- SET -
SECURE ELECTRONIC TRANSACTION

Christof Strauch - Daniel Kuhn

Agenda

- Einleitung & Historie
- Anforderungen & Realisierung
- Vorstellung der Akteure
- Grundlagen (Dual Signature, SET-Transaktionen)
- Payment Process anhand eines Beispiels
- Komplexitätsbetrachtung
- Diskussion & Pressespiegel
- Ausblick

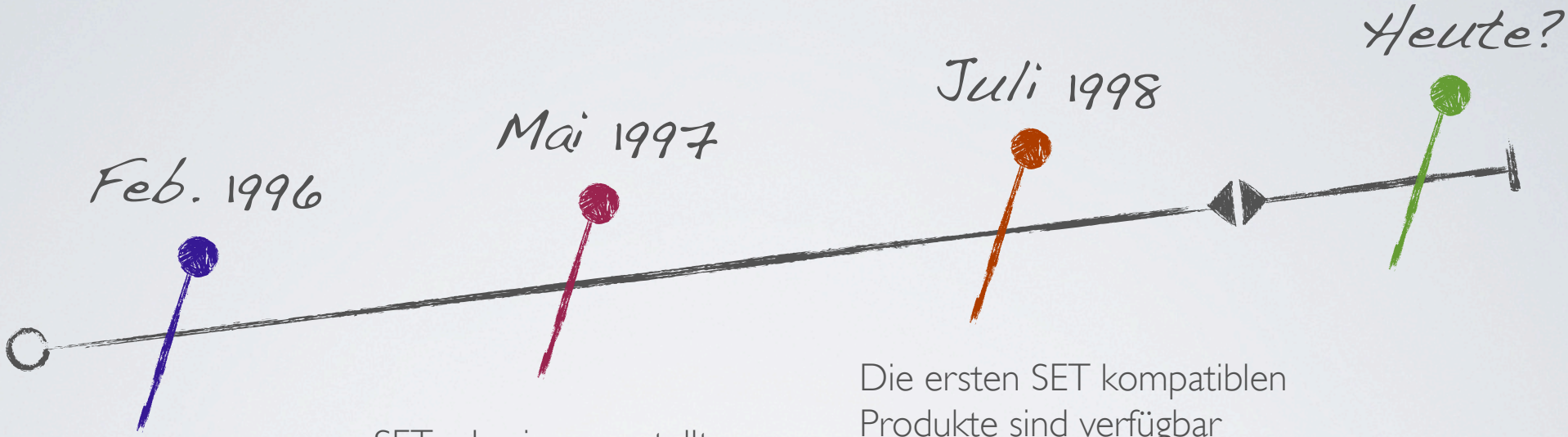
Einleitung

- SET = Secure Electronic Transaction
- offene & interoperable Verschlüsselungs- und Sicherheits-spezifikation
- kein Zahlungssystem, sondern eine Menge von Sicherheits-protokollen und Formaten
- zur Absicherung von Kreditkartentransaktionen über offene Netzwerke (wie das Internet)

Einleitung

- SET stellt folgende Dienste bereit
  - sicherer Kommunikationskanal zwischen den Akteuren
  - Vertraulichkeit durch Verwendung von X.509v3 Zertifikaten
  - sicherstellen der Vertraulichkeit der Transaktion (Bezahlinformationen und Bestellinformationen)
- Schwergewichtige Spezifikation bestehend aus 3 Teilen
  - gesamt 971 Seiten
  - im Vergleich zu SSL+TLS mit 134 Seiten

Historie



MasterCard und Visa kooperieren bei der Entwicklung eines Sicherheitsstandards

SET v.1 wir vorgestellt

Die ersten SET kompatiblen Produkte sind verfügbar

an der Entwicklung beteiligte Unternehmen:

- IBM
- Microsoft
- Netscape
- RSA
- Terisa
- VeriSign

Anforderungen

- klassische Schutzziele in der Kryptografie bezogen auf Kreditkarten Transaktionen
  - Vertraulichkeit der Zahlungs- und Bestellinformationen
    - Informationen nur den beabsichtigten Empfängern zugänglich
    - Zahlungsinformation: Bank (über Payment Gateway)
    - Bestellinformationen: Händler
    - reduziertes Risiko der Fälschung durch beteiligte Akteure oder Dritte
  - Integrität aller übertragenen Daten

Anforderungen

- Authentizität
  - Karteninhaber als legitimer Nutzer des Kreditkartenkontos durch Knüpfung eines Kreditkartenbesitzers an eine Kontonummer
  - Händler als Berechtigter zur Durchführung von Kreditkarten-Transaktionen (Kreditkarteninhaber müssen in der Lage sein, Händler zu identifizieren, mit denen sie sichere Transaktionen durchführen können)
- Nicht-Abstreitbarkeit durch Authentizität und Integrität

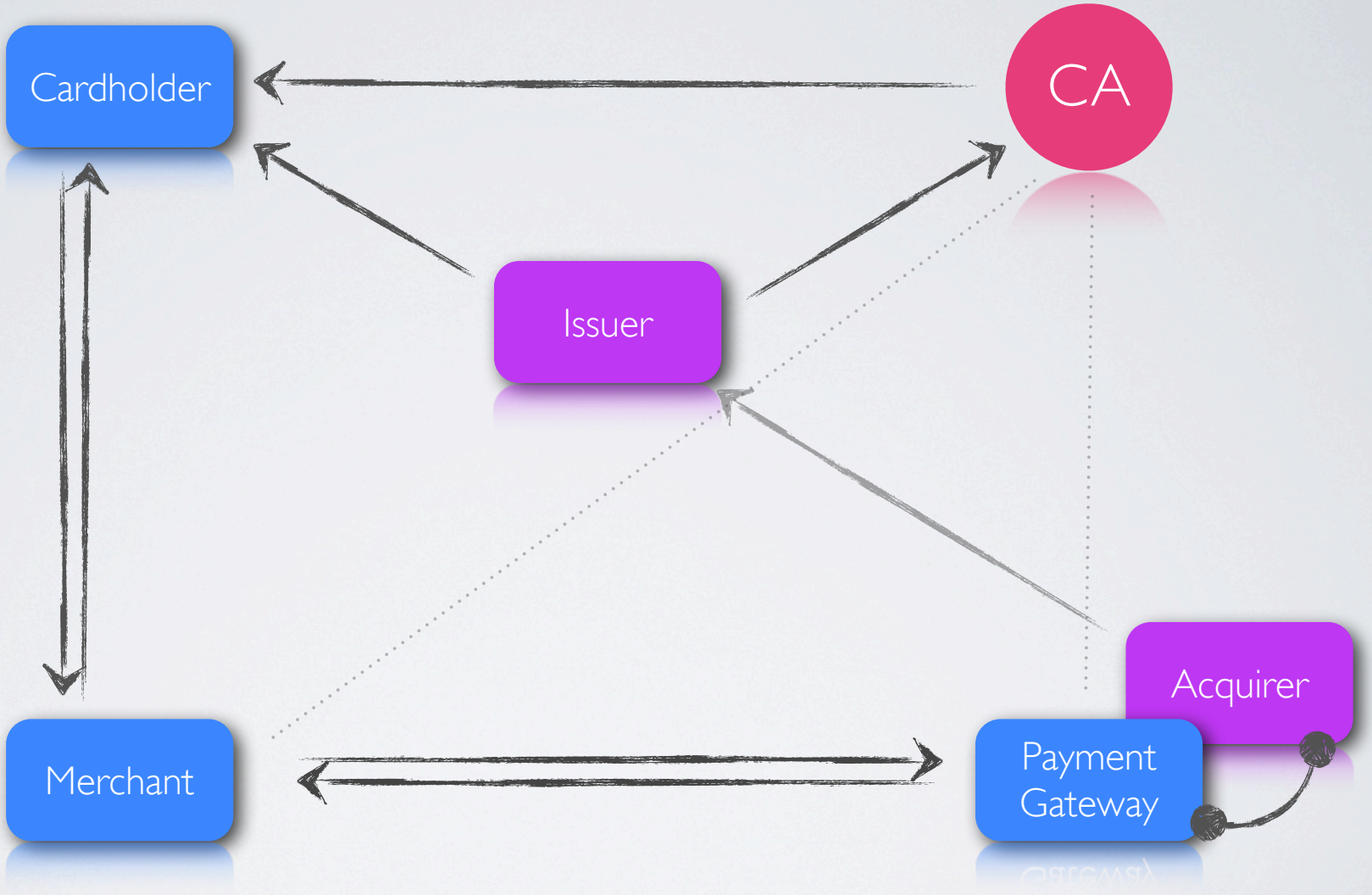
Anforderungen

- Anwendung „wirkungsvoller“ Sicherheitspraktiken
  - Verschlüsselung durch DES
  - Digitale Signaturen mit RSA
  - Zertifikate nach ITU X.509v3
- Unabhängigkeit vom Transportprotokoll
  - sichere Funktionsweise mit TCP/IP
  - keine Störeffekte bei der Verwendung anderer Sicherheitsmechanismen wie IPSec oder SSL/TLS
- Interoperabilität
  - Protokolle unabhängig von Hardware-Plattformen, Betriebssystemen, Web-Software etc.

Akteure

- Übersicht
  - Karteninhaber (Cardholder)
  - Händler (Merchant)
  - Kreditkarten-Aussteller (Issuer)
  - Händlerbank (Acquirer)
  - Zahlungsgateway (Payment-Gateway)
  - Certification Authority (CA)

Akteure



Akteure

- Karteninhaber (Cardholder)
  - Privat- oder Unternehmenskunde
  - Interagieren über ihren PC mit Händlern über das Internet
  - autorisiert durch den Besitz einer Kreditkarte die vom Finanzinstitut ausgegeben wurde
- Händler (Merchant)
  - Person oder Organisation, die Waren oder Dienstleistungen anbietet
  - wenn der Händler Kreditkartenzahlungen akzeptiert, benötigt er eine Geschäftsbeziehung mit einem Kapitalnehmer (Acquirer)

Akteure

- Kreditkarten-Aussteller (Issuer)
  - Finanzinstitution (z.B. Bank), die Kunden Kreditkarten ausstellt
  - ist verantwortlich für die Zahlung der durch den Karteninhaber veranlassten Beträge bei Bestellungen
- Händlerbank (Acquirer)
  - Finanzinstitution/Bank
  - Abrechnungsmöglichkeiten für Händler
  - Kreditkarten-Autorisierungen und Kreditkarten-Zahlungen
  - bietet Unterstützung für verschiedene Kreditkarten-Marken
  - bietet Verifikationsmöglichkeiten (Gültigkeit? Kreditlimit im Rahmen?)

Akteure

- Zahlungs-Gateway (Payment-Gateway)
  - wird durch die Händlerbank (Acquirer) oder einen Drittanbieter in dessen Auftrag betrieben
  - bearbeitet Zahlungsnachrichten des Händlers (Merchant)
  - stellt eine Schnittstelle zwischen SET und bereits vorhandenen Netzwerken für Kreditkartenfunktionen (Autorisierung, Zahlung) dar
  - SET-Nachrichten des Händlers können mit dem Zahlungs-Gateway über das Internet ausgetauscht werden
  - das Zahlungs-Gateway hat ferner eine direkte oder eine Netzwerk-Verbindung mit dem Finanzverarbeitungssystem der Händlerbank (Acquirer)

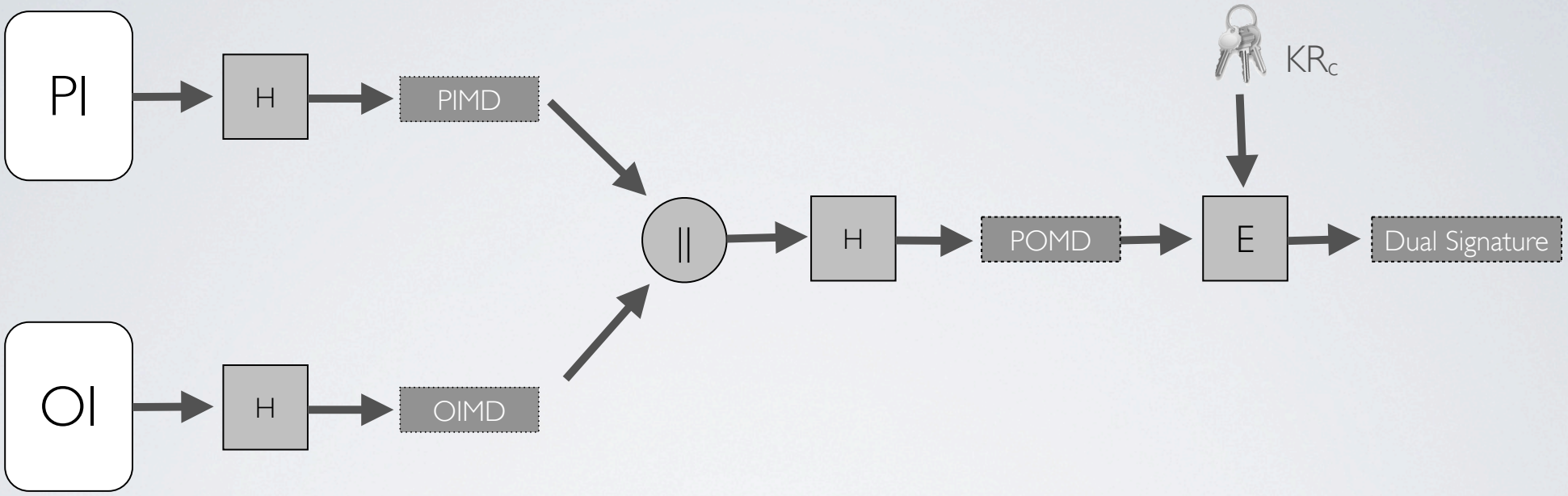
Wissensziele bis jetzt

- Was sind die Grundlegenden Anforderungen?
- Wie sind diese Realisiert?
- Wer sind die Akteure?
- Wie sind deren Aufgaben?

Grundlagen - Dual Signature

- Gegeben
  - Bestellinformationen & Zahlungsinformationen
  - für 2 unterschiedliche Empfänger (Händler & Bank)
- Problem
  - Austauschbarkeit der Zahlungsinformationen
  - Datenspeicherung & Betrug
- Lösung durch Dual Signature
  - Verknüpfung beider Informationen, sodass diese untrennbar miteinander verbunden sind
  - Informationen nur durch legitimen Empfänger lesbar
- Resultat:
  - Händler kann keine andere Bestellung mit den Zahlungsinformationen tätigen
  - Kunde kann den Händler nicht des Betrugs bezichtigen
  - Vertraulichkeit der Informationen

Grundlagen - Dual Signature

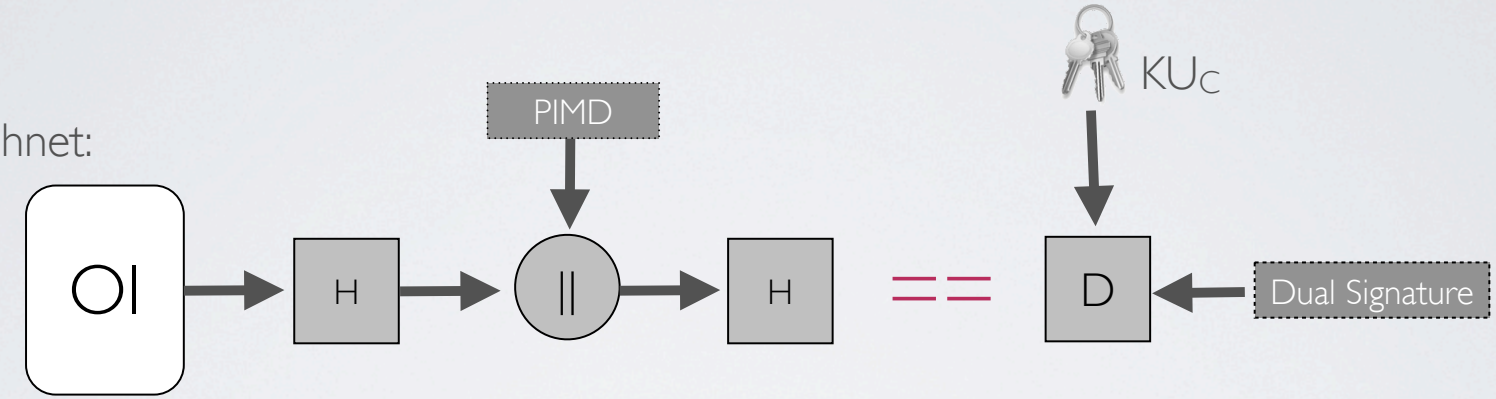


PI = Payment information
OI = Order information
H = Hash-Function
|| = Concatenation

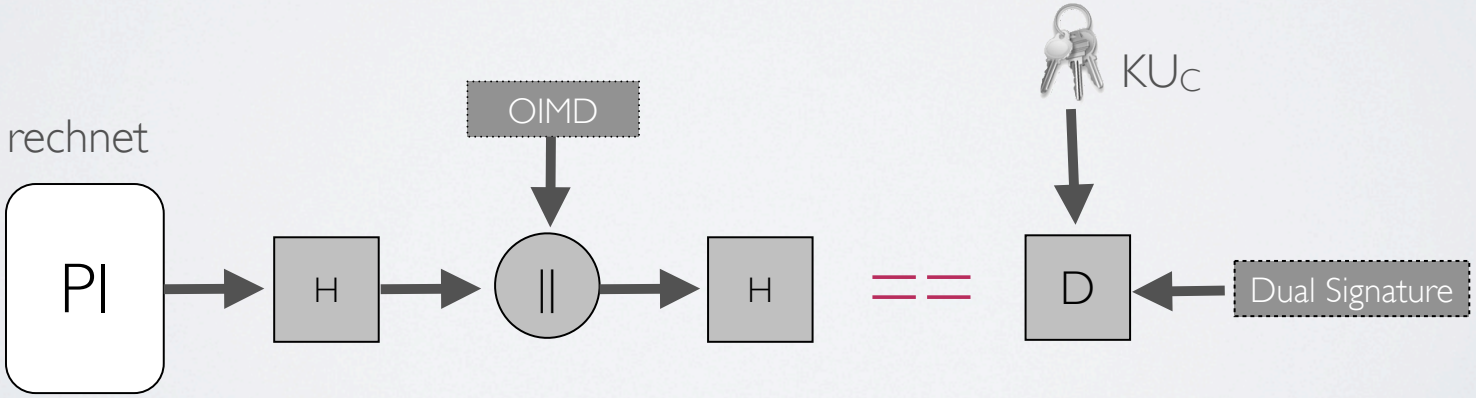
PIMD = PI Message Digest
OIMD = OI Message Digest
POMD = Payment Order Message Digest
E = Encryption (RSA)
KRc = Cardholders private key

Grundlagen - Dual Signature

Händler rechnet:



Bank (Issuer) rechnet



KU_C = Public Key des Cardholders

Grundlagen - SET Transaktionen

- verfügbare SET-Transaktionen
  - card holder registration
  - merchant registration
  - purchase request
  - payment authorization
  - payment capture
  - certificate inquiry and status
  - purchase inquiry
  - authorization reversal
  - capture reversal
  - credit reversal
  - credit
  - Payment Gateway cert. Request

Karteninhaber und Händler müssen sich zuerst an der CA registrieren um SET zu benutzen

Wenn die CA nicht in der Lage ist die Zertifikat-Anfrage zu

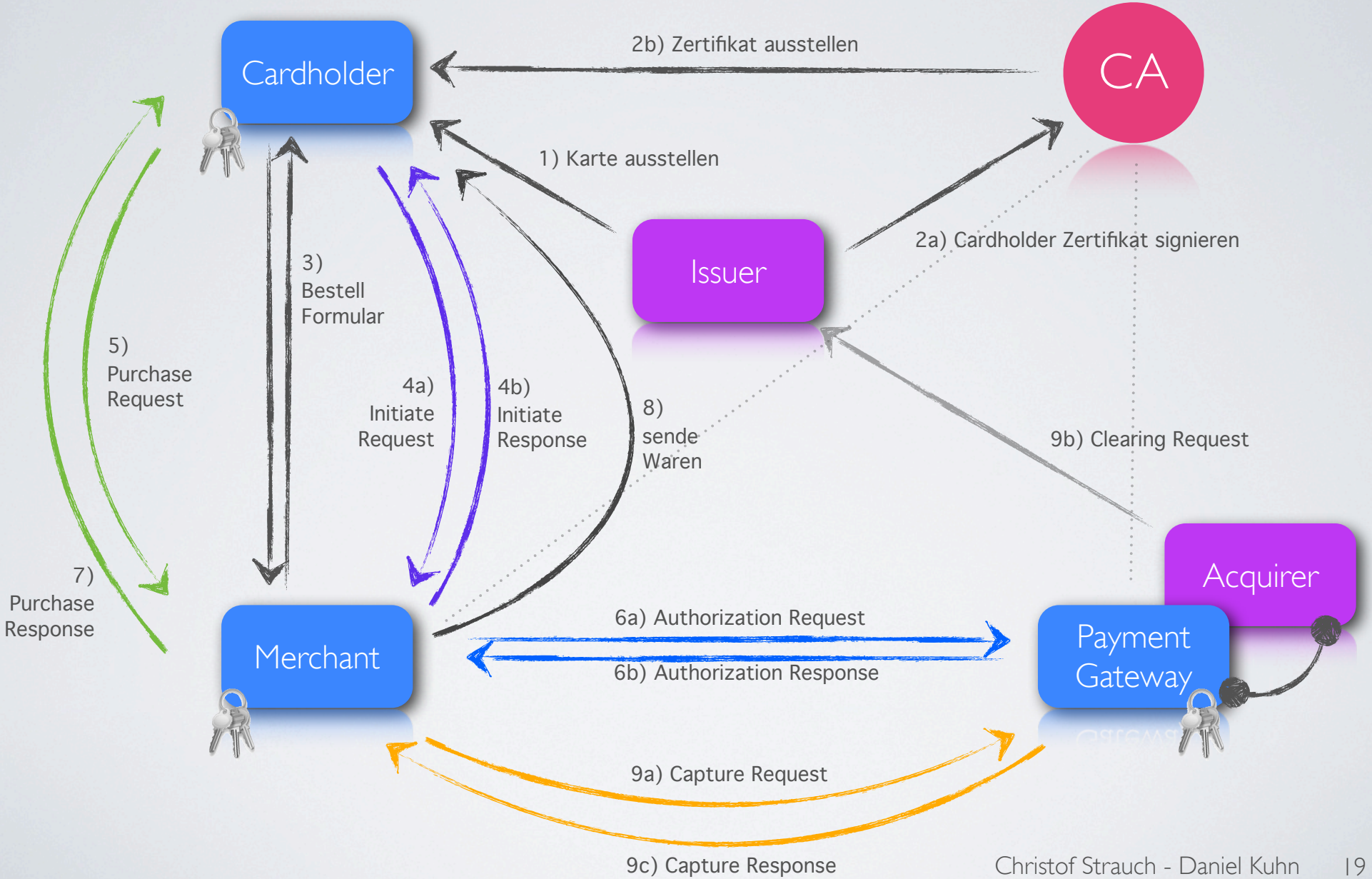
zum checken des Bearbeitungsstatus der Bestellung (nachdem der Purchase Request erhalten wurde)

korrigieren der jeweiligen Aktion (authorization request, capture request, credit request)

Stornieren einer Zahlung durch den Händler (z.B. bei

erlaubt dem Händler die Zertifikate des Payment-Gateways zu erhalten (Key-Exchange & signature Zertifikate)

Payment Process



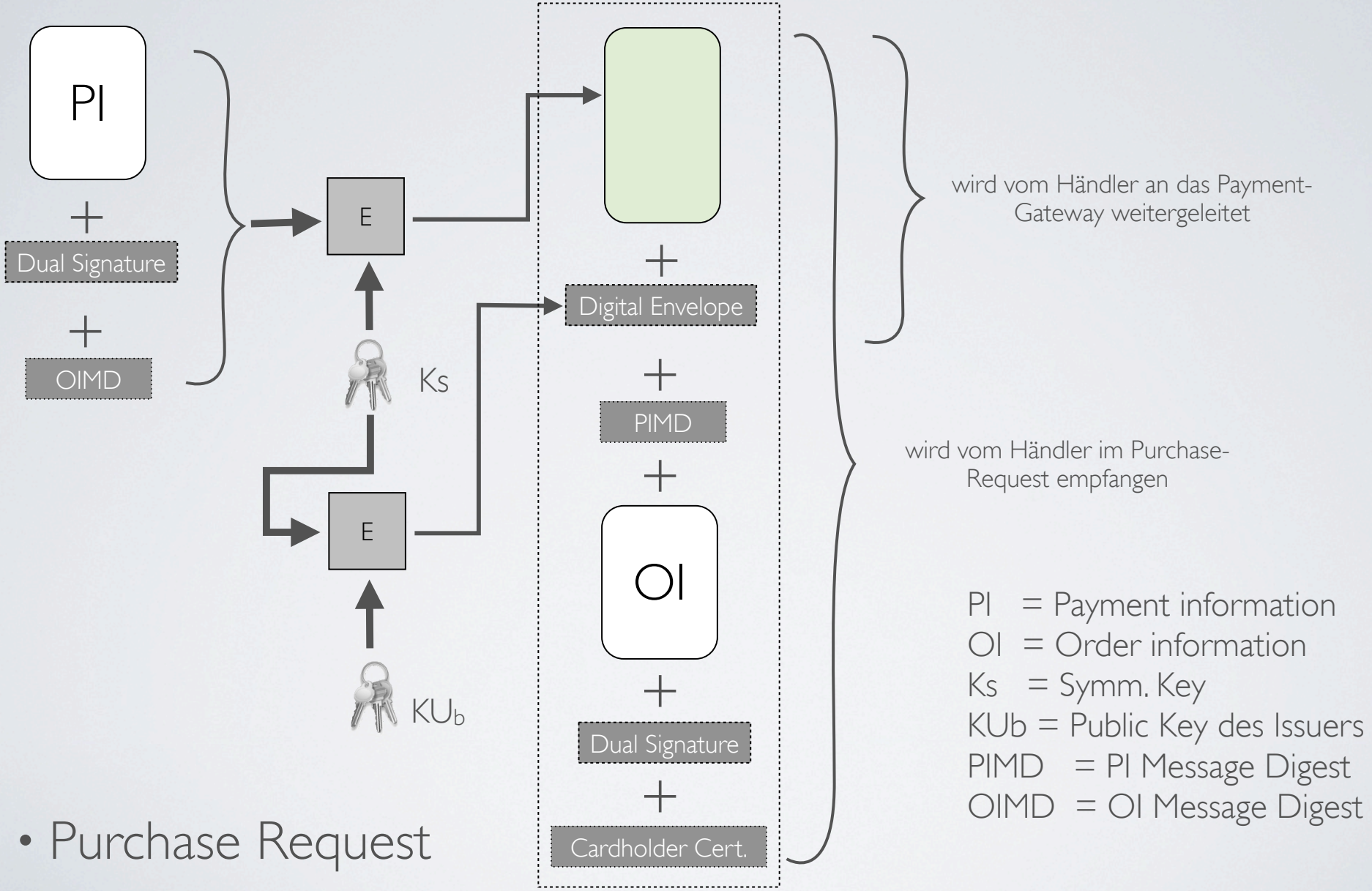
Purchase Request Transaction

- Initiate Request
  - Kreditkarten-Marke
  - zugeordnete Transaktions-ID (Referenz auf Transaktion)
  - Anforderung des Händler Zertifikats (Signatur Zertifikat)
  - Anforderung des Payment-Gateway Zertifikats (Schlüsselaustausch Zertifikat)
  - Nonce

Purchase Request Transaction

- Initiate Response
  - Transaktions-ID
  - Nonce des Cardholders
  - Nonce des Händlers (für die nächste Cardholder-Message)
  - signiert mit dem Private Key des Händlers
  - Zertifikate des Payment Gateways & Händlers (Merchant)
- Cardholder Aktionen
  - Verifikation der Zertifikate mittels der CA
  - erstellt Order Information (OI), Purchase Information (PI) und Dual Signature
    - TransaktionID ist in beide Integriert
    - OI beinhaltet nur eine Referenz auf eine Bestellung, nicht Artikel, Mengen oder Preise

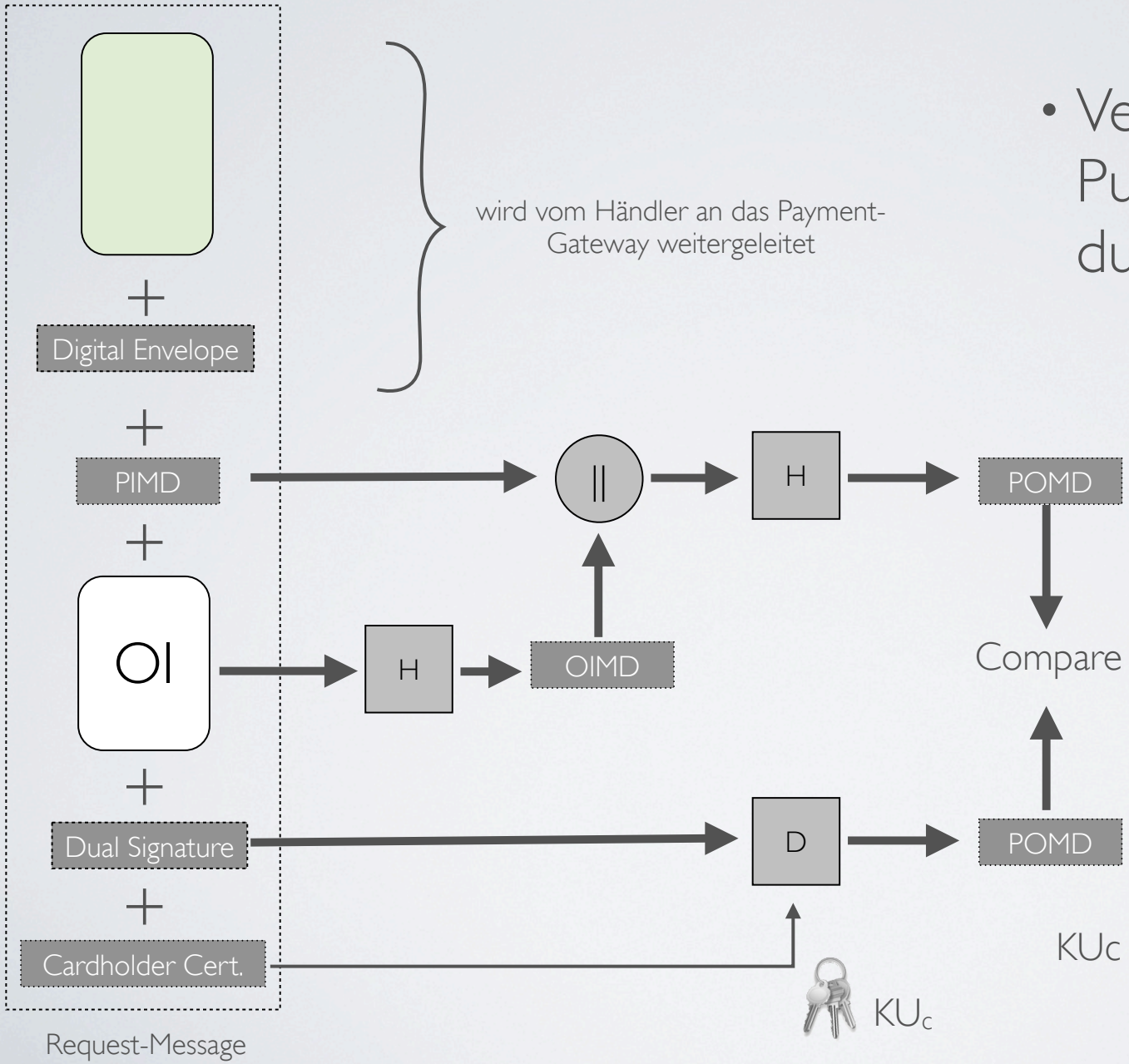
Purchase Request Transaction



PI = Payment information
OI = Order information
Ks = Symm. Key
KUb = Public Key des Issuers
PIMD = PI Message Digest
OIMD = OI Message Digest

- Purchase Request

Purchase Request Transaction



- Verarbeitung des Purchase Requests durch Merchant

KUc = Public Key des Cardholders

Purchase Request Transaction

- Verarbeitung des Purchase Request durch Merchant
  - Verifizieren des Cardholder Zertifikats mittels CA
  - Verifizieren der Dual Signature
  - Payment Authorization
    - verschlüsselte Payment Information und Digital Envelope an Payment-Gateway weiterleiten
- Purchase Response
  - Bestätigung der Bestellung
  - Transaktions-ID
    - signiert mit Private Key des Händlers
  - Signatur-Zertifikat des Händlers

Komplexitätsbetrachtung

- Anzahl der Nachrichten
  - Cardholder - Merchant: **4**
  - Merchant - Payment-Gateway: **2**
  - Payment-Gateway - Issuer: **3**
  - zzgl. Zertifikats-Prüfungen bei CA / mittels CRLs
- kryptographische Operationen:
  - 6 digitale Signaturen
  - 9 RSA Ver-/Entschlüsselungszyklen
  - 4 DES Ver-/Entschlüsselungszyklen
  - 4 Zertifikatsverifikationen

Diskussion

- Vorteile
  - sicherer als reine Kreditkartenzahlung
    - Vertraulichkeit der Kreditkarteninformationen
    - Dual Signature: Integritätsschutz, sichere Verknüpfung von Bestell- und Zahlungsinformationen
    - Authentifizierung der beteiligten Akteure
    - Nicht-Abstreitbarkeit der SET-Transaktionen
  - Vorteile gegenüber Transaktionen via SSL
    - Authentifizierung aller Akteure
    - Vertraulichkeit nicht nur auf dem Transportweg
  - zu Beginn Unterstützung durch Kreditkartengesellschaften und Software-Unternehmen
  - portierbar für andere Bezahlarten / Konten

Diskussion

- Nachteile
  - Algorithmus auf ein Verschlüsselungsverfahren (DES, RSA) festgelegt
  - PKI notwendig
    - führt zu Akzeptanzproblemen (Kunden, Händler, Banken)
  - Protokoll-Overhead: Nachrichten, Roundtrips, Verschlüsselungen/Signaturen
  - SET-Wallet Anwendung auf Client-PC notwendig
    - Angriffe auf die SET-Wallet Anwendungen möglich
  - Händler und Banken müssen SET unterstützen
    - mit Betriebskosten verbunden (z.B. Payment-Gateway)
  - Umfang der SET-Spezifikation
  - Verschlüsselung zur Zeit des Entstehens von SET in manchen Ländern für Auslandsgeschäfte verboten

Presse-Spiegel

- „Sechs Monate nach Einführung der Version 1.0 [...] dümpele das Verfahren vor sich hin, es sei viel zu komplex für den praktischen Einsatz, auch fehlten effektiv arbeitende Implementierungen. " (Matthew Friedmanm, InternetWeek Newsletter, 1997)
- "Das moderne Internet-Bezahlverfahren SET (Secure Electronic Transaction) setzt nicht einer der von eco/vivendo untersuchten Online-Shops ein." (Studie von Electronic Commerce Forum e.V. und vivendo Internet AG, 1000 Internet-Shops unter den Aspekten Einkaufskomfort, Verbraucherschutz und Sicherheit betrachtet, 1999)
- Wäre SET in der Hand eines einzigen Anbieters so wie CyberCash, dann wäre es vermutlich auch schon vom Markt verschwunden. Aber so probieren daran noch einige Anbieter herum. Auch die haben gemerkt, dass die Leute bei sich zuhause keine Zusatzsoftware installieren wollen. Also wurde die Idee geboren, SET über den Server des Anbieters laufen zu lassen. Vielleicht ist das ja jetzt erfolgreich. Zumindest kommen inzwischen neue Produktangebote für diesen Bereich auf den Markt." (Telepolis-Interview mit Rüdiger Grimm, E-Payment-Experte an der TU Ilmenau, 2001)
- "SET-Angebote im Netz sind noch rar, denn der Aufbau der Trustcenter nimmt einige Zeit in Anspruch. Darüber hinaus haben bisher nur relativ wenige Kunden bei ihrer Bank ein Zertifikat beantragt. Und nicht zu unterschätzen sind auch die Kosten für den Händler: Er muss die Kasse in seinem Online-Shop für etwa 1000 Euro über einen Dienstleister implementieren. Für jede Buchung zahlt er einen Abschlag zusätzlich zum Disagio, den er an die Kartengesellschaft entrichtet. [...] Die Macht der Kreditkarten-Gesellschaften dürfte aber ausreichen, um SET langfristig durchzusetzen. Bisher sind in Deutschland nur wenige Shops SET-fähig." (Dr. Klaus Mahnart, TecChannel, 2000/2002)

Diskussion

- Wieso hat sich SET nicht durchgesetzt?
  - Akzeptanzprobleme v.a. beim Kunden (Zertifikat, Wallet-Software)
  - Schwergewichtig
  - Infrastruktur für Zertifikats-Distribution
  - Nachrichten-Overhead
  - Kosten für Händler und Banken im Vergleich zu SSL/TLS wesentlich höher

Ausblick

- Nachfolgesysteme
  - MasterCard Secure Code
  - Verified by Visa
- Unterschiede zu SET
  - leichtgewichtiger:
    - Verzicht auf PKI
    - Client-Zertifikate
    - Verschlüsselungen auf Client
  - erfüllt weniger Sicherheitsanforderungen als SET

Literatur und Quellen

- Literatur
  - Stallings, W.: Network Security Essentials, 1999, Prentice-Hall New Jersey
  - Sair, S. : Secure Electronic Transaction, Southern Methodist University Dallas/Texas , Spring 2005
- Internetquellen
  - http://trumpf-3.rz.uni-mannheim.de/www/sem96s/webrum.uni-mannheim.de/bwl/zenner/seminar/set.htm
  - http://ddi.cs.uni-potsdam.de/Lehre/e-commerce/elBez2-5/page14.html
  - http://www.tecchannel.de/sicherheit/identity_access/401380/bezahlen_im_internet/index10.html
  - http://www.davidreilly.com/topics/electronic_commerce/essays/secure_electronic_transactions.html
  - http://www.ellinogermaniki.gr/ep/agroweb/htmls/lessons/commerce1/423.htm
  - http://www.indicthreads.com/1496/security-and-threat-models-secure-electronic-transaction-set-protocol/
  - http://www.redbooks.ibm.com/redbooks/pdfs/sg244978.pdf

Fragen?

Vielen Dank für Ihre/eure Aufmerksamkeit!