Tema 6
e-Commerce

SW Corporativo

Curso 2018-19

Objetivos del Tema 6

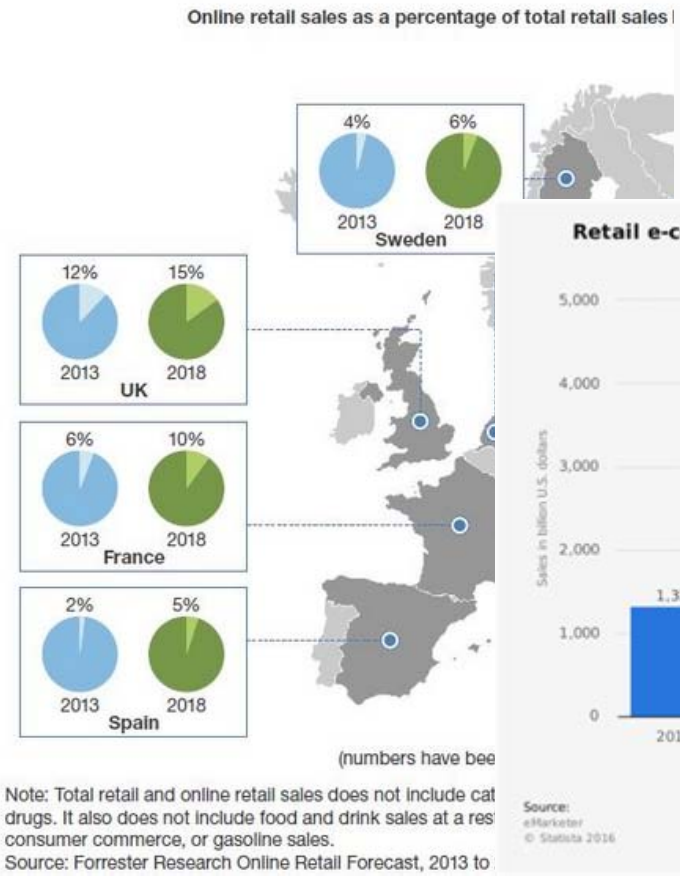
- Conocer los conceptos básicos en torno al e-Commerce, especialmente en el contexto de la Seguridad que requieren este tipo de transacciones.

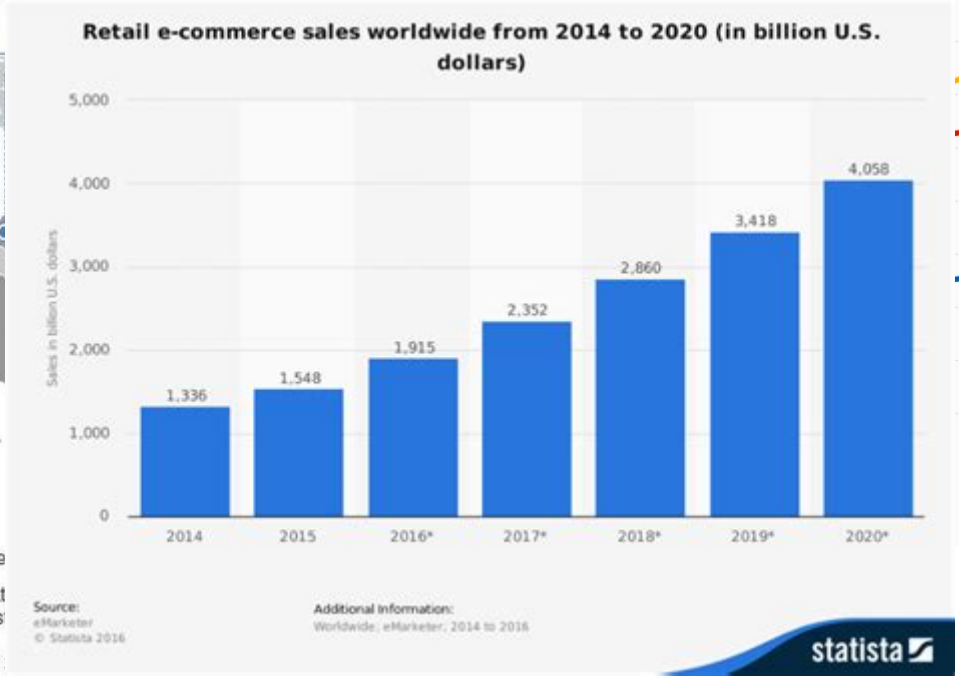
- Entender de importancia de e-Commerce dentro de los procesos operativos de la Empresa.

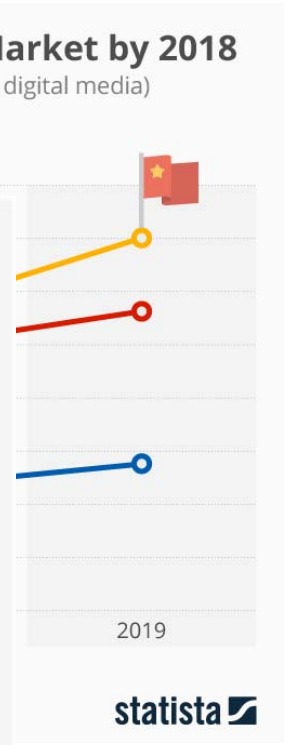
- Relación con el Canal de Ventas e importancia respecto al CRM (Ventas)

Compra on-line

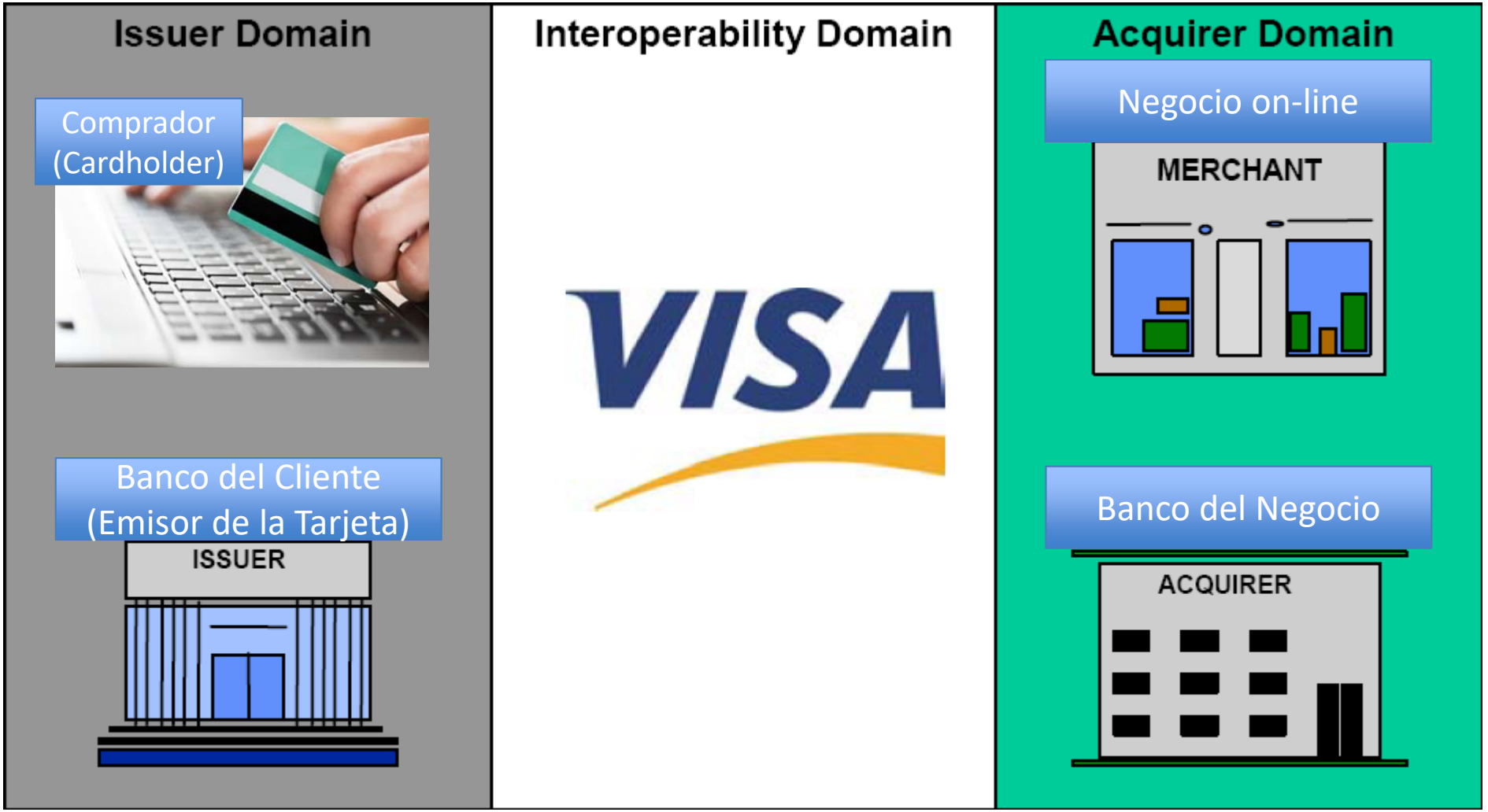
Figure 2 Forecast: European Online Channel Share By Country, 2013 And 2018 (EU-7)



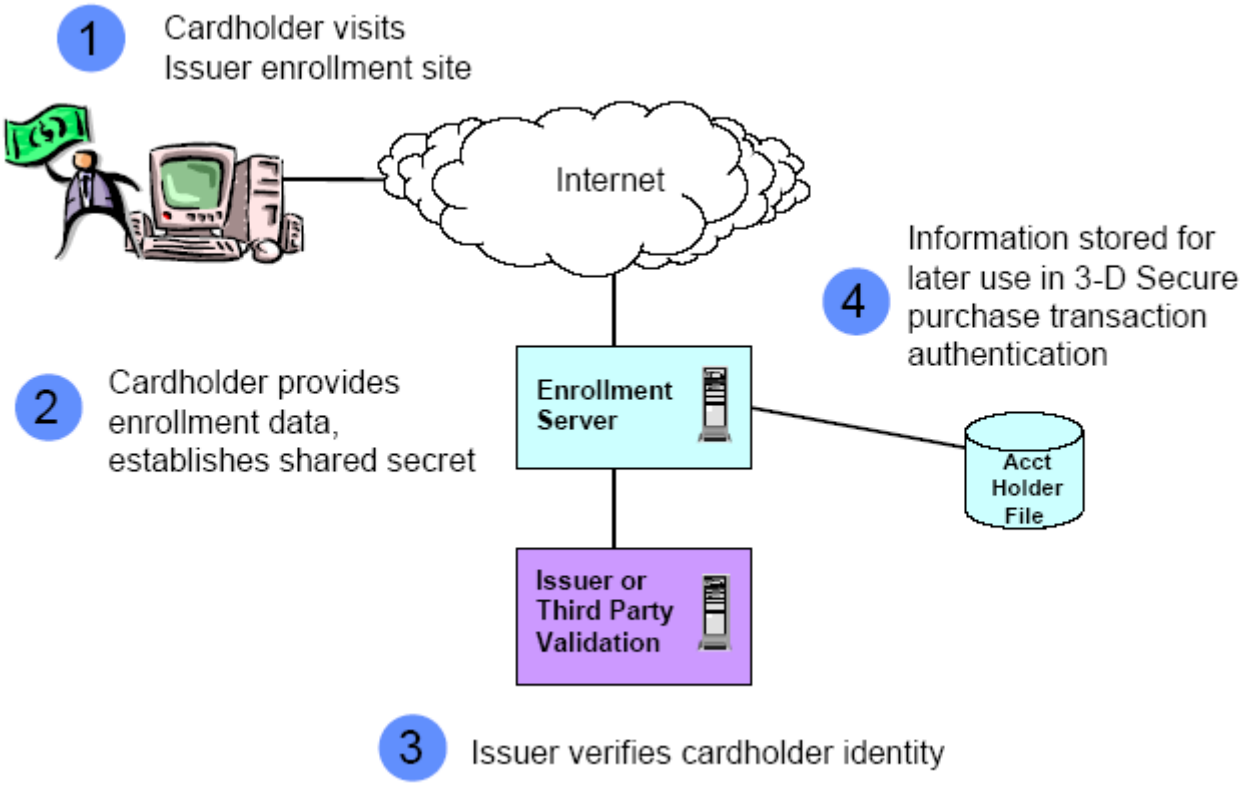




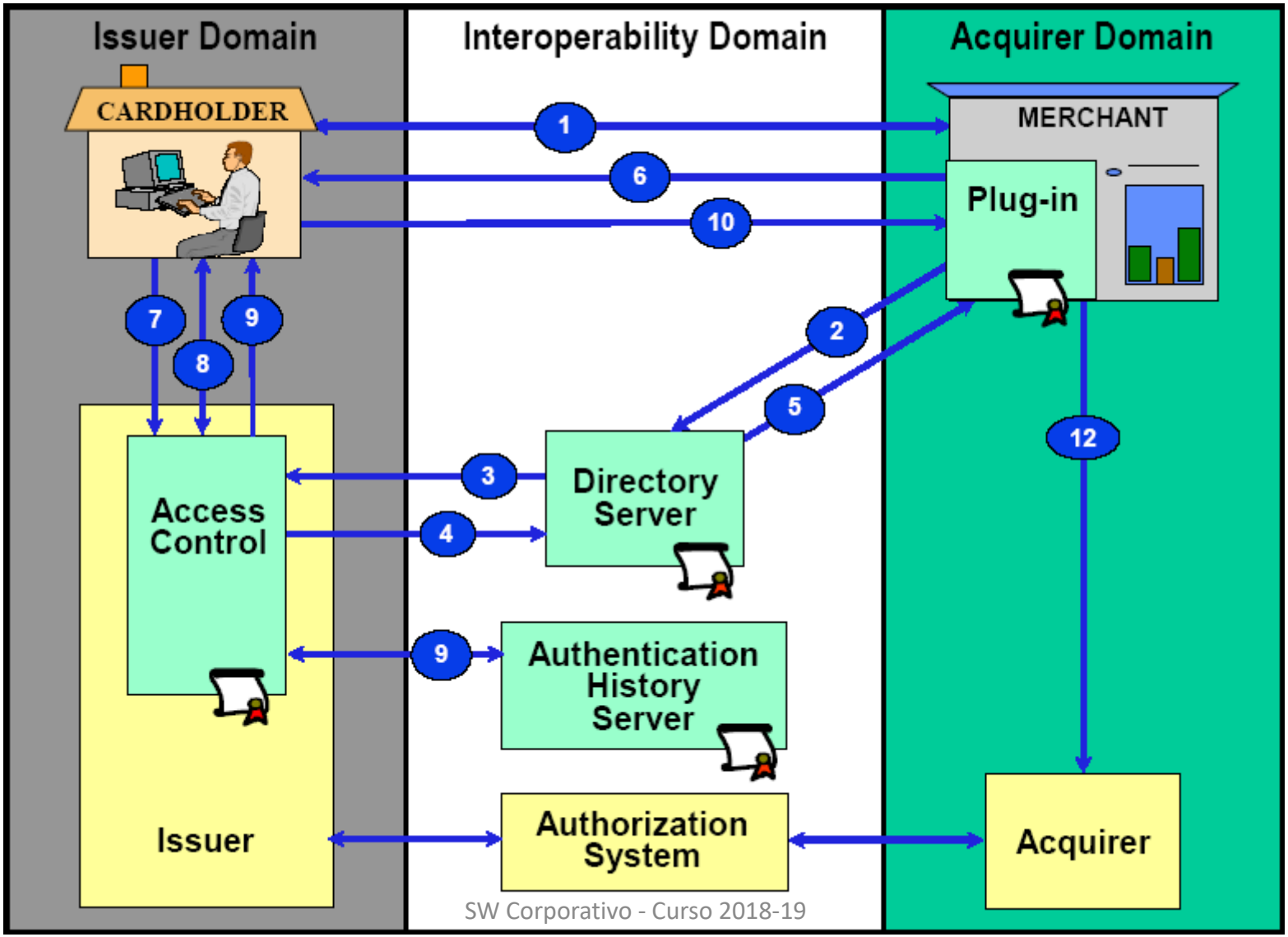
Modelo de los 3-D..ominios



Proceso de Registro del Usuario/Comprador



Flujo de Mensajes y Arquitectura de la Transacción de la Compra

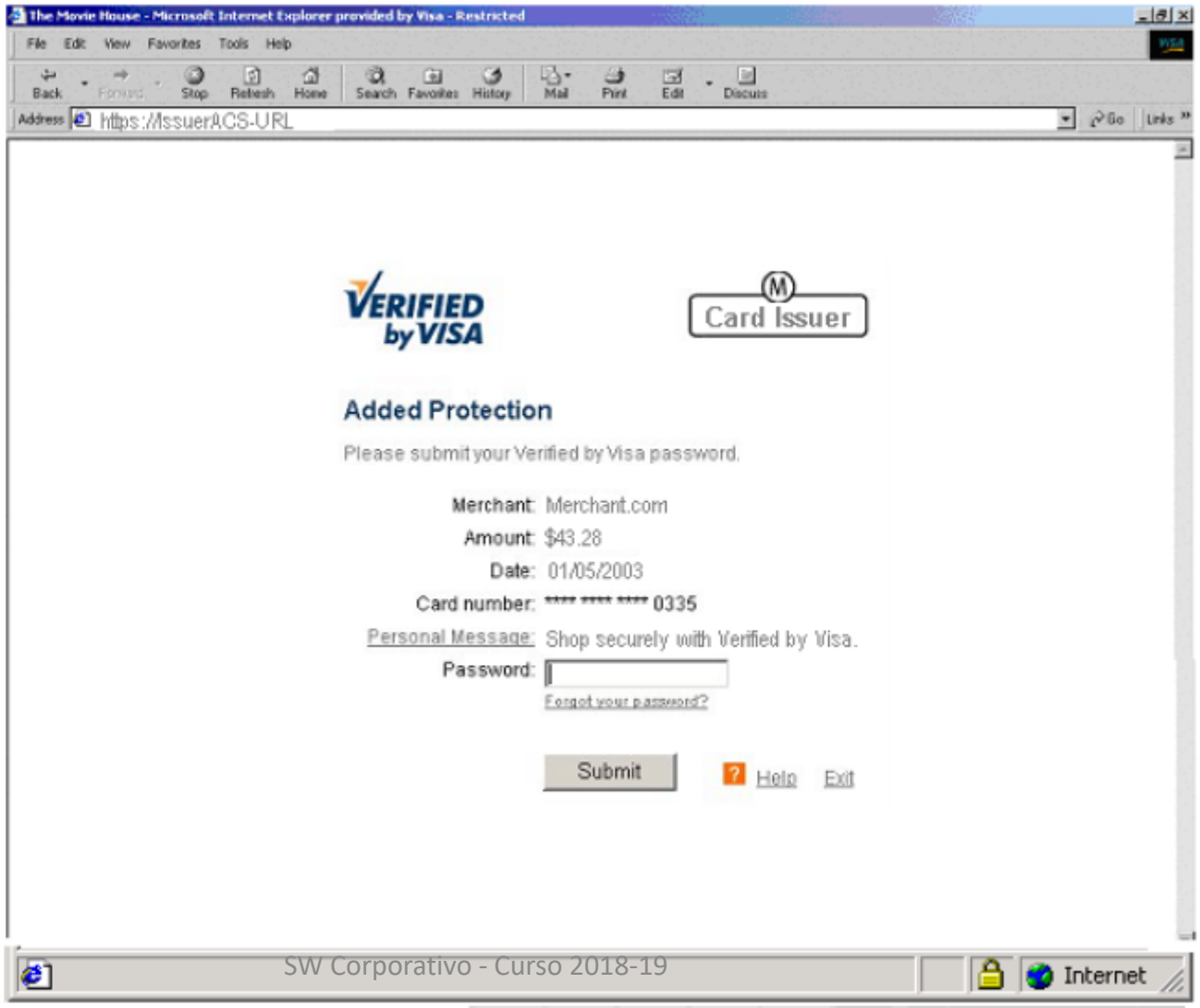


Step 1	Shopper browses at merchant site, adds items to shopping cart, then finalizes purchase. (Note: Merchant now has all necessary data, including PAN and user device information.)
Step 2	Merchant Server Plug-in (MPI) sends PAN (and user device information, if applicable) to Directory Server.
Step 3	Directory Server queries appropriate Access Control Server (ACS) to determine whether authentication (or proof of authentication attempt) is available for the PAN and device type. (If no appropriate ACS is available, the Directory Server creates a response for the MPI and processing continues with Step 5.)
Step 4	ACS responds to Directory Server.
Step 5	Directory Server forwards ACS response (or its own) to MPI. If neither authentication nor proof of authentication attempt is available, 3-D Secure processing ends, and the merchant, acquirer, or payment processor may submit a traditional authorization request, if appropriate.
Step 6	MPI sends Payer Authentication Request[2] to ACS via shopper's device.
Step 7	ACS receives Payer Authentication Request.

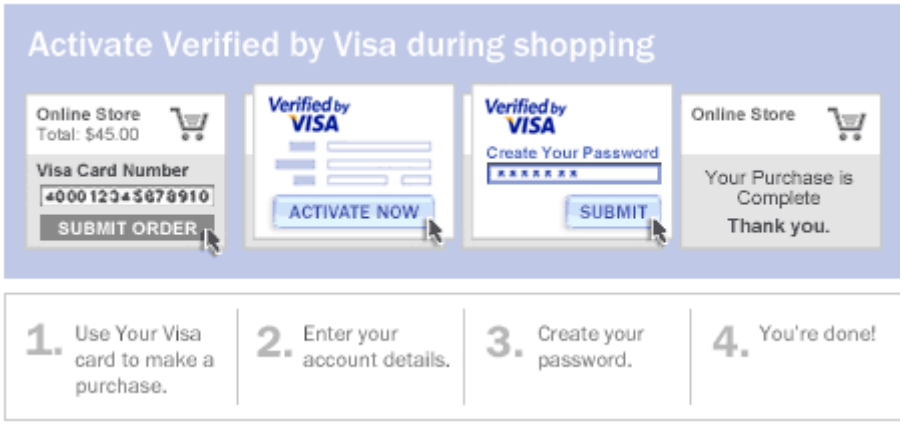
Step 8	ACS authenticates shopper using processes applicable to PAN (password, chip, PIN, etc.). Alternatively, ACS may produce a proof of authentication attempt. ACS then formats Payer Authentication Response[3] message with appropriate values and signs it.
Step 9	ACS returns Payer Authentication Response to MPI via shopper's device. ACS sends selected data to Authentication History Server.
Step 10	MPI receives Payer Authentication Response.
Step 11	MPI validates Payer Authentication Response signature (either by performing the validation itself or by passing the message to a separate Validation Server).
Step 12	Merchant proceeds with authorization exchange with its acquirer.
	Following Step 12, acquirer processes authorization with issuer via an authorization system such as VisaNet, then returns the results to merchant.

Autenticación del comprador contra el ACS

Access Control Server – authenticate shopper

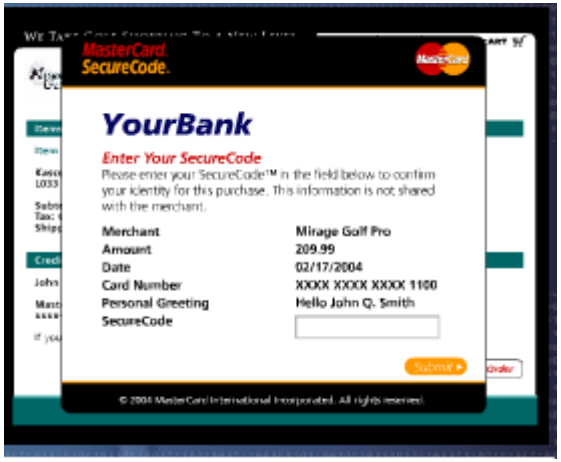


Verified by **Visa**

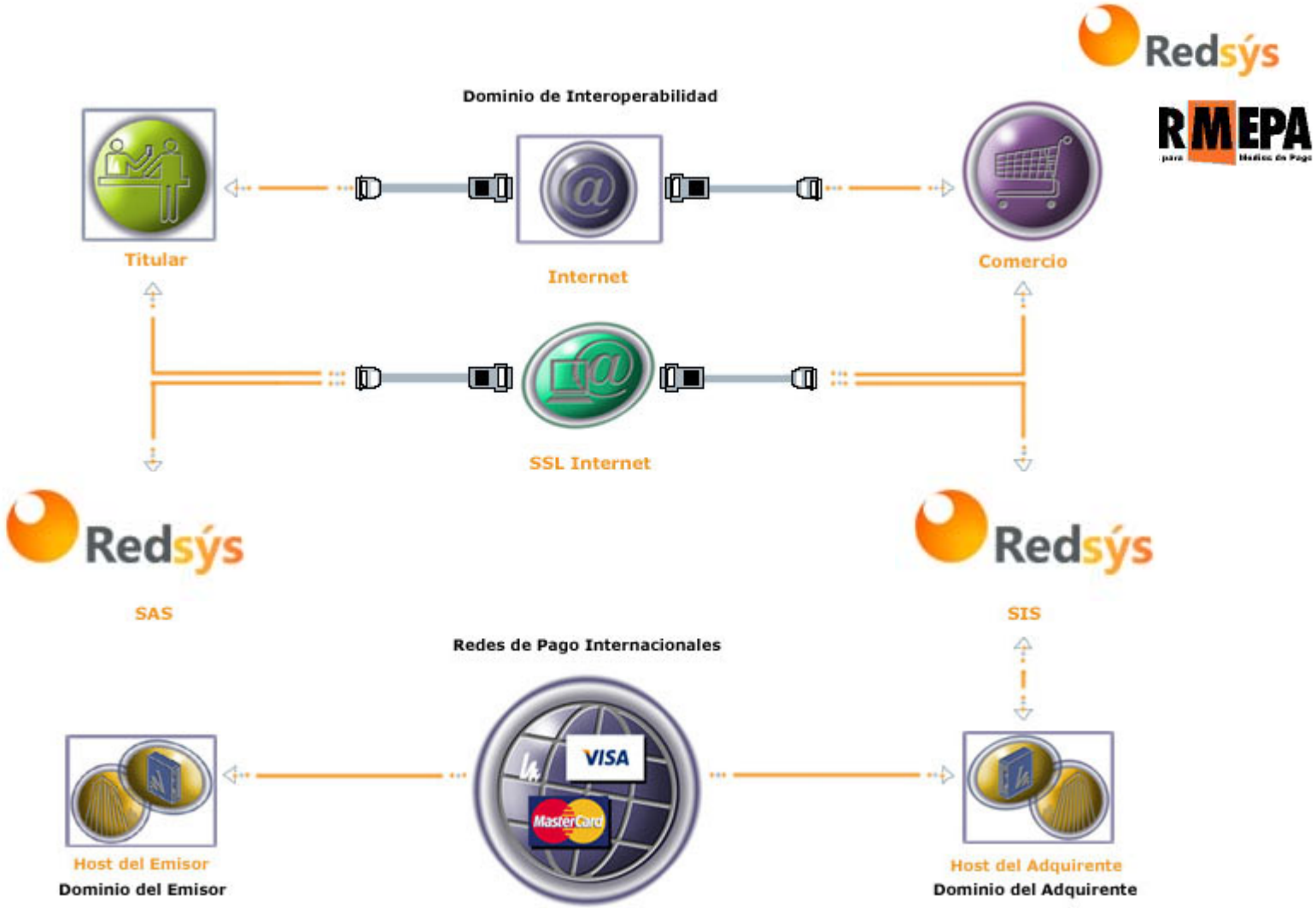


Master Card Secure Code

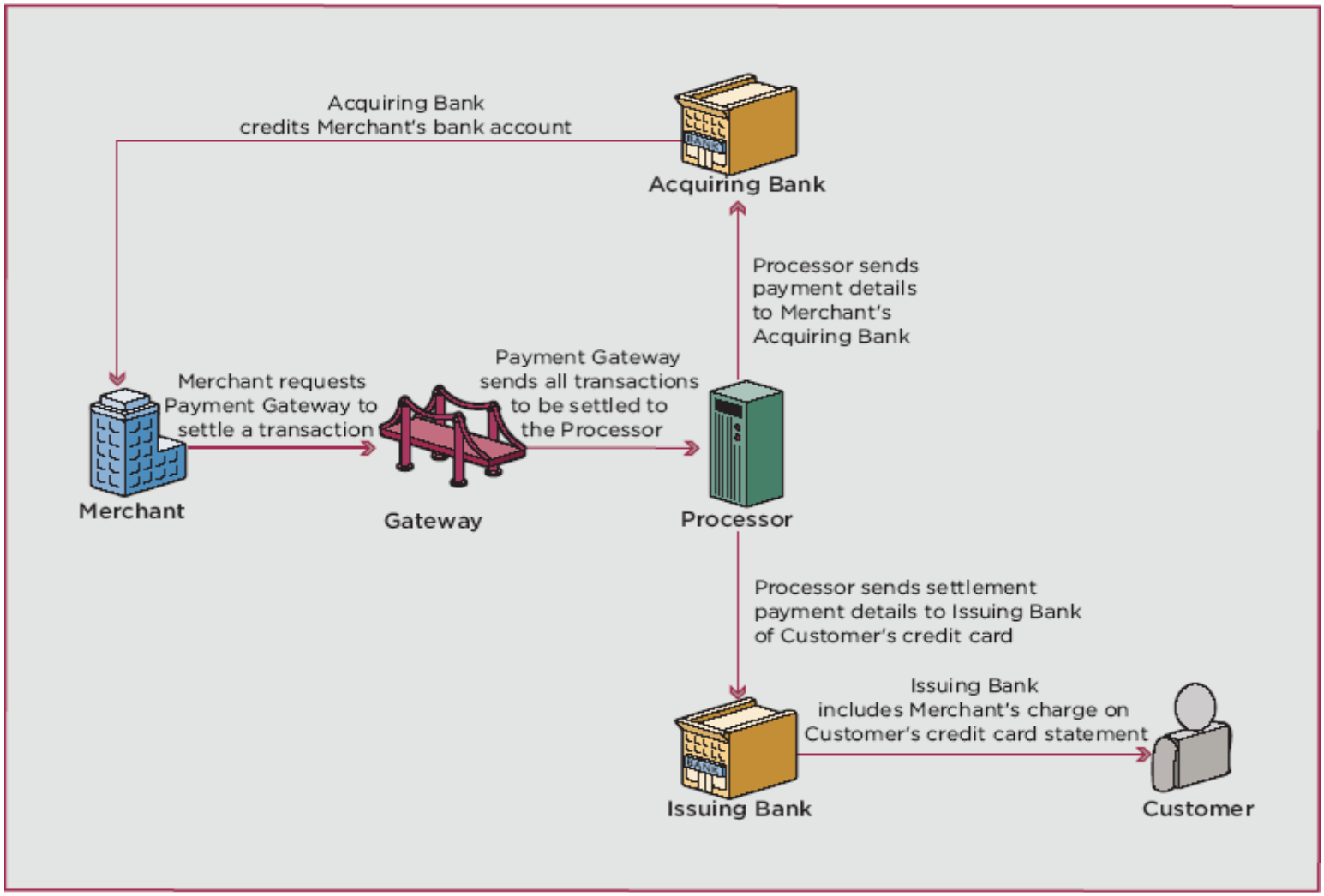
MasterCard SecureCode®
Protects Online
Transactions



Servicios de Medios de Pago



Pasarelas de Pago



Pasarelas de Pago On-line

amazon pay

offsite plataformas oneshot
prestashop magento
woocommerce shopify

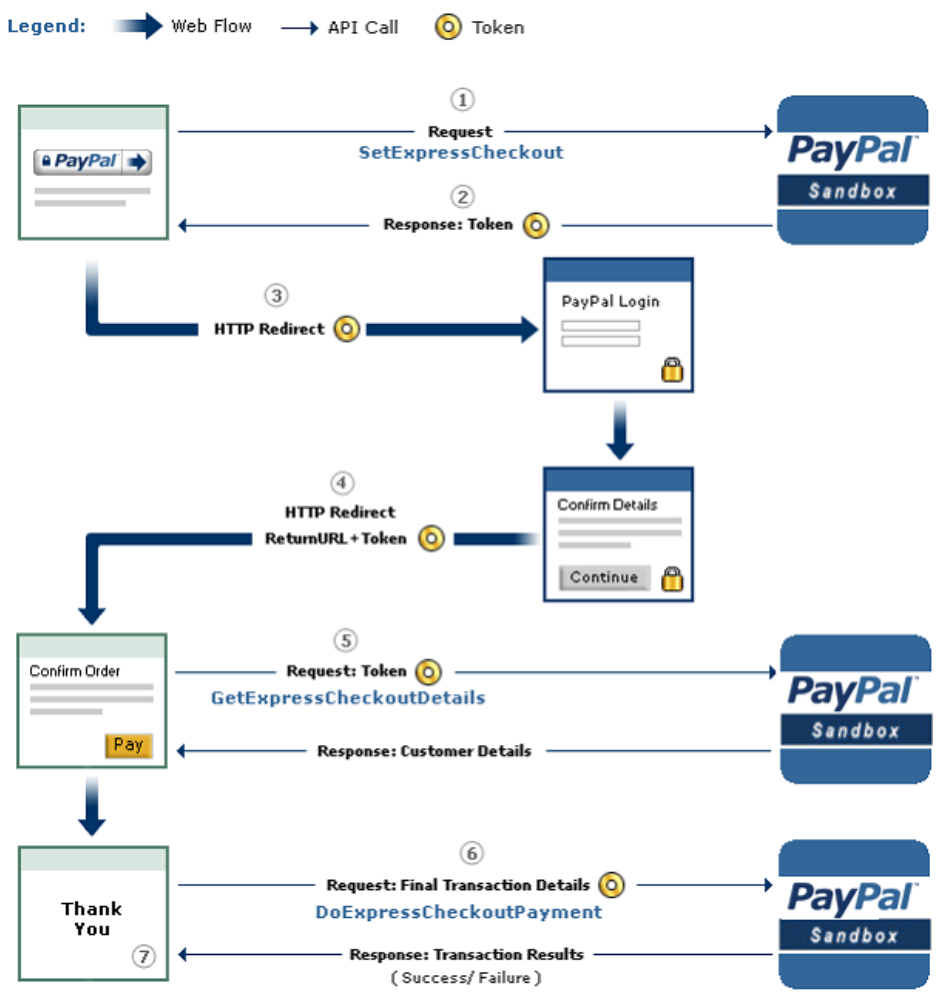
sage | pay

offsite token insite prestashop
oneshot magento woocommerce
recurring mobile

PayPal™

offsite recurring mobile
transferencias oneshot
prestashop magento
woocommerce shopify

Paypal


Legend:
Web Flow
API Call
Token
1
Request
SetExpressCheckout
PayPal
Sandbox
2
Response: Token
PayPal
3
HTTP Redirect
PayPal Login
4
HTTP Redirect
ReturnURL + Token
Confirm Details
Continue
Confirm Order
Pay
5
Request: Token
GetExpressCheckoutDetails
Response: Customer Details
PayPal
Sandbox
Thank
You
7
6
Request: Final Transaction Details
DoExpressCheckoutPayment
Response: Transaction Results
(Success/ Failure)
PayPal
Sandbox

…y otras

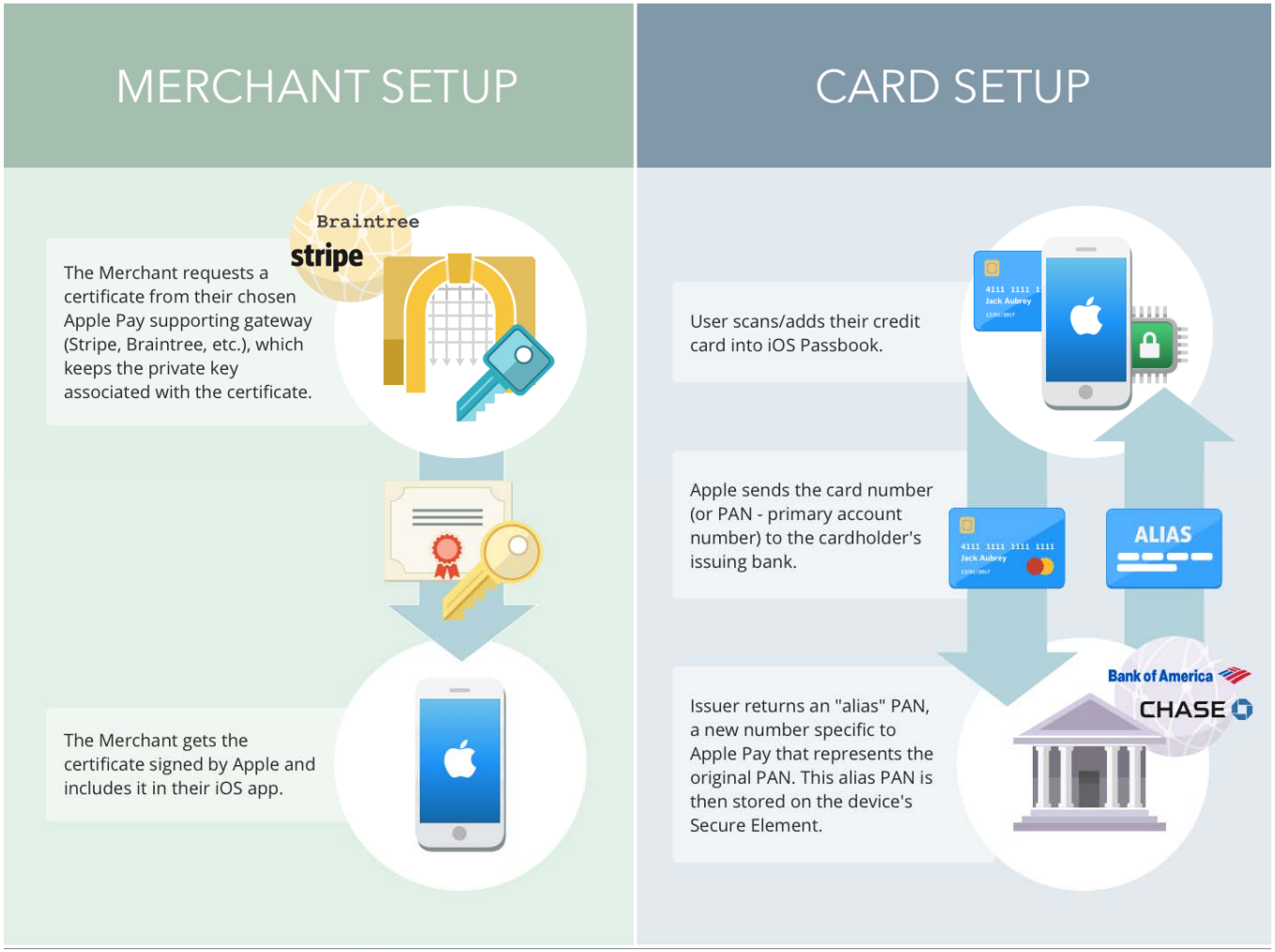
stripe

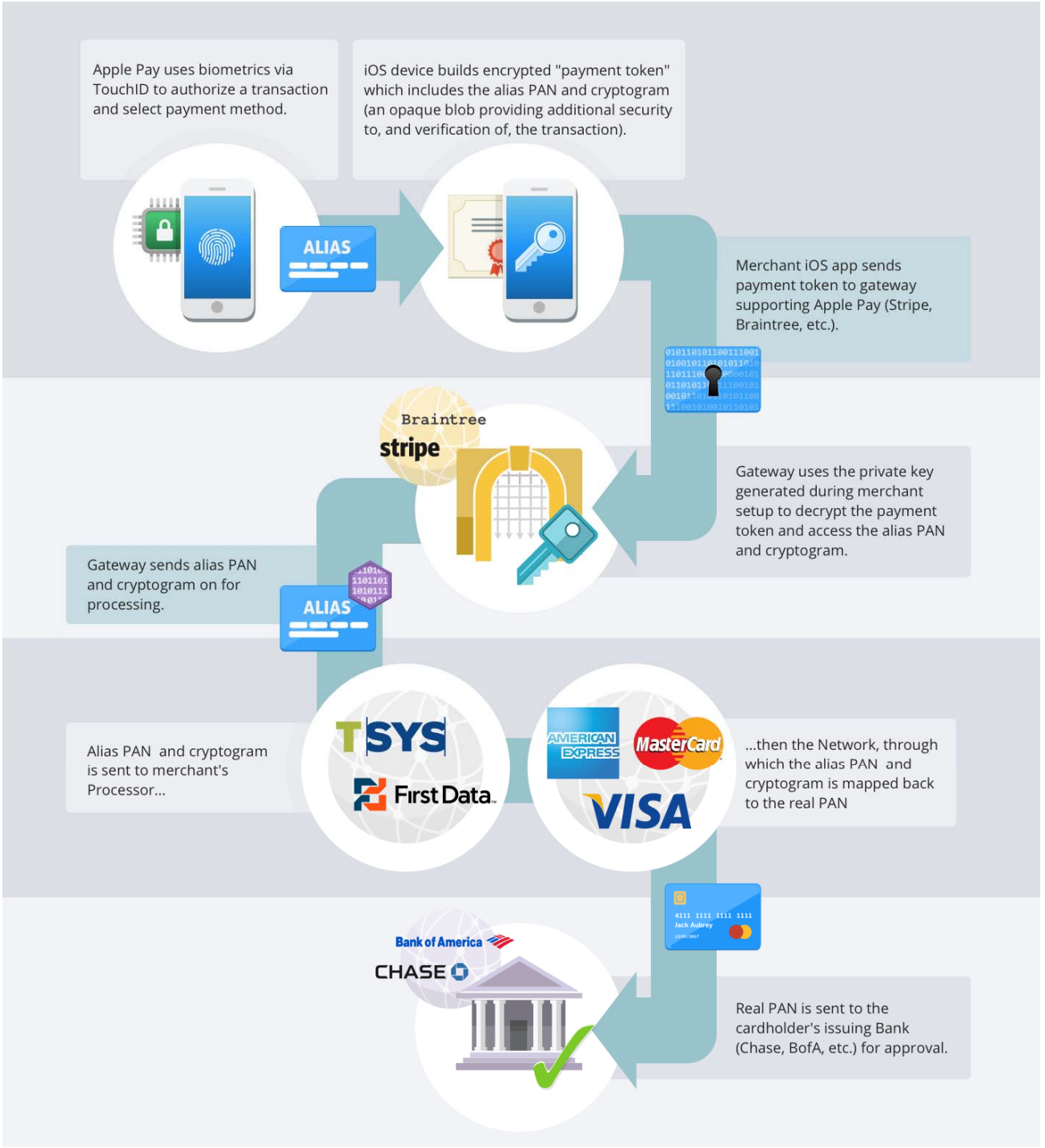
recurring insite mobile shopify
magento prestashop
woocommerce oneshot token
applepay sepa

Braintree

recurring insite mobile oneshot
saas prestashop magento,
oscommerce shopify

Cómo funciona Apple Pay?




Apple Pay uses biometrics via TouchID to authorize a transaction and select payment method.
iOS device builds encrypted "payment token" which includes the alias PAN and cryptogram (an opaque blob providing additional security to, and verification of, the transaction).
ALIAS
Merchant iOS app sends payment token to gateway supporting Apple Pay (Stripe, Braintree, etc.).
Braintree
stripe
Gateway uses the private key generated during merchant setup to decrypt the payment token and access the alias PAN and cryptogram.
Gateway sends alias PAN and cryptogram on for processing.
ALIAS
Alias PAN and cryptogram is sent to merchant's Processor...
TSYS
First Data.
AMERICAN EXPRESS
MasterCard
VISA
...then the Network, through which the alias PAN and cryptogram is mapped back to the real PAN
Bank of America
CHASE
Real PAN is sent to the cardholder's issuing Bank (Chase, BofA, etc.) for approval.

Módulos E-Commerce Populares

- Prestashop
- Magento
- WooCommerce
- OsCommerce
- OpenCart