Get SET for secure electronic transactions

Ir. R. de Wolf

SET (Secure Electronic Transaction) is een internationale standaard voor credit- en debitcardtransacties over het Internet. In dit artikel worden de risico's beschreven die samenhangen met het gebruik van creditcards op het Internet. In een beschrijving van SET wordt ingegaan op de maatregelen die in het SET-protocol zijn getroffen om deze risico's te verminderen. Tot besluit wordt een indruk gegeven van de huidige stand van zaken omtrent de invoering van SET.

Inleiding

De vierde Compact in 1998 had als thema 'Electronic commerce'. Daarin heeft u kunnen lezen dat de betrouwbare gegevensuitwisseling over Internet één van de belangrijkste voorwaarden is voor electronic commerce. De risico's die met het gebruik van het medium Internet samenhangen 'kunnen worden voorkomen door het treffen van afdoende veiligheidsmaatregelen in combinatie met het ontwikkelen van organisatorische en juridische kaders', aldus Biesheuvel en Olde Olthof in het inleidende artikel. De auteurs in Compact 1998/4 gaven hier zelf invulling aan door te pleiten voor de ontwikkeling van TTP-diensten en door de behandeling van juridische vraagstukken en technische oplossingen die samenhangen met electronic commerce.

Dit artikel gaat in op een belangrijke technische ontwikkeling ten behoeve van het 'business-to-consumer'-segment van de electronic-commercemarkt. Consumenten blijken behoefte te hebben aan elektronische betaalmethoden op het Internet die aansluiten bij reeds beschikbare betaalmiddelen, zoals creditcards en debitcards (pinpassen en chipkaarten). Dit impliceert de noodzaak tot een koppeling tussen bestaande financiële infrastructuren en het Internet voor het doorgeleiden van betaalgegevens. Met de publicatie van de specificaties van het SET-protocol (Secure Electronic Transaction) in mei 1997 is de basis gelegd voor de implementatie van een veilige methode voor het uitvoeren van creditcardbetalingen via het Internet.

Allereerst worden de risico's geschetst die samenhangen met de gebruikelijke wijze waarop creditcardbetalingen over het Internet plaatsvinden. In de daaropvolgende beschrijving van SET wordt ingegaan op de maatregelen die in het protocol zijn getroffen om deze risico's te verminderen. Tot besluit wordt een indruk gegeven van de huidige stand van zaken omtrent de invoering van SET. In enkele bijlagen van het artikel wordt een vergelijking gegeven tussen SET en SSL en wordt de toepassing van cryptografie en certificaten in SET kort toegelicht.

Transacties zonder SET

Ter inleiding van de beschrijving van het SET-protocol wordt in deze paragraaf nader ingegaan op de wijze waarop creditcardtransacties zonder SET plaatsvinden. In een vergelijking tussen de traditionele, niet-elektronische betaalwijze en de gebruikelijke elektronische betaalwijze over het Internet worden de risico's geschetst die aan de laatste methode zijn verbonden.

Rollen

In de bestaande financiële infrastructuren zijn bij transacties met betaalkaarten enkele partijen betrokken. De rollen van deze partijen zullen hier kort worden toegelicht, omdat hieraan in het vervolg van het artikel veelvuldig zal worden gerefereerd.

Een houder van een betaalkaart wordt aangeduid als de *cardholder*. Een *merchant* is een aanbieder van goederen of diensten die de cardholder de mogelijkheid biedt met een betaalkaart af te rekenen. De cardholder is door zijn *issuer* voorzien van een betaalkaart en een daaraan verbonden rekening. Een issuer kan bijvoorbeeld een creditcardmaatschappij zijn, zoals Visa/MasterCard, maar ook een bankinstelling die pinpassen en creditcards aan haar cliënten ter beschikking stelt. Merchants accepteren doorgaans kaarten van meerdere issuers, maar hebben voor de afwikkeling van de betalingen liever met slechts één partij te maken: een *acquirer*. Acquirers voorzien de merchant van autorisatie en vereffeningsdiensten voor een reeks issuers. Een acquirer ontvangt hiervoor per transactie een percentage van het te vereffenen bedrag.

Niet-elektronische creditcardtransacties

In deze subparagraaf wordt kort ingegaan op de waarborgen die aanwezig zijn in het proces van het op traditionele, niet-elektronische wijze betalen met een creditcard. In figuur 1 zijn de belangrijkste stappen in dit proces weergegeven. In de figuur is tevens het onderscheid aangegeven tussen informatiestromen (dunne pijlen) en geldstromen (dikke pijlen) tussen de betrokken partijen. Het in de figuur omkaderde clearingnetwerk omvat de bestaande financiële infrastructuur voor het verrekenen van schulden en vorderingen die ontstaan als gevolg van creditcardtransacties.

Indien bijvoorbeeld in een winkel of restaurant met een creditcard wordt betaald, start het betaalproces wanneer de cardholder zijn kaart aan de kassier overhandigt.

1 Betaalopdracht

Volgens de oorspronkelijke betaalwijze maakt de kassier een doordruk van de kaart op een creditcardslip. Dit is een formulier waarmee cardholders betaalopdrachten kunnen geven. Op de slip worden handmatig of met behulp van een kasregister de overige betaalgegevens vastgelegd, zoals het transactiebedrag en de datum. De slip wordt door de cardholder van een handtekening voorzien. De kassier controleert de handtekening op de slip met die op de creditcard en overhandigt de cardholder zijn kaart, tezamen met een doordruk van de getekende slip en eventueel de kassabon.

2 Autorisatiecontrole

De fraudegevoeligheid van creditcards maakt echter aanvullende maatregelen noodzakelijk. Op een creditcard staan immers alle gegevens die noodzakelijk zijn voor het uitvoeren van een betaalopdracht (het kaartnummer, de verloopdatum van de kaart en de handtekening van de cardholder). De handtekeningcontrole biedt de merchant geen waarborg dat de betaling met een geldige creditcard heeft plaatsgevonden. Daarom is het gebruikelijk dat een merchant na inname van de creditcard een autorisatiecontrole uitvoert. Hiertoe geeft de merchant telefonisch of on line via een autorisatieterminal het kaartnummer en het aankoopbedrag aan de acquirer door. Deze controleert onder meer of de kaart niet geblokkeerd is, of de cardholder nog voldoende krediet heeft en of er geen betalingsachterstanden zijn. Vaak zijn autorisatieterminals geïntegreerd met kasregisters, waardoor de merchant niet meer het bedrag via de autorisatieterminal hoeft in te voeren. De autorisatieterminal drukt, nadat toestemming is verkregen van de acquirer, een bon af waarop de cardholder zijn handtekening plaatst. De cardholder ontvangt de doorslag van de bon als bewijs van aankoop en betaling.

In veel gevallen wordt de handtekeningcontrole vergeten of niet adequaat uitgevoerd. De merchant vertrouwt in deze gevallen de cardholder 'op zijn blauwe ogen'.

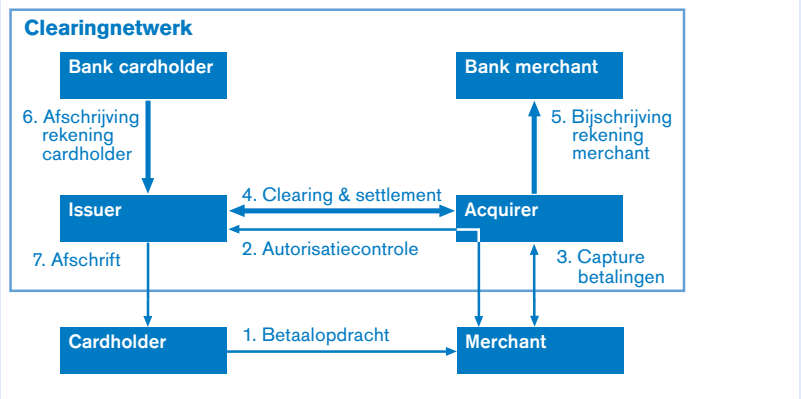
3 Capture betalingen

Met de getekende slips of kassabonnen kan de merchant de eerder geautoriseerde betalingen bij de acquirer innen. Hiertoe verzamelt de merchant bij dagafsluiting de getekende betaalopdrachten en verstuurt deze aan de acquirer. De vereffening tussen de acquirer en de merchant wordt in creditcardterminologie aangeduid met een 'capture' van betaalopdrachten.

Overige stappen

De acquirer vereffent via het clearingnetwerk van de betreffende issuer de positie die door captureverzoeken is ontstaan (4). De acquirer schrijft het bedrag over op een bankrekening van de merchant (5). De issuer schrijft maandelijks het totaalbedrag van in die maand uitgevoerde creditcardtransacties af van de betaalrekening van de cardholder (6). Tevens ontvangt de cardholder van de issuer maandelijks een overzicht van de samenstelling van het afgeschreven bedrag (7). De cardholder dient het afschrift te controleren met de verzamelde creditcardslips en/of kassabonnen (reconciliatiecontrole).

Samenvattend biedt deze wijze van betaling en afwikkeling de volgende waarborgen:

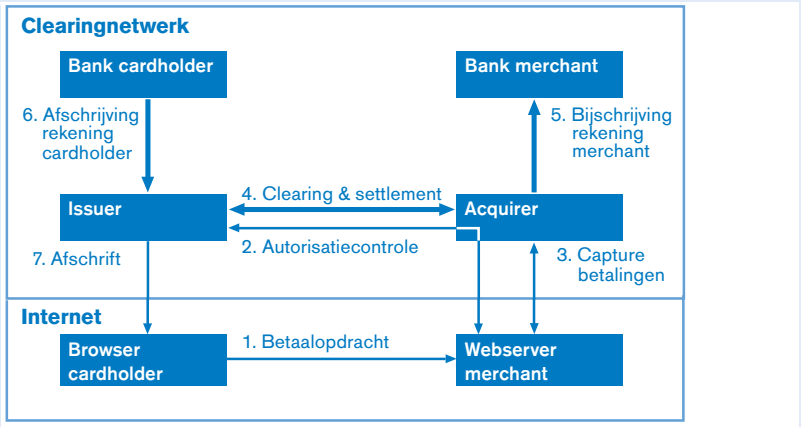


Figuur 1. De belangrijkste stappen in niet-elektronische creditcardtransacties.

- handtekening cardholder ter goedkeuring van de betaalopdracht;
- dus ook de handtekeningcontrole ter authenticatie van de cardholder;
- autorisatiecontrole van de transactie ter goedkeuring van de transactie door de acquirer;
- capture van geautoriseerde bedragen met getekende creditcardslips of kassabonnen;
- maandelijkse betalingsoverzichten ter reconciliatie van betalingen door de cardholder.

Elektronische creditcardtransacties

Deze subparagraaf behandelt kort de risico's die aanwezig zijn in het proces van het op elektronische wijze betalen met een creditcard via het Internet, zonder dat hierbij gebruik wordt gemaakt van het SET-protocol. Hierbij dienen de in de vorige subparagraaf behandelde waarborgen als leidraad. In figuur 2 zijn de belangrijkste stappen in dit proces weergegeven. Het belangrijkste onderscheid met figuur 1 betreft de omgeving (Internet) en de vorm (webbrowser en webserver) waarin de cardholder respectievelijk de merchant zich presenteert.



Figuur 2. Elektronische creditcardtransacties.

Als via de website van een merchant met een creditcard wordt betaald, dan start het betaalproces nadat de cardholder zijn aankoop heeft vastgelegd. Vaak biedt een merchant op zijn website een interactieve catalogus aan. Met een webbrowser kan een bezoeker van de website artikelen in een virtuele boodschappenmand plaatsen. De onderliggende applicatie houdt de gegevens bij van de artikelen die in de boodschappenmand zijn geplaatst,

inclusief het totaalbedrag. Nadat de gewenste artikelen zijn verzameld, kan de bezoeker aangeven met creditcard te willen betalen.

1 Betaalopdracht
Voor de overdracht van creditcardgegevens is het gebruikelijk dat de webserver van de merchant met behulp van SSL of SHTTP een cryptografisch versleutelde sessie start met de webbrowser van de cardholder. De merchant presenteert via deze verbinding een webpagina met een formulier waarmee de cardholder de betaalgegevens naar de merchant verstuurt.

Met een versleutelde verbinding tussen de cardholder en de merchant is de vertrouwelijkheid en integriteit van de creditcardgegevens gedurende het transport over het Internet redelijk gewaarborgd. Zonder deze beveiligde verbinding kunnen echter anderen dan de merchant kennisnemen van de creditcardgegevens of kunnen de betaalgegevens gedurende het transport over het Internet worden gewijzigd.

Door een niet of onvoldoende beveiligde verbinding met de merchant bestaat het risico dat de vertrouwelijkheid en de integriteit van creditcardgegevens tijdens transport verloren gaan.

De cardholder heeft ondanks de met SSL versleutelde verbinding geen zekerheid of de partij aan de andere kant van de verbinding wel een echte merchant is, kortom of de ontvangen berichten authentiek zijn (zie bijlage 1 'SSL versus SET'). Tevens kan de cardholder te maken hebben met een merchant die geen machtiging heeft om via een acquirer creditcardbetalingen te accepteren. In beide gevallen draagt de cardholder zijn creditcardgegevens over aan een organisatie die geen contractuele verplichting heeft tot geheimhouding van deze gegevens.

Door de onzekerheid over de authenticiteit van de merchant en over de vraag of deze gemachtigd is creditcardbetalingen te accepteren bestaat het risico dat de vertrouwelijkheid van de creditcardgegevens verloren gaat.

Bij elektronische creditcardtransacties kan de eerder beschreven handtekeningcontrole niet worden uitgevoerd. Dit is op zich niet nieuw. Bij telefonische bestellingen (denk aan de 'commercial presentations') geeft de cardholder zijn creditcardgegevens door aan een telefoniste, die deze invoert in een autorisatieterminal. Hierbij kan eveneens geen handtekeningcontrole worden uitgevoerd. Opgemerkt dient te worden dat ook bij 'face-to-face'-verkoop de handtekeningcontrole vaak wordt vergeten of niet adequaat wordt uitgevoerd.

Door het ontbreken van de handtekening ter goedkeuring van transacties en dus ook van de handtekeningcontrole bestaat het risico dat de merchant creditcards accepteert die niet aan degene toebehoren die ze presenteert.

2 Autorisatiecontrole
Indien de merchant over faciliteiten beschikt voor on line autorisatie van betaalopdrachten, zal de cardholder binnen enkele seconden worden bericht of de transactie is goedgekeurd. Vaak zal de merchant autorisatiecontroles batchgewijs uitvoeren en de cardholder later per e-mail berichten of de transactie is goedgekeurd.

In beide gevallen zal de merchant de betaalgegevens moeten opslaan om later de capturing van de creditcardbetalingen te kunnen uitvoeren. Ook is het gebruikelijk dat merchants vastleggen wat zij aan wie hebben verkocht, mogelijk met vermelding van de gebruikte betaalmiddelen. Deze gegevensverzamelingen dienen adequaat te worden afgeschermd tegen toegang vanaf het Internet[1].

Het risico bestaat dat onbevoegden kennisnemen van bij merchants opgeslagen creditcardgegevens.

3 Capture betalingen
Een ander onderscheid met de niet-elektronische betaalwijze is dat de merchant niet beschikt over een door de cardholder getekende vastlegging van de betaling. De cardholder heeft op zijn beurt geen betaalbewijs, vergelijkbaar met de doordruk van de creditcardslip of kassabon. De capture van de betaalopdracht vindt plaats op grond van de door de acquirer geregistreerde autorisatie van de betaling. De capture zal echter later plaatsvinden dan het moment waarop de acquirer de transactie heeft goedgekeurd. Aanvullende maatregelen dienen te waarborgen dat alleen betaling plaatsvindt aan de gerechtigde merchant.

Het risico bestaat dat in geval van diefstal van autorisatiegegevens bij een merchant, anderen dan de merchant de capturing van creditcardbetalingen uitvoeren.

Overige stappen
De overige stappen in het betaalproces verlopen zoals eerder beschreven bij niet-elektronische creditcardbetalingen. Ten aanzien van de laatste stap in het betaalproces, de reconciliatie op grond van het afschrift, dient te worden opgemerkt dat veel fraudegevallen pas tijdens de reconciliatie worden ontdekt. De cardholder heeft van betalingen over het Internet echter geen betaalbewijzen waarmee reconciliatie adequaat kan worden uitgevoerd. Ook is een termijn verbonden aan de mogelijkheid betalingen terug te draaien (storneren).

Door het ontbreken van betaalbewijzen van aankopen via het Internet bestaat het risico dat cardholders fraudegevallen niet of te laat ontdekken.

In geval van onrechtmatige afschrijvingen zal de cardholder deze proberen te storneren. De issuer zal dergelijke claims proberen te verhalen op de acquirer. Deze heeft echter geen bewijs dat de cardholder de betaling heeft goedgekeurd. Bij de merchant valt niets te halen omdat deze na de capture van de betaling de goederen vaak al geleverd heeft (zij het niet aan de cardholder).

Samenvattend zijn aan de elektronische betaalwijze de volgende risico's verbonden:
A verlies vertrouwelijkheid en integriteit creditcardgegevens tijdens transport;
B verlies vertrouwelijkheid creditcardgegevens door onzekerheid over de authenticiteit van de merchant en over de transactiemachtiging van de merchant;

1) De zowel beruchte als befaamde computerhacker Kevin Mitnick werd in 1995 gearresteerd en in staat van beschuldiging gesteld voor onder meer de diefstal van 20.000 creditcardnummers van een op Internet actieve onderneming.

C verlies betrouwbaarheid creditcardtransacties door het ontbreken van een handtekening en de daarmee gepaard gaande handtekeningcontrole;
D verlies vertrouwelijkheid creditcardgegevens door onvoldoende beveiligde vastlegging door merchant;
E verlies betrouwbaarheid creditcardtransacties doordat capture van betalingen slechts op grond van goedgekeurde autorisatieverzoeken plaatsvindt;
F verlies betrouwbaarheid creditcardtransacties omdat reconciliatie niet adequaat kan worden uitgevoerd en hierdoor mogelijk fouten niet worden ontdekt.

Uit het bovenstaande kan worden geconcludeerd dat creditcardbetalingen over het Internet aanzienlijk minder waarborgen bieden dan de traditionele niet-elektronische betaalwijze. Daarnaast heeft de cardholder na een aankoop via het Internet weinig zekerheid dat de merchant na ontvangst van de betaling over zal gaan tot de levering van de bestelde artikelen.

Secure Electronic Transaction

Inleiding

Het SET-protocol vormt de basis van de koppeling van bestaande financiële infrastructuren voor clearing en autorisatie van creditcardtransacties met het Internet. Het protocol is ontwikkeld in een gezamenlijke inspanning van Visa en MasterCard, in samenwerking met organisaties als IBM, Netscape, SAIC, RSA, VeriSign en Microsoft. De eerste productiestandaard van SET, versie 1.0, is vrijgegeven op 31 mei 1997. Deze versie richt zich op betalingen met creditcards. Versie 2.0 is in de zomer van 1998 beschikbaar gekomen en biedt tevens de mogelijkheid tot on-linebetalingen met pinpassen.

De betrokkenheid van IBM bij de ontwikkeling van SET heeft geresulteerd in de consolidatie van veel door IBM ontwikkelde technologieën in het SET-protocol, zoals het Internet Keyed Payments (IKP)-protocol, het Secure Electronic Payment Protocol (SEPP) en Secure Transaction Technology (STT). De betrokkenheid van de creditcardissuers Visa en MasterCard heeft geleid tot een goede aansluiting op de praktijk van de afwikkeling van creditcardtransacties. Zo biedt SET ondersteuning voor een reeks branchespecifieke velden in betaalopdrachten, zoals voor het achteraf in rekening brengen van kosten voor de minibar in hotels, voor fooien in restaurants of voor brandstofkosten bij autoverhuurbedrijven.

SET-specificatie

De SET 1.0-specificatie telt circa 1300 pagina's. In een poging de SET-specificatie inzichtelijk te houden is deze vastgelegd in drie boeken. De boeken zijn in digitale vorm via het Internet verkrijgbaar ([SET97abc]). Het eerste boek richt zich op niet-ingewijden in public key cryptografie en betaalsystemen en bevat achtergrondinformatie en processchema's. Het tweede boek richt zich op softwareontwikkelaars en bevat de technische specificaties van het SET-protocol. Het derde boek richt zich onder meer op cryptografen en systeemprogrammeurs ter ondersteuning van beveiligingsanalyses, respectievelijk de bouw van SET-componenten in besturingssystemen.

Scope

De SET-specificatie richt zich op de stappen 1 (Betaalopdracht), 2 (Autorisatie betaling) en 3 (Capture van betalingen), zoals deze eerder in dit artikel zijn beschreven. De specificatie beschrijft voor deze stappen zowel de berichtformaten als de interactie tussen de betrokken partijen. Als transportprotocol kan zowel gebruikgemaakt worden van HTTP (WWW-pagina's), SMTP (Internet-mail) als TCP (datapakketten). SET schrijft tevens voor op welke wijze cryptografische algoritmen als RSA en DES moeten worden toegepast (zie bijlage 2 'Cryptografie in SET'). Daarnaast definieert SET een aantal opties, zoals de optie voor het informeren naar de status van de betaling (order inquiry).
Voor de berichtenuitwisseling in de stappen 4 tot en met 7 wordt gebruikgemaakt van de bestaande standaarden voor autorisatie, capture, clearing en rapportage (afschriften). De protocollen ter ondersteuning van het aankoopproces vallen eveneens buiten de scope van SET.

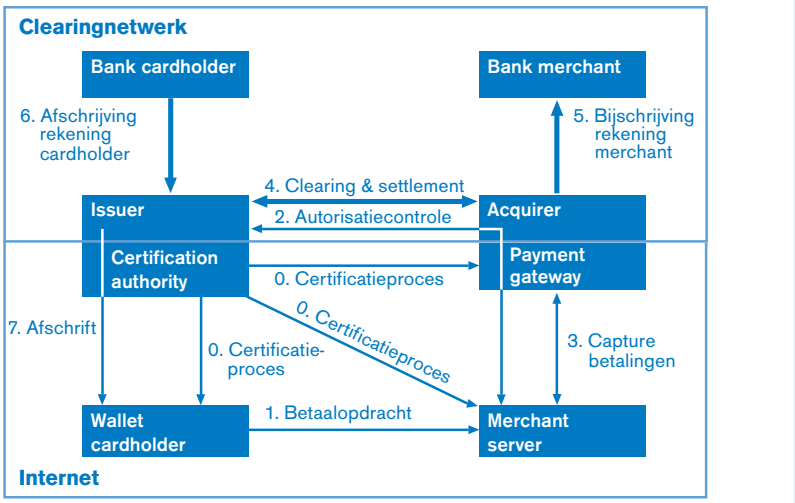
Maatregelen in SET

In de inleiding is een aantal risico's naar voren gebracht die verbonden zijn aan creditcardbetalingen over het Internet. De beveiligingsmaatregelen die in het SET-protocol zijn getroffen, dekken een groot deel van deze risico's af. Deze maatregelen worden hieronder kort toegelicht:
* Tijdens het transport van SET-berichten over het Internet wordt door middel van public key encryptie de vertrouwelijkheid van transactiegegevens gewaarborgd.
* Met digitale handtekeningen wordt de authenticiteit van berichten van de betrokken partijen gewaarborgd.
* Door de 'vingerafdrukken' van elk SET-bericht voor en na transport te vergelijken wordt de integriteit van de transactiegegevens gewaarborgd.
* Met certificaten kunnen de betrokken partijen aantonen voor welke creditcards deze zijn gemachtigd SET-transacties uit te voeren.
* Door de scheiding van autorisatie-, betaal- en aankoopgegevens krijgen de betrokken partijen alleen inzicht in voor hen relevante gegevens (separation of concern).

Bovengenoemde maatregelen veronderstellen de aanwezigheid van een Public Key Infrastructure (PKI). Voor een korte behandeling van PKI's, certificering en cryptografie in SET wordt verwezen naar de bijlagen van dit artikel. In de zo dadelijk volgende beschrijving van SET-transacties worden deze maatregelen in het kader van de leesbaarheid niet per bericht herhaald.

Rollen

Eerder in dit artikel zijn de rollen beschreven van de bij creditcardtransacties betrokken partijen. In SET worden twee nieuwe rollen gedefinieerd: de *payment gateway* en de *certification authority*, vaak afgekort met CA. De payment gateway verwerkt SET-berichten die vanaf het Internet worden ontvangen tot standaardberichtformaten van de acquirer en stuurt deze door naar het clearingnetwerk, en vice versa. De payment gateway fungeert dus als doorgeefluik. De CA geeft certificaten uit die nodig zijn als bewijs dat de bij SET-transacties



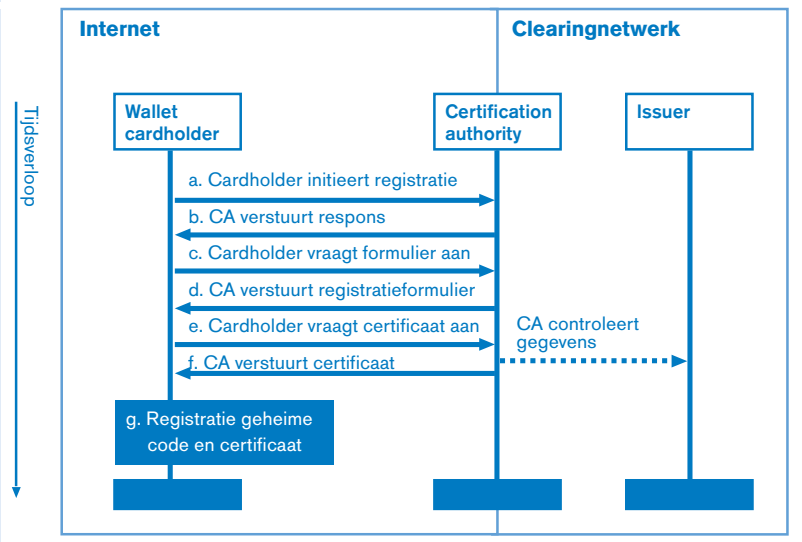
Figuur 3. Elektronische creditcardbetalingen met SET.

betrokken partijen zijn gerechtigd betalingen met een bepaald type creditcard uit te voeren (cardholder), te accepteren (merchant) en te verwerken (payment gateway). In bijlage 3 'Certificatie in SET' wordt ingegaan op de rol van de CA's en de verschillende soorten certificaten in het SET-protocol.

SET-transacties

Deze subparagraaf behandelt de wijze waarop de eerder beschreven risico's die zijn verbonden aan creditcardbetalingen over het Internet, in het SET-protocol zijn afgedekt.

In figuur 3 zijn de belangrijkste stappen in een SET-transactie weergegeven. Uit deze figuur blijkt duidelijk de overeenkomst met de eerder beschreven betaalwijzen. Het belangrijkste onderscheid met figuur 2 betreft de vorm (wallet en merchant server) waarin de cardholder respectievelijk de merchant zich presenteert en de rollen van de CA en payment gateway. De wallet is een programma waarmee de cardholder SET-transacties kan uitvoeren. De merchant server is een computersysteem dat is ingericht voor het afhandelen van SET-transacties voor de merchant.



Figuur 4. Stap 0 in een SET-transactie: het certificatieproces van een cardholder.

0 Certificatieproces

Voordat de cardholder, merchant en payment gateway kunnen participeren in een SET-transactie dienen zij te zijn voorzien van een certificaat. In figuur 3 is weergegeven dat de CA deze certificaten verspreidt. De CA stelt een aantal voorwaarden aan het verstrekken van een certificaat, zodat sprake is van een certificatieproces. Ter illustratie wordt het on-linecertificatieproces voor de cardholder kort toegelicht.

In figuur 4 is stap 0 (Certificatieproces) van een SET-transactie schematisch weergegeven. De verticale lijnen representeren de bij het certificatieproces betrokken partijen in de tijd bezien. De tijd verstrijkt van boven naar beneden. De horizontale pijlen representeren berichten die tussen partijen worden verstuurd. De rechthoeken representeren belangrijke registraties die de partijen uitvoeren. In de figuur is onderscheid gemaakt tussen SET-berichten (doorgetrokken pijlen) en berichten in het standaardformaat van de bestaande financiële infrastructuur van de acquirer, issuer en andere betrokkenen (gestippelde pijlen). Deze protocollen vallen buiten het bestek van dit artikel en zullen niet nader worden toegelicht.

a *Cardholder initieert registratie*
De wallet van de cardholder stuurt, bijvoorbeeld tijdens de installatieprocedure van de wallet, aan de CA een verzoek voor haar certificaten. Deze certificaten zijn nodig voor de beveiliging van de berichtenuitwisseling in de volgende stappen.

b *CA verstuurt respons*
De CA stuurt de cardholder haar certificaten, één voor het zetten van digitale handtekeningen en één voor het uitwisselen van encryptiesleutels.

c *Cardholder vraagt registratieformulier aan*
Omdat dit formulier per soort creditcard kan verschillen, stuurt de wallet de CA een verzoek voor het registratieformulier, inclusief het nummer van de creditcard.

d *CA verstuurt registratieformulier*
De CA stuurt het formulier onversleuteld naar de cardholder. Eventuele wijzigingen tijdens het transport worden door de standaard integriteitscontrole ontdekt.

e *Cardholder vraagt certificaat aan*
De cardholder genereert met de wallet een sleutelpaar, vult het formulier in en verstuurt dit. De wallet voegt de net gegenereerde publieke sleutel van de cardholder, een sleutel voor de beveiliging van het te ontvangen certificaat en een aselect gekozen nummer aan het bericht toe. De creditcardgegevens van de cardholder worden apart versleuteld en aan het bericht toegevoegd. De CA controleert de creditcardgegevens en de inhoud van het registratieformulier met het ledenbestand van de issuer.

f *CA verstuurt certificaat*
Als de gegevens correct zijn en de cardholder voldoet aan de gestelde criteria, dan stelt de CA een certificaat samen met onder meer de publieke sleutel van de cardholder. Hiertoe kiest de CA aselect een nummer, combineert dit met het door de cardholder gekozen nummer om een geheime waarde te creëren. De com-

binatie van de geheime waarde en de creditcardgegevens wordt met een hashfunctie gecodeerd en in het certificaat opgenomen. Het certificaat wordt door de CA voorzien van haar digitale handtekening. Hierop genereert de CA een SET-bericht met het aselecte nummer van de CA en gegevens over het type creditcard, versleutelt dit met de sleutel uit stap e en verstuurt het bericht samen met het getekende certificaat naar de cardholder.

g *Cardholder registreert certificaat en geheime code*
De wallet ontsluit de gegevens uit het ontvangen bericht met de sleutel uit stap e. De wallet slaat de geheime waarde en het certificaat van de cardholder op voor later gebruik in het betaalproces.

Kenmerkend voor het certificatieproces van een cardholder is het samenstellen van de geheime waarde. De geheime waarde is een aanvullende maatregel ter autorisatie van de cardholder. De cardholder dient immers in het bezit te zijn van enerzijds de bij het certificaat behorende geheime sleutel voor het plaatsen van digitale handtekeningen en anderzijds de geheime code als bewijs dat het certificaat aan hem toebehoort. De geheime code is dus te vergelijken met de viercijferige geheime code van pinpassen.

Het certificatieproces van merchants en payment gateways verloopt vrijwel gelijk aan het hierboven beschreven proces, maar onderscheidt zich op twee belangrijke punten:

* De merchant en de payment gateway ontvangen twee certificaten, één voor het zetten van digitale handtekeningen en één voor het uitwisselen van encryptiesleutels.
* In tegenstelling tot het volledig on-linecertificatieproces van cardholders zal het certificatieproces van merchants en payment gateways stringente off-linecontroles bevatten.

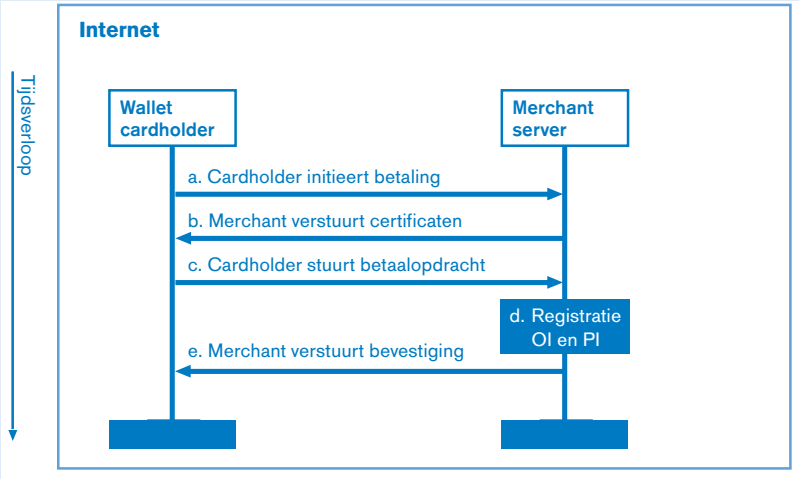
Samenvattend bieden de op een PKI gebaseerde maatregelen waarborgen omtrent de integriteit en vertrouwelijkheid van betaalgegevens tijdens transport. Tevens biedt SET zekerheid over de authenticiteit van de betrokken partijen door middel van digitale handtekeningen. Hiermee zijn de risico's A, B en C uit de paragraaf 'Transacties zonder SET' afgedekt.

1 Betaalopdracht

Een SET-transactie start nadat de cardholder zijn aankoop heeft vastgelegd. Het aankoopproces verloopt op vrijwel dezelfde wijze als beschreven bij de betaalwijze met creditcards over het Internet. In figuur 5 is stap 1 van een SET-transactie, de betaalopdracht, schematisch weergegeven.

a *Cardholder initieert betaling*
Nadat de aankoop is vastgelegd, geeft de cardholder aan te willen betalen via een SET-transactie. Hierdoor wordt de walletsoftware geactiveerd en geeft de cardholder aan welk type creditcard voor de betaling zal worden gebruikt. De wallet genereert hierop een SET-bericht ter initiatie van de betaling en verstuurt dit naar de merchant.

b *Merchant verstuurt certificaten*
Als reactie op de ontvangst van de initiatie door de cardholder verstuurt de merchant server een bericht met de certificaten van zichzelf en van de payment gateway die betalingen met het opgegeven type creditcard accepteert. Het laatste certificaat wordt benut voor de veilige overdracht van creditcardgegevens naar de payment gateway, zonder dat de merchant deze kan lezen. Tevens bevat de respons een transactienummer.



Figuur 5. Stap 1 in een SET-transactie: de betaalopdracht.

c *Cardholder stuurt betaalopdracht*
De wallet van de cardholder stuurt na ontvangst van de certificaten van de merchant en de payment gateway de betaalopdracht naar de merchant. Het SET-bericht voor een betaalopdracht is verdeeld in twee delen. Het eerste deel, de *Order Instruction (OI)*, is bestemd voor de merchant en het tweede deel, de *Payment Instruction (PI)*, is bestemd voor de payment gateway. De OI wordt gegenereerd op grond van gegevens uit het aankoopproces, waaronder het totaalbedrag. De PI bevat gegevens van de creditcard die voor de betaling zal worden gebruikt, zoals de geheime code (zie stap 0). De OI en PI worden met elkaar verbonden door beide te voorzien van het transactienummer. Om ook de OI en PI met elkaar in verband te kunnen brengen zonder de berichten te kunnen lezen, wordt een *dual signature* meegestuurd. Dit is een versleuteld samenstel van de 'vingerafdrukken' van beide berichten. De PI wordt zodanig versleuteld dat alleen de payment gateway deze kan lezen. Het geheel van de OI, de versleutelde PI en de dual signature wordt naar de merchant verstuurd.

d *Merchant registreert OI en PI*
De merchant controleert na ontvangst van de betaalopdracht de ontvangen dual signature met de ontvangen OI en PI. Na deze controle worden de OI, PI en dual signature door de merchant opgeslagen voor de autorisatiecontrole later in het betaalproces.

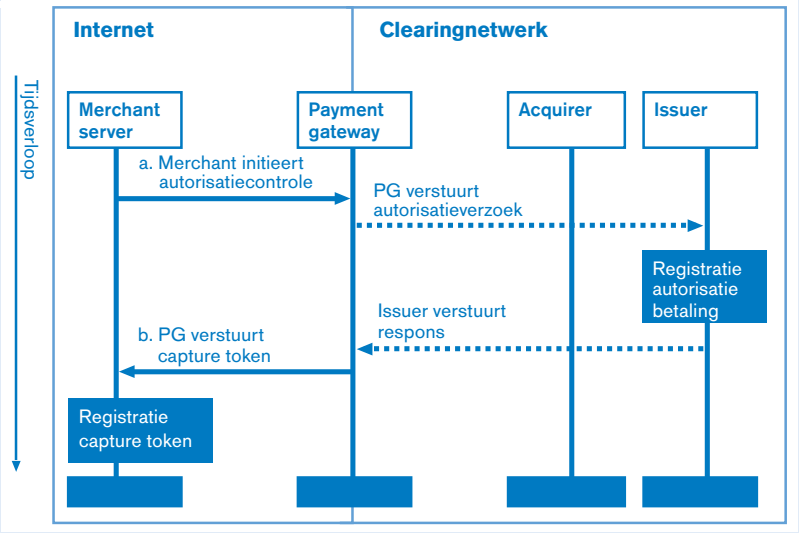
e *Merchant verstuurt bevestiging*
De merchant stuurt de cardholder een bevestiging dat de betaalopdracht zal worden uitgevoerd, mits de issuer de betaling autoriseert.

Deze stap in een SET-transactie kenmerkt zich door de scheiding tussen OI en PI in de betaalopdracht, zodanig dat de PI alleen leesbaar is door de payment gateway. Hierdoor komt een merchant nooit in het bezit van de creditcardgegevens van een cardholder. De OI en PI hebben echter los van elkaar geen waarde. Daarom worden de berichten met elkaar in verband gebracht door het transactienummer en de dual signature.

Samenvattend biedt SET door de afscherming van betaalgegevens voor merchants waarborgen omtrent de vertrouwelijkheid van deze gegevens. Hiermee is risico D uit de paragraaf 'Transacties zonder SET' afgedekt.

2 Autorisatiecontrole

De merchant is vrij in het kiezen van het moment waarop de autorisatiecontrole plaatsvindt. De controle kan gelijktijdig met stap 1e worden uitgevoerd of pas nadat de bevestiging is verstuurd. In figuur 6 is stap 2 van een SET-transactie, de autorisatiecontrole, schematisch weergegeven.



Figuur 6.
Stap 2 in een SET-transactie: de autorisatiecontrole.

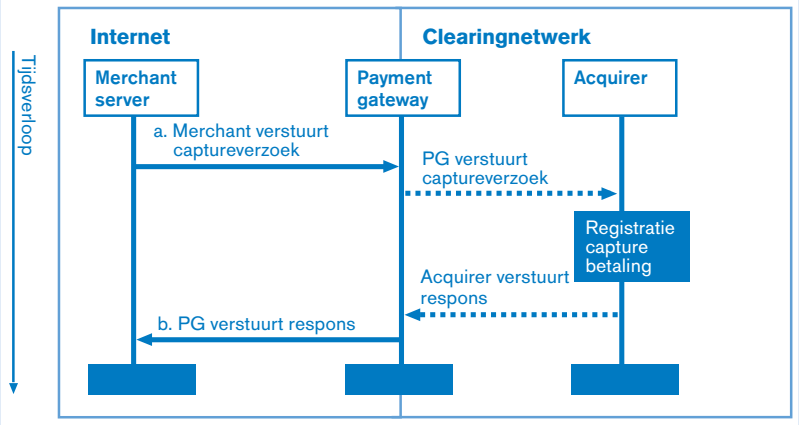
a *Merchant initieert autorisatiecontrole*
De merchant stelt een autorisatieverzoek samen op grond van de gegevens in de OI. Dit wordt tezamen met de PI en de certificaten van de merchant en de betreffende cardholder naar de payment gateway verstuurd.
De payment gateway ontsluit het autorisatieverzoek uit het versleutelde SET-bericht en controleert de consistentie tussen de autorisatiegegevens en de PI. Tevens controleert de payment gateway de dual signature met het samenstel van de OI-vingerafdruk uit het autorisatieverzoek en de PI. De payment gateway selecteert op grond van de door de cardholder gebruikte creditcard het clearing- en autorisatienetwerk van de betreffende issuer. Met de creditcardgegevens uit de PI en de ordergegevens uit het autorisatieverzoek stelt de payment gateway een autorisatieverzoek samen en verstuurt dit met het voor dit netwerk gebruikelijke berichtformaat en protocol. De issuer controleert na ontvangst van het autorisatieverzoek onder meer de kredietlimiet van de cardholder en betalingsachterstanden. Na goedkeuring van het verzoek brengt de issuer het betreffende bedrag als reservering in mindering op het krediet van de creditcard. Tevens worden de autorisatiegegevens, zoals het bedrag en de merchant die het bedrag heeft gereserveerd, door de issuer geregistreerd. Deze gegevens dienen overeen te komen met de gegevens van de capture van de betaling in een later stadium van de SET-transactie.

b *Payment gateway verstuurt autorisatietoken*
Als het verzoek door de issuer is goedgekeurd, stelt de payment gateway een SET-bericht samen, bestaande uit een autorisatiebevestiging en een 'capture token'. Het capture token bevat onder meer de betaalgegevens en is niet leesbaar voor de merchant. De payment gateway verstuurt vervolgens het bericht naar de merchant. De merchant ontsluit de gegevens uit het versleutelde SET-bericht en registreert het capture token. Met het token is de merchant gemachtigd de payment gateway in een later stadium te verzoeken om tot betaling over te gaan.

Deze stap in een SET-transactie kenmerkt zich door het capture token, dat dient als een digitaal equivalent van de getekende creditcardslips of aankoopbonnen zoals beschreven in de paragraaf 'Transacties zonder SET'. Hierdoor vindt de capturing van creditcardbetalingen plaats op grond van enerzijds de registratie van de issuer en anderzijds de registratie van de merchant in de vorm van capture tokens.
Samenvattend biedt SET door de aparte registratie van capture tokens door de merchant waarborgen omtrent de betrouwbaarheid van SET-transacties. Hiermee is risico E uit de paragraaf 'Transacties zonder SET' afgedekt.

3 Capture betalingen

Na de autorisatie van de betaling zal de merchant overgaan tot de capture van het betreffende aankoopbedrag. In figuur 7 is stap 3 van een SET-transactie, de capture van de betaling, schematisch weergegeven.



Figuur 7.
Stap 3 in een SET-transactie: de capture van de betaling.

a *Merchant verstuurt captureverzoek*
De merchant stelt een captureverzoek samen op grond van onder meer het te innen bedrag en het transactienummer. Dit wordt tezamen met het capture token en de certificaten van de merchant naar de payment gateway verstuurd.
De payment gateway ontsluit het captureverzoek uit het versleutelde SET-bericht en controleert de consistentie tussen het captureverzoek en de inhoud van het capture token. De payment gateway geeft na deze controles via het clearingnetwerk het captureverzoek door aan de acquirer. De acquirer controleert na ontvangst van het captureverzoek of de capturegegevens overeenkomen met een eerder geautoriseerde betaling. Na deze controle registreert de acquirer de wijziging in de positie van het met de issuer te vereffenen bedrag.

b *Payment gateway verstuurt respons*
Nadat de acquirer de capture heeft vastgelegd, stelt deze een capture respons samen en verstuurt deze via de payment gateway naar de merchant. De merchant zal de ontvangen capture responses opslaan ter controle van de ontvangsten. De capture responses gelden ook als schuldbekentenis van de acquirer totdat de ontvangsten zijn geboekt.

Overige stappen

De overige stappen in het betaalproces verlopen zoals de eerder beschreven betaalwijzen zonder gebruik te maken van het SET-protocol.

Ten aanzien van de laatste stap in het betaalproces, de reconciliatie op grond van het afschrift, dient te worden opgemerkt dat SET niet voorziet in maatregelen die risico F volledig afdekken. SET voorziet in digitale betaalbewijzen, waarmee de reconciliatie door de cardholder adequaat kan worden uitgevoerd. De reconciliatie vindt echter nog steeds handmatig plaats omdat de gegevens van de maandelijkse afschriften moeten worden vergeleken met de gegevens in de wallet. Hierbij bestaat het risico dat de cardholder fouten maakt.
Enkele onderzoekers hebben een voorstel gedaan voor een deels geautomatiseerde reconciliatie in SET ([Hwan98]). Met deze methode wordt door de wallet per SET-transactie een unieke code aan de merchant doorgegeven. De merchant geeft deze code door aan de issuer, die de codes op de maandelijkse afschriften vermeldt. De cardholder kan vervolgens de codes en de bedragen van elk afschrift in de wallet invoeren, waarna de wallet deze automatisch vergelijkt met de overeenkomstige betalingen.

Als afsluiting van deze paragraaf worden de kenmerken van SET nog eens op een rijtje gezet:
* behoud vertrouwelijkheid en integriteit creditcardgegevens tijdens transport;
* zekerheid over de (lever)betrouwbaarheid en transactiemachtiging van de merchant;
* zekerheid over de authenticiteit van de betrokkenen en de autorisatie van betalingen;
* afscherming van creditcardgegevens voor de merchant;
* capture van betalingen op grond van vastleggingen van zowel de merchant als de issuer;
* reconciliatie op basis van de vastlegging van betalingen door de cardholder.

Stand van zaken

In de vakliteratuur en de pers is al veel geschreven over het SET-protocol. Met regelmaat is bericht over geslaagde pilotprojecten voor betalingen via het Internet op basis van SET. Ook was te lezen dat grote financiële instellingen en softwarehuizen veel tijd en geld hebben geïnvesteerd in de ontwikkeling van SET-toepassingen. Toch blijkt dat anderhalf jaar na de publicatie van de SET-standaard de brede invoering van het SET-protocol nog geen realiteit is. In deze slotparagraaf worden enkele kanttekeningen geplaatst bij het protocol en de invoering ervan, die mogelijk debet zijn aan deze vertraging.

Integriteit PC cardholder

De zwakke schakel in het SET-protocol is niet zozeer het protocol zelf, als wel de inbedding van het protocol in zijn omgeving: de belangrijkste randvoorwaarde voor de betrouwbare werking van het SET-protocol is de integriteit van de computersystemen waarop SET-applicaties draaien. De specificatie van SET geeft geen beveiligingsrichtlijnen om virussen, trojan horses en hackers van de systemen van betrokken partijen te weren. De Compact-edities 1994/2 (firewalls) en 1998/4 (veilige EC-oplossingen) geven een reeks handvatten voor de beveiliging van Internet-koppelingen en EC-toepassingen.
In het bijzonder is het onmogelijk de integriteit van de PC van de cardholder te waarborgen. De PC kent geen beveiligingsconcept zoals we dit kennen van veel besturingssystemen, waarmee gebruikers en programma's rechten en (file)permissies worden toegewezen. Daarnaast heeft de cardholder vaak een open verbinding met het Internet, zonder dat deze wordt beschermd door een firewall. Hierdoor is de PC blootgesteld aan de gevaren van het Internet, zoals virussen en hackers. Het is niet ondenkbaar dat de PC besmet wordt met een zorgvuldig ontworpen virus dat bijvoorbeeld de walletsoftware aantast en de creditcardgegevens naar een locatie op het Internet verstuurt.[2]

2) De door het tijdschrift 'Computer Idee' beschreven kraak van de Rabobank Internetbankieren website is gebaseerd op een computervirus dat de met SSL beveiligde informatie-uitwisseling met de Rabobank via een nep-Rabobanksite liet verlopen. Deze nep-site modificeerde vervolgens de betaalgegevens.

> Een zorgvuldig ontworpen virus kan de walletsoftware aantasten.

Nieuwe ontwikkelingen: C-SET en SET versie 2.0

Elke standaard is voor verbetering vatbaar. Zo ondersteunt versie 1.0 van SET alleen creditcardbetalingen. Versie 2.0 van het protocol biedt tevens ondersteuning voor smartcards en pinpassen. De release wordt halverwege 1999 verwacht. Sommigen verwachten nu al een vertraging van SET 2.0 omdat men denkt dat geen haast zal worden gemaakt met een nieuwe standaard indien de oude zich nog niet heeft bewezen.
Om de PC als zwakke schakel in SET weg te nemen hebben enkele Franse banken een voorstel gedaan voor het C-SET (Chip-Secured Electronic Transaction)-protocol. De gedachte achter C-SET is dat de opslag van sleutels en cryptografische berekeningen plaats dient te vinden in een apart resistent apparaat. Met de huidige stand van de technologie is het mogelijk hiervoor smartcards te gebruiken. Door de ontkoppeling van de PC en de 'geheimen' van de cardholder kan deze met zijn smartcard ook met andere computers betalingen verrichten. Hiertoe wordt de smartcard in een aan de PC gekoppelde kaartlezer geplaatst. Om tegen te gaan dat de toegangscode van de smartcard via het toetsenbord van de PC kan worden onderschept, dient de kaartlezer van een apart numeriek toetsenbord te zijn voorzien. C-SET is dus minder afhankelijk van de integriteit van het computersysteem waarmee betalingen worden uitgevoerd.

Complexiteit implementatie

De implementatie van de SET-standaard is complex. De specificatie alleen al telt 1300 pagina's. Banken en merchants ervaren veel problemen met de implementatie van de standaard. Ongeveer twintig softwareleveranciers hebben zich gestort op de ontwikkeling van SET-programmatuur, zoals wallets en software voor merchant servers, payment gateways en certification authorities. Teneinde de interoperabiliteit van verschillende SET-implementaties te kunnen waarborgen worden deze door de promotor van SET, de SETCo, onderworpen aan uitgebreide compliance tests. Deze compliance tests hebben het karakter van een verplichte certificering. Zonder certificaat mag met de implementaties niet aan het SET-verkeer worden deelgenomen. SETCo heeft de certificering uitbesteed aan Tenth Mountain Systems Inc. Omdat dit het enige bedrijf is dat de compliance tests mag uitvoeren, verloopt de certificering traag. Tot op heden hebben slechts enkele leveranciers het certificaat mogen ontvangen.

Complexiteit gebruik

Het gebruik van SET wordt door cardholders als complex ervaren. De risico's bij de huidige elektronische betaalmethoden met creditcards wegen voor de cardholder niet op tegen de moeite van het downloaden en installeren van walletsoftware en het aanvragen van certificaten bij een CA. Daarnaast is het concept van een PKI voor velen niet intuïtief te doorgronden. De huidige gebruikers zijn dan ook geen doorsnee cardholders. Vergelijkbaar met de introductie van de pinautomaten zal het enige tijd vergen voordat het 'brede publiek' vertrouwd raakt met begrippen als certificaten, sleutelparen en digitale handtekeningen. Per land is het succes van SET sterk afhankelijk van de PC-penetratiegraad en het Internet-gebruik.

Interesse

De interesse bij cardholders voor SET is niet groot. De risico's van het doen van aankopen via het Internet zijn voor cardholders beperkt. Met SSL, gerenommeerde merchants en kleine aankopen kan de cardholder best zonder SET. Daarnaast kenmerken SET-pilots zich door een matige interesse van merchants. Merchants voelen er niet veel voor om te investeren in non-proven technology. In veel landen is voor merchants een Point of Presence op het Internet nog een noviteit. De stap naar een op SET gebaseerde cybershop is voor deze groep te groot.

Kosten

Het gebruik van creditcards voor relatief kleine aankopen is erg duur. De kosten bedragen gemiddeld drie gulden vanwege de in de Verenigde Staten gecentraliseerde verwerking van creditcardbetalingen en de toeslag per transactie voor verzekeringen. Ter illustratie: transacties met pinpassen kosten enkele centen per keer. Daarnaast vergt de gelaagde beveiliging in SET relatief veel processorcapaciteit voor cryptografische berekeningen en bandbreedte voor het uitwisselen van berichten met de diverse bij een SET-transactie betrokken partijen

Certification Authorities

De hiërarchie van CA's begint gestalte te krijgen met het besluit het rootcertificaat (zie bijlage 3 'Certificatie in SET') in beheer te geven van SETCo. De richtlijnen rondom het verstrekken van certificaten zijn reeds vastgesteld, de richtlijnen rondom het intrekken van certificaten echter nog niet. Daarnaast resteren nog vragen als:

* Dient een cardholder na diefstal van zijn kaart een nieuw certificaat aan te vragen?
* Hoeveel certificaten heeft een persoon nodig: één per kaart, één per bank?
* Zijn meerdere certificaten per kaart mogelijk om betaling vanaf meerdere computers mogelijk te maken?
* Indien certificaten voor meerdere kaarten zijn te gebruiken, welke afspraken dienen dan tussen concurrerende banken te worden gemaakt over de verstrekking van certificaten voor elkaars kaarten?
* Wie betaalt voor fraude met het SET-protocol? Vaak betaalt de issuer de schade, maar in Europa raden zelfs Visa en MasterCard af SET versie 1.0 te gebruiken voor creditcardbetalingen om claims door cardholders tegen te gaan.

Conclusie

Uit het artikel kan worden geconcludeerd dat het SET-protocol evenveel of meer waarborgen biedt dan de traditionele niet-elektronische betaalwijze met creditcards. Tevens worden met SET de risico's van huidige betaalmethoden via het Internet sterk gereduceerd. Nu staat een aantal technologische en organisatorische hindernissen de brede invoering van SET nog in de weg. De verdere ontwikkeling van het protocol en de voortschrijdende regulering van het SET-verkeer maken echter binnen afzienbare tijd secure electronic transactions tot werkelijkheid.

Literatuur

[Hwan98]
Jing-Jang Hwang and Sue-Chen Hsueh, *Greater protection for credit card holders: a revised SET protocol*, Computers Standards & Interfaces 19, 1998, p. 1-8.

[SET97a]
Secure Electronic Transaction (SET) specification, Book 1: Business Description, version 1.0, May 1997.

[SET97b]
Secure Electronic Transaction (SET) specification, Book 2: Programmer's Guide, version 1.0, May 1997.

[SET97c]
Secure Electronic Transaction (SET) specification, Book 3: Formal Protocol Definition, version 1.0, May 1997.

Bijlagen

Bijlage 1 SSL versus SET

Secure Sockets Layer (SSL) versie 3.0 is de de-factostandaard voor het versleutelen van webpagina's. SSL is een zogenaamd transportbeveiligingsmechanisme: het verzorgt een cryptografisch beveiligde pijpleiding tussen bijvoorbeeld de browser van de cardholder en de webserver van de merchant.

De beveiliging van een SSL-verbinding is gebaseerd op de in de browser opgeslagen SSL-certificaten. Door de data met de publieke sleutels uit de certificaten te versleutelen is gewaarborgd dat alleen de houders van deze certificaten de data kunnen lezen. Indien een creditcardbetaling plaatsvindt over een met SSL beveiligde verbinding heeft de merchant nog steeds geen zekerheid over de authenticiteit van de cardholder. In SET is dit probleem opgelost door gebruik te maken van twee certificaten: één voor de beveiliging van gegevens (Key-Exchange Key Certificate) en één om digitale handtekeningen te plaatsen (Signature Key Certificate).

Om waarde te kunnen hechten aan certificaten van cardholders, merchants en payment gateways dienen deze te worden getekend door Certification Authorities (zie bijlage 3 'Certificatie in SET'). SSL-certificaten worden uitgegeven door diverse organisaties die geen eenduidig beleid hebben voor de uitgifte, de verificatie en het intrekken van certificaten.

SSL maakt gebruik van 40-, 56- of 128-bits-encryptie. De eerste twee encryptievormen zijn met de huidige stand van de techniek in ruim een week te kraken en dus onvoldoende voor het waarborgen van de vertrouwelijkheid van creditcardgegevens. De sterke 128-bits-encryptie is vrijwel niet te kraken, maar het gebruik ervan is door exportbeperkingen van de Amerikaanse overheid aan banden gelegd. SET maakt gebruik van 160-bits-encryptie voor een beperkte hoeveelheid 'financiële' velden in SET-berichten. Hierdoor is deze toepassing van sterke encryptie niet in strijd met de geldende exportbepalingen.

In een SET-transactie worden betaal- en aankoopgegevens van elkaar gescheiden, zodat alleen de payment gateway kan beschikken over de betaalgegevens. Met SSL is een dergelijk onderscheid niet te maken, waardoor ook de merchant in het bezit komt van de betaalgegevens. Hierdoor bestaat het risico dat de creditcardgegevens niet goed worden beheerd en in verkeerde handen vallen.

Ten slotte valt of staat de beveiliging van zowel SSL als SET met de integriteit van het computersysteem waarmee betalingen worden uitgevoerd. Zowel SSL (denk aan de kraak van de Rabobank Internetbankieren website) als SET is gevoelig voor virussen of trojans die de beveiligingsmaatregelen in de protocollen ongedaan maken.

Bijlage 2 Cryptografie in SET

Het SET-protocol combineert een aantal cryptografische technieken om de vertrouwelijkheid, integriteit en authenticiteit van de berichtenuitwisseling in SET te waarborgen. Voor een gedetailleerde toelichting op de in SET gebruikte cryptografische technieken wordt verwezen naar de bijlagen in 'Oplossingen voor veilige electronic commerce over Internet' van R.L. Moonen in Compact 1998/4.

Kort gezegd is (*symmetric key*) encryptie de transformatie van data in een, voor iedereen zonder een encryptiesleutel, onleesbare vorm. Hiermee is de vertrouwelijkheid van data tijdens het transport over een openbaar netwerk zoals het Internet gewaarborgd, mits de sleutel niet in verkeerde handen valt. Om dit laatste tegen te gaan maakt SET gebruik van een combinatie van symmetric key encryptie en *asymmetric* ofwel *public key* encryptie. Bij de laatste techniek wordt een combinatie van privé- en publieke encryptiesleutels gebruikt. De mathematische relatie tussen beide sleutels garandeert dat berichten die zijn versleuteld met de privé-sleutel alleen kunnen worden gelezen door iemand die in het bezit is van de publieke sleutel, en vice versa. Public key encryptie is in verhouding tot secret key encryptie rekenintensief en dus langzaam. Daarom worden in SET alle

Figuur 8.
Schematische weergave van het encryptie- en decryptieproces in SET.

berichten versleuteld met secret key encryptie en wordt alleen van public key encryptie gebruikgemaakt voor de uitwisseling van geheime encryptiesleutels en creditcardgegevens.

SET voorziet per bericht in een integriteitscontrole en een digitale handtekening. Hiertoe wordt van elk bericht met het hashingalgoritme SHA-1 een Message Authentication Code (MAC) berekend. Deze MAC wordt vervolgens versleuteld met de geheime sleutel van de afzender. Deze code wordt door de ontvanger uitgepakt met de publieke sleutel van de afzender en vergeleken met de MAC van het ontvangen bericht. Hiermee is de ontvanger zeker van de authenticiteit en de integriteit van het bericht.

Figuur 8 geeft een vereenvoudigde schematische weergave van de stappen in het encryptie- en decryptieproces in SET. Dit proces is gelijk voor de uitwisseling van elk SET-bericht tussen de bij SET-transacties betrokken partijen.

Bijlage 3 Certificatie in SET

Een voorwaarde voor het gebruik van public key encryptie is dat elke partij in het bezit is van een privé- en een publieke sleutel. Daarnaast dient elke partij in staat te worden gesteld de publieke sleutel te publiceren en te distribueren. Hiertoe wordt een Public Key Infrastructure ingericht. In een PKI worden publieke sleutels gepubliceerd door deze bij een certification authority (CA) te registreren. Dit is een instantie die de toewijzing van publieke sleutels aan partijen beheert en certificaten uitreikt waarin de publieke sleutel en gegevens over de bezitter zijn opgenomen. Deze certificaten worden door de uitgevende CA van een digitale handtekening voorzien.

Met de publieke sleutel van de CA kan een certificaat worden gecontroleerd op authenticiteit, ofwel kan worden gecontroleerd of de CA 'garant staat' voor de eigenaar van het certificaat. Omdat in SET per type creditcard een CA nodig is, dienen de certificaten van deze CA's te worden getekend door een overkoepelende CA. Hetzelfde geldt voor bijvoorbeeld landsgrenzen overstijgende CA's. Zo ontstaat een vertrouwensstructuur tussen CA's, waarbij een 'super-CA' met een zogenaamd rootcertificaat de certificaten van de CA's op het hoogste niveau heeft getekend.

Omdat in SET aan het verlenen van een certificaat aan een payment gateway strengere eisen worden gesteld dan aan een merchant, waarvoor weer strengere eisen gelden dan voor een cardholder, zijn in SET twee methoden in gebruik voor de verstrekking van certificaten. De methode voor de cardholder voorziet, vanwege het beperkte risico, in een on line-aanvraagprocedure, waarbij het certificaat direct beschikbaar wordt gesteld. De methode voor merchants vergt stringente off-linecontroles, zoals de toetsing van kredietwaardigheid, betalingsachterstanden en leverbetrouwbaarheid. Het certificaat voor payment gateways dient alleen te worden verstrekt op aanvraag van een erkende acquirer. Deze acquirer zal voor een bepaald bedrag garant moeten kunnen staan, om als payment gateway te mogen fungeren.
De certification authority kan de issuer zelf zijn of een derde partij waaraan deze diensten door één of meer issuers zijn uitbesteed. Naast een computersysteem dat certificaten verspreidt is dus sprake van een orgaan dat aanvullende controles uitvoert tijdens de certificatie van merchants en payment gateways.

Het certificaat van de cardholder zegt bijvoorbeeld 'deze publieke sleutel is eigendom van Bob en kan worden gebruikt voor betaalkaarten X van Visa en Y van Mastercard. Getekend: certification authority Z'. Dit certificaat bevat niet de creditcardgegevens zelf, maar een vingerafdruk van deze gegevens. De payment gateway berekent de vingerafdruk met de ontvangen creditcardgegevens en geheime waarde van de cardholder en vergelijkt deze met de vingerafdruk van de creditcardgegevens in het certificaat van de cardholder.