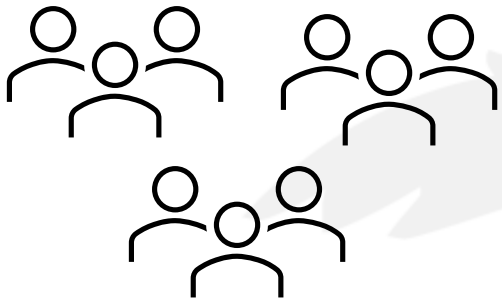
PAI – 1. VERIFICADORES DE INTEGRIDAD EN LA TRANSMISIÓN PUNTO-PUNTO PARA ENTIDAD FINANCIERA

Dr. Ángel J. Varela Vaca
Grupo de Investigación **IDEA Research Group**,
Departamento de Lenguajes y Sistemas Informáticos
Universidad de Sevilla

1. **Contexto**
2. Problemas de seguridad
3. Objetivos y requisitos
4. Entrega

Contexto



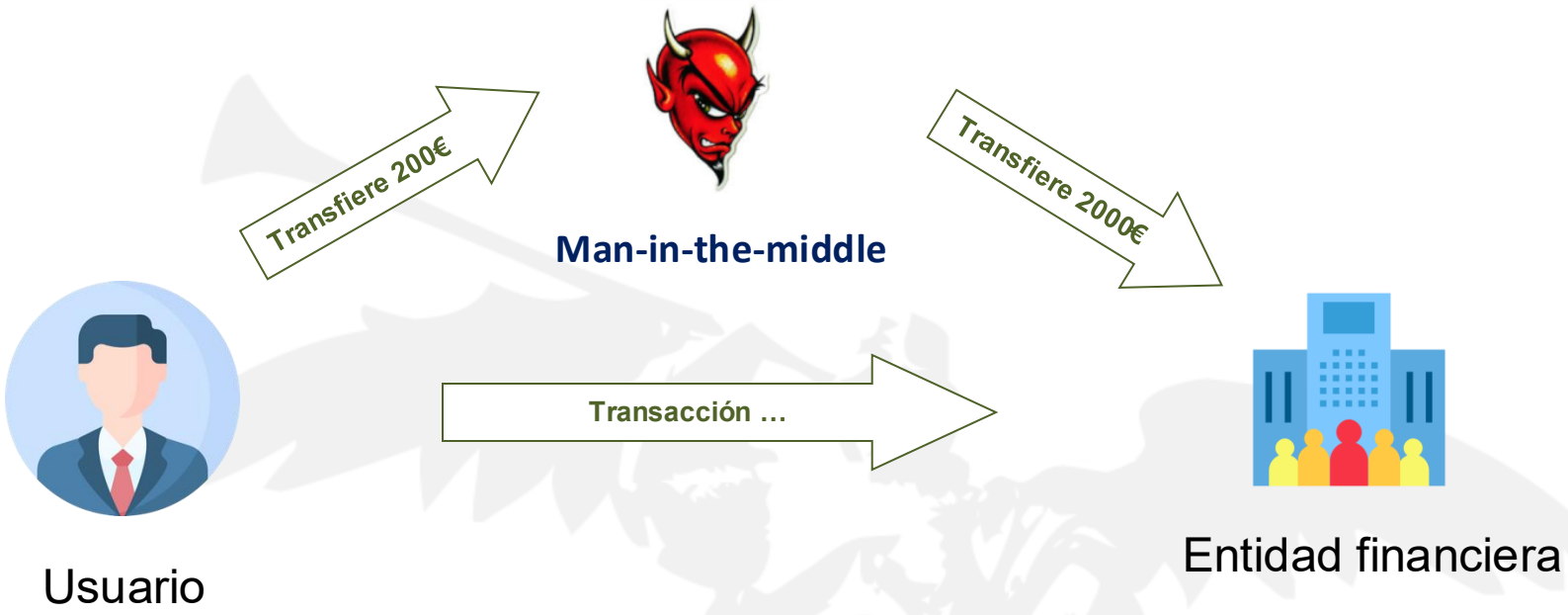
Usuarios

Transacciones

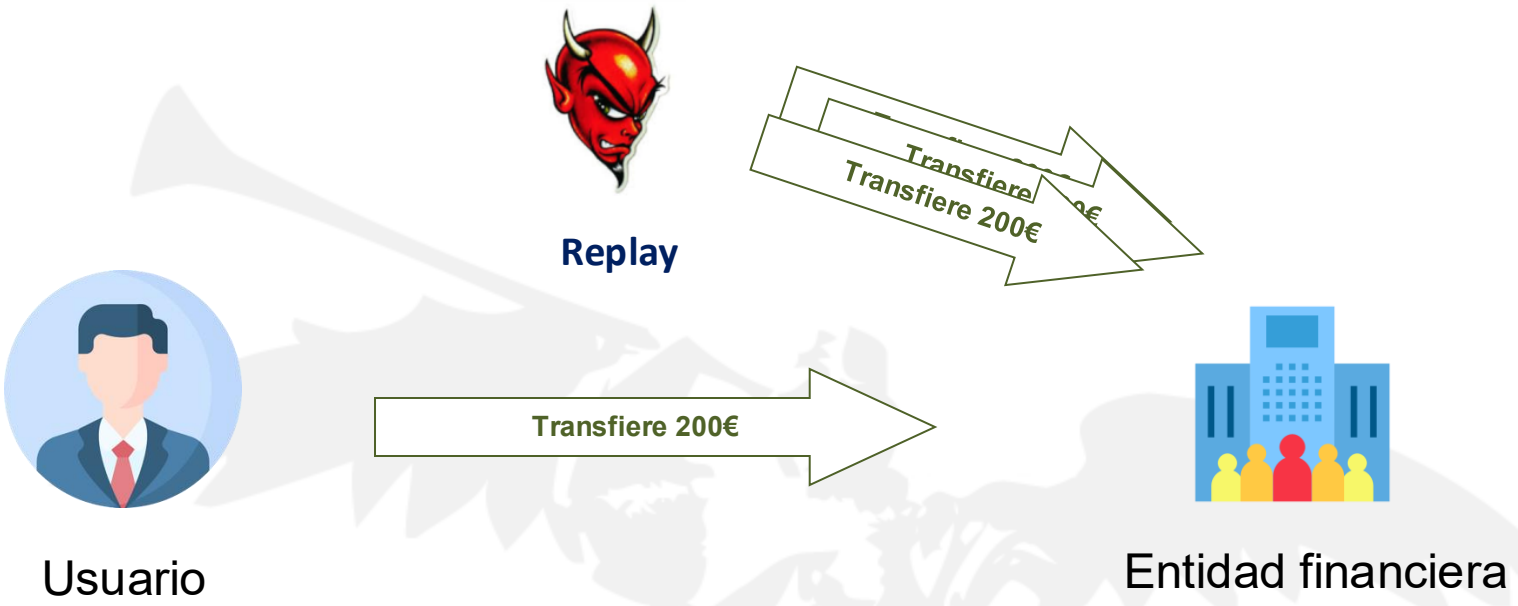
Entidad financiera

1. Contexto
2. **Problemas de seguridad**
3. Objetivos y requisitos
4. Entrega

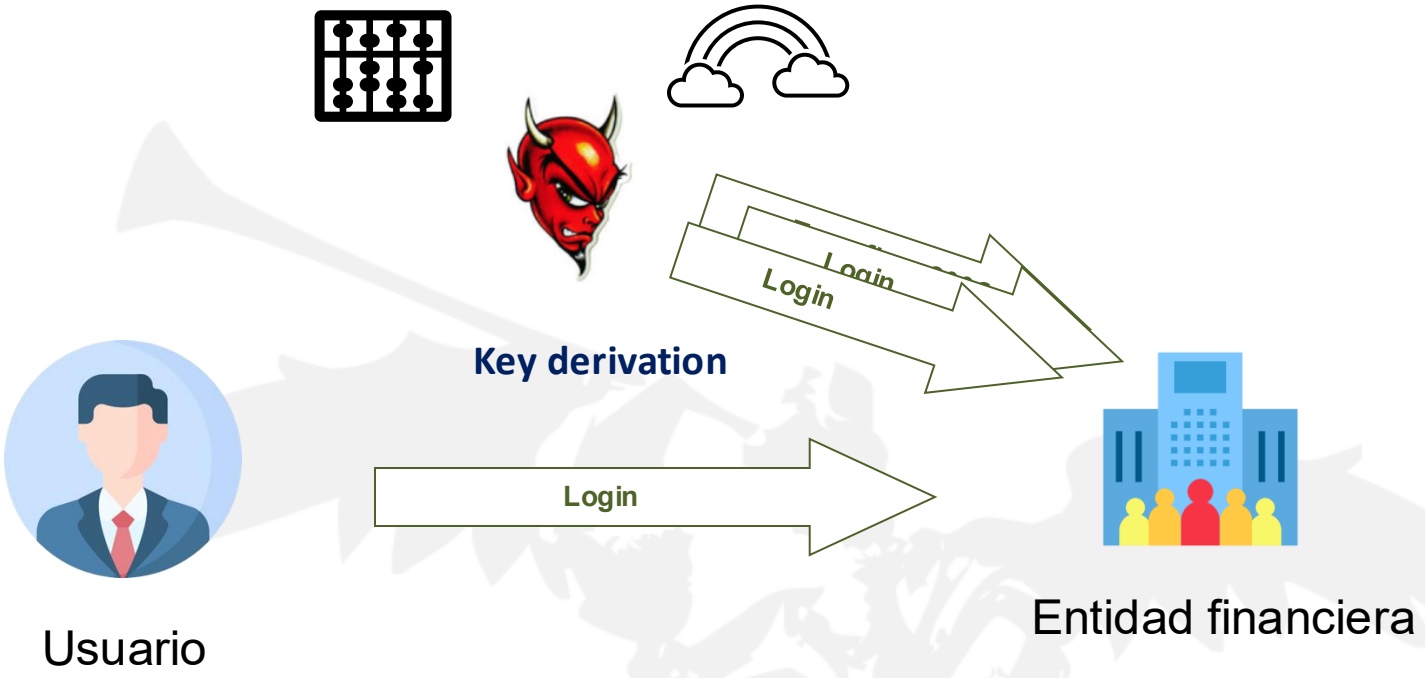
¿Problemas de seguridad?



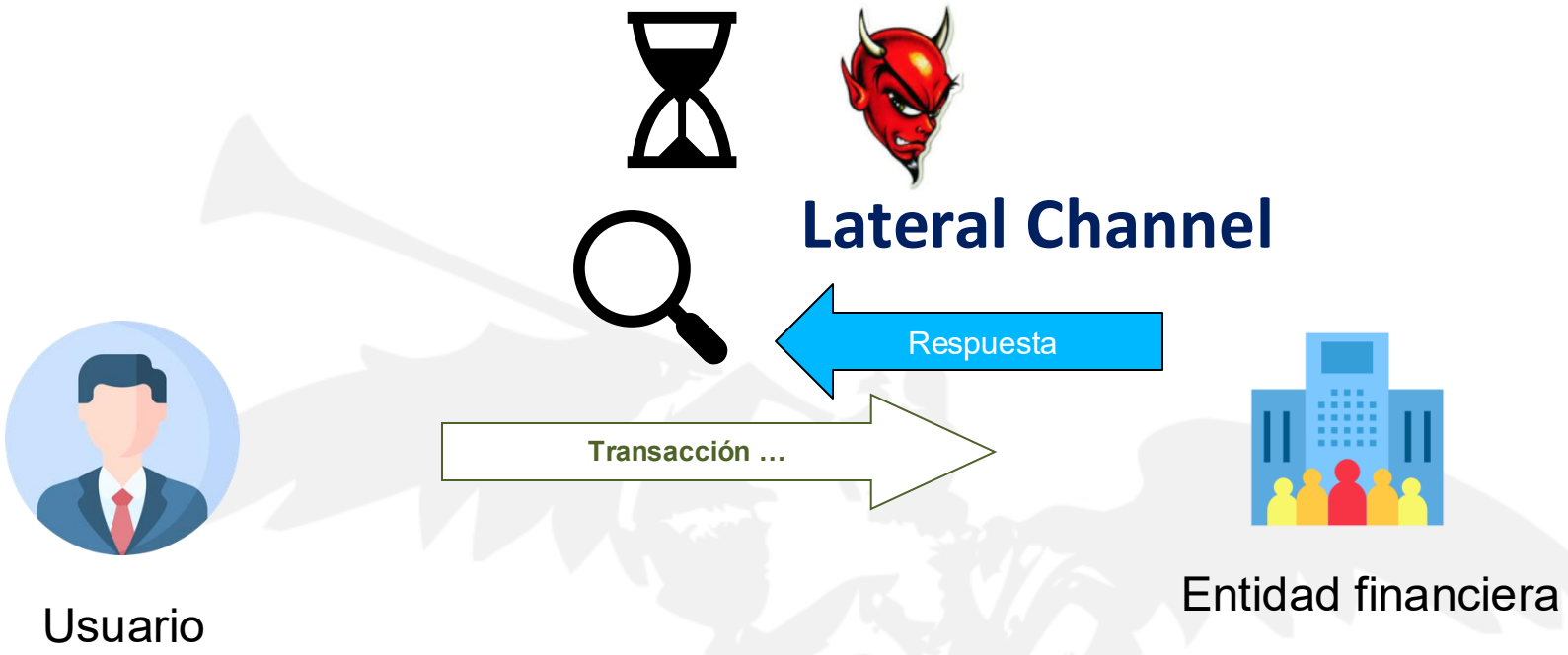
¿Problemas de seguridad?



¿Problemas de seguridad?



¿Problemas de seguridad?



1. Contexto
2. Problemas de seguridad
3. **Objetivos y requisitos**
4. Entrega

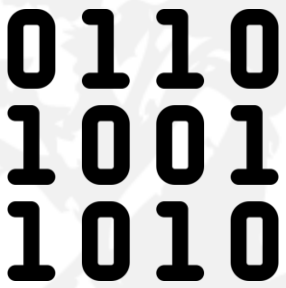
Política Seguridad

*"Se debe preservar la **integridad en el almacenamiento de credenciales de usuario**"*

*"En todas las transacciones **por medios electrónicos no seguros se debe conservar la integridad** de las comunicaciones"*

Key size

HMAC



Hashing

Objetivos

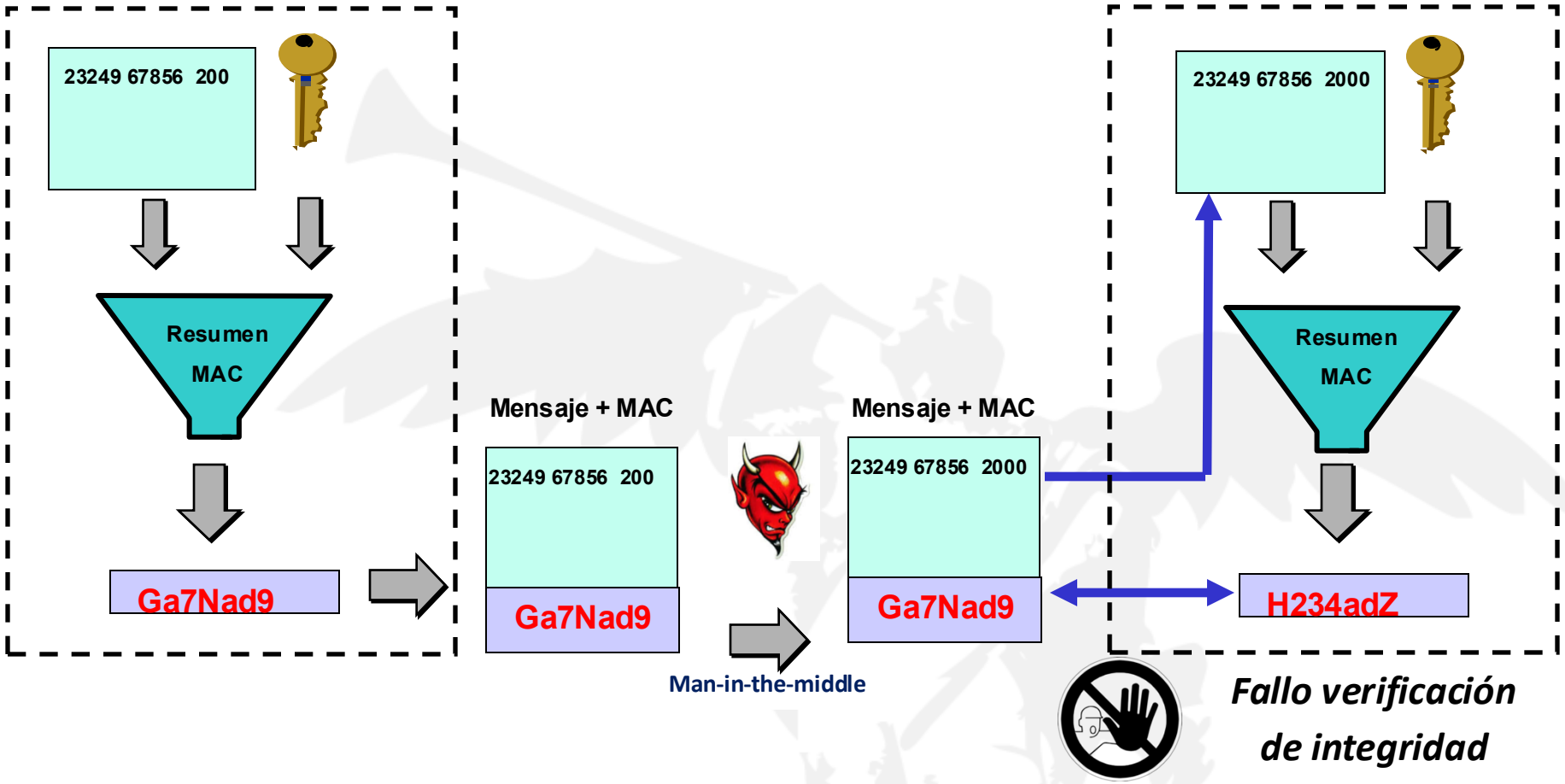
1. **Desarrollar un sistema cliente-servidor usando sockets**, que permita enviar datos de nombre de usuarios, contraseñas, y mensajes de transacciones cumpliendo los aspectos indicados en Política de Seguridad de la empresa.
2. **Desarrollar en el servidor un mecanismo que permita registrar, almacenar y comprobar las credenciales de usuario** preservando la integridad de la información.
3. **Desarrollar el verificador de integridad para los mensajes de transferencia** bancaria que se transmiten a través de las redes públicas ***evitando los ataques*** de *man-in-the-middle,* de *replay (tanto en el servidor como en el cliente), de key derivation, de canal lateral*, usando mecanismos de MAC, NONCE, TAMAÑOS DE CLAVE ADECUADOS y SECURE-COMPARATOR.
4. Analice y discuta las ***diferentes opciones que existen para la compartición segura de claves*** y cuál sería más adecuado para evitar incidentes de seguridad.

Requisitos funcionales:

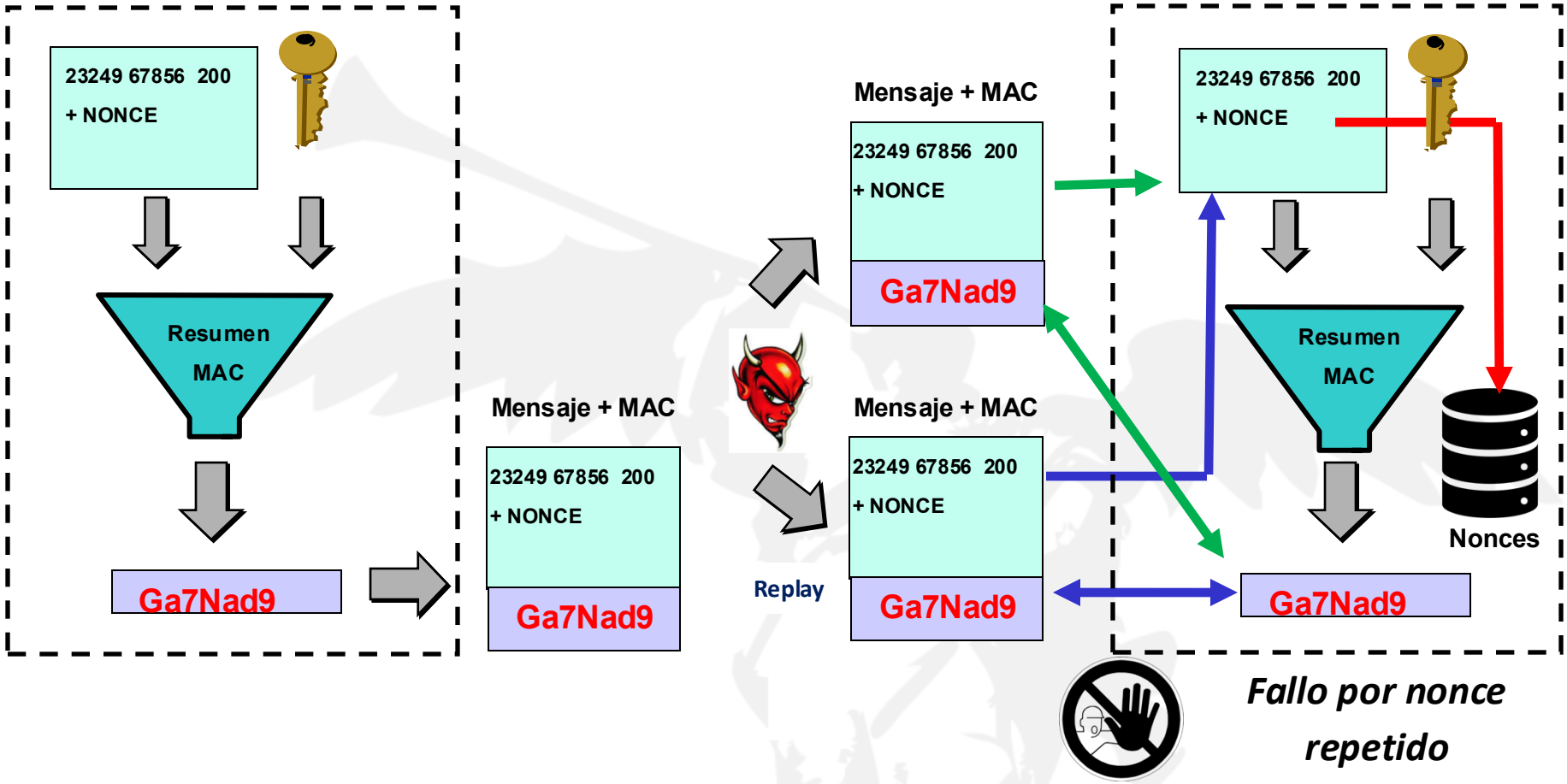
1. **Registro de usuarios**
2. **Inicio de sesión**
3. **Verificar credenciales**
4. **Cerrar sesión**
5. **Gestión de usuarios preexistentes**
6. **Transacciones**
7. **Persistencia de datos**
8. **Interfaz de comunicación**

Requisitos información:

1. **Datos de usuarios**
2. **Registro inicial**
3. **Transacciones**
4. **Mensajes del sistema**


23249 67856 200
Resumen
MAC
Ga7Nad9
Mensaje + MAC
23249 67856 200
Ga7Nad9
Man-in-the-middle
Mensaje + MAC
23249 67856 2000
Ga7Nad9
23249 67856 2000
Resumen
MAC
H234adZ
Fallo verificación
de integridad

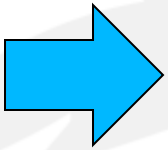
Recomendaciones



1. Contexto
2. Problemas de seguridad
3. Objetivos y requisitos
4. **Entrega**

¿Cómo y qué entrego en el PAI?

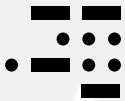
Especificación



Entregable

Informe

Test/Logs



Código/Configuración

Deadline: 7 de octubre

Penalizaciones: 10%

Muchas gracias por vuestra colaboración