

Autenticación de usuarios

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Ana I. González-Tablas Ferreres

José María de Fuentes García-Romero de Tejada

Lorena González Manzano

Pablo Martín González

uc3m | Universidad **Carlos III** de Madrid

COSEC



ÍNDICE

- 13. Autenticación de usuarios
 - Introducción
 - Autenticación basada en secretos
 - Autenticación mediante token
 - Autenticación biométrica

ÍNDICE

- 13. Autenticación de usuarios
 - **Introducción**
 - Autenticación basada en secretos
 - Autenticación mediante token
 - Autenticación biométrica

INTRODUCCIÓN

- Autenticación
 - Procedimiento de comprobación de la identidad de un usuario
- Factores de autenticación
 - Basadas en algo que el usuario conoce (secretos)
 - Basadas en algo que el usuario tiene (tokens)
 - Basadas en algo que el usuario es (biometría)
 - Combinaciones de lo anterior (varios factores)

ÍNDICE

- 13. Autenticación de usuarios
 - Introducción
 - **Autenticación basada en secretos**
 - Autenticación mediante token
 - Autenticación biométrica

AUTENTICACIÓN MEDIANTE SECRETOS

- El usuario dispone de determinada información secreta que sólo él y el sistema conocen
- Incluye métodos basados en contraseñas, PIN, desafío-respuesta, etc.
- Método de autenticación simple y extendido
- Necesaria una gestión de las contraseñas

AUTENTICACIÓN MEDIANTE SECRETOS – GESTIÓN DE CONTRASEÑAS

- Criterios de calidad
 - Fácil de recordar (débil) versus aleatoria (menos débil)
 - Longitud, complejidad
- Custodia de la contraseña por el usuario
 - No divulgación (ingeniería social, *phishing*, etc.)
- Almacenamiento de contraseñas en el sistema
 - Almacenamiento del resumen de cada contraseña
 - Cifrado de las contraseñas
- Caducidad de contraseñas
 - Cuanto mayor sea la criticidad del sistema, menor debe ser el periodo de validez de las contraseñas

AUTENTICACIÓN MEDIANTE SECRETOS – GESTIÓN DE CONTRASEÑAS

- Recuerdo de contraseñas
 - Establecer un número mínimo de contraseñas diferentes consecutivas
- Bloqueo de contraseñas / baja de cuentas de usuario
 - En caso de sospecha de uso fraudulento
- Problemática en la reutilización de contraseñas para acceso a diferentes sistemas
- Amenazas
 - Ataques de fuerza bruta y de diccionario
 - Intercepción de contraseñas
 - Ataque a la base de datos del sistema (talón de Aquiles)
 - Ingeniería social

AUTENTICACIÓN MEDIANTE SECRETOS – GESTIÓN DE CONTRASEÑAS

- Programas de ruptura de contraseñas
 - L0phtcrack , John the Ripper, Pwdump
 - Diccionarios y listados (teléfonos, matrículas...)
- Programas de gestión de las contraseñas
 - Password Safe (<http://www.schneier.com/passsafe.html>)
 - SplashID (<http://splashdata.com/splashid/>)

ÍNDICE

- 13. Autenticación de usuarios
 - Introducción
 - Autenticación basada en secretos
 - **Autenticación mediante token**
 - Autenticación biométrica

AUTENTICACIÓN MEDIANTE TOKEN

- Dispositivos criptográficos
 - Tarjetas inteligentes, tokens USB
 - Autenticación mediante firma digital

- Tokens OTP

AUTENTICACIÓN MEDIANTE TOKEN – ONE TIME PASSWORD (OTP)

- OTP (*One-Time Password*)
- Contraseñas desechables de un solo uso (sesión, transacción)
- Se generan mediante un token que posee el usuario o software específico
- Evitan los inconvenientes derivados de la gestión de contraseñas clásicas
- Custodia segura del token



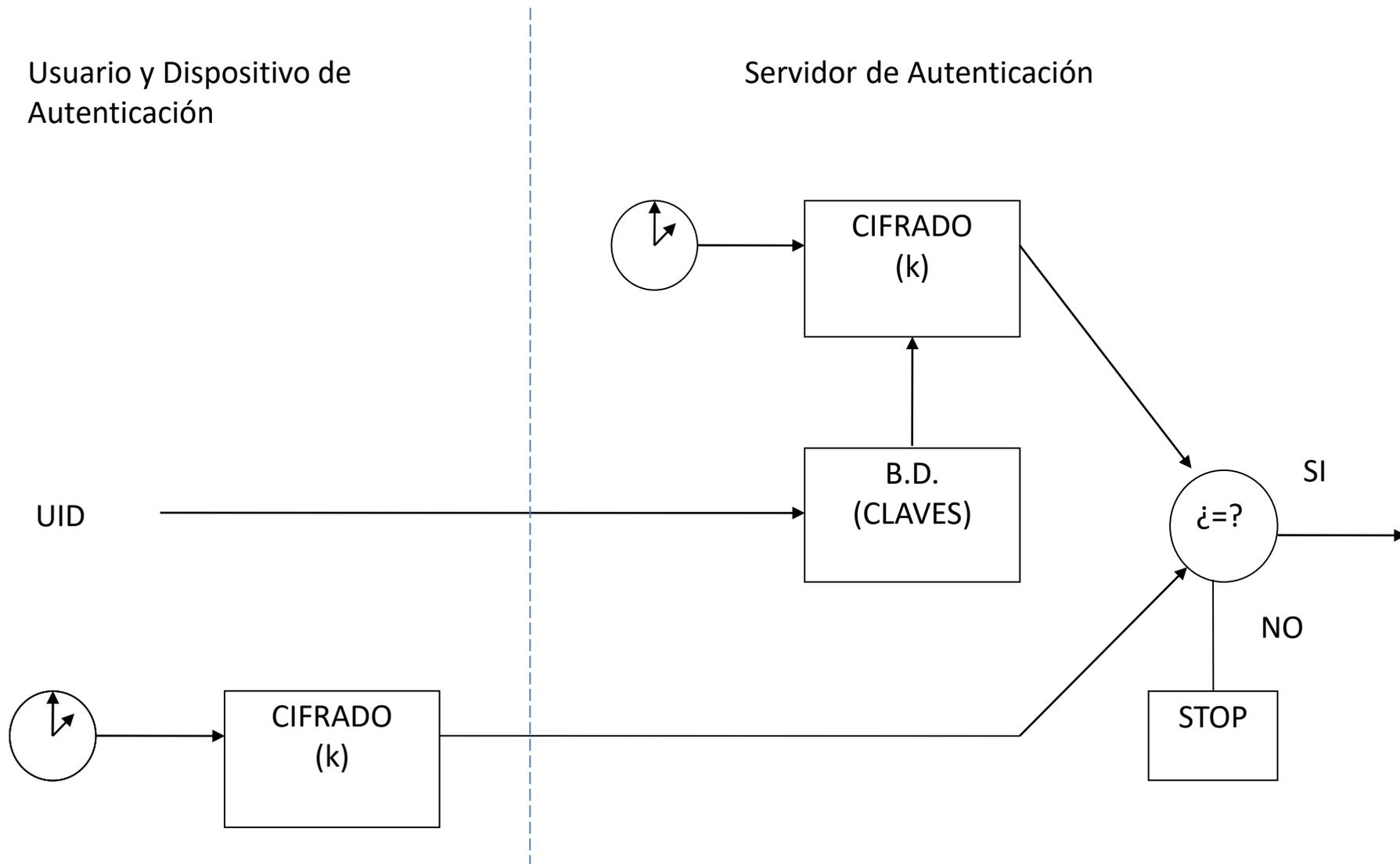
Autor: Sylvain Maret

<https://commons.wikimedia.org/wiki/File:Clock-Based-OTP.png>

AUTENTICACIÓN MEDIANTE TOKEN – ONE TIME PASSWORD (OTP)

- Se basan en aleatoriedad, evitando ataques por predicción
- Tipos
 - **Síncronos**: existe sincronía entre los relojes del token y el servidor de autenticación
 - **Encadenados**: La generación de un OTP depende del OTP anterior
 - Basados en **desafíos**: La generación de un OTP depende del desafío enviado por el servidor de autenticación y un contador interno

AUTENTICACIÓN MEDIANTE TOKEN – OTP SÍNCRONO



AUTENTICACIÓN MEDIANTE TOKEN – OTP ENCADENADO

- Aplicación de una función f irreversible de forma encadenada
- Generación de una serie de OTPs basadas en el valor anterior
 $f(s), f(f(s)), f(f(f(s))) \dots f(\dots(f(f(f(s))))\dots)$

– Uso de las OTPs de forma inversa

$f(\dots(f(f(f(s))))\dots)\dots f(f(f(s))), f(f(s)), f(s)$

AUTENTICACIÓN MEDIANTE TOKEN – OTP ENCADENADO

- Inicialización
 1. El servidor de autenticación elige la función f
 2. El usuario elige el máximo nº de autenticaciones (n)
 3. El token inicializa la semilla s y calcula $f^n(s)$
 4. El usuario envía n y $f^n(s)$ al servidor de autenticación por un canal seguro
 5. El servidor de autenticación registra $f^n(s)$ junto con el ID del usuario
- Uso
 6. El token envía el ID y $f^{n-1}(s)$ al servidor de autenticación
 7. El servidor de autenticación recupera $f^n(s)$ mediante el ID

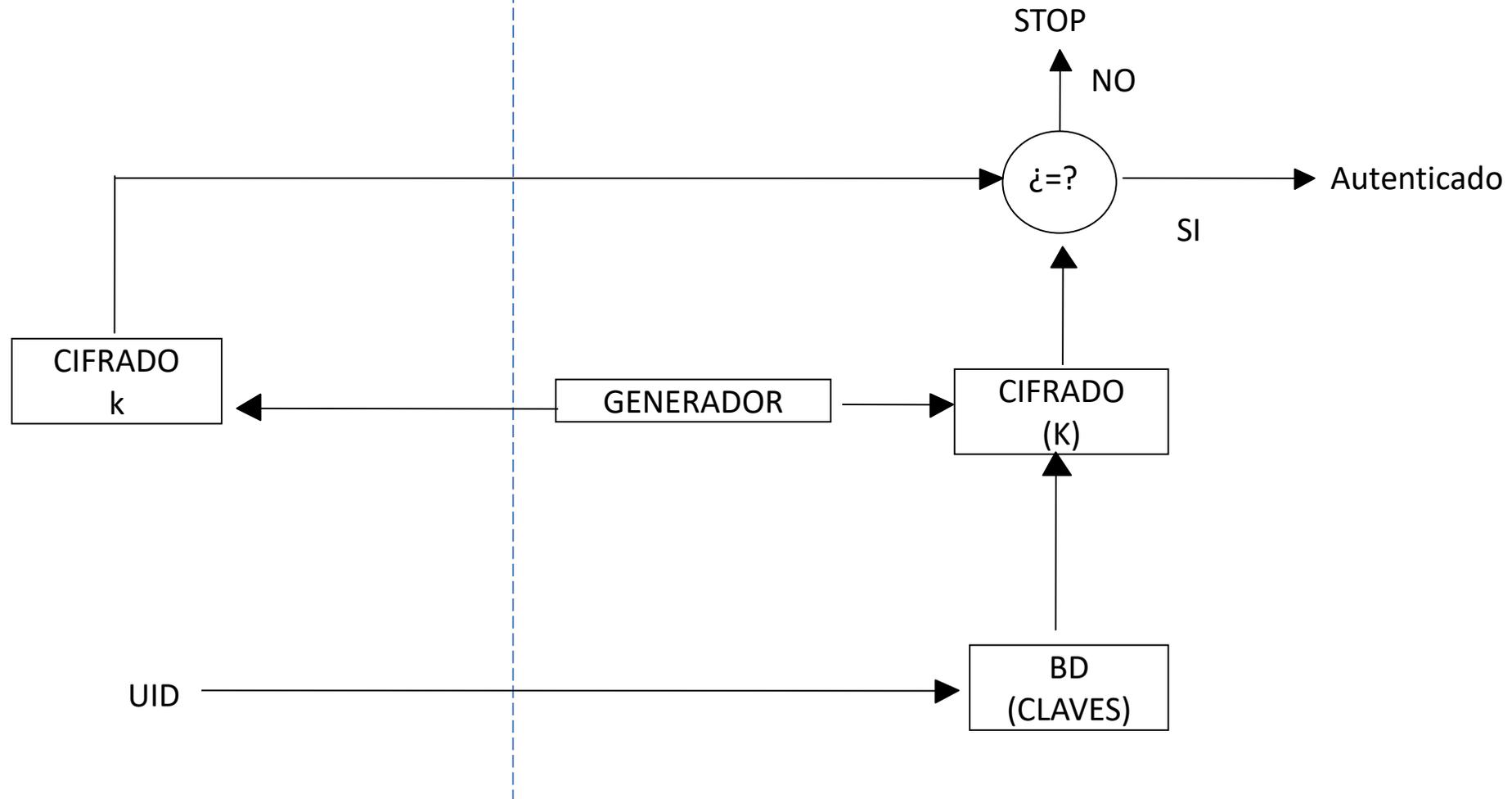
AUTENTICACIÓN MEDIANTE TOKEN – OTP ENCADENADO

8. El servidor de autenticación calcula $f(f^{n-1}(s))$ y comprueba si coincide con $f^n(s)$ almacenado
 9. El servidor de autenticación borra $f^n(s)$ del registro y almacena en su lugar $f^{n-1}(s)$
 10. El servidor de autenticación resta 1 a n
 11. Se repite el proceso hasta que $n=0$
- Un atacante que intercepte un OTP deberá ser capaz de invertir la función f para conocer el siguiente valor OTP
- Normalmente se emplean funciones resumen

AUTENTICACIÓN MEDIANTE TOKEN – OTP BASADO EN DESAFÍO

Usuario y Dispositivo
de Autenticación

Servidor de Autenticación



ÍNDICE

- 13. Autenticación de usuarios
 - Introducción
 - Autenticación basada en secretos
 - Autenticación mediante token
 - **Autenticación biométrica**

AUTENTICACIÓN BIOMÉTRICA

- El sistema autentica al usuario basándose en rasgos biométricos (característica física única e irrepetible)
- Existe un proceso de registro en el sistema (extracción del patrón biométrico y almacenamiento)
- El proceso de autenticación implica la obtención del patrón biométrico del usuario, y su comparación con el patrón almacenado
- Múltiples técnicas biométricas (huella dactilar, iris, vascular, geometría de la mano, escritura y firma manuscrita, voz, ...)
 - Diferentes tasas de eficacia (falsos positivos / falsos positivos)

AUTENTICACIÓN BIOMÉTRICA



CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

COSEC

uc3m | Universidad **Carlos III** de Madrid

