1.a Faktura

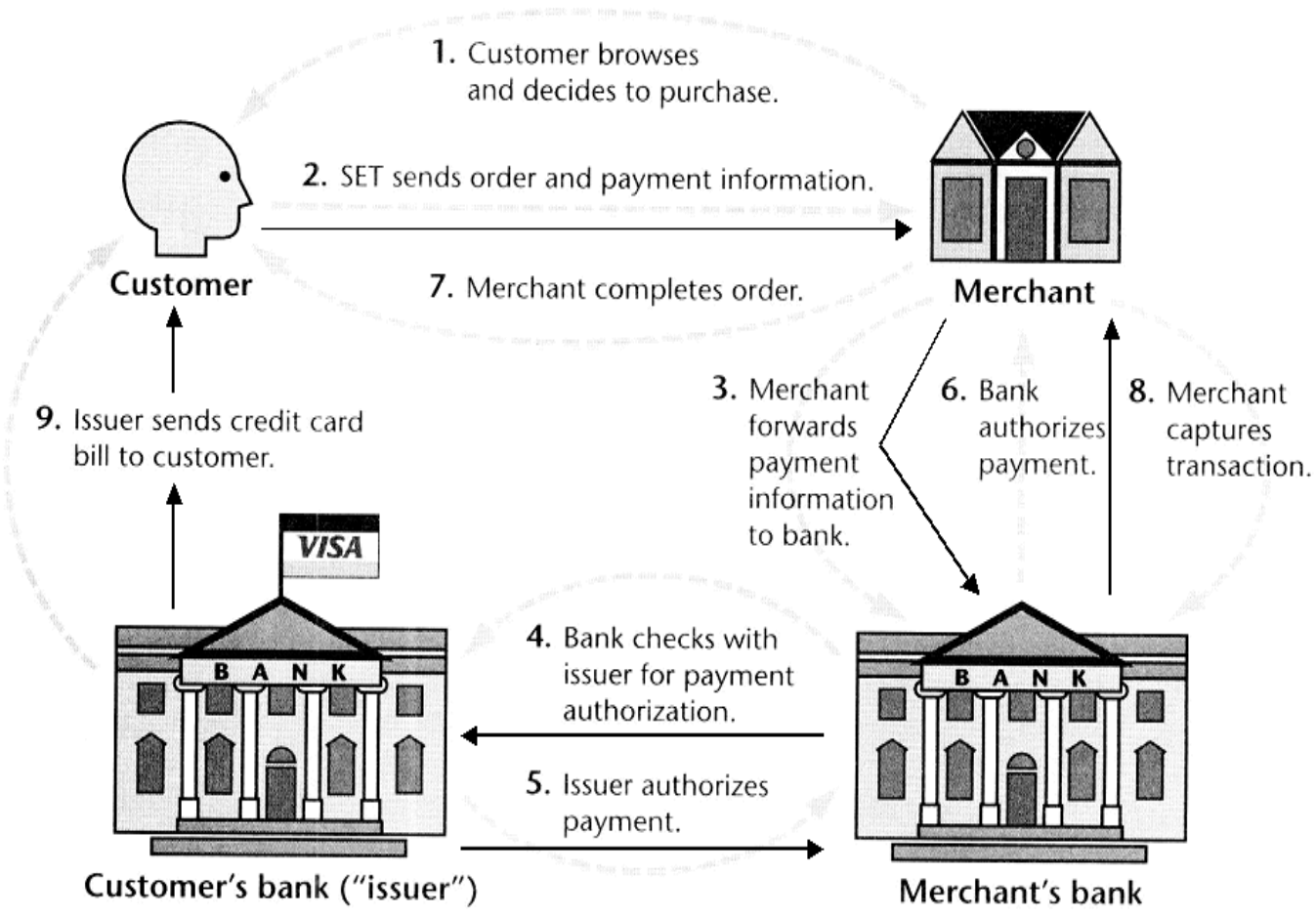
Smer: Kupac ← Trgovac

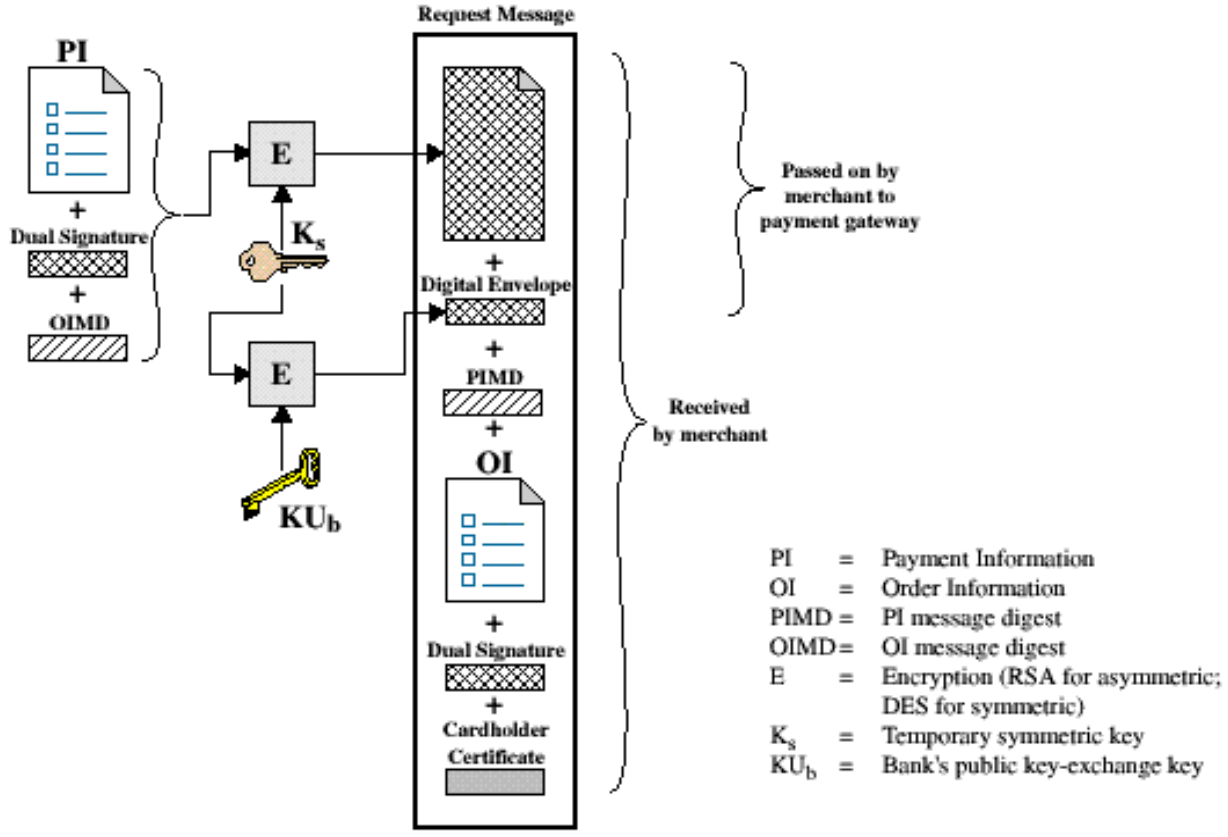
1.b Info. o načinu plaćanja (vrsta pl. kartice) + zahtev za sertifikatima (trgovac + banka obrade)

Smer: Kupac → Trgovac

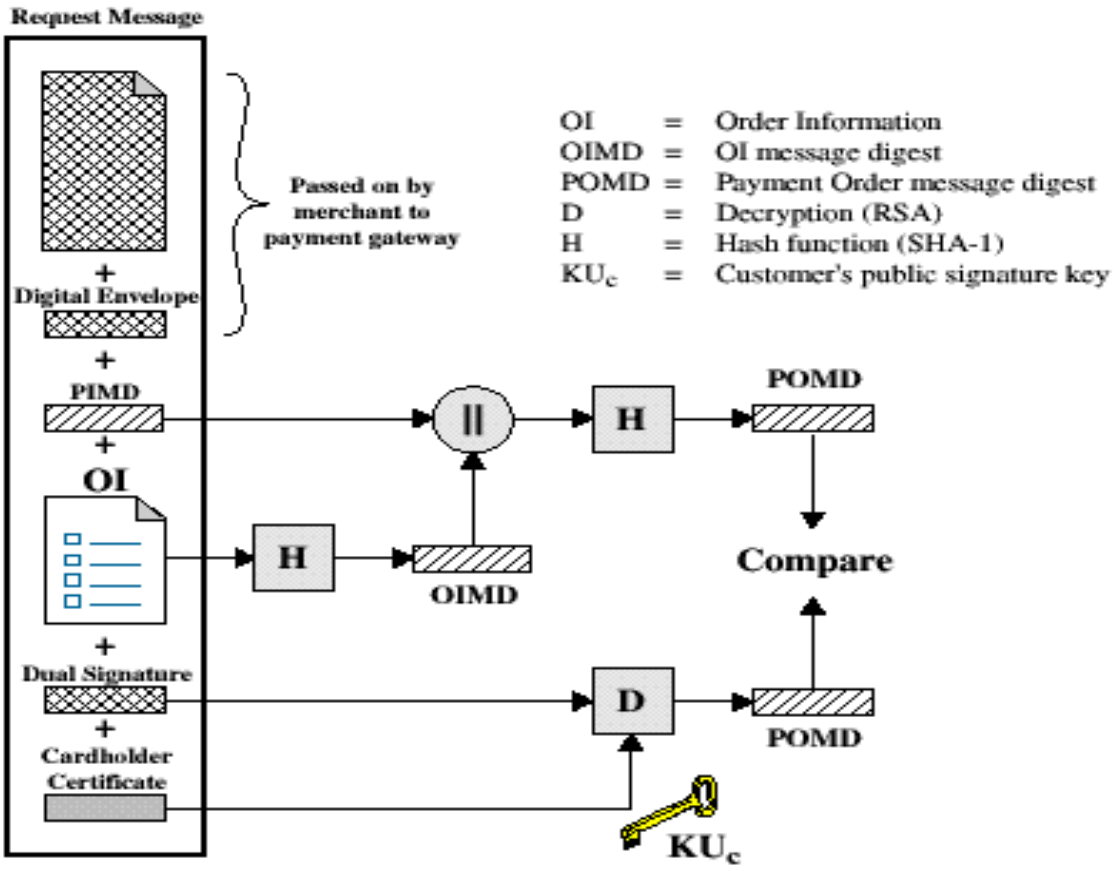
1.c ID transakcije + Sertifikati ((trgovac + banka obrade)

Smer: Kupac ← Trgovac





PI = Payment Information
OI = Order Information
PIMD = PI message digest
OIMD = OI message digest
E = Encryption (RSA for asymmetric; DES for symmetric)
K_s = Temporary symmetric key
KU_b = Bank's public key-exchange key


Request Message
Passed on by merchant to payment gateway
+
Digital Envelope
+
PIMD
+
OI
+
Dual Signature
+
Cardholder Certificate
||
H
POMD
H
OIMD
Compare
D
POMD
KUc
OI = Order Information
OIMD = OI message digest
POMD = Payment Order message digest
D = Decryption (RSA)
H = Hash function (SHA-1)
KUc = Customer's public signature key

Koraci prilikom kupovine kreditnom/debitnom karticom uz upotrebu SET protokola su sledeći:

1.Kupac pokazuje interesovanje za kupovinu putem kreditne/debitne kartice.

2.Trgovčev sistem formira fakturu i šalje je kupcu. Kupac koristi softver nalik CyberCash Wallet-u, koji prima fakturu i prenosi podatke o kupčevoj kreditnoj/debitnoj kartici trgovcu. Ovaj softver će, verovatno, biti ugrađen u Web čitač.

3.Kupac bira Visa ili MasterCard kreditnu/debitnu karticu za plaćanje, ili neku drugu koja se može koristiti putem SET softvera za plaćanje.

4.Kupčev softver započinje proces plaćanja putem slanja zahteva trgovčevom softveru da mu dostavi trgovčev javni ključ za enkripciju, kao i javni ključ platne "kapije" (tj. javni ključ sistema poslovne banke) koju trgovac koristi. Ovaj zahtev ukazuje na to koju će kreditnu/debitnu karticu kupac koristiti, s obzirom na to da trgovac može da koristi različite platne "kapije" za različite vrste kartica. Kupčevom softveru potrebni su javni ključevi trgovca i platne "kapije" da bi mogao da pošalje podatke o kreditnoj/debitnoj kartici trgovcu.

5.Trgovčev softver generiše odgovor na zahtev kupca i šalje ga kupčevom softveru. Odgovor sadrži: jedinstveni identifikator transakcije koji generiše trgovčev sistem; sertifikat trgovčevog javnog ključa; i sertifikat javnog ključa platne "kapije".

6.Kupčev softver tada proverava javni ključ trgovca i platne "kapije".

7.Kupčev softver generiše dva paketa informacija, koja šalje nazad trgovcu: paket informacija o narudžbini (Order Informations - OI) i paket instrukcija za kupovinu (Payment Instructions - PI). Svaki paket se zasebno šifrira. Paket instrukcija za kupovinu (PI) se šifrira javnim ključem platne "kapije", pošto trgovac ne treba da ima pristup ovom paketu. Trgovac treba da vidi paket informacija o narudžbini (OI). Ovaj paket sadrži identifikator transakcije, naziv kartice koja se koristi i datum transakcije. Trgovac ne sme da vidi broj kreditne/debitne kartice kupca. Paket instrukcija za kupovinu (PI) koristi poslovna banka prilikom obrade transakcije. On se kanališe preko trgovca do platne "kapije", što znači da trgovac ne može da dešifruje ovaj paket, već ga samo prosleđuje platnoj "kapiji" u neizmenjenom obliku. Ovaj paket sadrži broj kreditne/debitne kartice sa datumom njenog isteka, vrednost kupljene robe/usluga i opis narudžbine.

8.Kupčev softver prenosi pomenuta dva paketa informacija (OI i PI) do trgovca.

9.Trgovčev softver proverava da sadržaj poruke kupca, koja sadrži OI i PI pakete, nije usput izmenjen. Ako je poruka neizmenjena, softver započinje proces traženja autorizacije od trgovčeve poslovne banke.

10.Trgovčev softver generiše zahtev za autorizaciju plaćanja kreditnom/debitnom karticom. Ovaj zahtev sadrži identifikator transakcije, koji je trgovac generisao na početku procesa plaćanja.

11.Trgovac šalje platnoj "kapiji" svoje poslovne banke poruku šifriranu upotrebom javnog ključa platne "kapije". Ova poruka sadrži: zahtev za autorizovanje; PI paket koji je poslao kupac; i trgovčev javni ključ sa sertifikatom.

12.Platna "kapija" dešifruje poruku i njene komponente. Ponovo se vrši provera očuvanosti integriteta poruke (tj. njene eventualne izmene) tako što se upoređuje identifikator zahteva za autorizovanjem sa identifikatorom u kupčevom PI paketu i proverava da li je trgovac pokušao da izmeni podatke u kupčevom PI paketu.

13.Platna "kapija" zatim šalje zahtev za autorizovanje plaćanja emitentu kreditne/debitne kartice kupca preko uobičajenih bankarskih kanala, tj. istih onih kanala preko kojih bi banka zahtevala autorizovanje za bilo koju klasičnu transakciju kreditnom/debitnom karticom.

14.Banka koja je emitovala kreditnu/debitnu karticu šalje nazad šifru za odobrenje ili odbijanje platnoj "kapiji", kao odgovor na zahtev za autorizovanjem. I ovo se odvija preko uobičajenih bankarskih mreža.

15.Platna "kapija" generiše poruku sa autorizacionom šifrom, koja se šalje nazad trgovcu. Ova poruka sadrži odgovor banke koja je emitovala kreditnu/debitnu karticu.

16.Platna "kapija" šifrira i šalje poruku sa autorizacionom šifrom trgovčevom softveru.

17.Trgovčev softver dešifruje poruku o autorizaciji koju je dobio od platne "kapije". Softver zatim ispituje da li je zahtev odobren ili nije, i memoriše odgovor o autorizaciji.

18.Ako je transakcija odobrena, trgovčev softver kreira poruku koja se šalje kupčevom softveru. Ova poruka informiše kupca da je plaćanje prihvaćeno i da će proizvodi/usluge koje je kupio biti isporučeni.

19.Kupčev softver obrađuje primljenu poruku i informiše kupca da je plaćanje prihvaćeno.

Može nam se, na prvi pogled, učiniti da je ova procedura previše komplikovana, ali ne treba smetnuti s uma da je veći deo poslova potpuno automatizovan, te da će se koraci 4-19 u ovom procesu obaviti za manje od jednog minuta. SET protokol dozvoljava i razne varijacije ove procedure, u zavisnosti od konkretnih okolnosti. Recimo, trgovci kojima je važna obrada podataka u realnom vremenu mogu zahtevati prenos novca na svoj račun istovremeno sa zahtevom za autorizovanje plaćanja kreditnom/debitnom karticom.

SET protokol ima prednost nad ostalim platnim sistemima zbog toga što ne zahteva da neka treća strana prati transakcije kreditnim/debitnim karticama na Internetu. To će uticati na smanjenje troškova transakcija kreditnim/debitnim karticama preko Interneta. SET protokol koristi jaku enkripciju i modele za proveru autentičnosti. Trgovci nemaju uvid u broj kreditne/debitne kartice kupca. Takođe, novac se prebacuje na trgovčev račun u roku koji je jednak uobičajenom roku za transakcije kreditnim/debitnim karticama. Još jedna pogodnost SET protokola je i ta što ga podržavaju poznate kompanije kao što su MasterCard i Visa.
SET protokol ima i svoje nedostatke. Prvi je taj što će trgovci i kupci morati da instaliraju softver koji omogućava obradu SET transakcija. I poslovne banke će, takođe, morati da sklope ugovore sa nekom kompanijom koja će upravljati njihovom platnom "kapijom", ili će same instalirati platne "kapije". Osim toga, trgovci će morati da otvore račun kod neke poslovne banke koja je osposobljena da prima SET transakcije.

Ne treba sumnjati da će MasterCard i Visa svojim autoritetom uticati na to da SET postane dominantna metoda za obavljanje transakcija kreditnim/debitnim karticama preko Interneta, imajući u vidu da su brojne kompanije već počele da razvijaju softver koji će vršiti obradu SET transakcija kupaca, trgovaca i poslovnih banaka.