



SET

- SET: Secure Electronic Transaction
- beveiliging van kredietkaarttransacties over Internet

SET

1



Kredietkaarten en Internet

- **Probleem:**
 - veilige transfer/opslag van gegevens over kredietkaart en aankoop
 - zodat gebruiker vertrouwen heeft
- **Noodzakelijk:**
 - authenticatie van verkoper en koper
 - vertrouwelijke gegevensoverdracht
- **Bestaande systemen verschillen in**
 - type publieke-sleutelencryptie
 - type conventionele encryptie
 - algoritme voor de message digest
 - aantal partijen met een geheime sleutel
 - aantal partijen met certificaten

SET

2



Kredietkaarten: mogelijke protocols

- SSL / TLS
 - 1 of 2 partijen hebben geheime sleutels en/of certificaten
 - *IKP* (IBM)
 - SEPP (Secure Encryption Payment Protocol)
 - MasterCard, IBM, Netscape
 - STT (Secure Transaction Technology)
 - VISA, Microsoft
- } **verouderd**
- SET (Secure Electronic Transaction)
 - MasterCard, VISA, e.a.
 - is moeilijk ingeburgerd geraakt

SET

3



SET

- Betrokken bedrijven
 - Mastercard, Visa, IBM, Microsoft, Netscape, RSA, Verisign, ...
- open specificatie
- geen betalingssysteem
- verzameling beveiligingsprotocols en formaten
- gebruikt bestaande infrastructuur
- complexe specificatie
 - 971 pagina's (vgl. SSL 63 pagina's)
 - 3 boeken:
 - business description (80 pag.)
 - programmer's guide (629 pag.)
 - formal protocol description (262 pag.)

SET

4



SET: kenmerken (1)

- confidentialiteit
 - rekeninginformatie (nr, bedrag) is beveiligd
 - **alleen beschikbaar voor bank, niet voor verkoper !**
 - alle boodschappen worden conventioneel geëncrypteerd
- integriteit van gegevens
 - info over bestelling, persoon, betaling niet gewijzigd in transit
 - d.m.v. RSA handtekeningen of HMAC (SHA-1)

SET

5

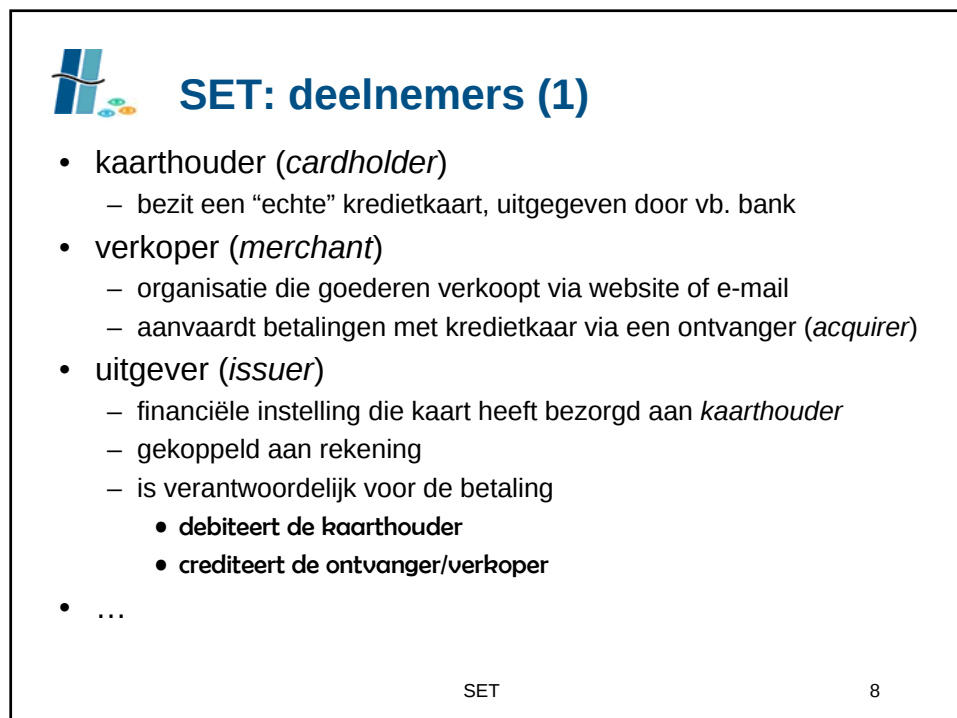
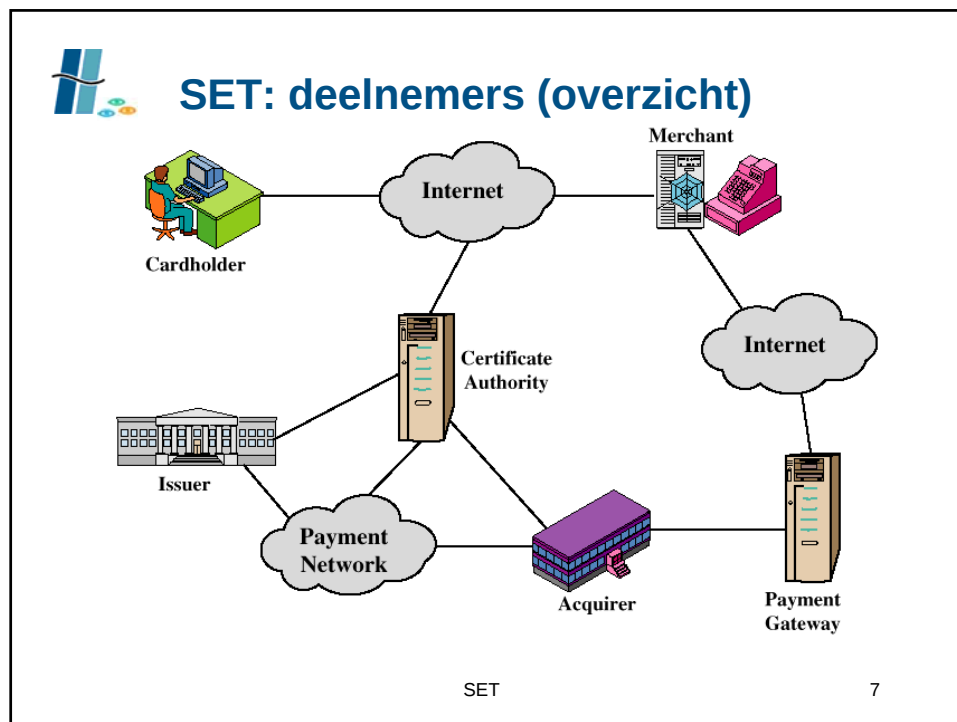


SET: kenmerken (2)

- authenticatie d.m.v. X.509 certificaten
 - authenticatie van rekeningnummer van kaarthouder
 - **verkoper is zeker dat kaarthouder en rekening gelegitimeerd zijn**
 - authenticatie van verkoper
 - **kaarthouder is zeker dat verkoper zijn kaart kan aanvaarden**
 - **kaarthouder is zeker dat verkoper is wie hij beweert te zijn**
- geen keuze voor de cryptografische algoritmes
 - reden: SET is slechts 1 toepassing (cf. IPSec en SSL)

SET

6





SET: deelnemers (2)

- ontvanger (*acquirer*)
 - financiële instelling die rekening heeft bezorgd aan *verkoper*
 - kan meer types kaarten behandelen
 - bezorgt authenticatie aan verkoper dat
 - kaartnummer actief is
 - bedrag de limiet niet overschrijdt
 - betaalt de verkoper
- betalingspoort (*payment gateway*)
 - operatie die uitgevoerd wordt door de ontvanger of een derde partij
 - interface tussen SET (verkoper) en betalingsnetwerken
 - staat in verbinding met financieel systeem van ontvanger
- certificatieautoriteit (CA)
 - bezorgt X.509 certificaten aan kaarthouder, verkoper, betalingspoort

SET

9



SET: transacties vooraf

- klant opent een kredietkaartrekening
 - bij bank die SET ondersteunt
- klant “krijgt” een certificaat getekend door de bank
 - vereist geïnstalleerde software !
 - klant genereert sleutelpaar
 - identiteit van klant wordt (fysiek) geverifieerd
 - autoriseert relatie tussen rekening en sleutelpaar van klant
- verkopers bezitten voor elk type kaart 2 certificaten
 - één voor plaatsen van handtekening
 - één voor uitwisselen van sleutels
- verkoper bezit het certificaat van de betalingspoort

SET

10



SET: transacties (1)

- alle transacties worden versleuteld
- klant plaatst een order bij de verkoper via website
- verkoper verzendt naar klant
 - order- en betalingsgegevens
 - een kopie van verkopercertificaat
- klant controleert of tegenpartij rechtmatige verkoper is
- klant verzendt naar verkoper
 - ordergegevens
 - kopie van klantcertificaat
 - betaalgegevens en kaartgegevens, doch **niet leesbaar voor verkoper!**
- verkoper kan klant verifiëren a.d.h.v. klantcertificaat

SET

11



SET: transacties (2)

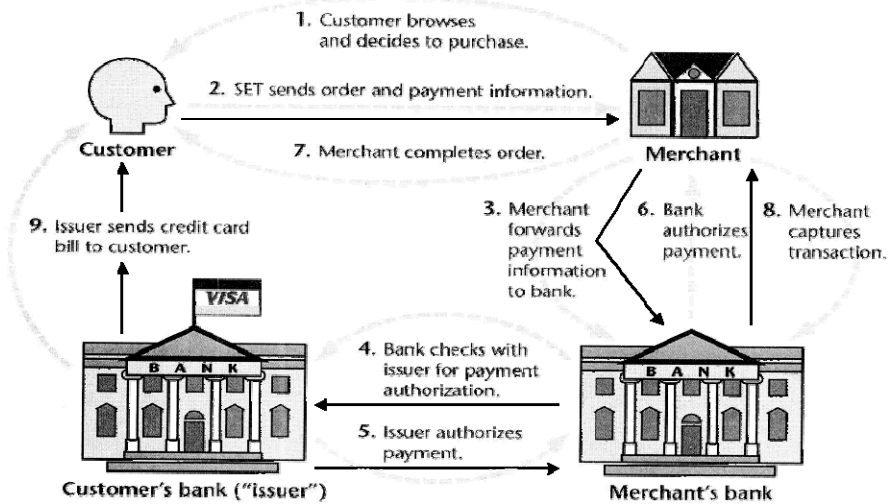
- verkoper vraagt toelating tot betaling
 - doorsturen betaalgegevens naar betaalpoort
- financiële instellingen wisselen gegevens uit
 - controle van geldigheid van financiële transactie
- verkoper krijgt bevestiging van toelating tot betaling
- verkoper bevestigt order
- verkoper levert de goederen of diensten
- verkoper vraagt uitbetaling aan betaalpoort

SET

12



SET: transacties (overzicht)



SET

13



SET: technologieën

- confidentialiteit:
 - DES 56 bit-key (???)
- Integriteit:
 - RSA-handtekening met SHA-1
- authenticatie rekening kaarthouder:
 - X.509 certificaten met RSA-handtekening
- authenticatie verkoper:
 - X.509 certificaten met RSA-handtekening
- privacy:
 - scheiding tussen order en betaling
 - gebruik van dubbele handtekening

SET

14



Dubbele handtekening

- verbindt twee boodschappen die bestemd zijn voor verschillende ontvangers
- klant verstuurt
 - ordergegevens naar verkoper
 - betalingsgegevens naar bank via de verkoper
- verkoper krijgt het kredietkaartnummer niet te zien
- bank krijgt de details van het order niet te zien
- toch moeten beide gegevens verbonden zijn om dispuut te vermijden
 - klant kan bewijzen dat de betaling bestemd is voor die welbepaalde goederen en niet voor een andere bestelling

SET

15



Dubbele handtekening: waarom?

- stel dat klant aan de verkoper twee boodschappen zendt:
 - getekende ordergegevens
 - getekende betaalgegevens
 - verkoper stuurt betaalgegevens door naar de bank
- indien verkoper een ander order van deze klant kan opvangen
 - verkoper zou kunnen beweren dat de betaling bedoeld was voor dit order en niet voor het origineel

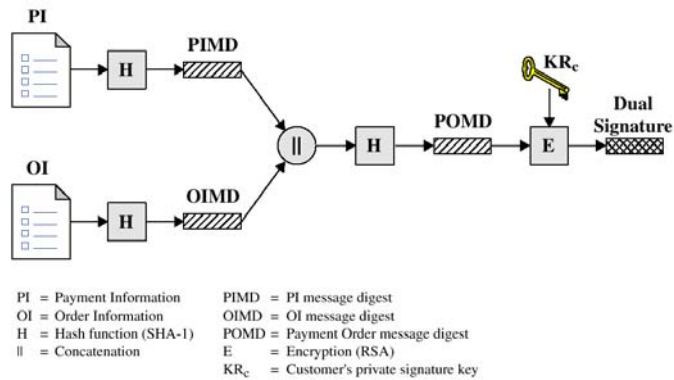
SET

16



Dubbele handtekening: hoe?

$$DS = E_{KR_c} [H(H(PI) \parallel H(OI))]$$



SET

17



Dubbele handtekening: hoe?

- neem de hash (SHA-1) van zowel de ordergegevens als van de betaalgegevens
- deze twee hashwaarden worden samengevoegd
- hiervan wordt opnieuw een hash berekend
- deze resulterende hash wordt geëncrypteerd met de private sleutel van de klant
- dit laatste vormt dus de dubbele handtekening

SET

18



DS: verificatie door verkoper

- $DS = E_{K_{RC}}[H(H(PI) || H(OI))]$
- verkoper gebruikt de publieke sleutel van de klant (certificaat)
- verkoper bezit:
 - DS
 - OI
 - $PIMD = H(PI)$ (message digest van de betaalgegevens)
- verkoper berekent
 - $H(OI)$
 - $H[PIMD || H(OI)]$
 - $D_{K_{UC}}[DS]$
- laatste twee moeten gelijk zijn

SET

19



DS: verificatie door bank

- $DS = E_{K_{RC}}[H(H(PI) || H(OI))]$
- bank gebruikt de publieke sleutel van de klant (certificaat)
- bank bezit:
 - DS
 - PI
 - $OIMD = H(OI)$ (message digest van de ordergegevens)
- bank berekent
 - $H(PI)$
 - $H[H(PI) || OIMD]$
 - $D_{K_{UC}}[DS]$
- laatste twee moeten gelijk zijn

SET

20



Dubbele handtekening: resultaat

- verkoper heeft ordergegevens ontvangen en de handtekening geverifieerd
- bank heeft betaalgegevens ontvangen en de handtekening geverifieerd
- de klant heeft de ordergegevens en de betaalgegevens met mekaar verbonden

SET

21



SET: transactietypes

- | | |
|----------------------------|--------------------------|
| • card holder registration | • purchase notification |
| • merchant registration | • sale transaction |
| • purchase request | • authorization reversal |
| • payment authorization | • capture reversal |
| • payment capture | • credit reversal |
| • certificate query | |
| • purchase inquiry | |

SET

22



Aankoopaanvraag: *purchase request*

- onderstel dat bestelling klaar is (geen SET)
 - in browser goederen geselecteerd en order geplaatst
- van klant naar verkoper
 - orderinformatie voor verkoper
 - betaal informatie voor bank
- Aankoop omhelst 4 boodschappen
 - Initiate Request
 - Initiate Response
 - Purchase Request
 - Purchase Response

SET

23



Purchase Request: Initiate Request

- basisvereiste:
 - kaarthouder bezit certificaat van verkoper en gateway
- klant stuurt naar verkoper
 - aanvraag voor deze certificaten
 - merk/type kredietkaart
 - ID dat deze aanvraag en het antwoord erop identificeert
 - nonce

SET

24



Purchase Request: Initiate Response

- antwoord van verkoper
 - getekend met zijn private sleutel
 - nonce van klant
 - nonce van verkoper (nieuw, terug te sturen met antwoord van klant)
 - ID
 - handtekeningcertificaat van verkoper
 - sleuteluitwisselingscertificaat van gateway

SET

25



Purchase Request: Purchase Request

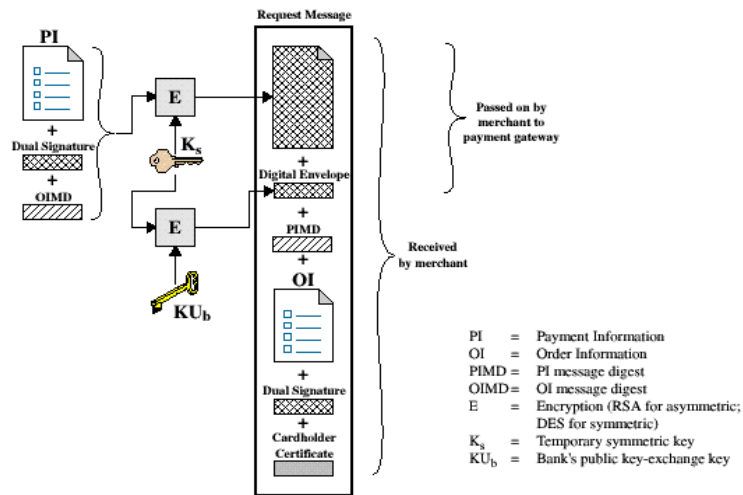
- kaarthouder
 - verifieert ontvangen certificaten
 - creëert ordergegevens (OI) en betaalgegevens (PI)
- kaarthouder stelt boodschap samen
 - aankoop gerelateerde gegevens bestemd voor payment gateway
 - PI, dubbele handtekening, OIMD
 - geëncrypteerd met tijdelijke sleutel Ks
 - Ks wordt geëncrypteerd met publieke sleutel van gateway
 - order gerelateerde gegevens bestemd voor de verkoper
 - OI, dubbele handtekening, PIMD
 - certificaat van kaarthouder

SET

26



Purchase Request: Purchase Request



SET

27



Verkoper ontvangt Purchase Request

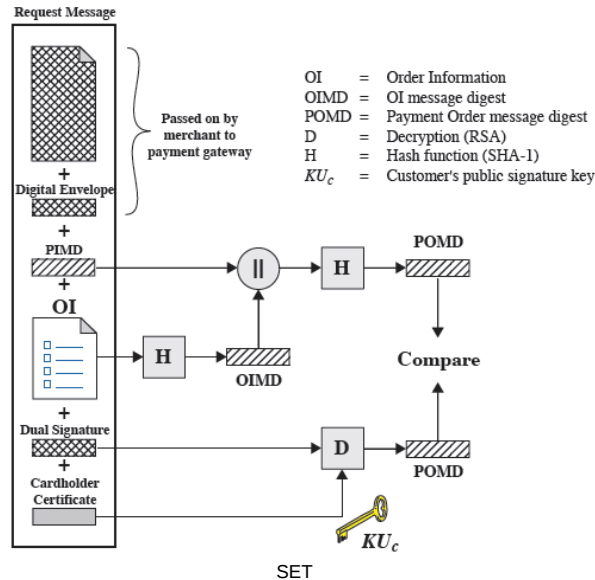
- verifieert het certificaat van het kaarthouder
- verifieert de dubbele handtekening
- verwerkt het order
- stuurt de betaal informatie door naar de gateway
- stuurt een purchase response naar klant (kaarthouder)

SET

28



Verkoper verifieert Purchase Request



29



Antwoord verkoper: Purchase Response

- boodschap
 - accepteert het order
 - refereert naar het transactienummer
 - getekend door private sleutel van verkoper
- kaarthouder ontvangt dit antwoord en
 - verifieert certificaat van de verkoper
 - verifieert de handtekening van de verkoper
 - neemt de nodige acties:
 - vb. software toont boodschap met status van het order

SET

30



SET: transactietypes

- card holder registration
- merchant registration
- purchase request
- payment authorization
- payment capture
- certificate query
- purchase inquiry
- purchase notification
- sale transaction
- authorization reversal
- capture reversal
- credit reversal

SET

31



Betalingsproces

- bestaat uit twee delen
 - payment authorization: toelating tot betaling vanwege gateway
 - payment capture: verkoper vraagt uitbetaling aan gateway

SET

32



Payment Authorization

- verkoper krijgt de verzekering van de gateway
 - dat transactie toegelaten is door de kaartuitgever
 - dat hij zijn geld zal krijgen
- verkoper vraagt toestemming (*authorization request*)
- verkoper krijgt toestemming (*authorization response*)

SET

33



Authorization Request

boodschap naar gateway bevat

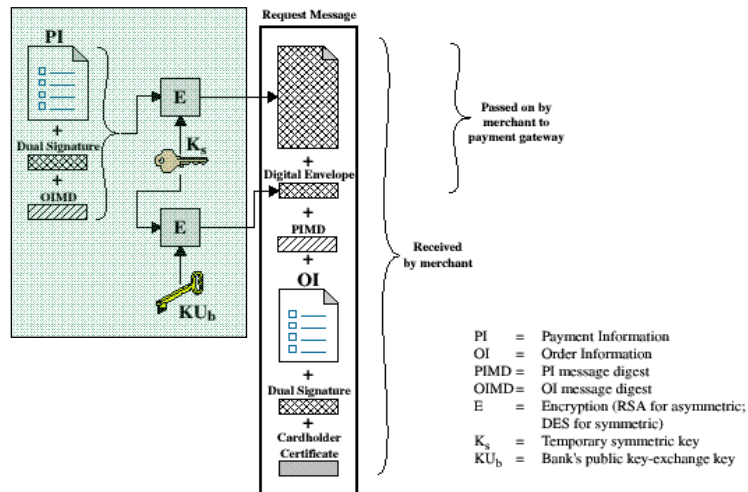
1. info afkomstig van klant
 - PI (betalingsinformatie), dubbele handtekening, OIMD (hash over de orderinformatie), digitale omslag (zie figuur hiervoor)
2. machtigingsblok
 - transactie-ID
 - getekend met private sleutel verkoper
 - geëncrypteerd met sessiesleutel
 - digitale omslag: sessiesleutel geëncrypteerd met publieke sleutel van gateway
3. certificaten
 - kaarthouder
 - verkoper (handtekening, sleuteluitwisseling)

SET

34



Purchase Request: Purchase Request



SET

35



Acties Payment Gateway

- verifieert alle certificaten
- decrypteert digitale omslag → sessiesleutel
- verifieert handtekening verkoper op transactie-ID
- decrypteert digitale omslag van betaalblok
- verifieert dubbele handtekening op betaalblok
- verifieert gelijkheid van
 - transactie-ID van verkoper
 - transactie-ID van klant (kaarthouder) vermeld in PI
- vraagt en krijgt de toelating tot betaling van kaartuitgever

SET

36



Authorization Response

- boodschap vanwege gateway bevat
 1. toestemming tot betaling
 - machtigingsblok getekend door gateway en geëncrypteerd met nieuwe sessiesleutel
 - digitale omslag: sessiesleutel geëncrypteerd met publieke sleutel verkoper
 2. *capture token* informatie
 - informatie bedoeld om later geld “af te halen”
 - behandeld zoals in 1.
 - door verkoper ongewijzigd terug te sturen naar gateway
 3. certificaat
 - handtekeningcertificaat van gateway
- verkoper kan goederen leveren aan klant

SET

37



Payment Capture

- verkoper vraagt betaling aan de payment gateway
- *capture request*
 - verkoper maakt aanvraag
 - bevat bedrag, transactie-ID
 - tekent en encrypteert met sessiesleutel
 - digitale omslag: K_s geëncrypteerd met publieke sleutel gateway
 - capture token
 - certificaten van verkoper
- gateway decrypteert
 - verifieert handtekeningen ontvangen informatie
 - verifieert info in capture request en capture token
 - vraagt aan uitgever de betaling van de verkoper
- *capture response*
 - antwoord gateway getekend en geëncrypteerd

38