

RANCANGAN SISTEM PEMBAYARAN OFF-LINE PADA POINT OF SALE (POS) & DI INTERNET BERBASIS SMARTCARD

Arrianto Mukti Wibowo
(*amwibowo@caplin.cs.ui.ac.id*)
Raditya Umbas
(*raditya@arjuna.csc.ui.ac.id*)

Fakultas Ilmu Komputer
Universitas Indonesia
Depok, Jawa Barat
1999

Penelitian didanai oleh Dewan Riset Nasional,
melalui program Riset Unggulan Terpadu, batch VI, 1998/199

Abstrak

Dalam dokumen ini tersaji draft rancangan suatu sistem pembayaran berbasis cek digital yang terjamin tidak kosong (cashier's check).

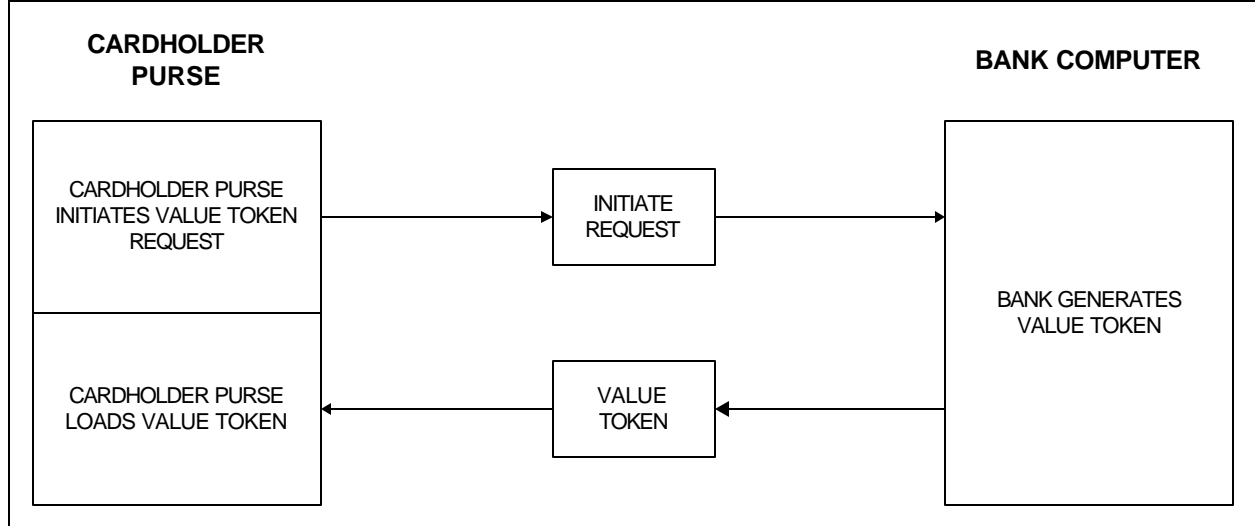
Sistem pembayaran ini berbasis smart card, sehingga dapat dipergunakan off-line, tidak terhubung dengan bank. Ini bermanfaat kalau kebetulan Point Of Sale (POS)-nya memang tidak memungkinkan terhubung secara langsung pada bank, seperti misalnya di taxi, bus atau di kapal penumpang. Namun tentu tidak menutup kemungkinan pula menggunakan sistem pembayaran off-line pada warung-warung yang tidak memiliki saluran komunikasi atau pada salesman yang berkeliling.

Selain itu sistem pembayaran ini juga bisa dipergunakan di jaringan publik yang tidak aman, seperti Internet. Protokol pembayaran dalam dokumen ini juga mencegah seseorang untuk menduplikasi cek digital-nya, sehingga mencegah *double spending*.

Daftar Isi



1. Protokol Loading Value: Mengambil uang dari rekening bank
2. Protokol Spending at POS: Membayar di POS off-line
3. Protokol Spending on the Internet: Membayar melalui Internet
4. Protokol Value Deduction: Mengurangi isi uang dalam smartcard
5. Protokol Payment Capture: Pedagang menuangkan cek digital ke bank

LOADING VALUE TOKEN



Cardholder
purse
initiates value
token request

Cardholder Purse

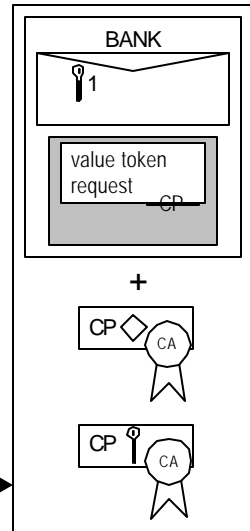
1. Cardholder unlocks the smartcard by keying in the PIN, and cardholder's software generates instruction to the cardholder purse to generate value token request.
2. Cardholder purse generates value token request with a nonce.
3. Cardholder purse digitally signs value token request by generating a message digest of the value token request and encrypting it with the cardholder purse private signature key. 
4. Cardholder purse encrypts value token request with a randomly generated symmetric key (#1). This key is then encrypted with the bank public key-exchange key. 
5. Cardholder purse transmits encrypted value token request to the bank.

value token
request

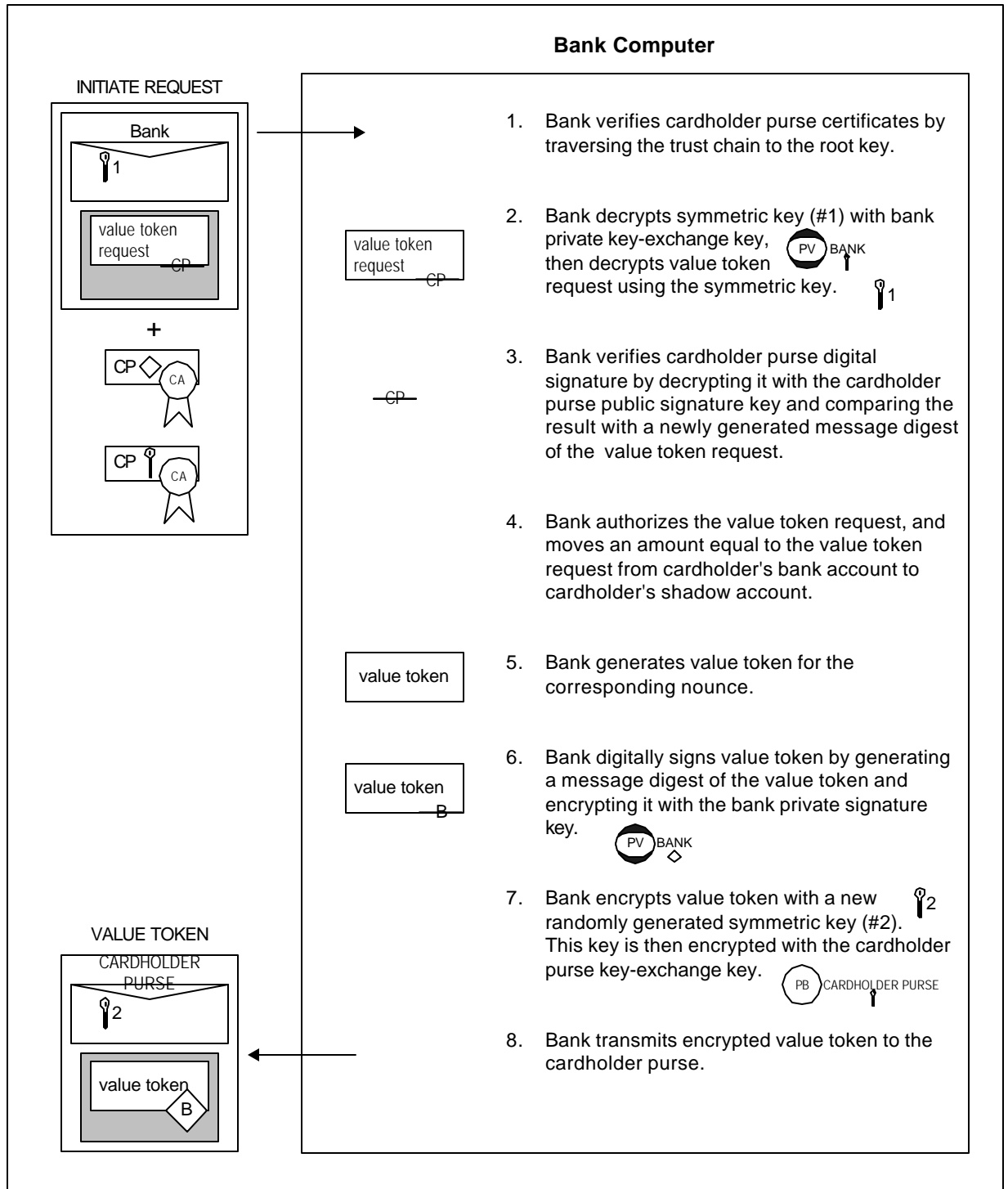
value token
request CP

value token
request CP

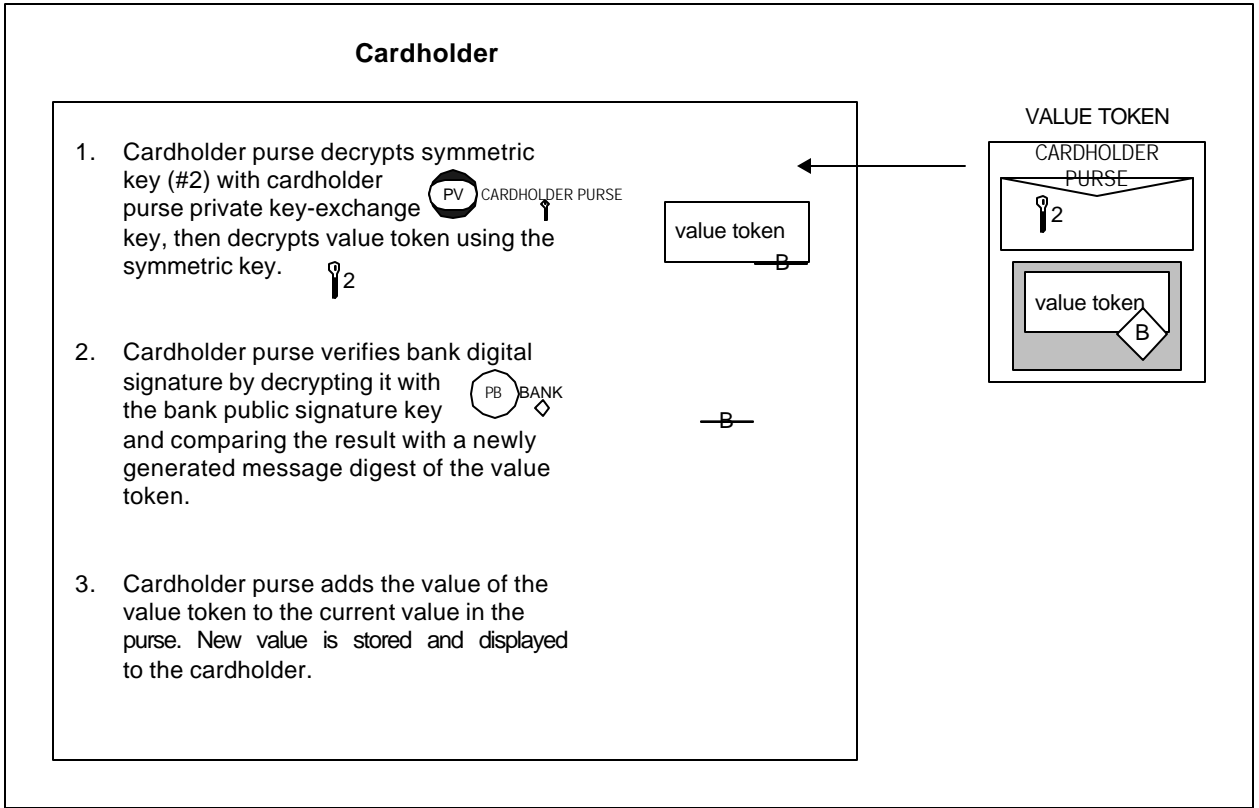
INITIATE REQUEST



**Bank:
Bank
generates
token value**



**Cardholder
purse loads
value token**



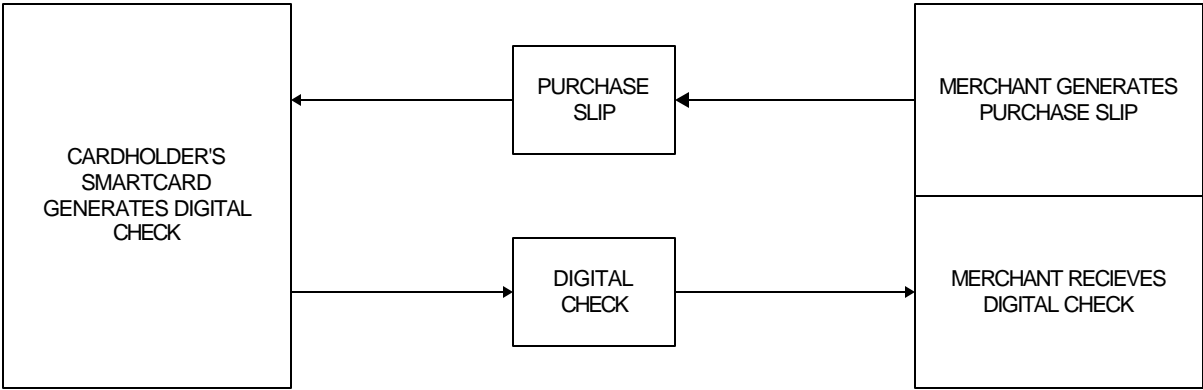
Note:

This protocol requires the smartcard to have bank certificate before the protocol begins. Even so, the protocol may be modified to exchange bank certificate in order to support multi-bank cards.

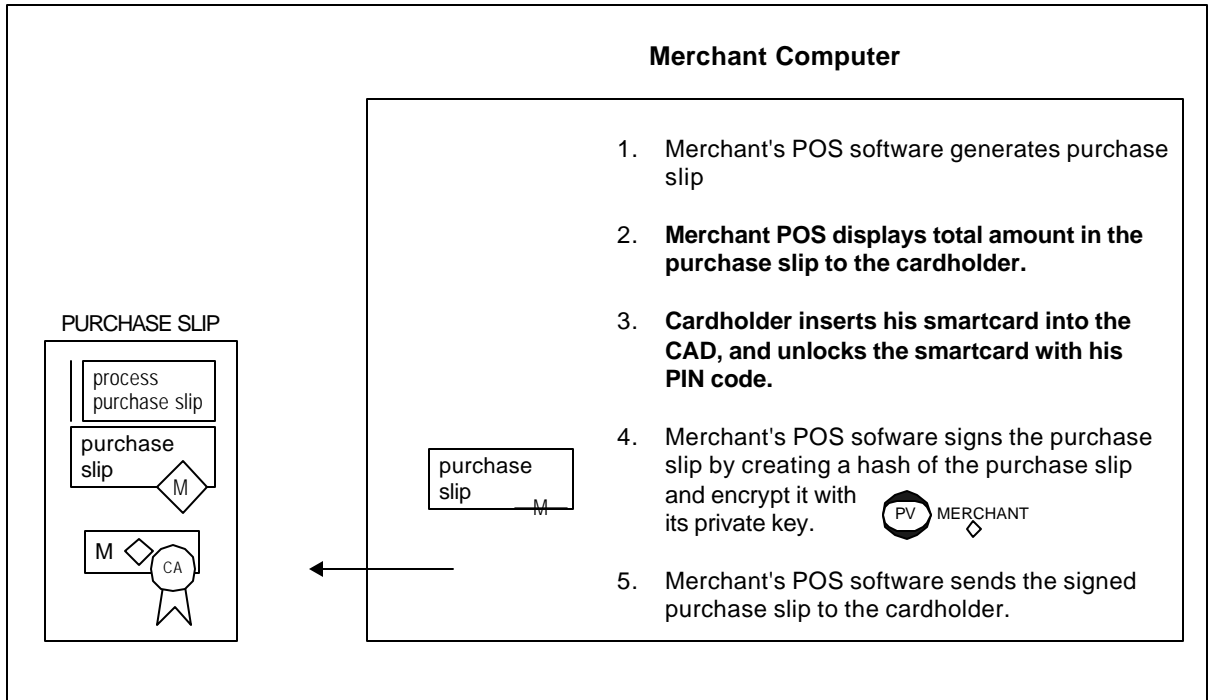
SPENDING AT POINT OF SALE

**CARDHOLDER
SMARTCARD**

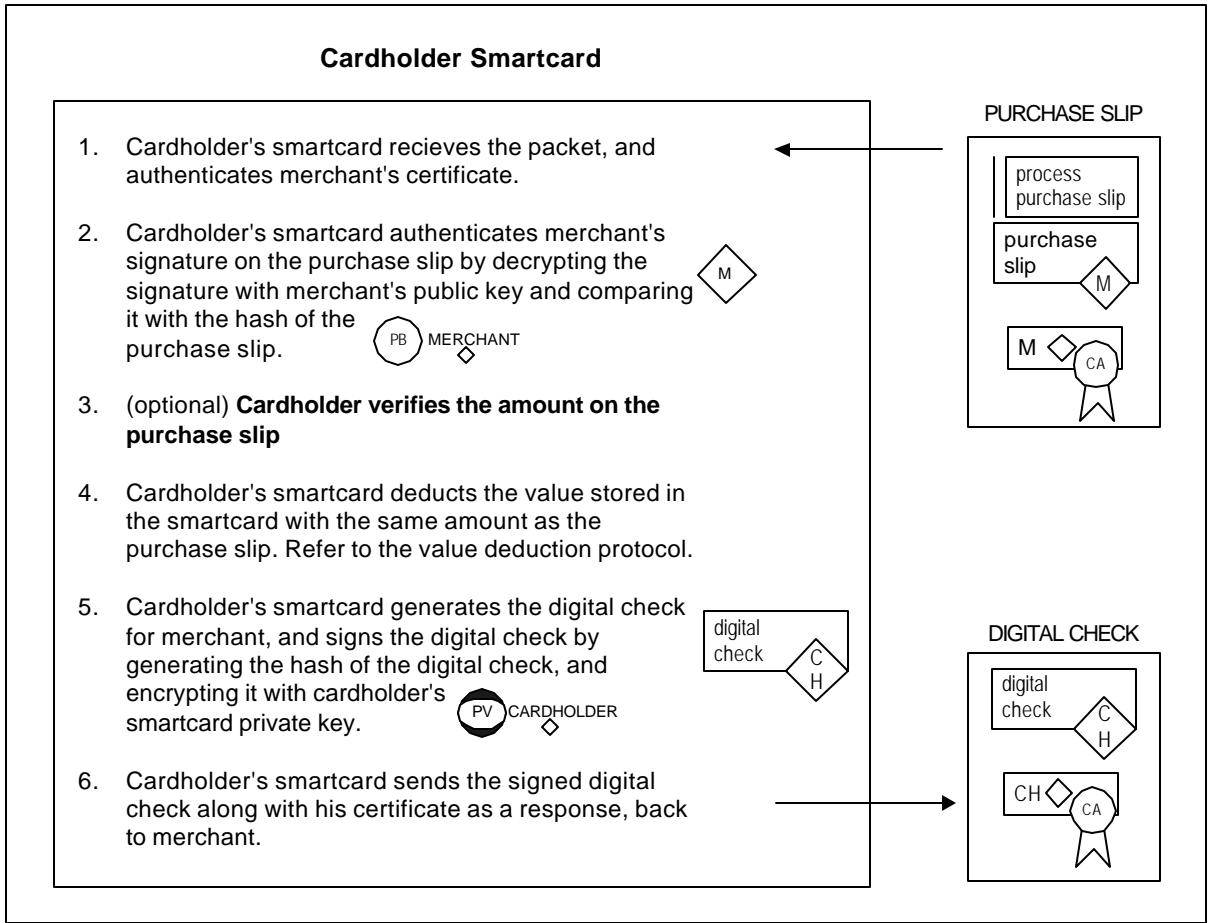
**MERCHANT
COMPUTER**



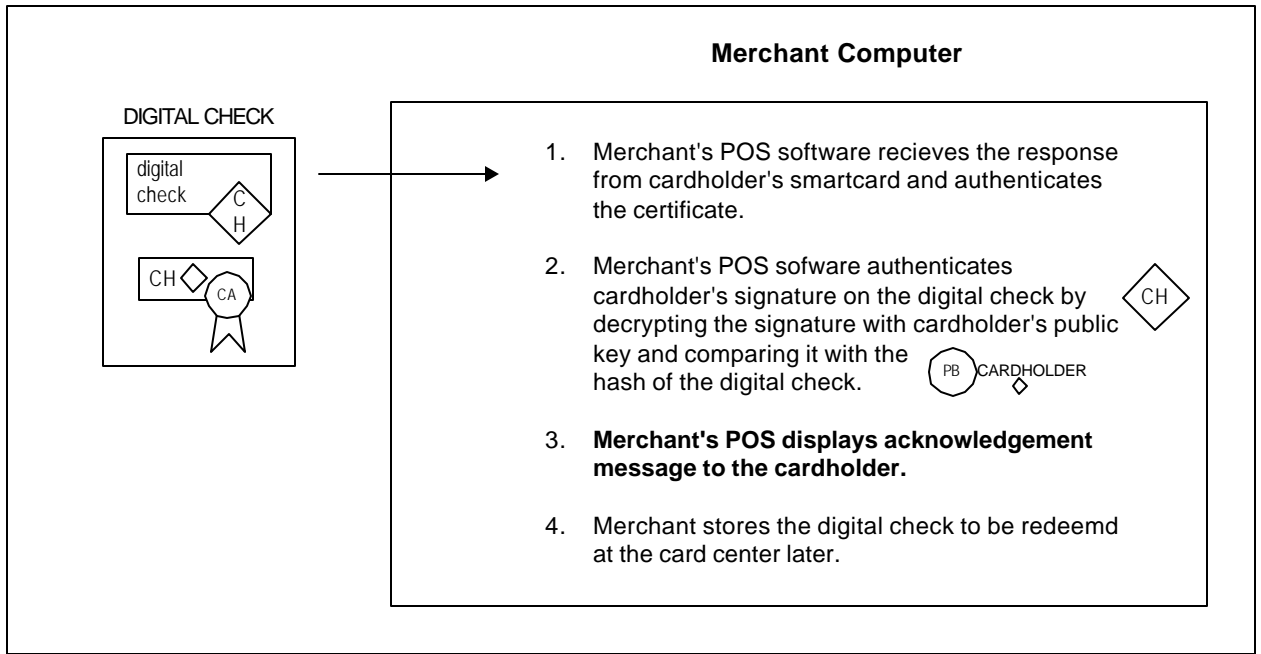
Merchant generates purchase slip



Cardholder smartcard generates digital check



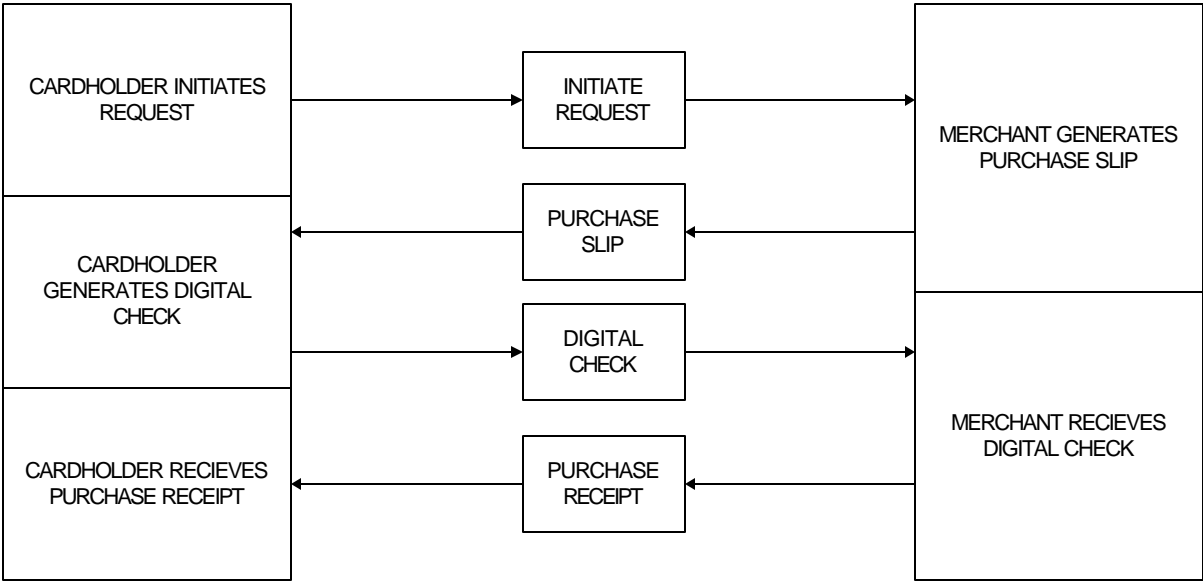
Merchant
receives
digital check



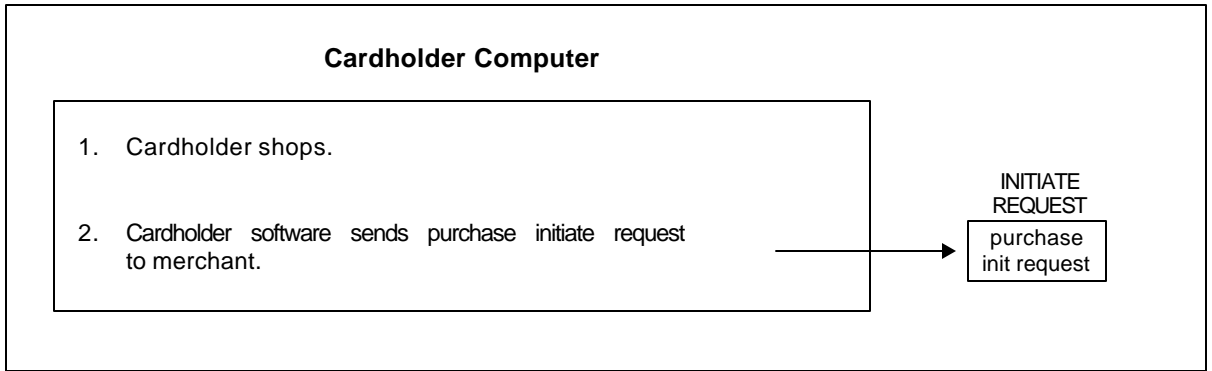
SPENDING VIA INTERNET

CARDHOLDER COMPUTER

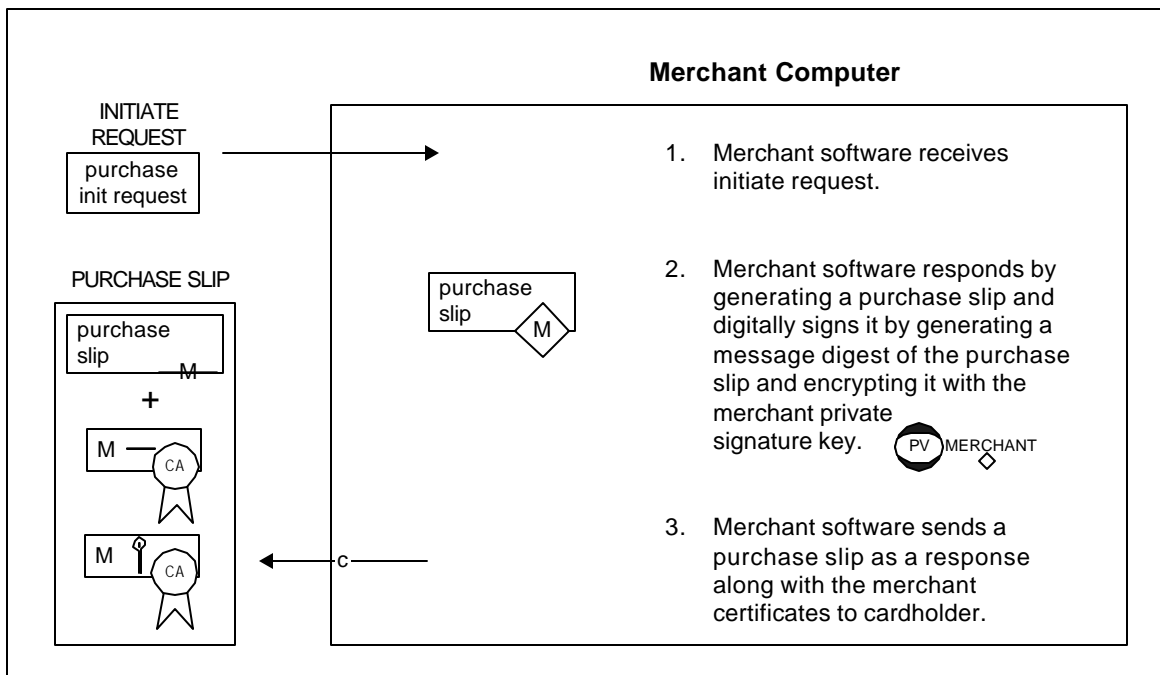
MERCHANT COMPUTER



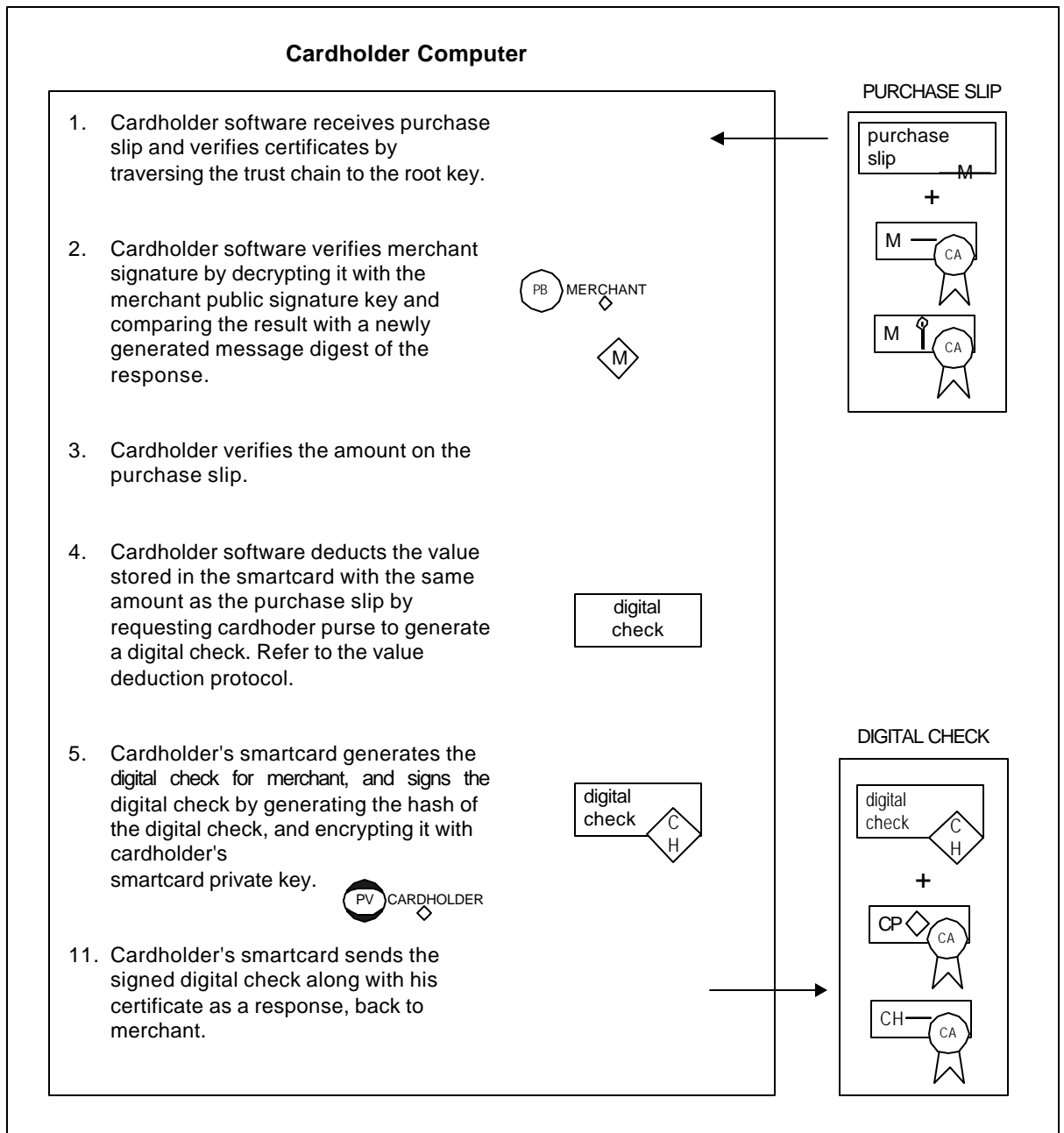
**Cardholder
initiates
purchase
request**



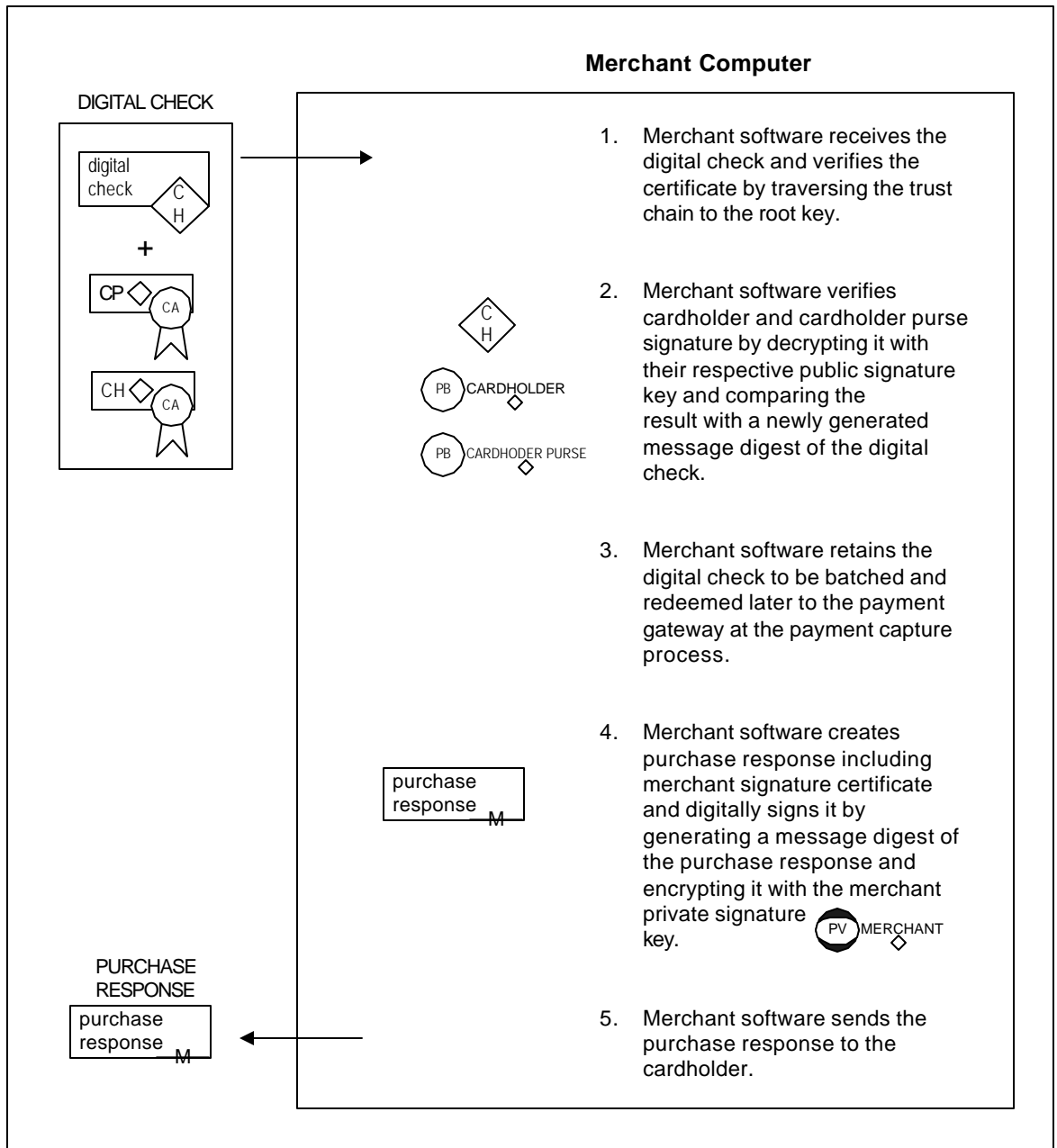
**Merchant
generates
purchase slip**



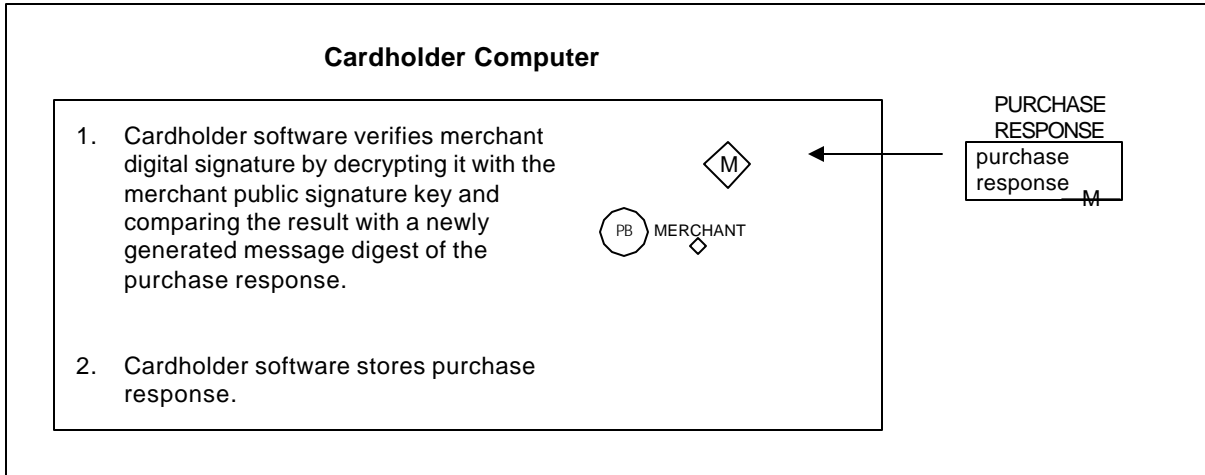
Cardholder generates digital check



Merchant
receives
digital check



**Cardholder
receives
purchase
response**



VALUE DEDUCTION

CARDHOLDER SOFTWARE

CARDHOLDER
GENERATES DIGITAL
CHECK REQUEST

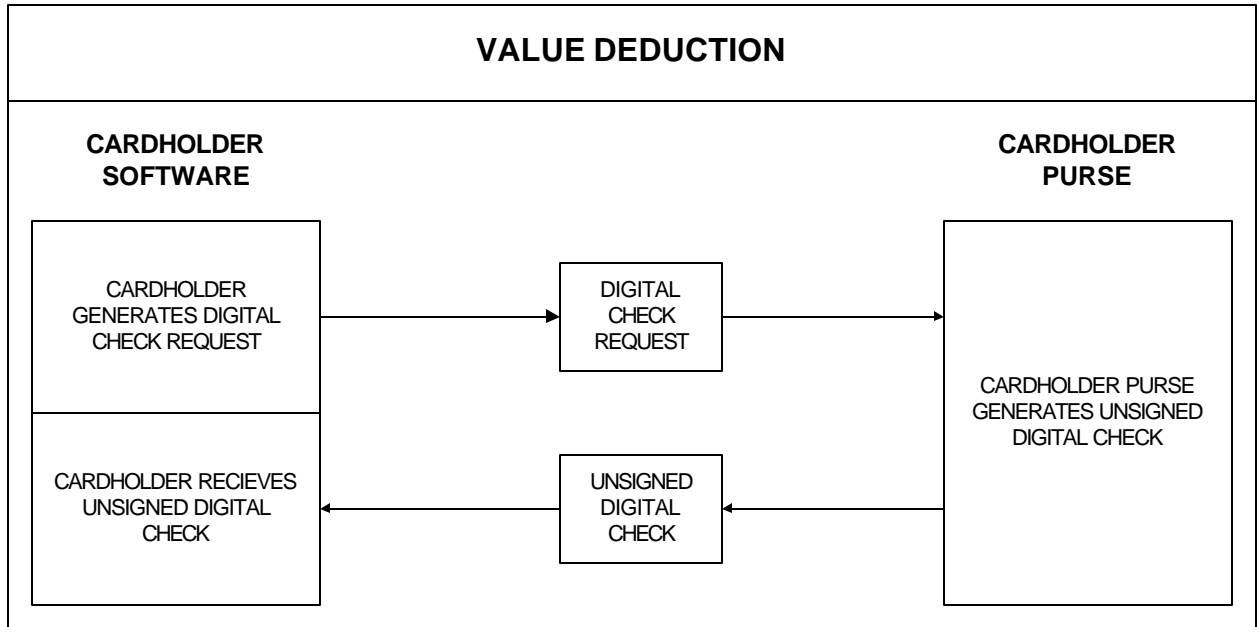
CARDHOLDER RECIEVES
UNSIGNED DIGITAL
CHECK

DIGITAL
CHECK
REQUEST

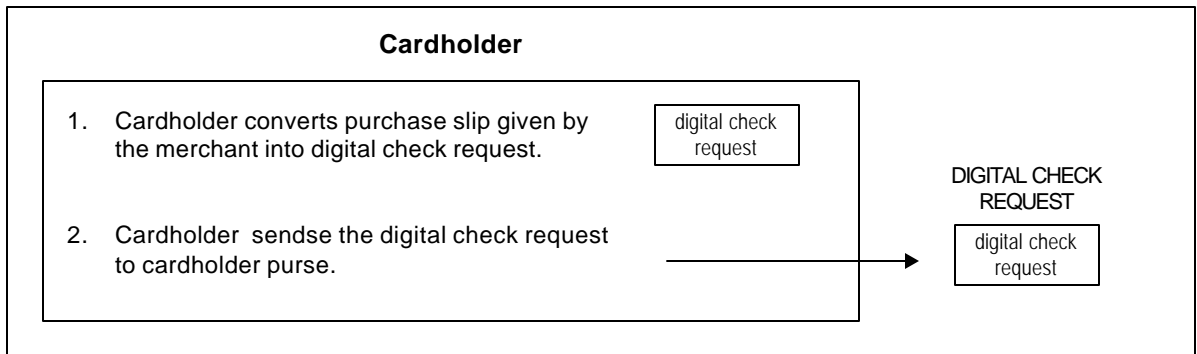
UNSIGNED
DIGITAL
CHECK

CARDHOLDER PURSE

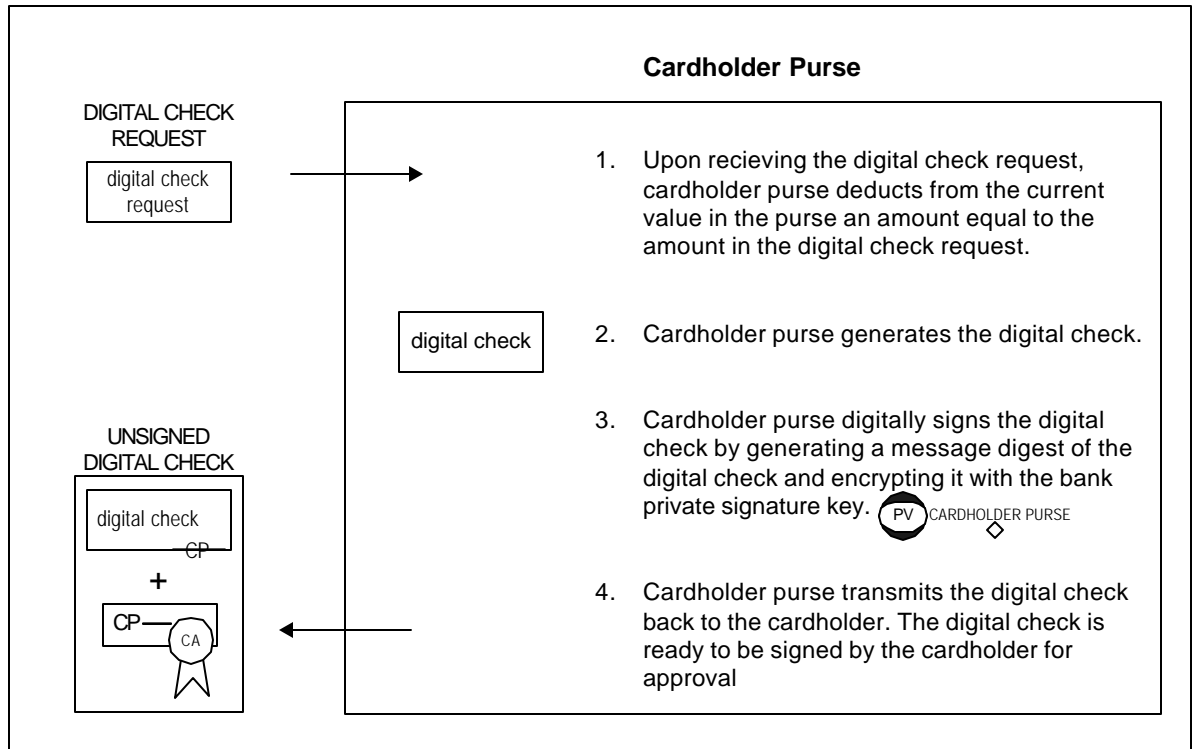
CARDHOLDER PURSE
GENERATES UNSIGNED
DIGITAL CHECK



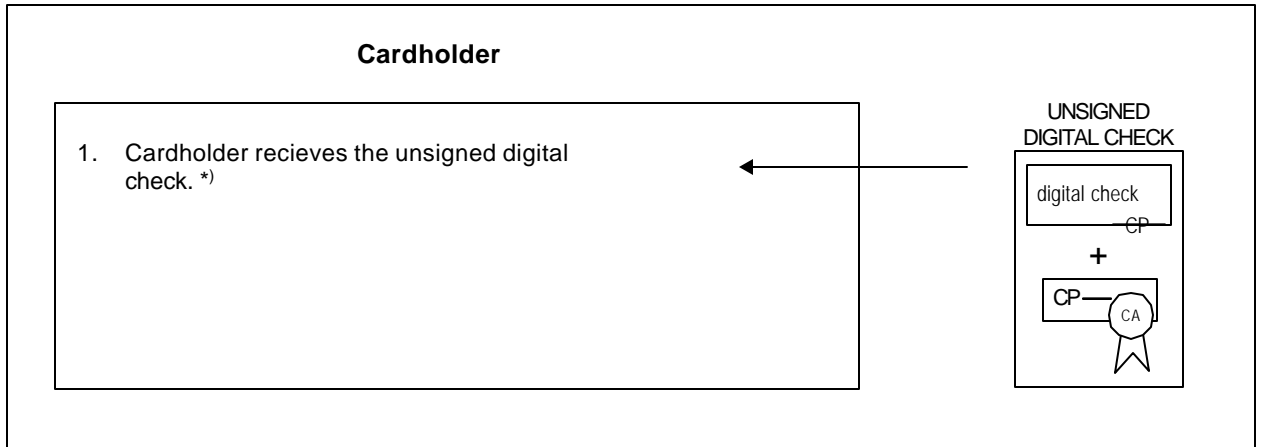
**Cardholder
generates
digital check
request**



**Cardholder
purse
generates
unsigned
digital check**



**Cardholder
receives the
unsigned
digital check**



- *) At this point, the digital check has been signed by the cardholder purse (acting on behalf of the bank, since the cardholder purse is only accessible by the bank), but has not been signed by cardholder for approval. However in the other protocols, this unsigned digital check will simply be referred as digital check.