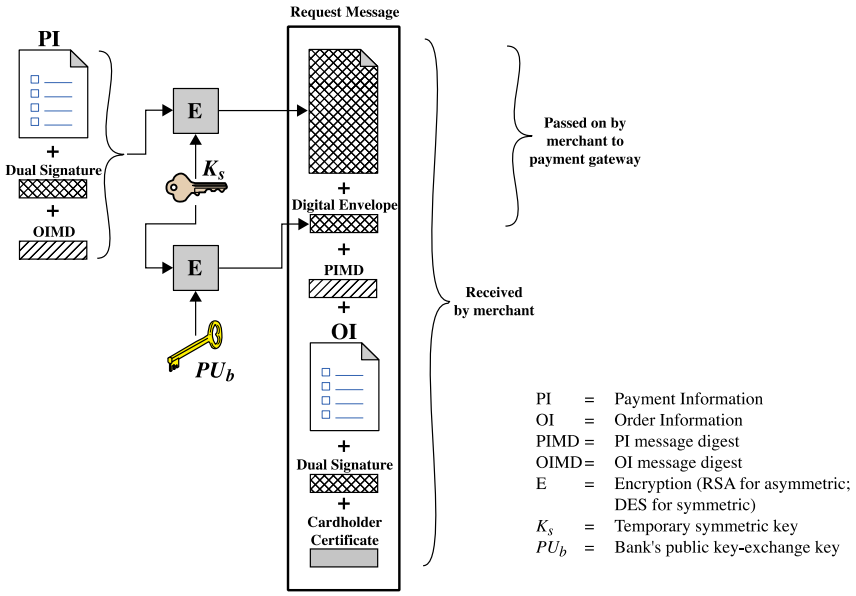
RELACIÓN DE EJERCICIOS

EJERCICIO 1:

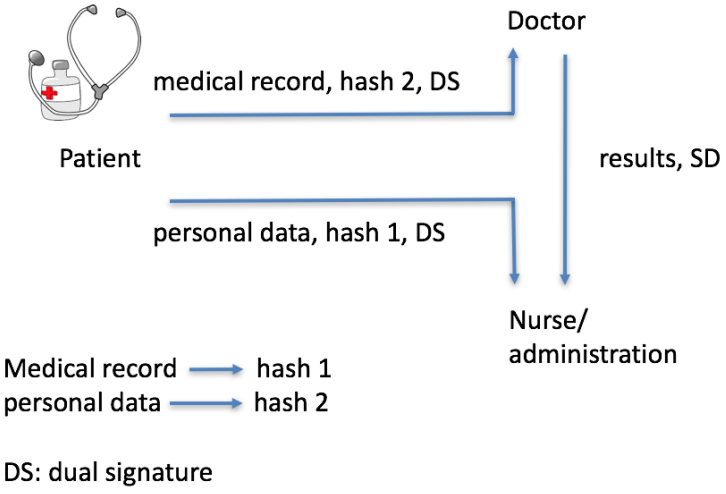
Teniendo en cuenta la siguiente figura:



¿Qué hace el banco al recibir el mensaje?

EJERCICIO 2:

Teniendo en cuenta el siguiente escenario:



Se pide realizar la firma dual y gestionar dicha firma en las diferentes entidades. Como se puede ver, existen tres tipos de actores: el paciente, el doctor y la enfermera, cada

uno de ellos gestionando específicos tipos de datos relacionados con los pacientes (ej. los datos personales, los historiales y los resultados de diagnóstico).

Es decir:

- Los pacientes: envían (1) sus historiales al doctor para que éste pueda analizarlo, y (2) sus datos personales a la enfermera para que ésta la pueda gestionar y cerrar el proceso.
- El doctor: analiza los registros médicos de los pacientes y redacta el informe médico (con los resultados del diagnóstico) para ser enviado a la enfermera.
- La enfermera: gestiona los datos del paciente y los asocia con los resultados recibidos del doctor.

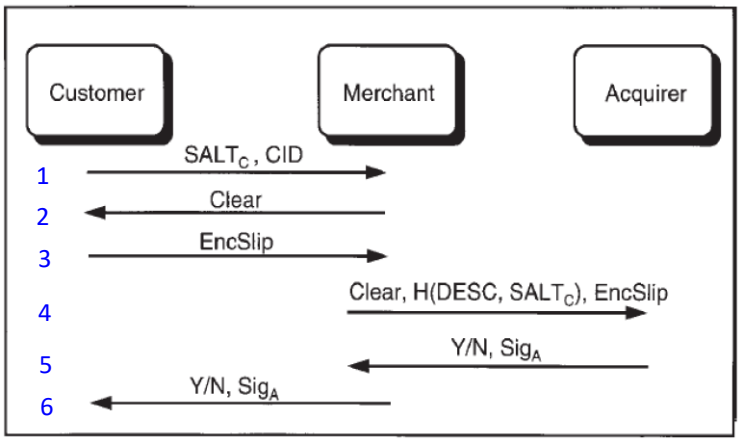
EJERCICIO 3:

Teniendo en cuenta la siguiente información:

Item	Description
CAN	Customer's account number (e.g., credit card number)
ID_M	Merchant ID; identifies merchant to acquirer
TID_M	Transaction ID; uniquely identifies the transaction
DESC	Description of the goods; includes payment information such as credit card holder's name and bank identification number
$SALT_C$	Random number generated by C; used to randomize DESC and thus ensure privacy of DESC on the M to A link
$NONCE_M$	Random number generated by a merchant to protect against replay
DATE	Merchant's current date/time
PIN	Customer's PIN which, if present, can be optionally used in 1KP to enhance security
Y/N	Response from card issuer; Yes/No or authorization code
R_C	Random number chosen by C to form CID
CID	A customer pseudo-ID which uniquely identifies C; computed as $CID = H(R_C, CAN)$
V	Random number generated in 2KP and 3KP by merchant; used to bind the Confirm and Invoice message flows

Item	Description
Common	Information held in common by all parties: PRICE, ID_M, TID_M, DATE, $NONCE_M$, CID, $H(DESC, SALT_C)$, [H(V)]
Clear	Information transmitted in the clear: ID_M, TID_M, DATE, $NONCE_M$, H(Common), [H(V)]
SLIP	Payment instructions: PRICE, H(Common), CAN, R_C, [PIN]
EncSlip	Payment instruction encrypted with the public key of the acquirer: PK_A (SLIP)
$CERT_X$	Public-key certificate of X, issued by a CA
Sig_A	Acquirer's signature: SK_A[H(Y/N, H(Common))]
Sig_M	Merchant's signature in Auth-Request: SK_M[H(H(Common), [H(V)])]
Sig_C	Cardholder's signature: SK_C[H(EncSlip, H(Common))]

Y el diagrama:



Se pide:

1. Sustituir los valores de cada transacción teniendo en cuenta la información dada.
2. Determinar cómo el banco receptor (Acquirer) valida la transacción y verifica la validez de la operación.
3. Contestar a las siguientes preguntas:
    a. ¿El banco valida la autenticidad del cliente?
    b. ¿El vendedor se autentica ante el cliente y el banco (Acquirer)?
    c. ¿El cliente y el vendedor proporcionan al banco (Acquirer) evidencias de su intervención en la transacción?