E-COMMERCE

3DS

Sommaire

Objectifs

- **A la fin de cette session, vous devriez être en mesure de:**

  - Déterminer le flux d'une opération E-COMMERCE
  - Identifier les composants de l'environnement 3D Secure
  - Assimiler le flux d'une autorisation 3D Secure
  - Lire et analyser des messages 3D Secure

Sommaire

Introduction

- **Ecommerce in brief:**
  - Enables selling/buying goods and services, through the internet, without time or location limits
  - Some advantages :

Customer	Merchant
☐ Lower Prices	☐ Higher Margins
☐ Accessibility and Convenience	☐ Scalability
☐ Wider Choice	☐ Consumer Insight

Introduction

- **E-Commerce**
  - E-commerce (electronic commerce) is the transaction of buying/selling goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet.
  - E-commerce typically uses the internet for at least one part of the transaction's life cycle
  - Ecommerce can be classified based on the type of participants in the transaction:
    - Business to Business (B2B)
    - Business to Consumer (B2C)
    - Consumer to Consumer (C2C)

Introduction

- Dans un processus de paiement d'une transaction dans un environnement à distance, l'authentification est la phase de vérification du porteur et de l'authenticité de sa possession de la carte.

- Le protocole 3D Secure a été développé par VISA afin de vérifier l'identité d'un client durant une transaction en ligne. Le protocole a par la suite été adopté par MCI, JCB … pour lancer leurs programmes d'e-commerce.

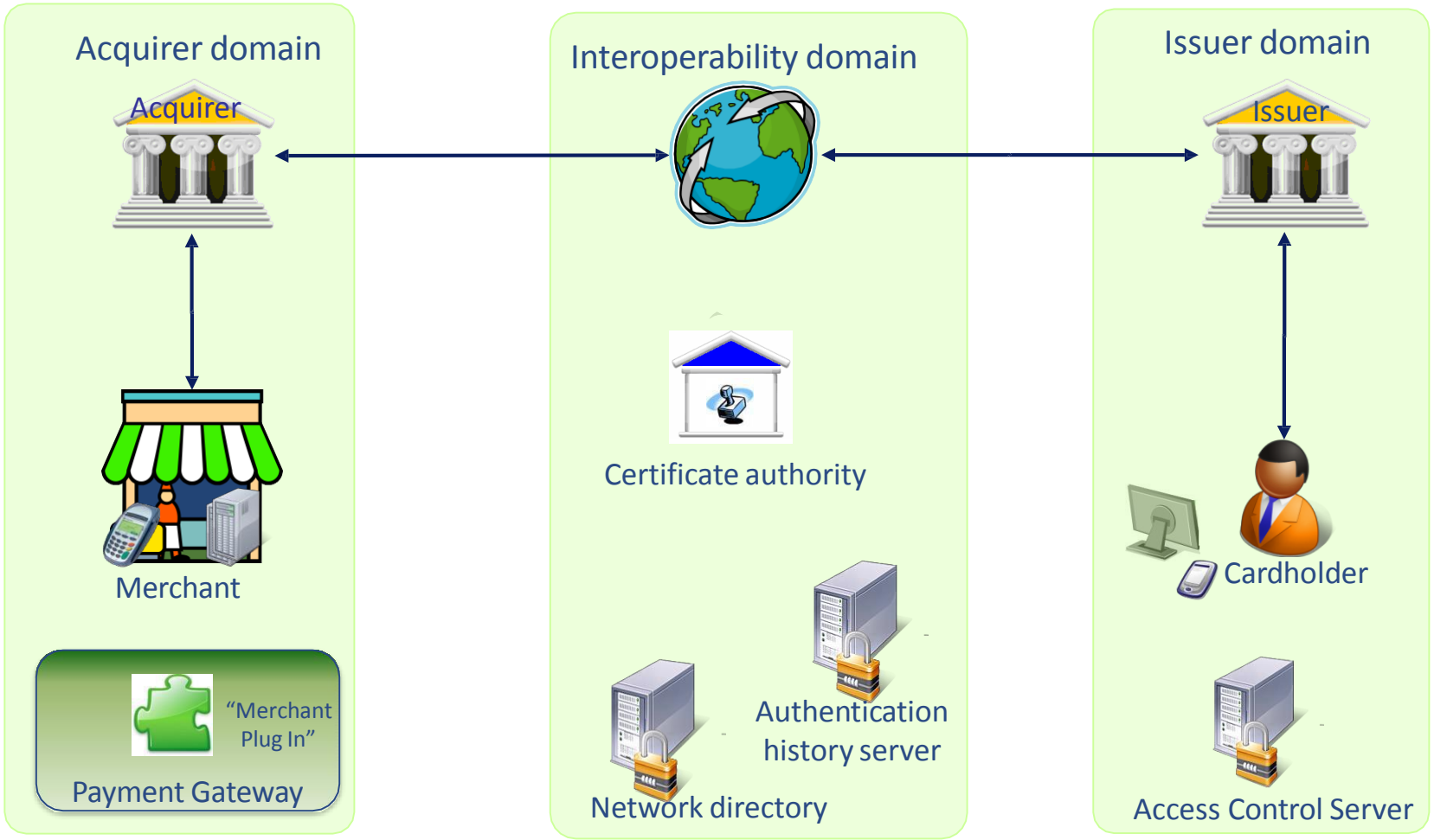
- Aux côtés du CVV, un code sur 3 positions qui est imprimé sur le dos de la carte, le 3D Secure offre un niveau supplémentaire de protection dans une transaction avec *Carte Non Présente.*

Introduction

- Le 3D Secure rajoute une étape supplémentaire d'authentification pour les paiements en ligne:
  - Les commerçants sont encouragés à utiliser le 3D Secure pour assurer une plus haute protection contre les tentatives de fraude.
  - Quand un commerçant ne supporte pas le 3D Secure, il est plus sensible aux transactions frauduleuses même si la transaction est correctement autorisée.
  - Les porteurs de cartes qui ne sont pas enrôlés 3D Secure ne remarqueront aucun changement dans le flux de leurs transactions.

Introduction

- Le 3D est pour les trois domaines:



Introduction

- **Les composants du 3DS (1/4)**
  - Le Domaine Acquéreur est composé de:
    - Commerçants qui:
      - Détiennent un contrat avec l'acquéreur
      - Acceptent des cartes appartenant à des réseaux de paiement électronique
      - Acceptent des transactions e-commerce
    - Merchant Server Plug In (MPI):
      - Crée et échange des messages d'authentification avec les réseaux de paiement et les composants de l'authentification émetteur
      - Met à jour la tranche de carte éligibles au protocole selon une fréquence prédéfinie
    - L'acquéreur:
      - Traite la demande d'autorisation selon les étapes d'authentification
      - Assure la compensation et le règlement pour les transactions e-commerce ainsi que le règlement des commerçants

Introduction

- **Les composants du 3DS (2/4)**
  - Le Domaine Emetteur est composé de:
    - Porteurs, navigateur et dispositif:
    - L'Emetteur qui:
      - Met à jour le Network Directory avec les tranches participantes
      - Définit le processus d'enrôlement
      - Définit les porteurs éligibles aux transactions 3D Secure
    - L' Access Control Server 'ACS':
      - Alimenté par les données d'authentification des clients durant un processus d'enrôlement
      - Vérifié durant la phase d'authentification d'une autorisation e-commerce

Introduction

- **Les composants du 3DS (3/4)**
  - Le Domaine d'interopérabilité est composé de:
    - Network Directory:
      - Enregistre les tranches de cartes participant au 3D Secure
      - Authentifie leur participation durant une transaction e-commerce
    - L'authentication History Server:
      - Enregistre les messages d'authentification échangés entre l'ACS et le MPI
    - Le Système d'autorisation, compensation et règlement:
      - À la suite du processus d'authentification la demande d'autorisation est envoyée à l'émetteur et la réponse émise à l'acquéreur
      - Gère la compensation et le règlement des transactions des côtés émetteur et acquéreur

Introduction

- **Les composants du 3DS (4/4)**
  - Le Domaine d'interopérabilité est composé de:
    - Autorité de certification:
      - Génère et distribue les certificats requis par différents composants des 3 domaines
    - Ces certificats incluent:
      - Le certificat du réseau de paiement nommé ''Root certificate''
        - Est un certificat auto-signé
      - À la suite du processus d'authentification la demande d'autorisation est envoyée à l'émetteur et la réponse émise à l'acquéreur
      - Gère la compensation et le règlement des transactions des côtés émetteur et acquéreur

Sommaire

Prérequis et configuration

- **Prérequis de sécurité**
  - Le protocole de sécurité utilisé sur la couche de transport pour le 3D Secure et le Transport Layer Security Protocol (**TLS**)
  - Le protocole standard est basé sur Secure Sockets Layer V3 (**SSL**)
    - Cela assure la sécurité des échanges de données (entre client/serveur)
    - Ca a également d'autres mécanismes pour:
      - Assurer l'intégrité des données transmises
      - Détecter les données perdues ou dupliquées
  - Les données échangées dans les canaux ci-après devraient également être sécurisées
    - Site commerçant et MPI
    - MPI et Directory Server
    - Directory Server et Access Control Server

Prérequis et configuration

- **Exigences de certification >> MPI au Directory Server (1/4)**
  - Le Domaine Acquéreur génère deux clés:
    - Clé publique
    - Clé privée

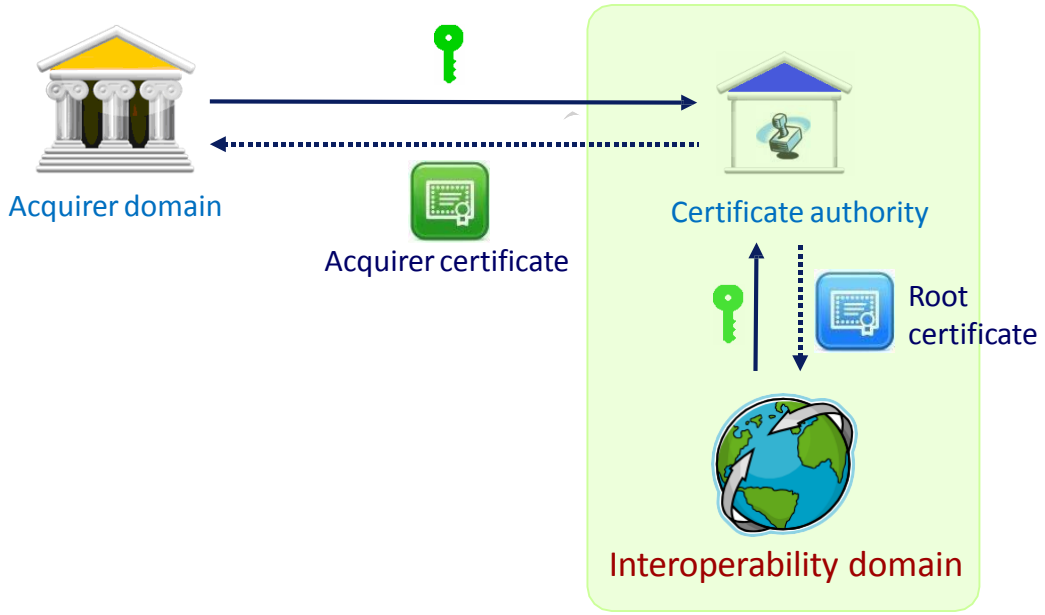
    } Keystore acquéreur

  - Le Domaine d'intéropérabilité génère deux clés
    - Clé publique
    - Clé privée

    } Keystore réseau

Prérequis et configuration

- **Exigences de certification >> MPI au Directory Server (2/4)**
  - Le Domaine Acquéreur communique la clé publique à la CA pour signature
  - La CA signe la clé et envoie le certificate à l'acquéreur
  - Le Domaine d'Intéropérabilité signe la clé publique

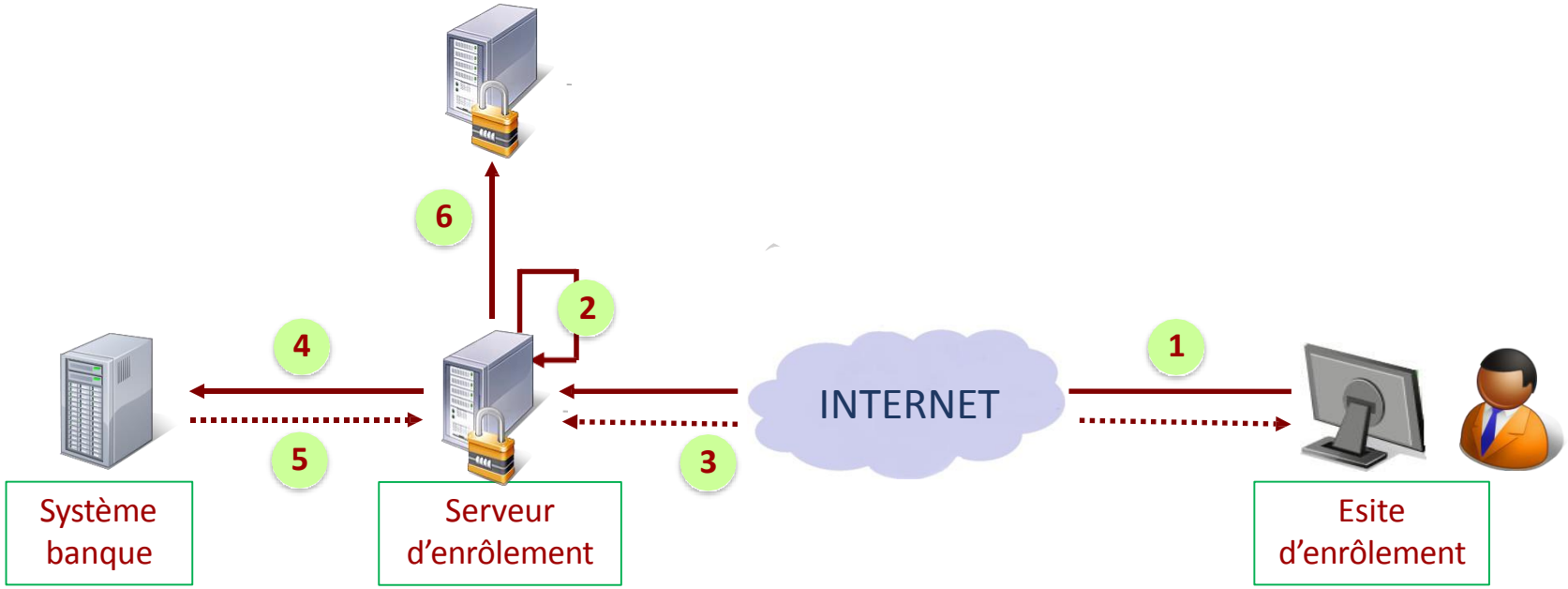


Prérequis et configuration

- **Exigences de certification >> MPI au Directory Server (3/4)**
  - Durant une transaction en ligne:
    1. Communication sécurisée avec le porteur
       - SSL server certificate
    2. Communication sécurisée avec le directory
       - SSL client certificate

Prérequis et configuration

- **Processus d'enrôlement du porteur**
  - Flux

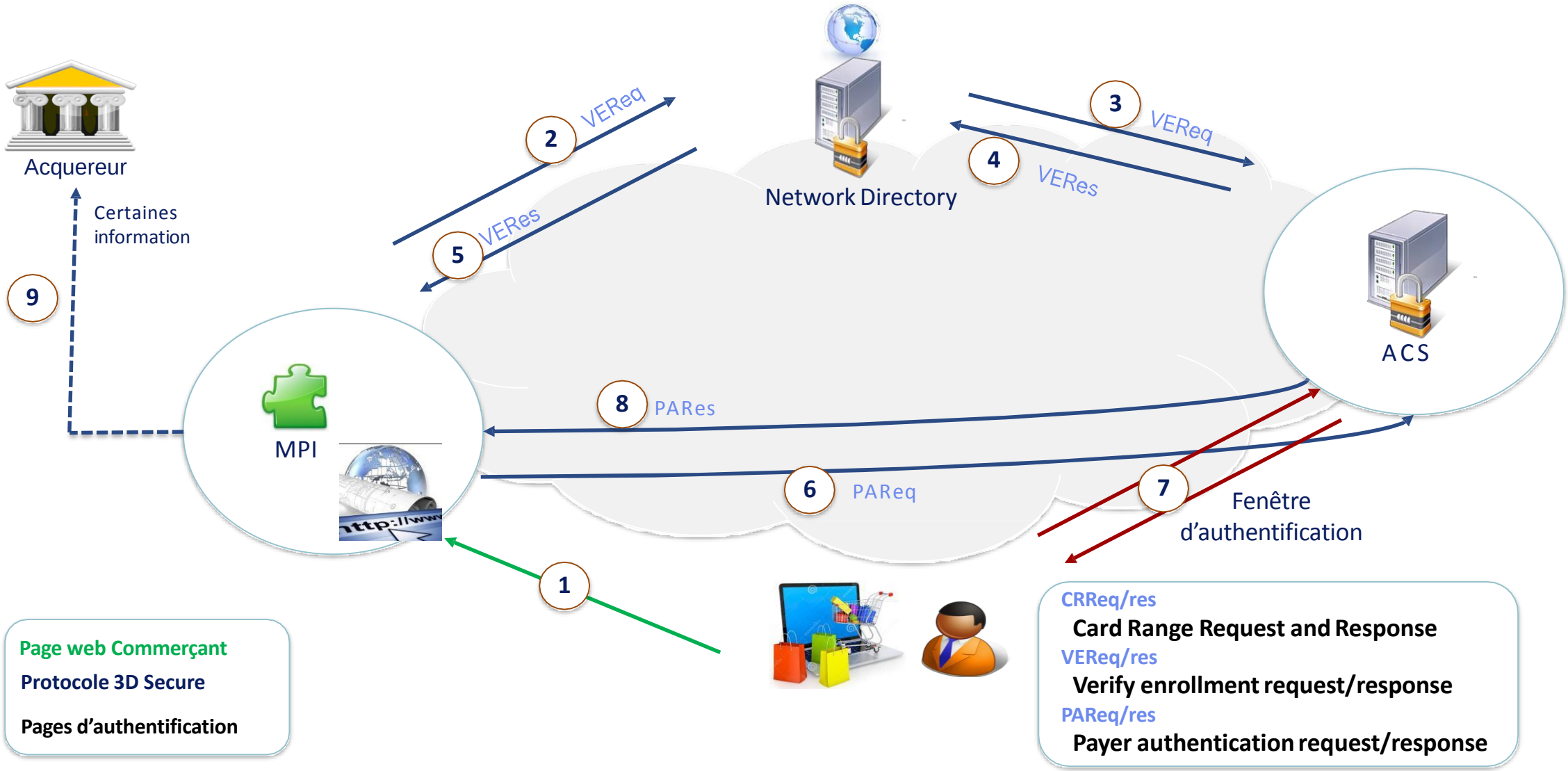


Sommaire

Flux d’une transaction 3D secure

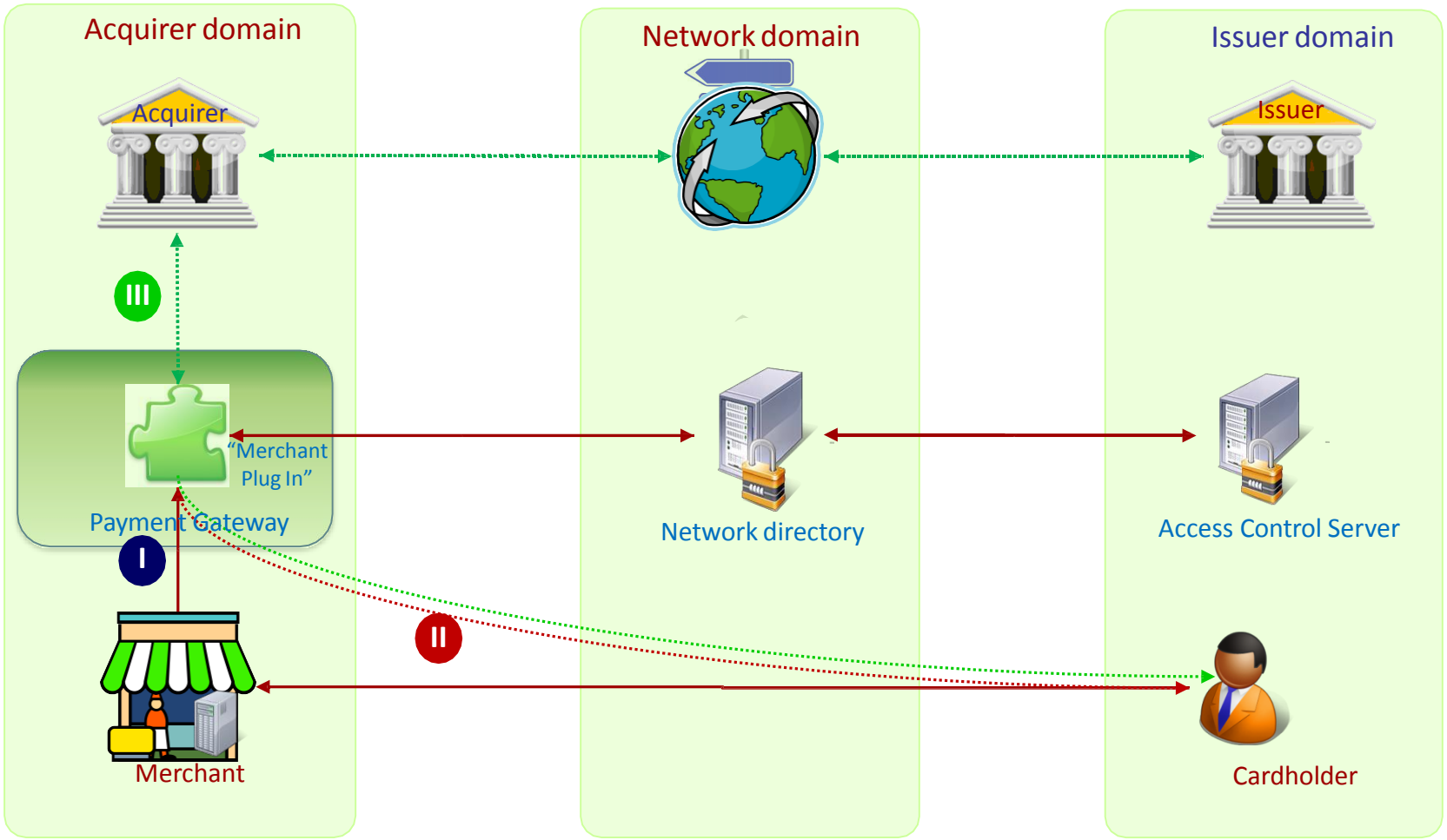
- **Exemple de processus:**
  - Le client se connecte au site commerçant
  - Il sélectionne les biens ou services à acheter
  - Il insére les données de la carte
  - Ces données sont vérifiées
  - L’autorisation est traitée
  - La réponse est affichée au client

3D-Secure flux transaction



Flux d’une transaction 3D secure

- **Flux de l’autorisation:**



Flux d’une transaction 3D secure

II Processus d’authentification

- Le porteur initie la transaction à travers un site web commerçant
- La requête est traitée par le MPI et routée au Network Directory
- Le Network Directory determine si le numéro de la carte est dans la tranche participante
- Le Network Directory route la requête à l’ACS approprié
- Le Network Directory reçoit la réponse de l’ACS indicant si l’authentification est dsponible pour ce compte
- Le Network Directory route la réponse au commerçant à travers le MPI

Flux d’une transaction 3D secure

Echec d’authentification

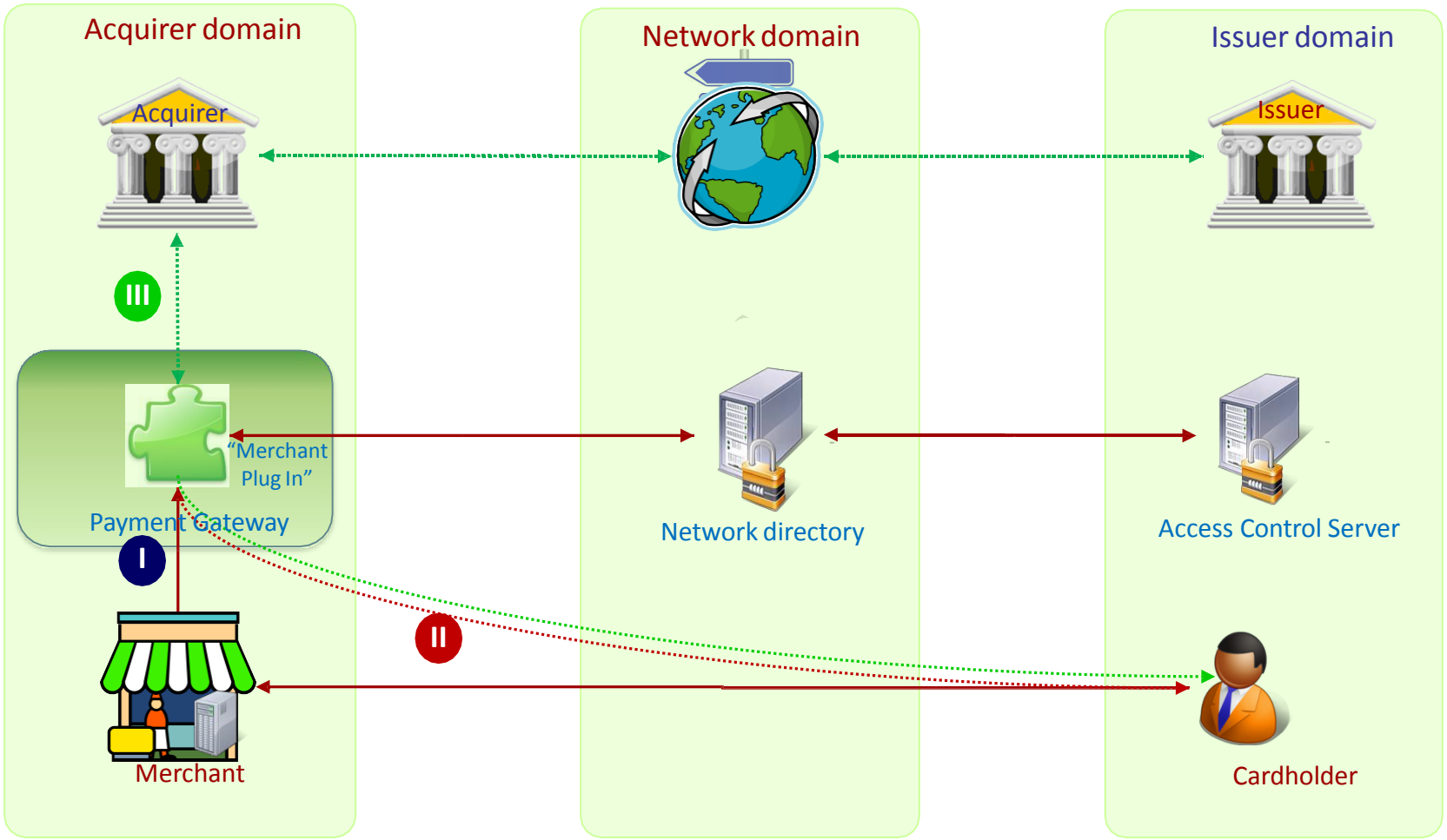
- Si la réponse est negative ou l’authentification échoue l’operation d’achat s’arrête

Processus d’autorisation

- Si l’authentification est OK ou l’operation n’est pas 3D Secure (côté commerçant) la demande d’autorisation est envoyée à l’acquéreur
- L’acquéreur la traite comme une autorisation normale

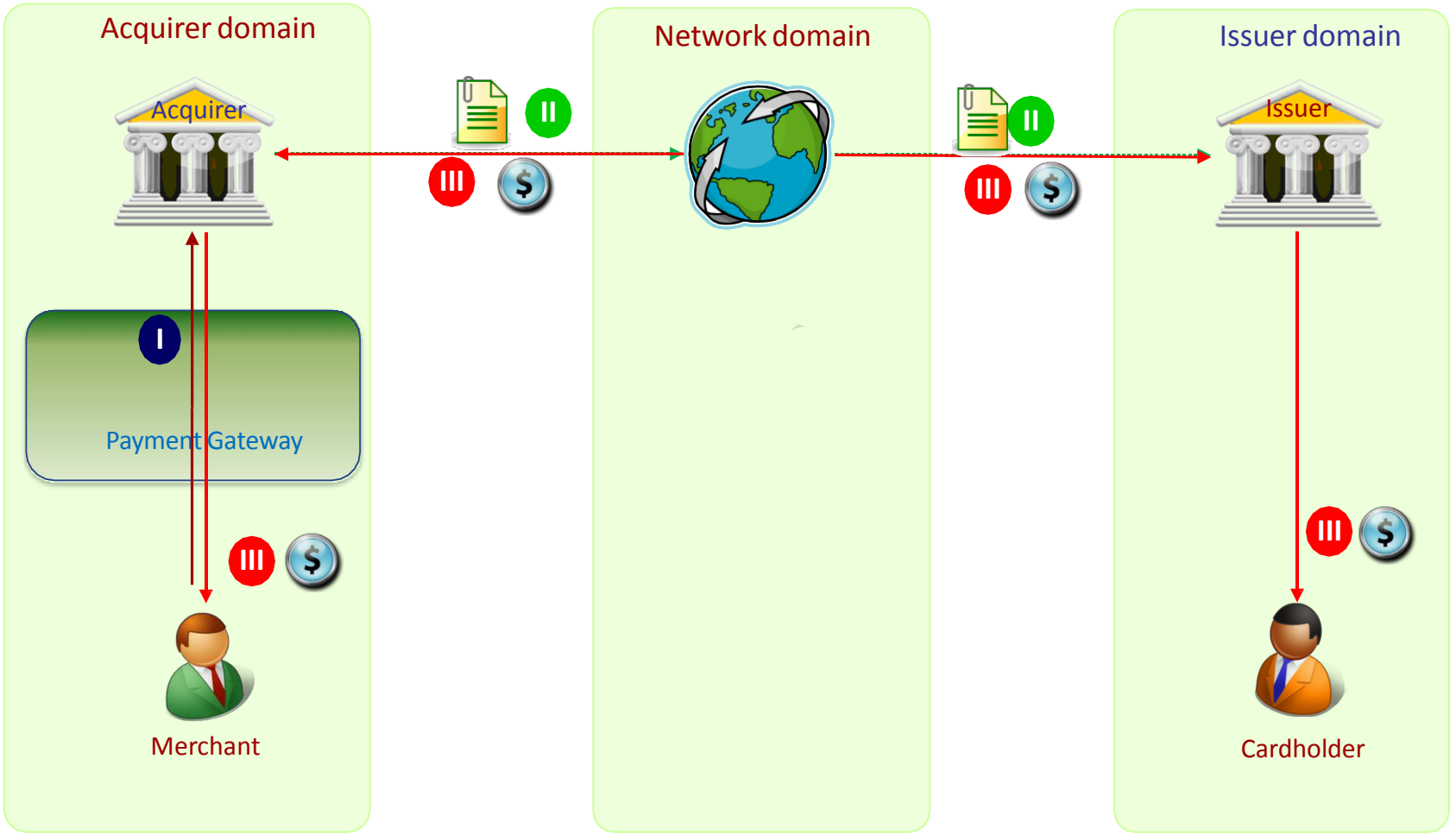
Flux d’une transaction 3D secure

- **Flux de l’autorisation:**



Flux d’une transaction 3D secure

- **Flux de compensation et réglement**

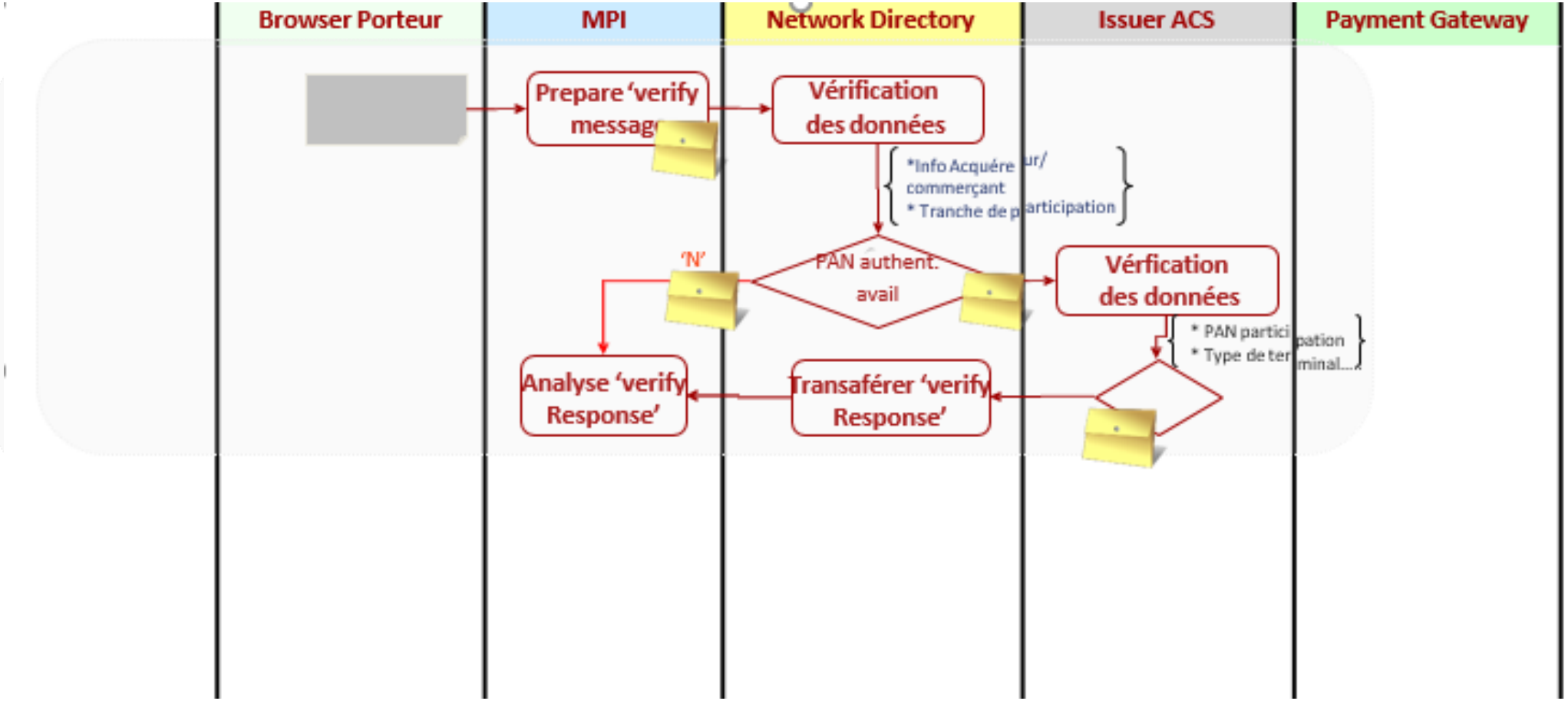


Flux d’une transaction 3D secure

- **Description**
  - Collecte de transaction
    - Les transactions sont soit captures par le commerçant ou automatiquement soumises
    - La Payment Gateway transfert les transactions à l’acquéreur
  - Compensation
    - L’acquéreur présente les transactions au réseau à travers le fichier outgoing
    - L’émetteur reçoit et traite ces transactions
  - Règlment
    - L’acquéreur transfert les fonds au compte bancaire du commerçant
    - L’émeteur paie pour les transactions du porteur
    - Le réseau collecte le fond des émetteur à transmettre aux acquéreurs

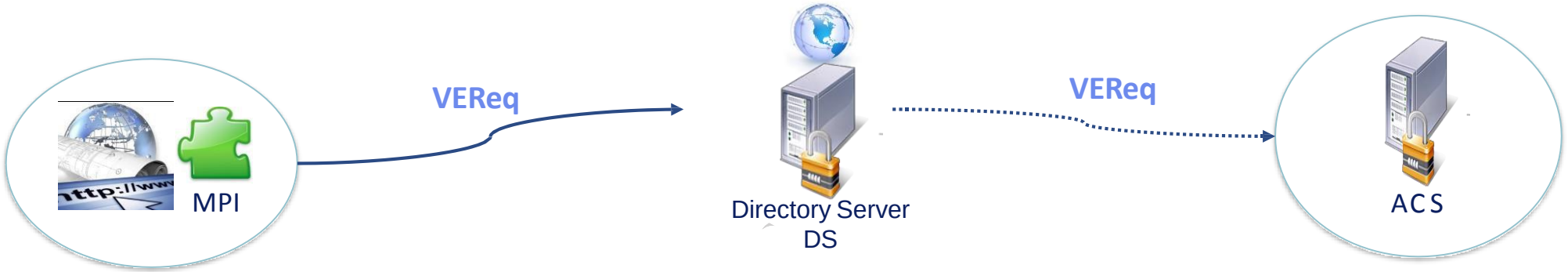
Flux d’une transaction 3D secure

- **Détails du processus: 1ere étape*: Vérification du porteur***

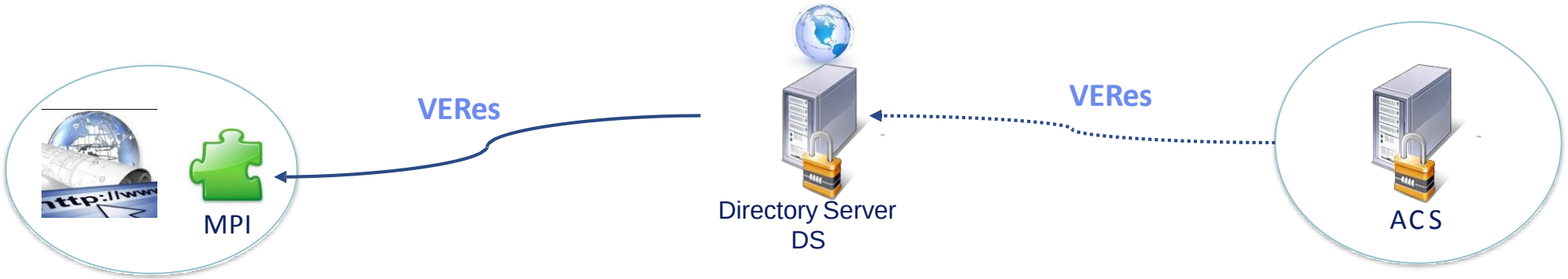


3D-Secure flux transaction

- **VEReq/ VERes (1/3)**
  - MPI envoie VEReq au DS pour déterminer si l'authentification est disponible pour un PAN donné



  - DS renvoie un message VERes ou transfert le VEReq à ACS, qui retourne VERes



3D-Secure flux transaction

- **VEReq/ VERes (2/3)**
  - Statut des demandes d'authentification
    - DS renvoie le message VERes, indiquant l'une des réponses suivantes:

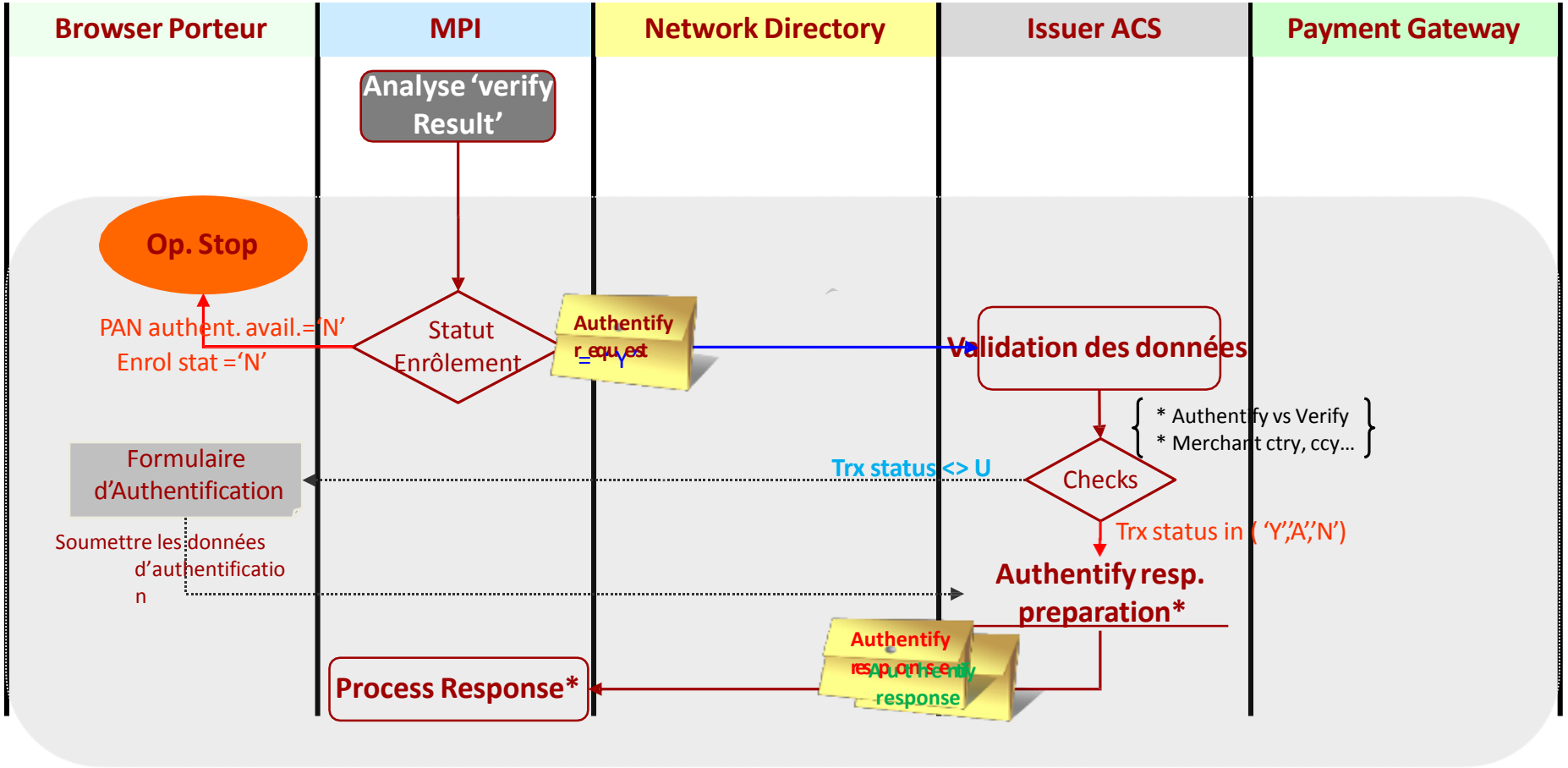
Valeur du statut	Résultat
Y	Authentification disponible : Porteur enrôlé
U	Impossible d'authentifier
N	Porteur non enrôlé

  - Electronic Commerce Indicator
    - Permet d'indiquer le niveau de sécurité utilisé quand le porteur fournit les informations de paiement

ECI=6	ECI=7
L'émetteur ou le titulaire de la carte ne participent pas au 3DS	L'authentification de paiement n'a pas été faite

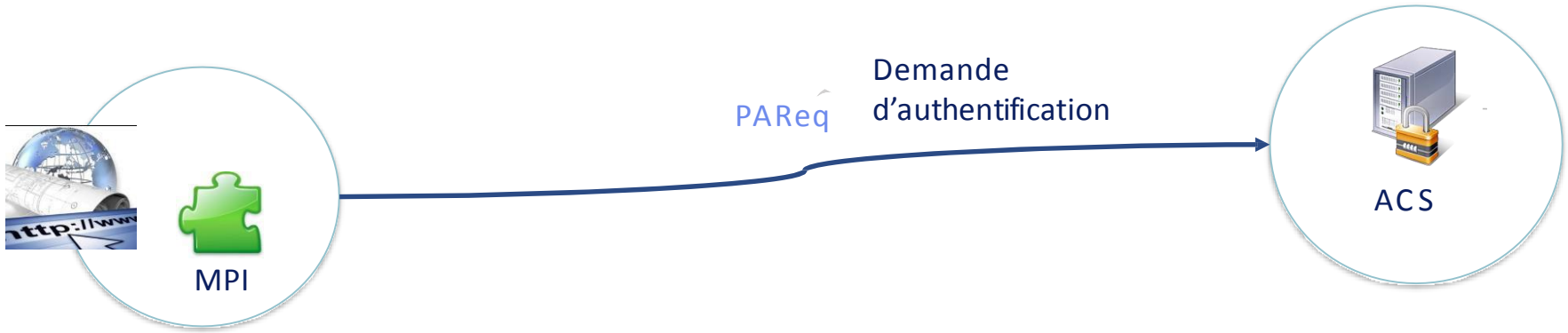
Flux d’une transaction 3D secure

- **Détails du processus: 2ème étape: *Phase d’authentification***



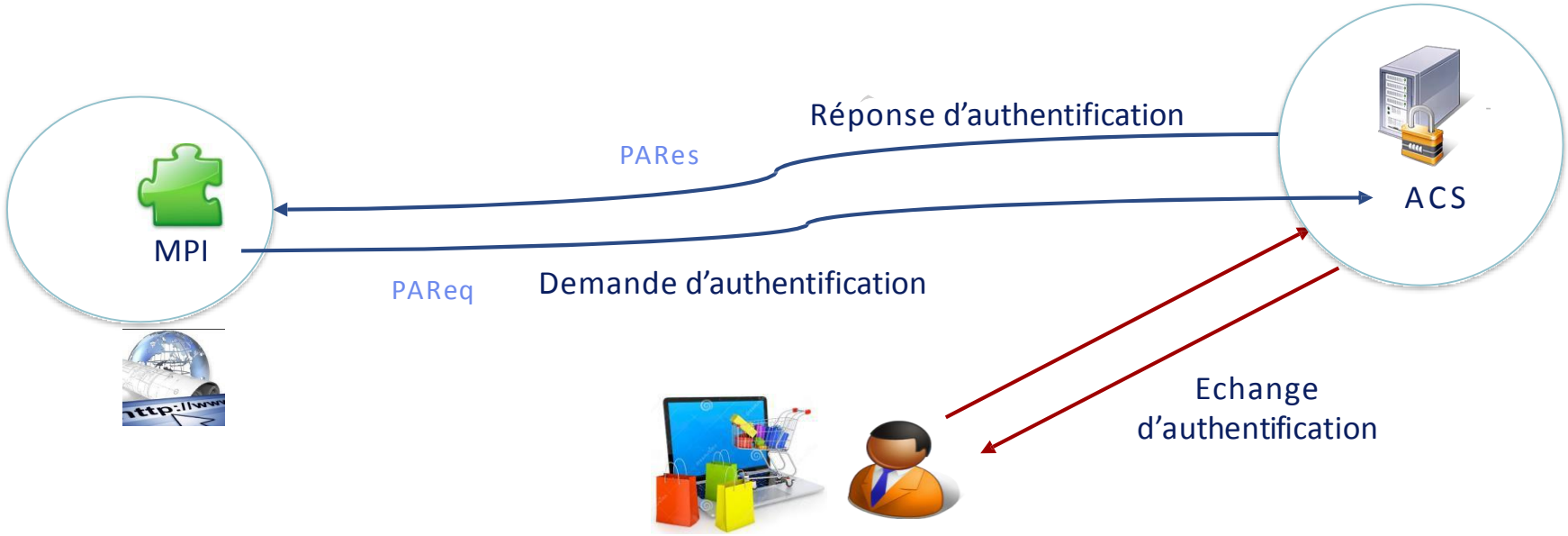
3D-Secure flux transaction

- **PAReq/ PARes (1/5)**
  - MPI envoie un message PAReq à l'ACS en utilisant l'URL reçu dans le VERes correspondant
  - PAReq contient les données de la demande d'achat sur la base desquelles les décisions d'authentification vont être prises



3D-Secure flux transaction

- **PAReq/ PARes (2/5)**
  - ACS retourne PARes contenant le résultat de l'authentification de l'émetteur de la carte
  - MPI valide la signature du message PARes afin de compléter le processus d'authentification



3D-Secure flux transaction

- **PAReq/ PARes (3/5)**
  - Statut des transactions
    - ACS retourne PARes indiquant le statut de l'authentification et l'une des réponses suivantes
  - CAVV
    - L'émetteur inclus le CAVV (Cardholder Authentication Verification Value) dans chaque message PARes ayant le statut 'Y' ou 'A'
  - Electronic Commerce Indicator
    - ECI indique le niveau de sécurité utilisé quand le porteur fournit les informations de paiement au commerçant

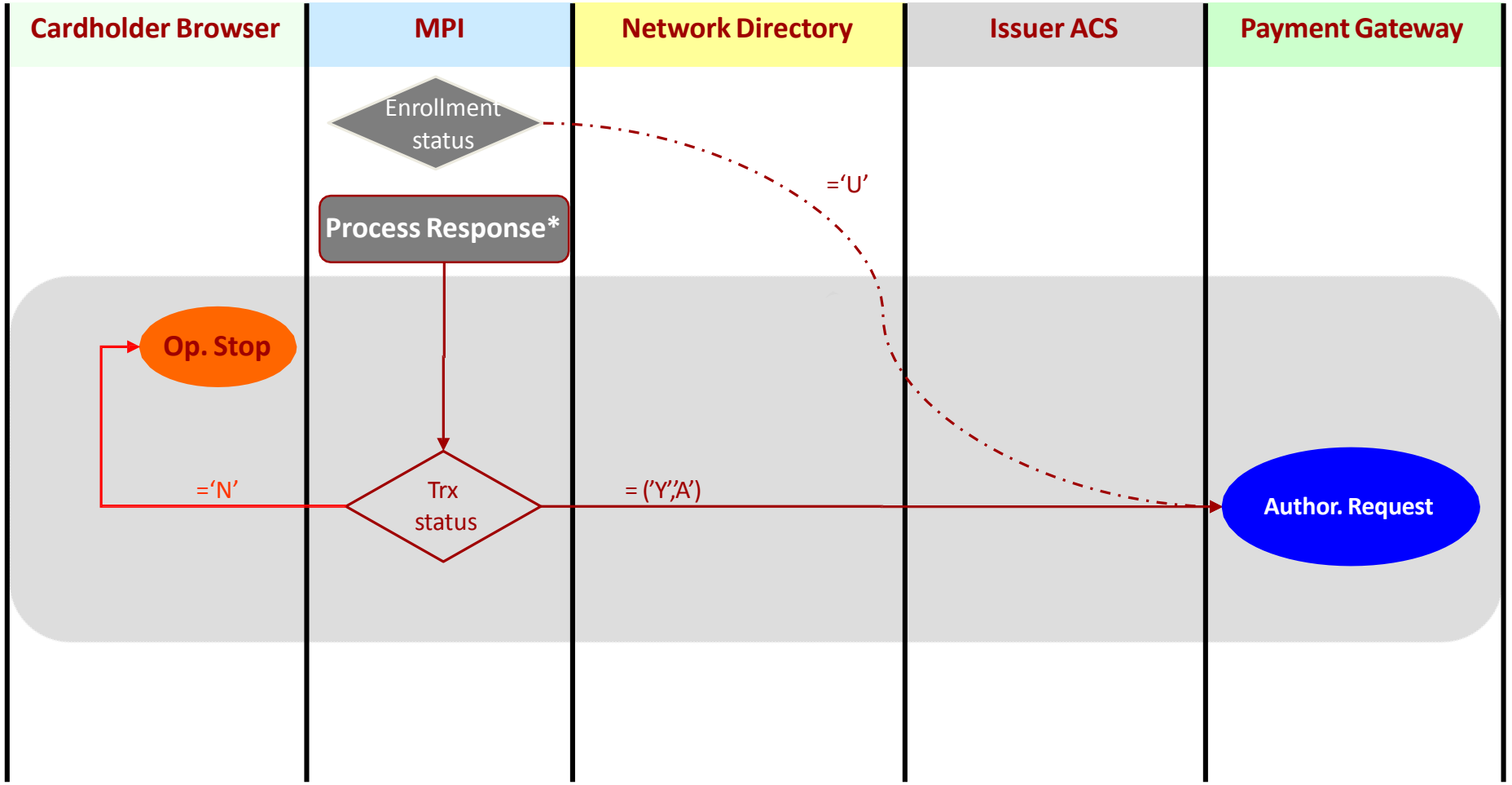
3D-Secure flux transaction

- **PAReq/ PARes (4/5)**
  - Statut des transactions / CAVV / Electronic Commerca Indicator

Résultats d'authentification	Statut transaction	CAVV	ECI
Authentification réussie	Y	Valeur présente	5 : Cette valeur est envoyé par l'ACS au niveau du message PARes lorsque l'authentification du porteur est réussie
Authentification non réussie	N	Valeur non présente	Valeur non présente
Authentification peut ne pas être effectuée	U	Valeur non présente	7 : envoyé par le commerçant lorsque l'opération a été effectuée sur un canal sécurisé (SSL / TLS), mais ACS n'a pas été effectuée
Tentatives de traitement effectuées	A	Valeur présente	6 : Peut signifier que l'émetteur ou le porteur ne participent pas au 3DS

Flux d’une transaction 3D secure

- **Détails du processus: 3ème étape: *Phase d’autorisation***



Sommaire

Description et format des messages

- **Messages 3D-secure**
  - Messages de Vérification
  - Messages d’Authentification
  - Messages de Chargement de tranches de cartes
  - Messages d’Erreur
  - Message d’Archivage

Description et format des messages

- **3D-secure messages (1/4)**
  - Messages de Vérification:
    - **VEReq (Verify Enrollment Request)**
      - Envoyé par le Merchant Server Plug-in (MPI) au Directory Server
    - **VERes (Verify Enrollment Response)**
      - Envoyé par l'ACS via le Directory Server, ou par le Directory Server

Description et format des messages

- **3D-secure messages (2/4)**
  - Messages d'Authentification:
    - **PAReq (Payer Authentication Request)**
      - Message envoyé par le Merchant Server Plug-in (MPI) à l'ACS à travers le système du porteur, fournissant les données requises pour l'authentification du porteur
    - **PARes (Payer Authentication Response)**
      - Message envoyé par l'ACS en réponse au PAReq indépendemment de l'authentification si elle est avec succès ou pas.

Description et format des messages

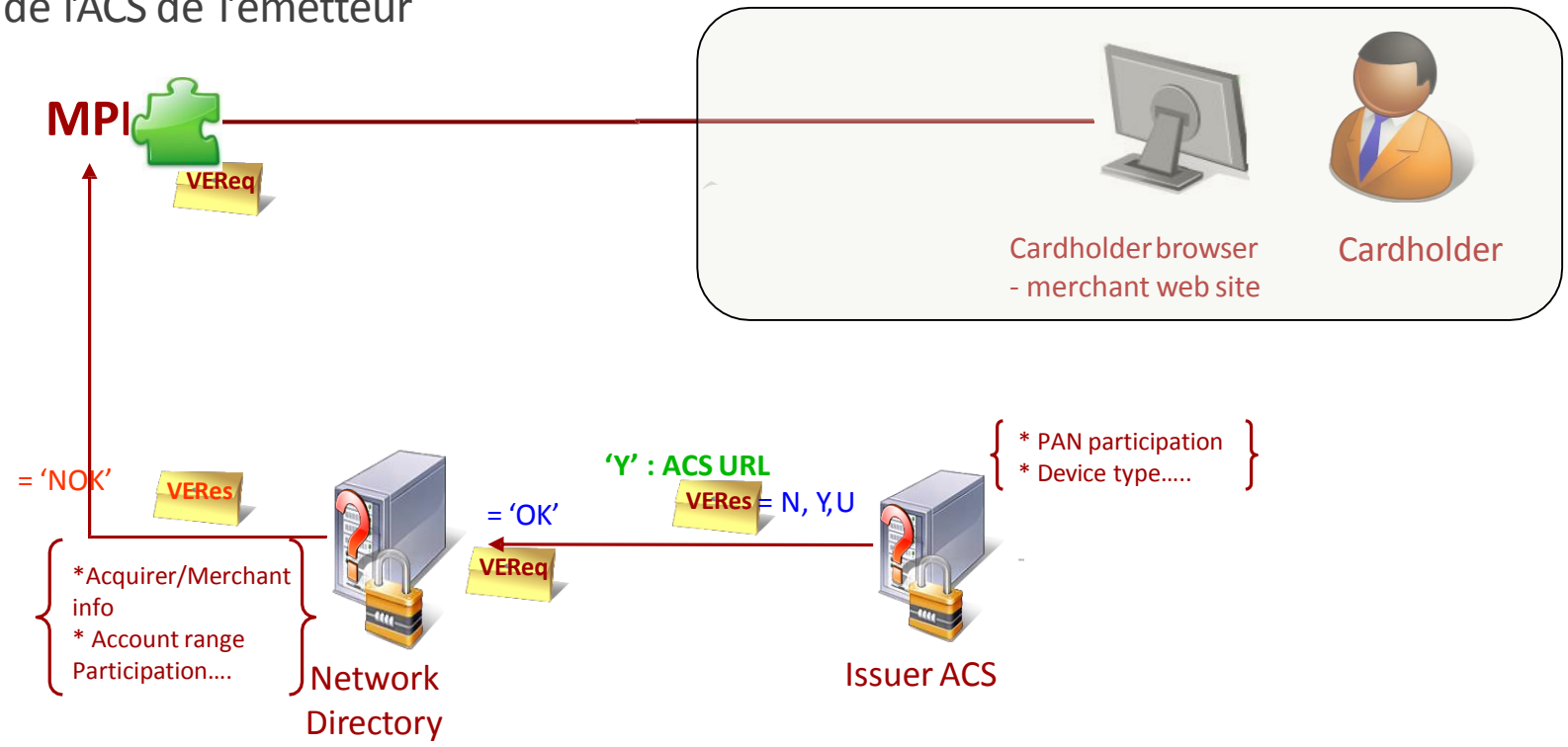
- **3D-secure messages (3/4)**
  - Messages de Chargement de tranches de cartes:
    - **CRReq (Card Range Request)**
      - Envoyé par le Merchant Server Plug-in (MPI) au Directory Server pour demander la liste des tranches de cartes participants afin de mettre à jour le cache interne du MPI
    - **CRRes (Card Range Response)**
      - Envoyé par le Directory Server au Merchant Server Plug-in (MPI) en réponse au message CRReq

Description et format des messages

- **3D-secure messages (4/4)**
  - Messages d'erreur:
    - *''Un message d'erreur doit être retourné si la requête reçue ou la réponse ne pourrait réussir au niveau du protocol''* Definition du 3D-secure Protocol Specification core Functions
    - Les messages d'erreur peuvent être:
      - Envoyés par DS au MPI si le DS reçoit un message CRReq invalide
      - Envoyés par DS au MPI si le DS reçoit un message VEReq invalide
      - Envoyés par ACS au MPI si l'ACS reçoit un message PAReq invalide

Description et format des messages

- **Messages 3D-secure MPI➔ Network Directory**
  - Requête de verification du PAN: **VEReq (1/3)**
    - Utilisé par le MPI pour vérifier que la carte est enrôlée 3D Secure
    - Prend l'URL de l'ACS de l'émetteur



Description et format des messages

- **Messages 3D-secure MPI➔ Network Directory**
  - Requête de verification du PAN: **VEReq (3/3)**
    - Exemple:

<?xml version="1.0" encoding="UTF-8"?>

<ThreeDSecure> <Message id="hps272919531109">

<VEReq><version>1.0.2</version><pan>5434298991100236</pan>

<Merchant>**<acqBIN>543238</acqBIN><merID>0011112223</merID><password>ao88Z9JK</password>**

</Merchant>

……

</VEReq>

</Message></ThreeDSecure>

Description et format des messages

- **Messages 3D-secure MPI➔ Network Directory**
  - Résultat de verification du PAN: **VERes**
    - Exemple:

<ThreeDSecure><Message id="hps-272919531109">

<VERes>

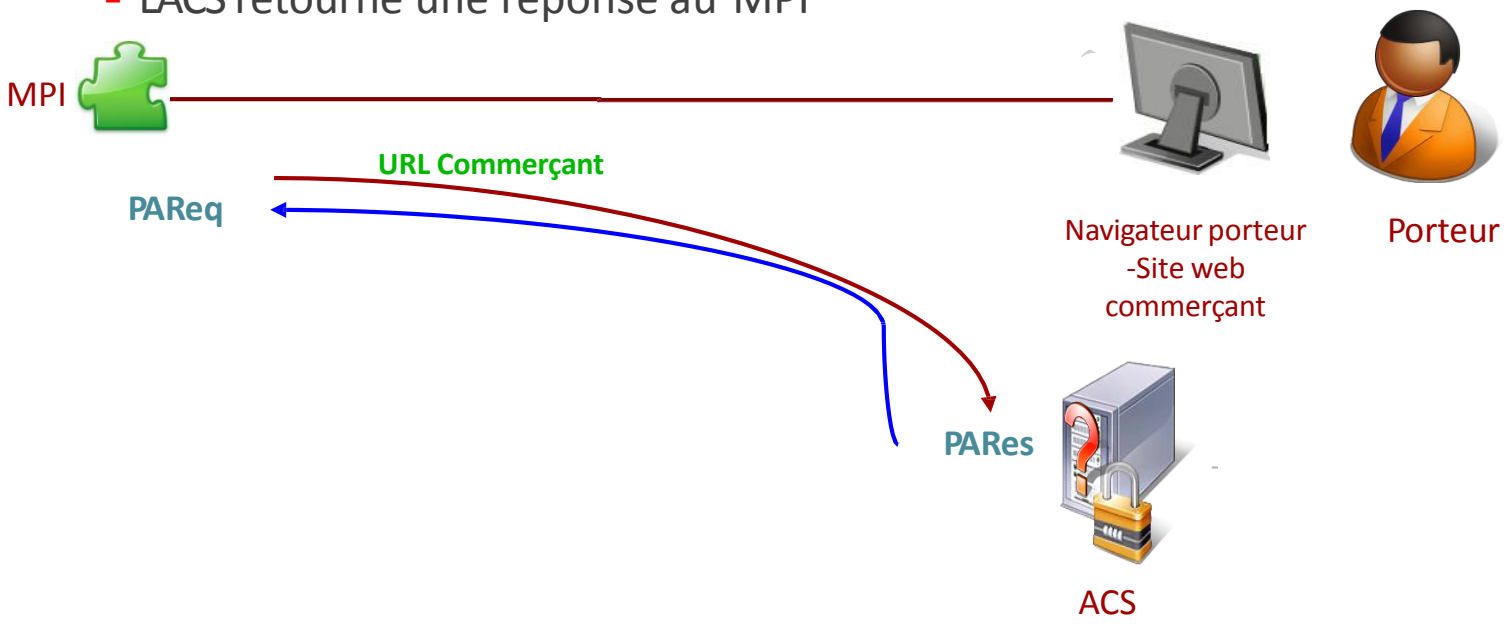
<version>1.0.2</version><CH><enrolled>**Y**</enrolled><acctID>4340338509381327</acctID></CH><url>https://www.securesuite.co.uk/hbos/tdsecure/pa.jsp?partner=halifax_mc&VAA=B</url><protocol>ThreeDSecure</protocol>

</VERes>

</Message></ThreeDSecure>

Description et format des messages

- **Messages 3D-secure MPI➔ ACS**
  - Résultat de l'authentification du PAN : **PAReq (1/3)**
    - Le MPI envoie une requête à travers le navigateur du porteur à l'ACS afin de collecter les données d'authentification
    - L'ACS authentifie le porteur selon la méthode d'enrôlement prédéfinie
    - L'ACS retourne une réponse au MPI



Description et format des messages

- **Messages 3D-secure MPI➔ ACS**
  - Résultat de l'authentification du PAN: **PAReq (3/3)**
    - Exemple:

<ThreeDSecure><Message id="PA8210010317343">

<PAReq><version>1.0.2</version>
<Merchant><acqBIN>457939</acqBIN><merID>0127214123</merID><name>COQMANAGEMENT</name><country>196</country><url>https://www.bains.com</url>**</Merchant>**

<Purchase><xid>AgAACAAHAggAAQADAQcDBAMEJTk=</xid><date>2011072722:02:11</date><amount>50.00</amount><purchAmount>000000005000</purchAmount><currency>840</currency><exponent>2</exponent>**</Purchase>**

<CH><acctID>BQEBqAbn3b2cXl51e30rZ2h5c4Y=</acctID><expiry>0912</expiry>**</CH>**

</PAReq>

</Message> </ThreeDSecure>

Description et format des messages

- **Messages 3D-secure MPI➔ ACS**
  - Réponse de l'authentification du PAN: **PARes**

<ThreeDSecure> <Message id="PA8210010317343">

<PARes id="PARes1217195908-492495"><version>1.0.2</version>

<Merchant><acqBIN>457939</acqBIN><merID>0127214123</merID> **</Merchant>**

<Purchase><xid>AgAACAAHAggAAQADAQcDBAMEJTk=</xid> <date>2008072722:02:11</date>
<purchAmount>000000005000 </purchAmount><currency>840</currency><exponent>2</exponent>

</Purchase>

<pan>0000000000007408</pan>

<TX><time>20080727 21:58:28</time><status>N</status>
<cavv>BwAQCDmQgAUFByeAQ5CAEEVcR7M=</cavv><eci>06</eci><ca
vvAlgorithm>1</cavvAlgorithm>**</TX>**

</PARes>

Description et format des messages

- **Messages 3D-secure**
  - Messages d’erreur (2/3)
    - Exemple 1:

<ThreeDSecure> <Message id="hps-75998556787">

<Error><version>1.0.2</version><errorCode>51</errorCode> <errorMessage> Merchant not participating</errorMessage>

<errorDetail>null</errorDetail>

</Error>

</Message></ThreeDSecure>

Description et format des messages

- **Messages 3D-secure**
  - Messages d’erreur (2/3)
    - Exemple 2:

<ThreeDSecure> <Message id="hps-517229021582">

<Error><version>1.0.2</version><errorCode>5</errorCode> <errorMessage> Format of one or more elements is invalid according to the specification.

</errorMessage>

<errorDetail>Message.id</errorDetail>

<vendorCode>VERes.id not matching VEReq.id.</vendorCode>

</Error>

</Message></ThreeDSecure>

Description et format des messages

- **Messages 3D-secure**
  - Messages d’erreur (2/3)
    - Exemple 2:

<ThreeDSecure> <Message id="hps-517229021582">

<Error><version>1.0.2</version><errorCode>5</errorCode> <errorMessage> Format of one or more elements is invalid according to the specification.

</errorMessage>

<errorDetail>Message.id</errorDetail>

<vendorCode>VERes.id not matching VEReq.id.</vendorCode>

</Error>

</Message></ThreeDSecure>

Description et format des messages

- **Messages 3D-secure MPI→ Network Directory**
  - Vérification de la tranche participative **CRReq (1/2)**
    - C'est un chargement global de tranche
    - Ne doit être fait avant 8h ni après 24h
    - Ne doit être fait à un moment fixe
    - Vise à mettre à jour le cache du MPI avec la liste des tranches de cartes participant aux 3D-Secure

Description et format des messages

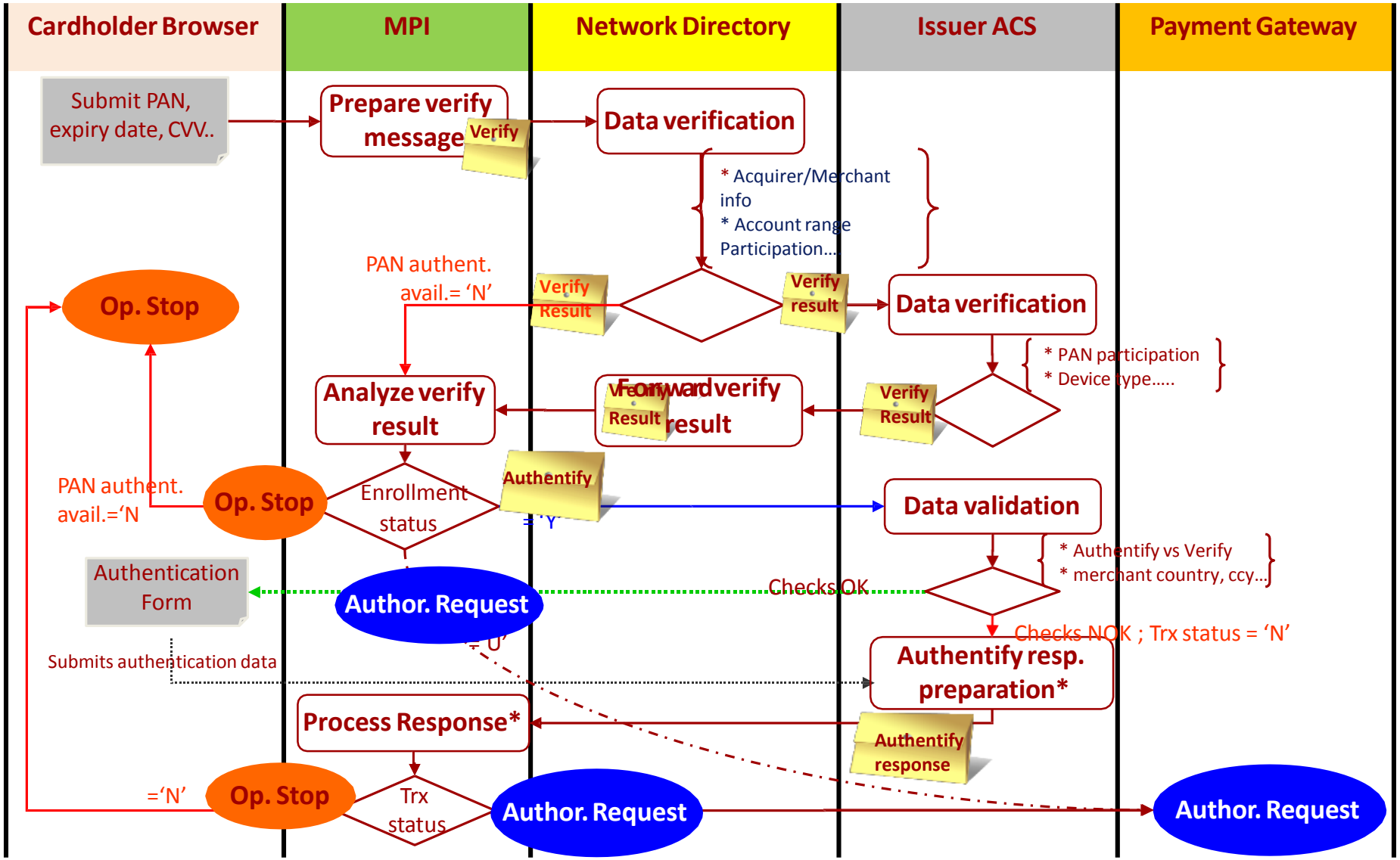
- **Messages 3D-secure MPI→ Network Directory**
  - Vérification de la tranche participative **CRReq (2/2)**
    - C'est un chargement global de tranche
    - Ne doit être fait avant 8h ni après 24h
    - Ne doit être fait à un moment fixe
    - Vise à mettre à jour le cache du MPI avec la liste des tranches de cartes qui participant aux 3D-Secure

Sommaire

Vos attentes par rapport à ce cours

- **Discussion : Vos attentes ont-elles été satisfaites ?**

Annexe


Cardholder Browser
MPI
Network Directory
Issuer ACS
Payment Gateway
Submit PAN, expiry date, CVV..
Prepare verify message
Verify
Data verification
* Acquirer/Merchant info
* Account range Participation...
PAN authent. avail.= 'N'
Verify Result
Verify result
Data verification
* PAN participation
* Device type.....
Op. Stop
Analyze verify result
Forward verify result
Verify Result
Verify Result
PAN authent. avail.='N
Op. Stop
Enrollment status
Authentify
= 'Y'
Data validation
* Authentify vs Verify
* merchant country, ccy...
Authentication Form
Author. Request
Checks OK
Checks NOK ; Trx status = 'N'
= 'U'
Submits authentication data
Authentify resp. preparation*
Process Response*
Authentify response
='N'
Op. Stop
Trx status
Author. Request
Author. Request