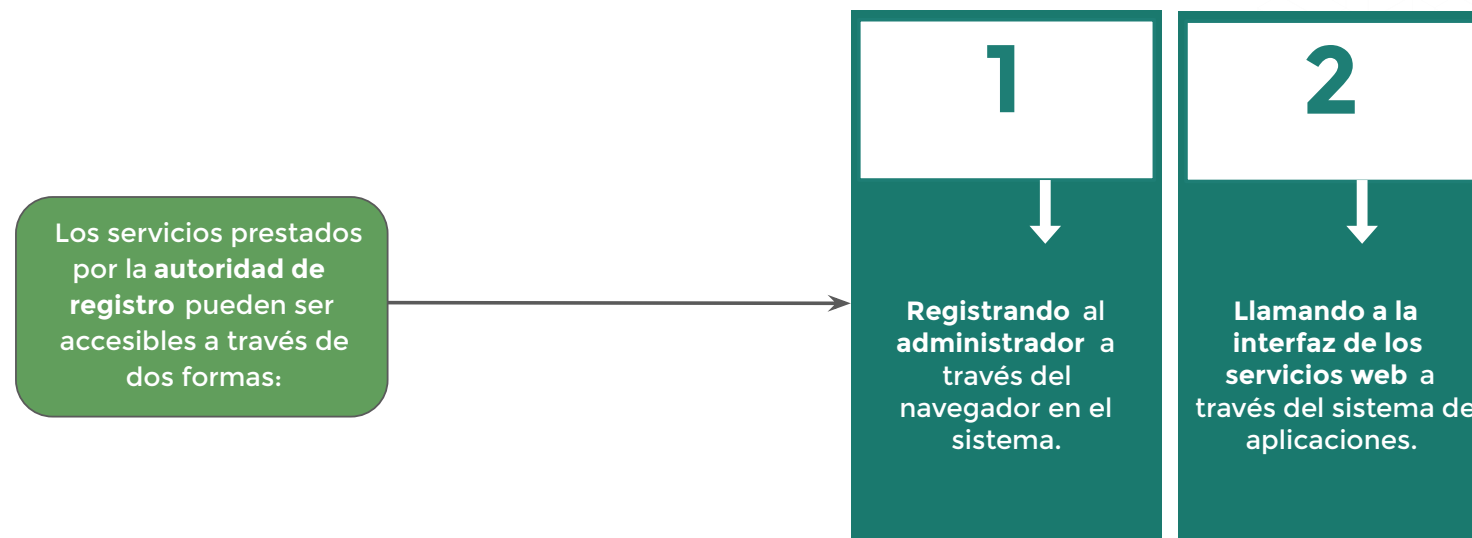
Autoridad de Registro

La **autoridad de registro** se utiliza para enviar todas las solicitudes a la **Autoridad de Certificación**. Autentica todas las identidades de los usuarios y registra la información del usuario final antes de la certificación.

Autoridad de Registro



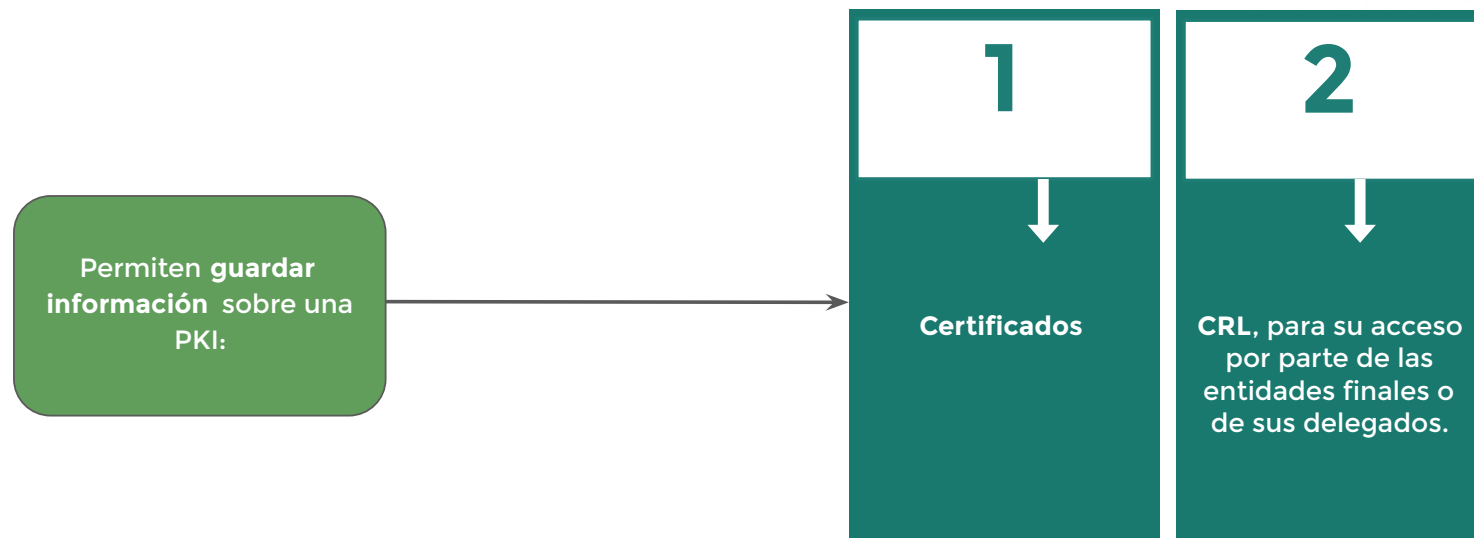
Autoridad de Registro



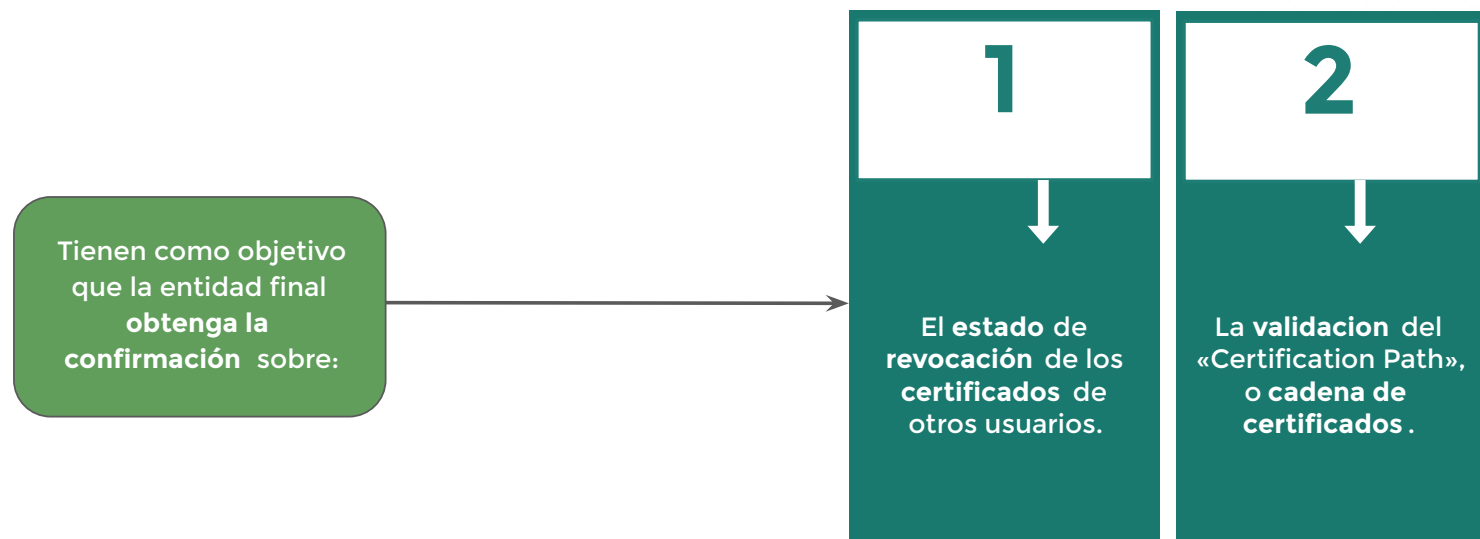
Autoridad de Registro



Repositorios



Repositorios



Autoridad de Validación

La **autoridad de validación** suministra información en línea acerca del estado de un certificado.

La **Autoridad de Certificación** actualiza la información de la **Autoridad de Validación** cada vez que se modifica el estado de un certificado, con lo que, a diferencia de las **CRL**, se dispone de información en tiempo real.

Autoridad de Validación

La autoridad de validación
suele proporcionar dos
servicios de validación.

1



A través de la
descarga de las **CRL**
para que el usuario
las interprete por sí
mismo.

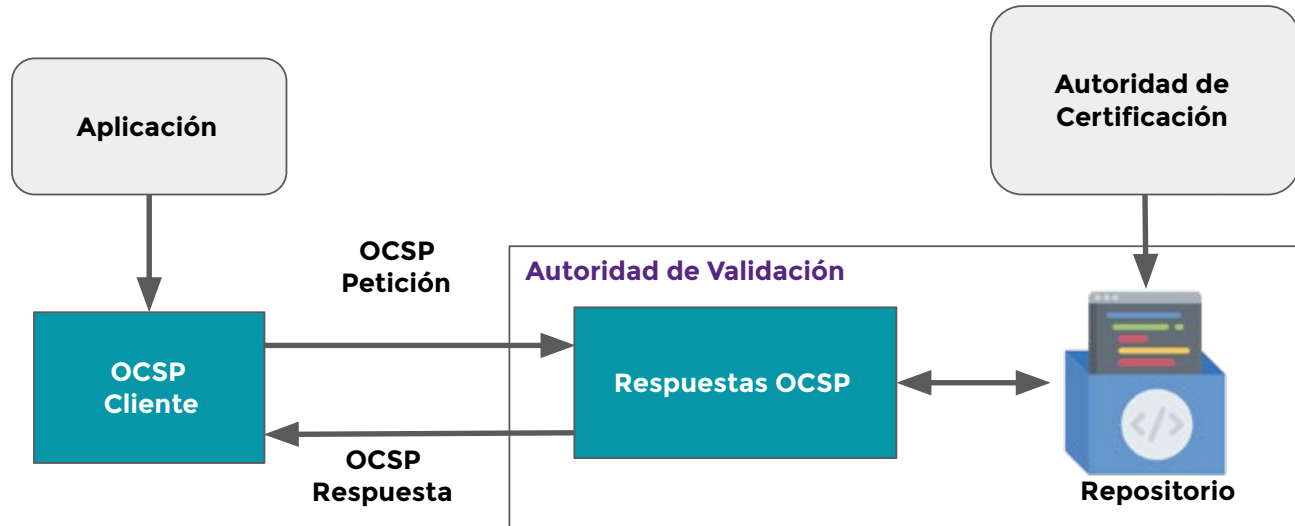
2



A través del protocolo **OCSP**:

Los usuarios y aplicaciones que
deseen obtener el estado de un
certificado, solo tienen que realizar
una petición **OCSP** (*Online Certificate
Status Protocol*) a la autoridad de
verificación para obtener dicho estado.

OCSP (Protocolo de Estado de Certificado en Línea)



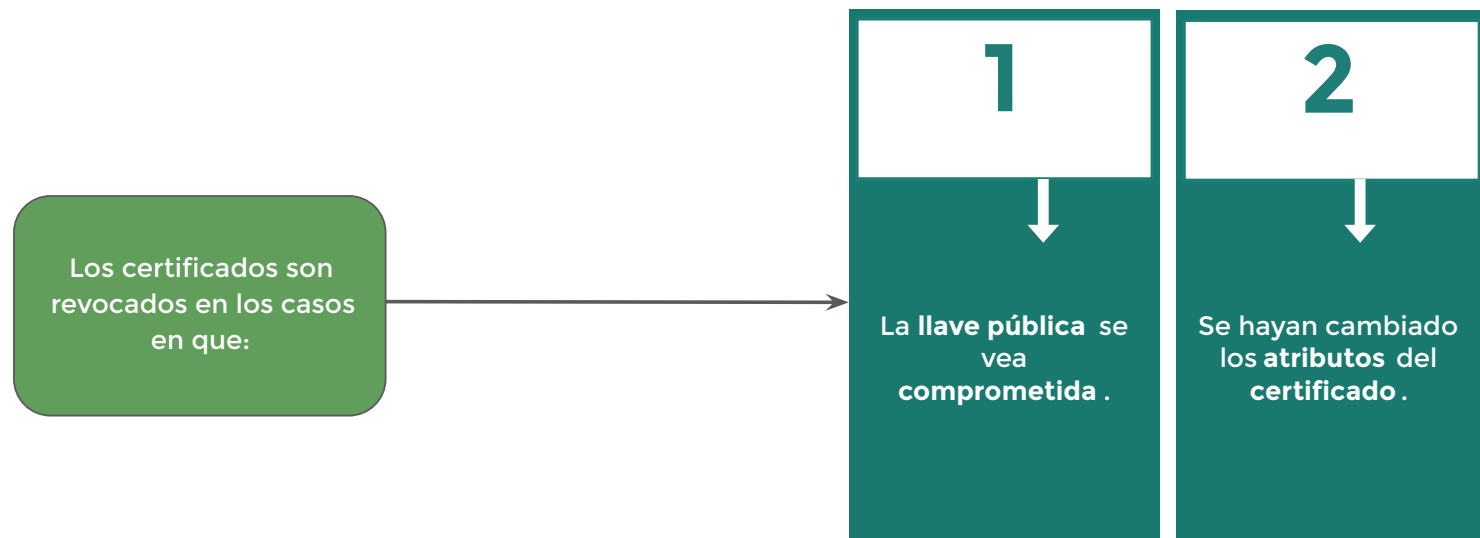


CRL (Listas de Revocación de Certificados)

Las **CRL** son listas de certificados que han dejado de ser válidos y por lo tanto en los que no se puede confiar.

Las **CRL** actúan en nombre de la **Autoridad de Certificación**, siendo de carácter **opcional**, aunque sumamente convenientes.

CRL (Listas de Revocación de Certificados)



Autoridad de Sellado de Tiempo

