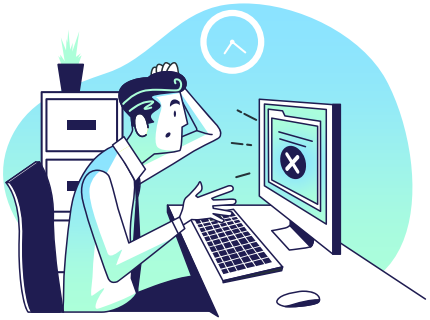
JAAS y seguridad

JAAS

Segun sus siglas es es Java Authentication and Authorization. Es una interfaz (API) que provee de mecanismos para la autenticacion y asignación de permisos

PROBLEM VS. SOLUTION



autorización

¿qué puedes hacer? , mediante el cual asignamos los permisos y roles de los usuarios estos pueden ser de forma declarativa o programatica

autenticación

¿quién eres? , permite conocer de manera fiable las personas que acceden.

Para ello se usan contraseñas, datos biometricos, datos identificativos

elementos

javax.security.auth.login: LoginContext y Configuration

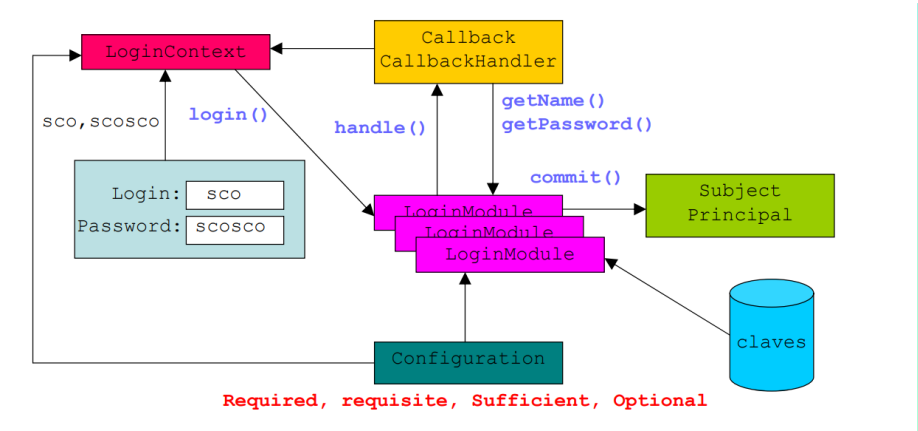
se intenta autentificar a un usuario a través de su nombre y password.

javax.security.auth.callback: Callback y CallbackHandler

implementa la interfaz CallbackHander. Para ello hay que definir un constructor, que simplemente recibirá el nombre de usuario y el password que se le pasa por parámetro desde el código que inició la autentificación

Interfaz javax.security.auth.spi.LoginModule

Comprueba credenciales del sujeto y prosigue o aborta dependiendo del resultado



PASOS

APLICACION

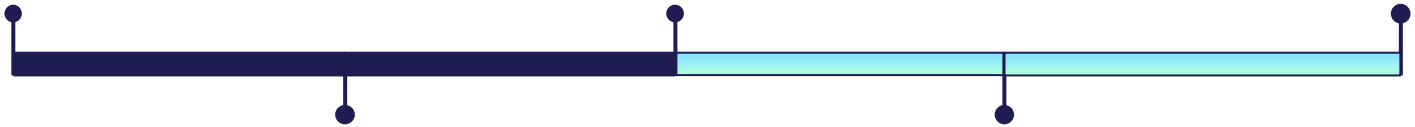
Pide el login

callbackhandler

Qrecibe los datos

loginmodule

Recibe las credenciales



Logincontext:

Llama a call handler con el usuario / contraseña

configuración

Define el logincontext y loginmodule

Loginmodule

Initialize()	Login()	Commit()	Abort()
Inicializa el mdulo	Comprueba credenciales	Funciona solo si login tiene acceso	Si el login falla s invoca este metodo

Logout()
Borra credenciales

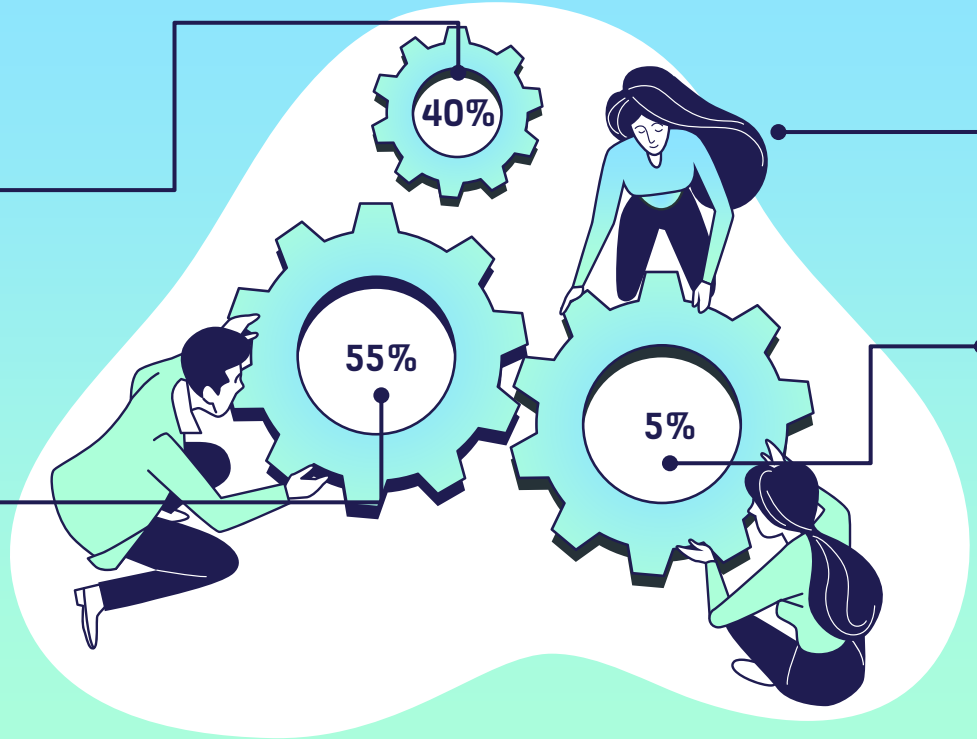
Configuracion : clase abstracta

optional

No influye en el proceso

required

Si falla llama a otro modulo de login



sufficient

Si el modulo tiene exito y ninguno otro falla tiene exito

requisite

Si el proceso login falla no se llama a otro modulo

SSL Y CERTIFICACIÓN

CONCEPTOS IMPORTANTES

COMPONENTES

SSL es el protocolo habitualmente usado para encriptar la comunicación cliente-servidor.

http: Es el de transmisión de información de la World Wide Web, es decir, el código que se establece para que el computador y el que contiene la información solicitada puedan “hablar” un mismo idioma a la de transmitir información por la red.

https: ofrece un canal cifrado que permite la comunicación segura entre servidor-cliente

conexión

01

Un navegador o servidor intenta conectarse a un sitio web (es decir, un servidor web) protegido mediante certificados SSL.

solicitud

02

El navegador o servidor solicita que el servidor web se identifique.

Envio

03

En respuesta el servidor web envía al navegador o servidor una copia de su certificado SSL.

Comprobación

04

El navegador o servidor evalúa si el certificado SSL es confiable. En caso afirmativo, envía una señal al servidor web.

confirmación

05

A continuación, el servidor web devuelve un reconocimiento firmado digitalmente para iniciar una sesión cifrada mediante SSL.

comparte

06

Los datos cifrados se comparten entre el navegador o servidor y el servidor web.

Conceptos importantes

encapsulamiento

Cuando el paquete se transfiere a través de la pila de protocolo TCP/IP, los protocolos de cada capa agregan o eliminan campos del encabezado básico. Cuando un protocolo del sistema de envío agrega datos al encabezado del paquete, el proceso se denomina encapsulado de datos.

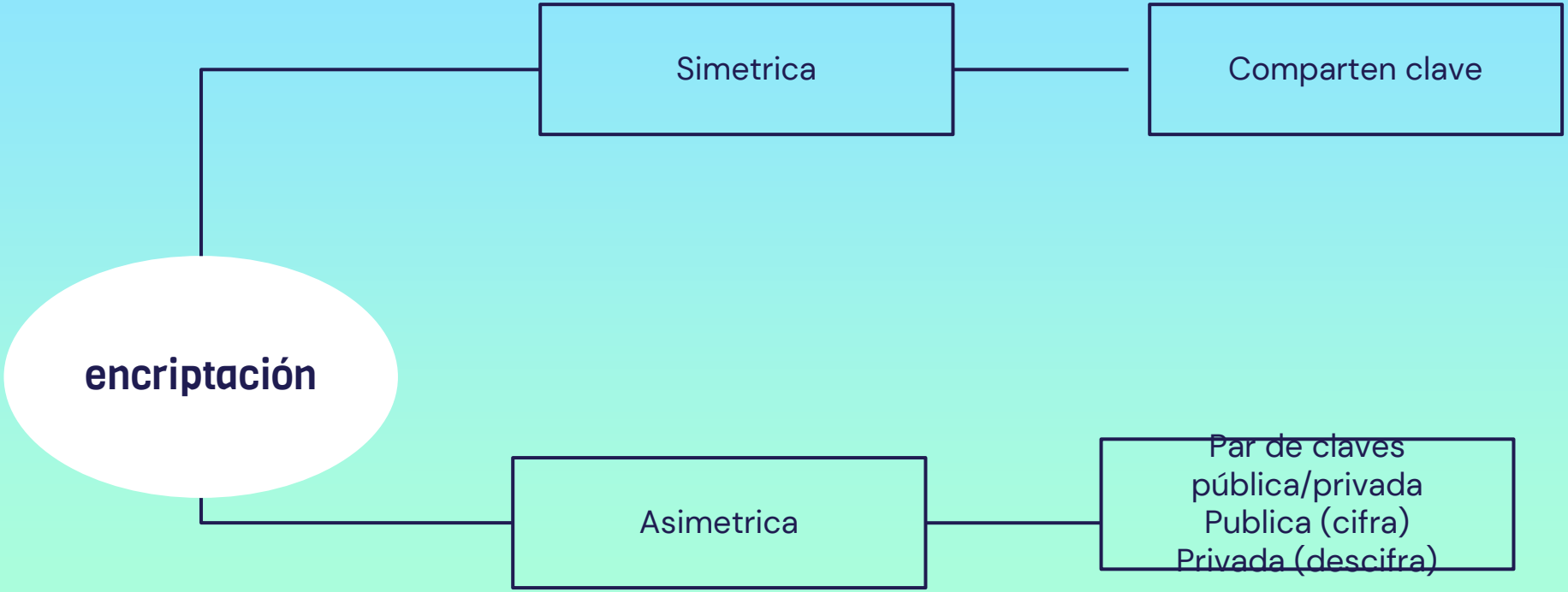
encriptacion

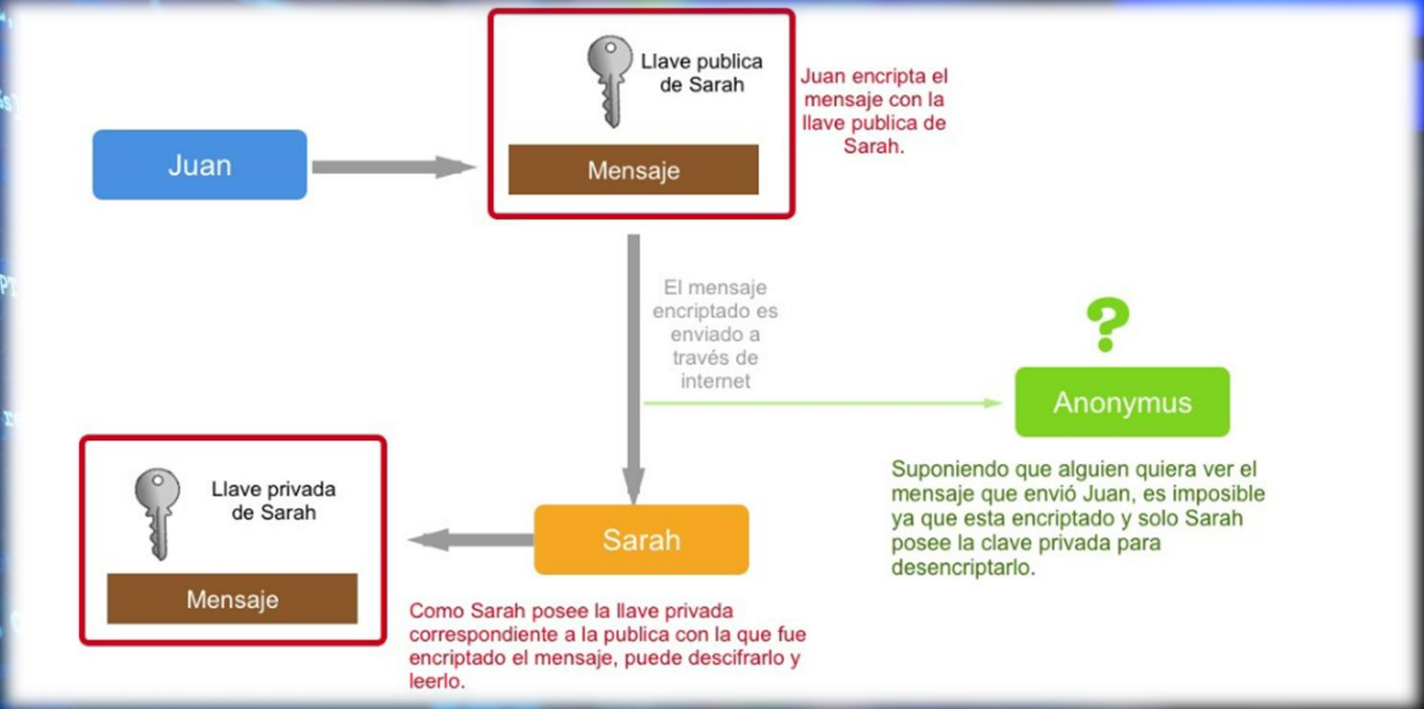
En la encriptación de datos actual se utiliza un algoritmo matemático para modificar el contenido que se quiere cifrar (dependiendo del sistema de cifrado, se usan diferentes algoritmos), para ello se genera una clave o claves que establecen la forma en que se «desordena la información» cuando se cifra y que después se emplea para descifrarla, es decir, volver a ordenarla.

Buenas practicas

Cambio continuo de contraseña,firewall, limitar accesos

Tipos de encriptación




Llave publica de Sarah
Mensaje
Juan
Juan encripta el mensaje con la llave publica de Sarah.
El mensaje encriptado es enviado a través de internet
?
Anonymus
Suponiendo que alguien quiera ver el mensaje que envió Juan, es imposible ya que esta encriptado y solo Sarah posee la clave privada para desencriptarlo.
Llave privada de Sarah
Mensaje
Sarah
Como Sarah posee la llave privada correspondiente a la publica con la que fue encriptado el mensaje, puede descifrarlo y leerlo.