Willkommen zur Vorlesung

Modellbasierte Softwaretechniken für sichere Systeme

im Sommersemester 2012

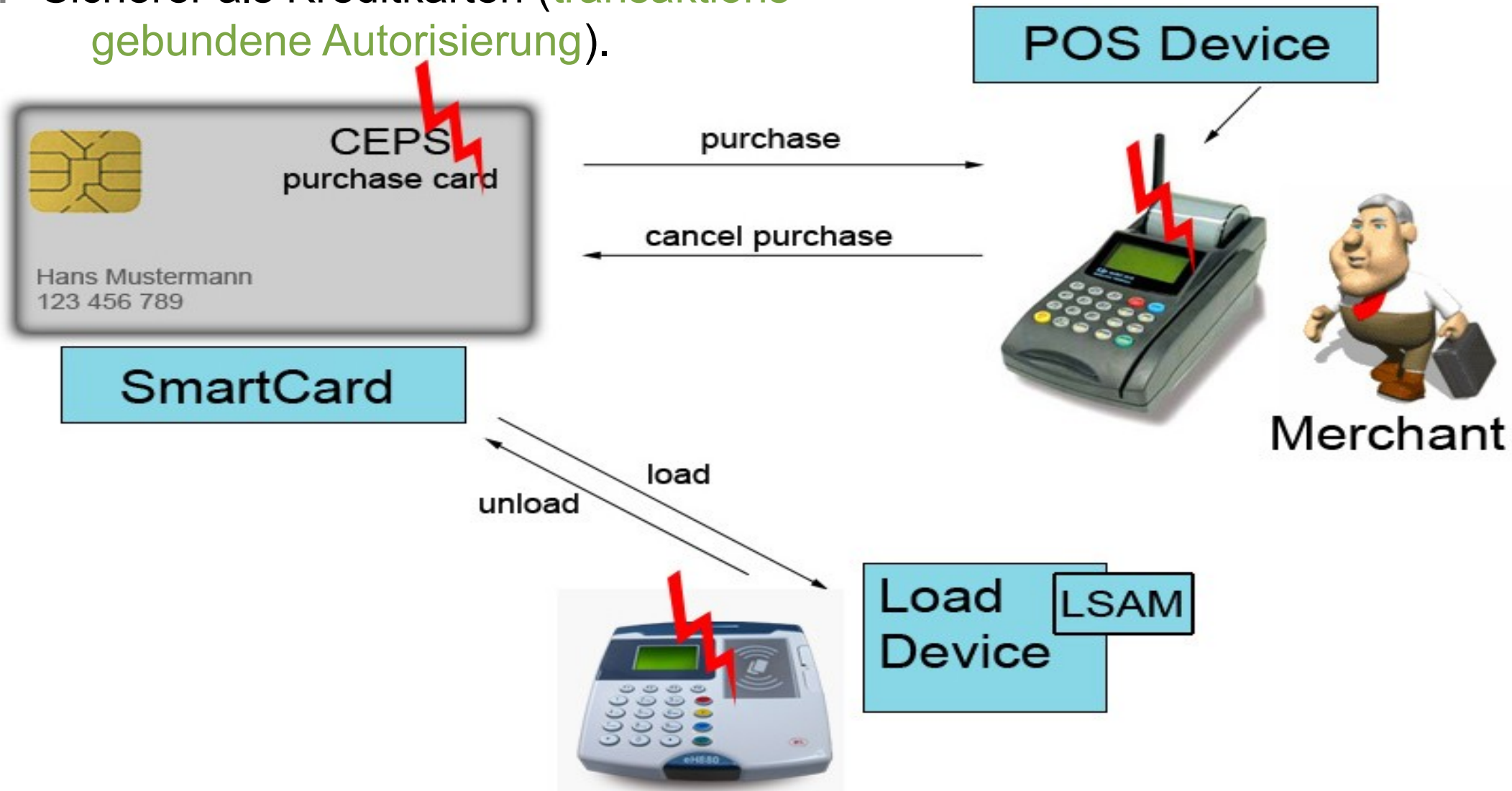
Prof. Dr. Jan Jürjens

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

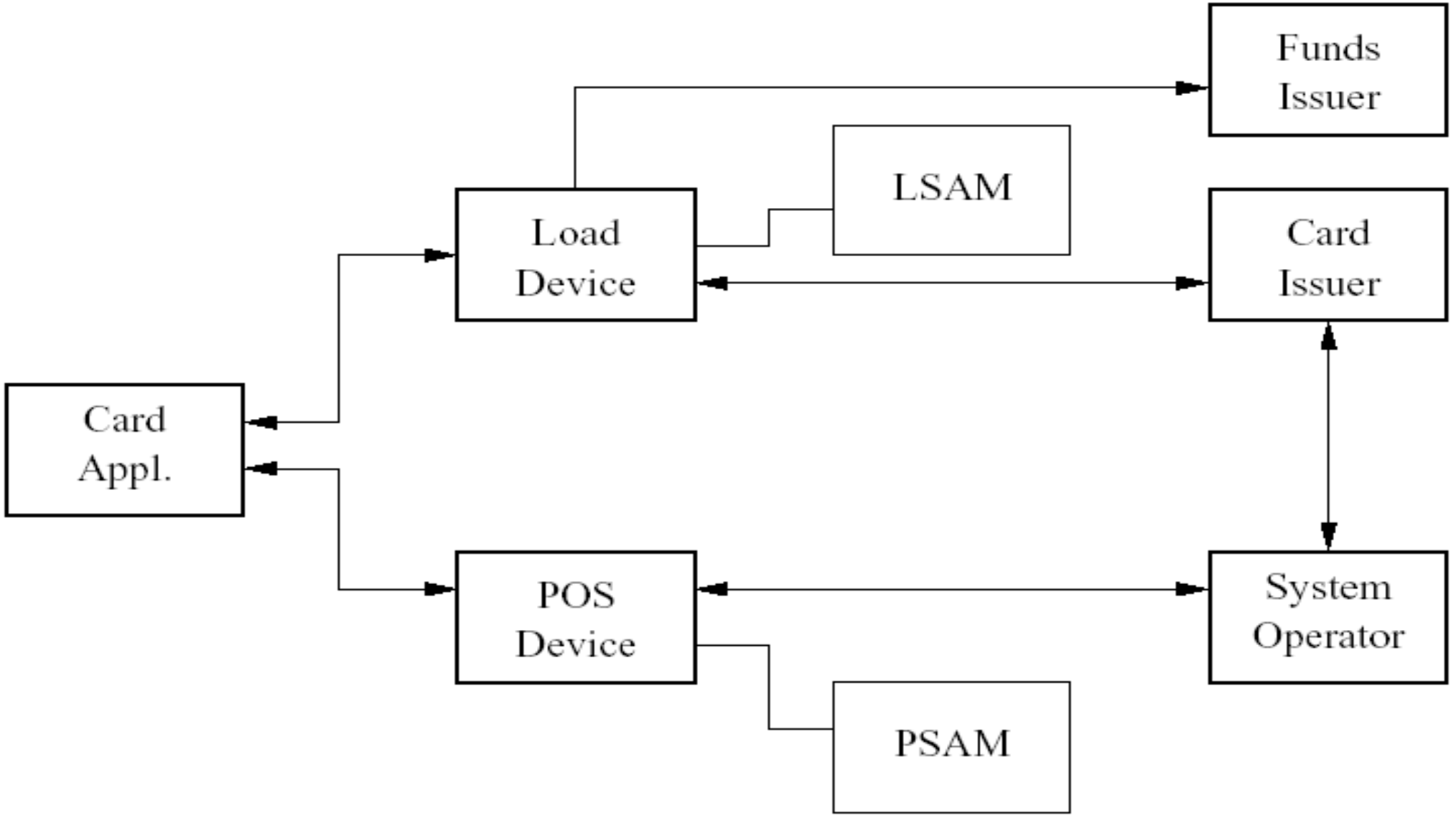
10. Elektronische Geldbörsen

Common Electronic Purse Specifications

Globaler Standard (90% des Marktes). Smartcard speichert Kontostand.
Kryptographie auf Chip sichert Transaktionen.
Sicherer als Kreditkarten (transaktions-gebundene Autorisierung).



CEPS Architektur-Überblick



Kauf- (Purchase-)Protokoll

Offline-Transaktion zum Bezahlen von Waren mit vorher aufgeladener Karte.

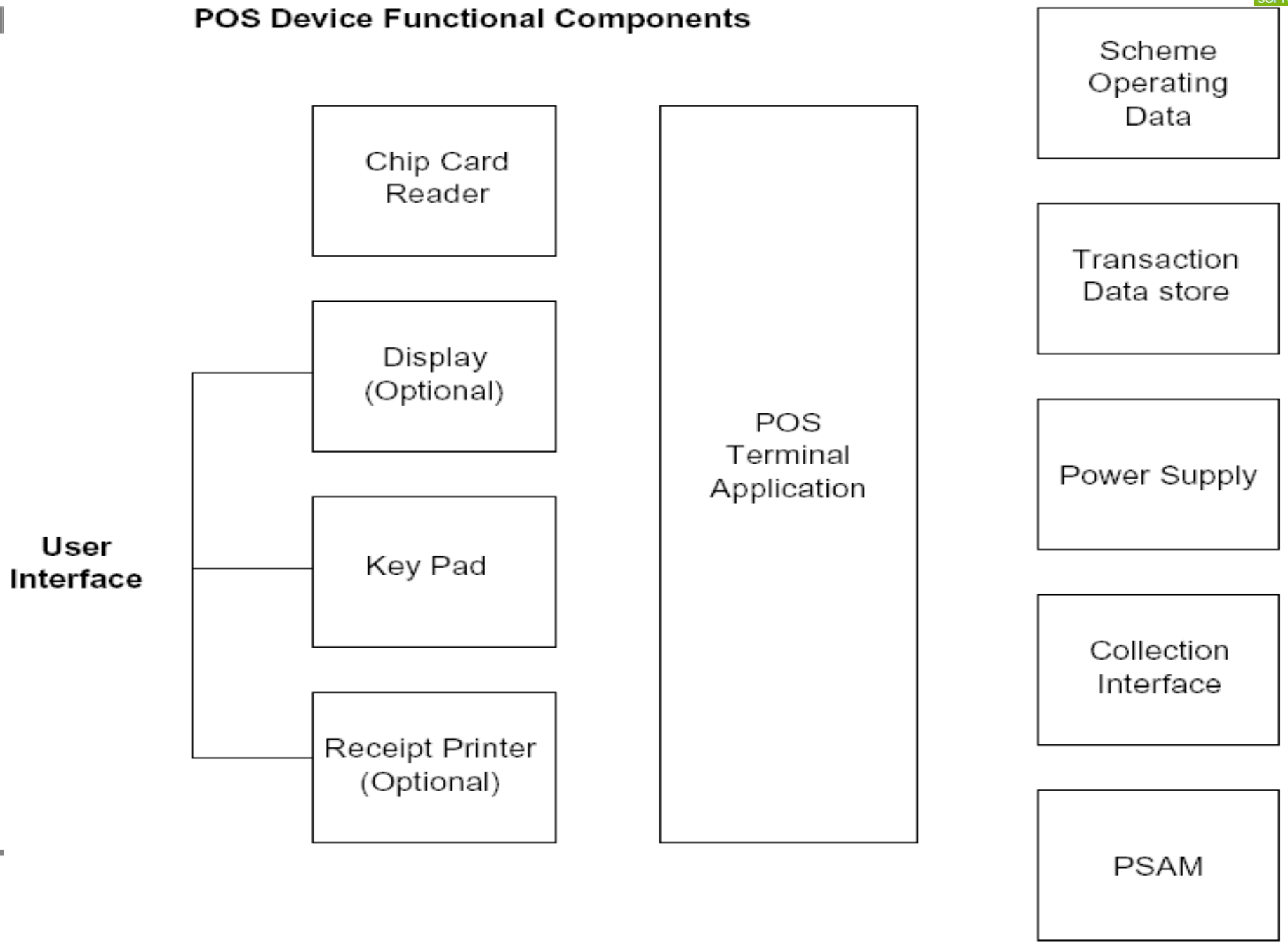
Protokollteilnehmer: Karte des Besitzers, POS-Gerät des Händlers.

POS-Gerät enthält Purchase Security Application Module (PSAM): alle sicherheitskritischen Datenverarbeitungen und Speicher für das POS Gerät.

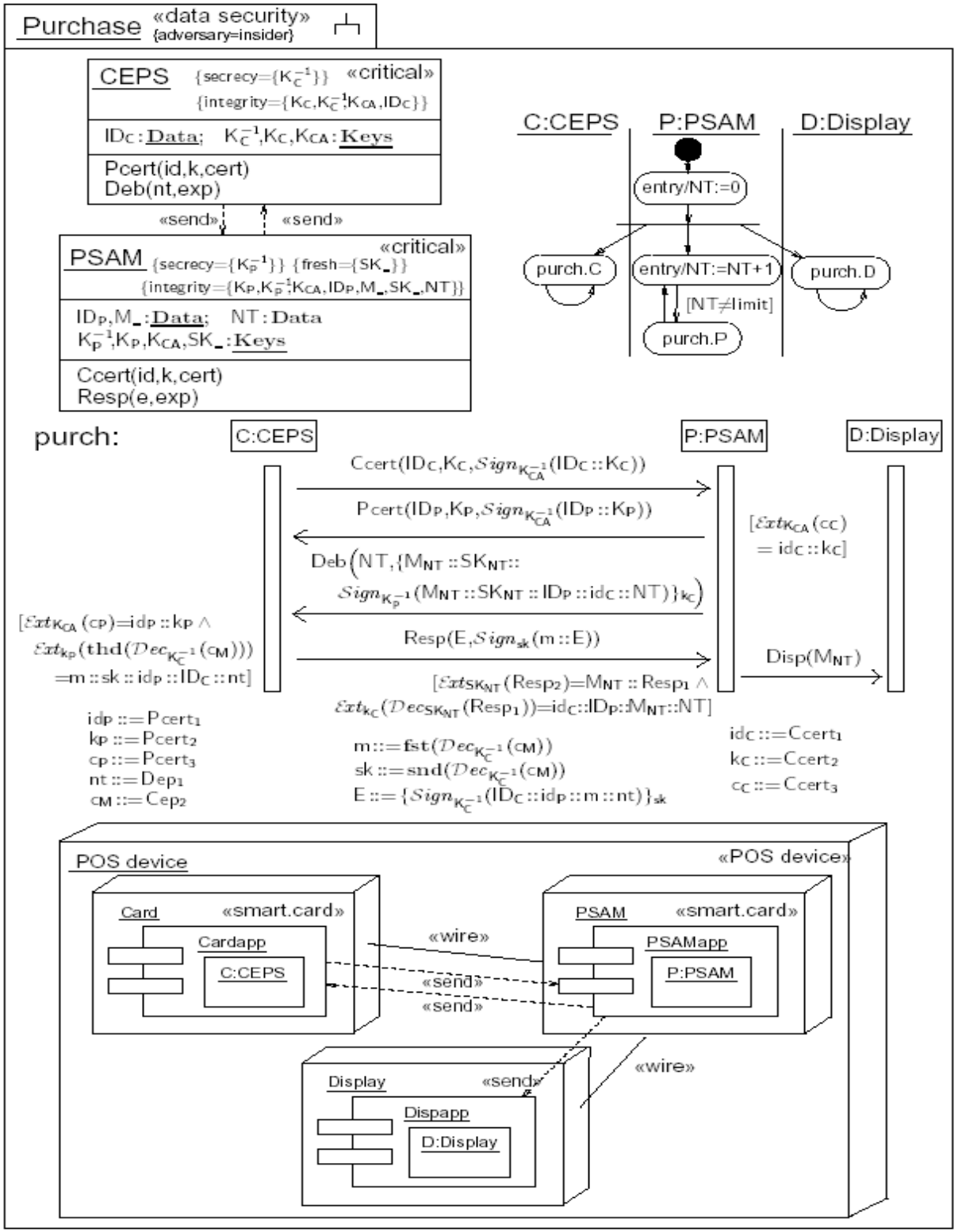
Kartenkontostand wird angepasst, Transaktiondaten werden gelogged und später zur finanziellen Abwicklung an den Kartenausgeber übersendet.

Benutzung an öffentlichen Stationen; Internetbenutzung vorgesehen.

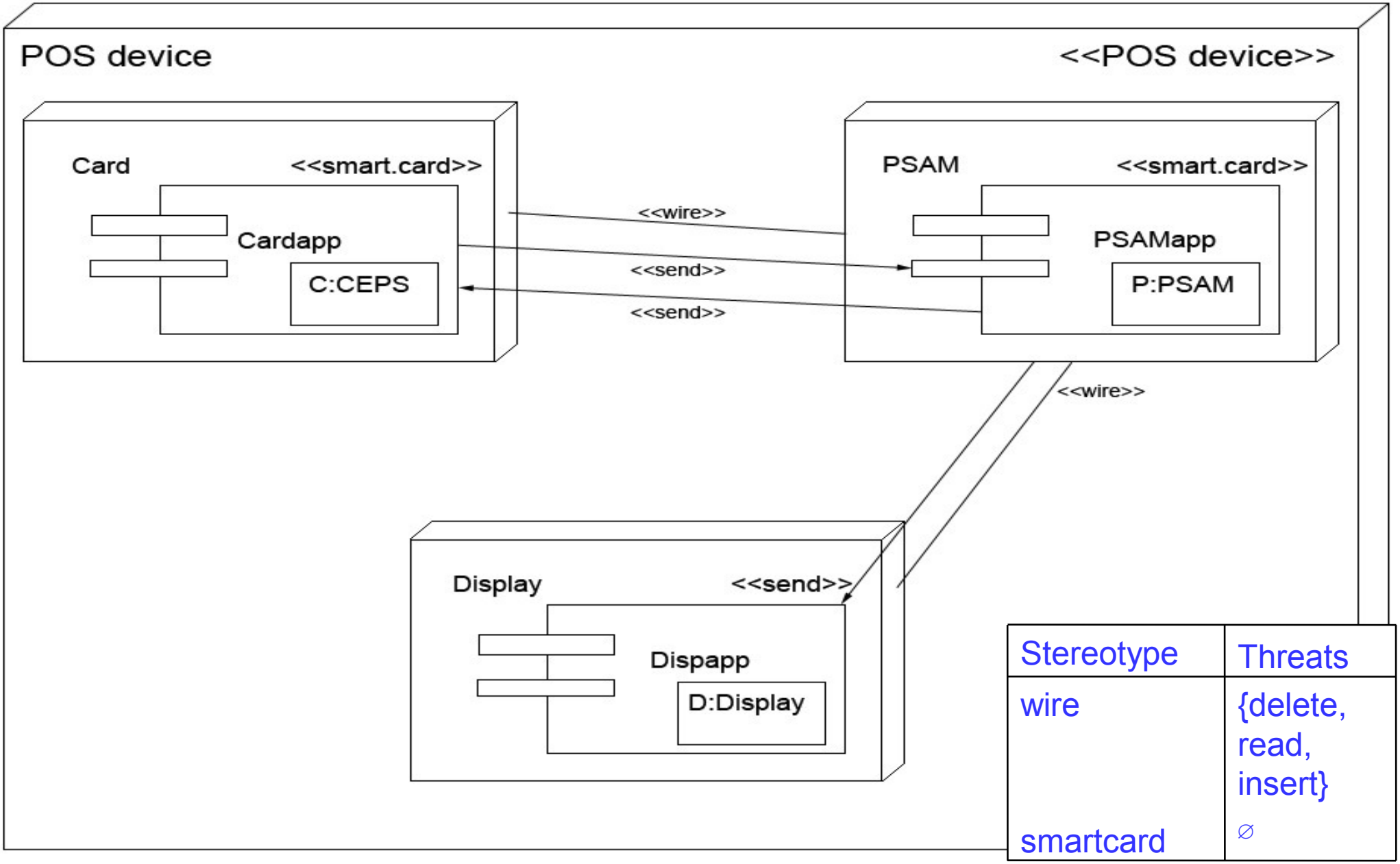
POS Device


POS Device Functional Components
User Interface
Chip Card Reader
Display (Optional)
Key Pad
Receipt Printer (Optional)
POS Terminal Application
Scheme Operating Data
Transaction Data store
Power Supply
Collection Interface
PSAM

UMLsec Spezifikation: Vogelperspektive

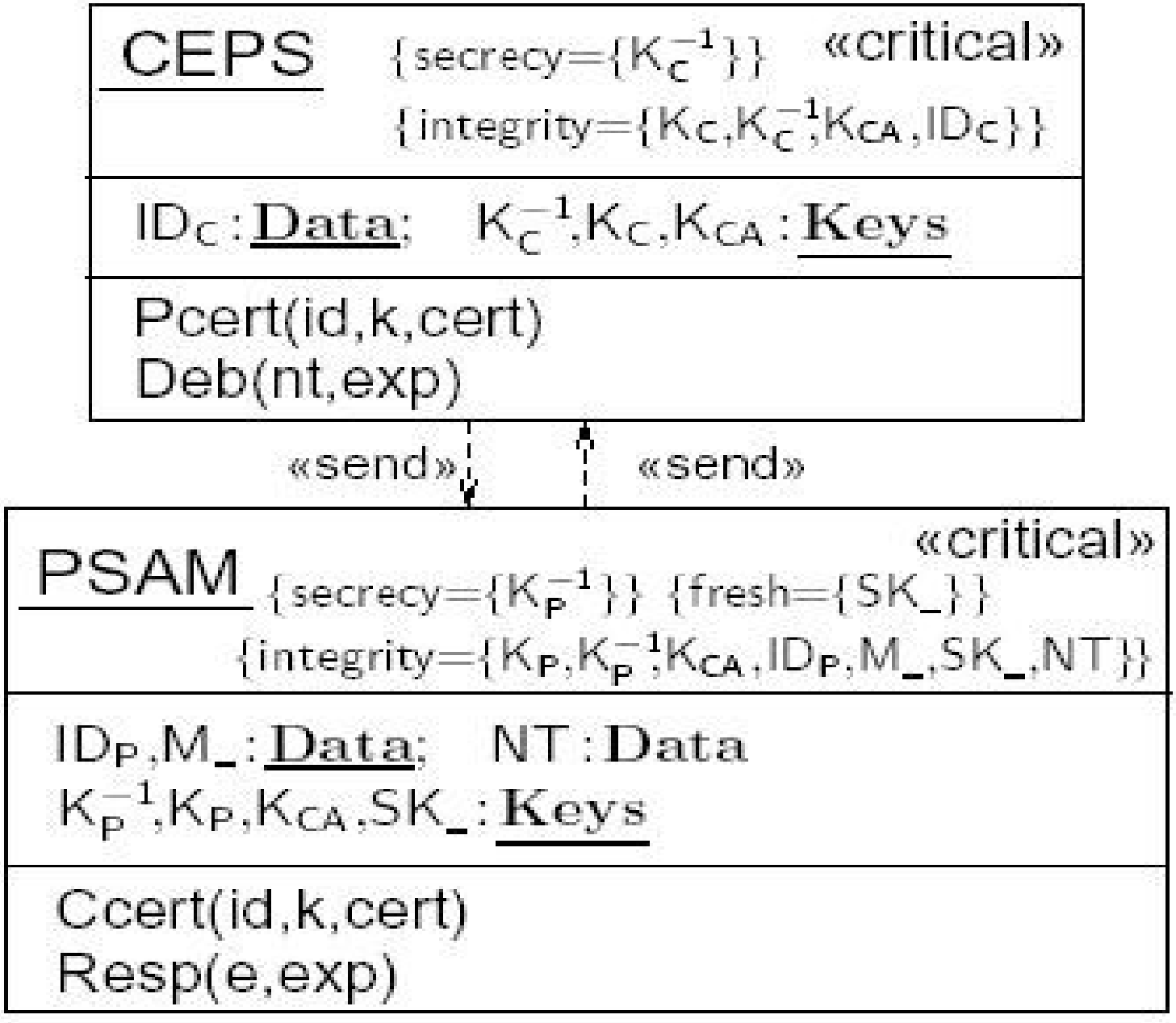


Purchase-Protokoll: Architektur

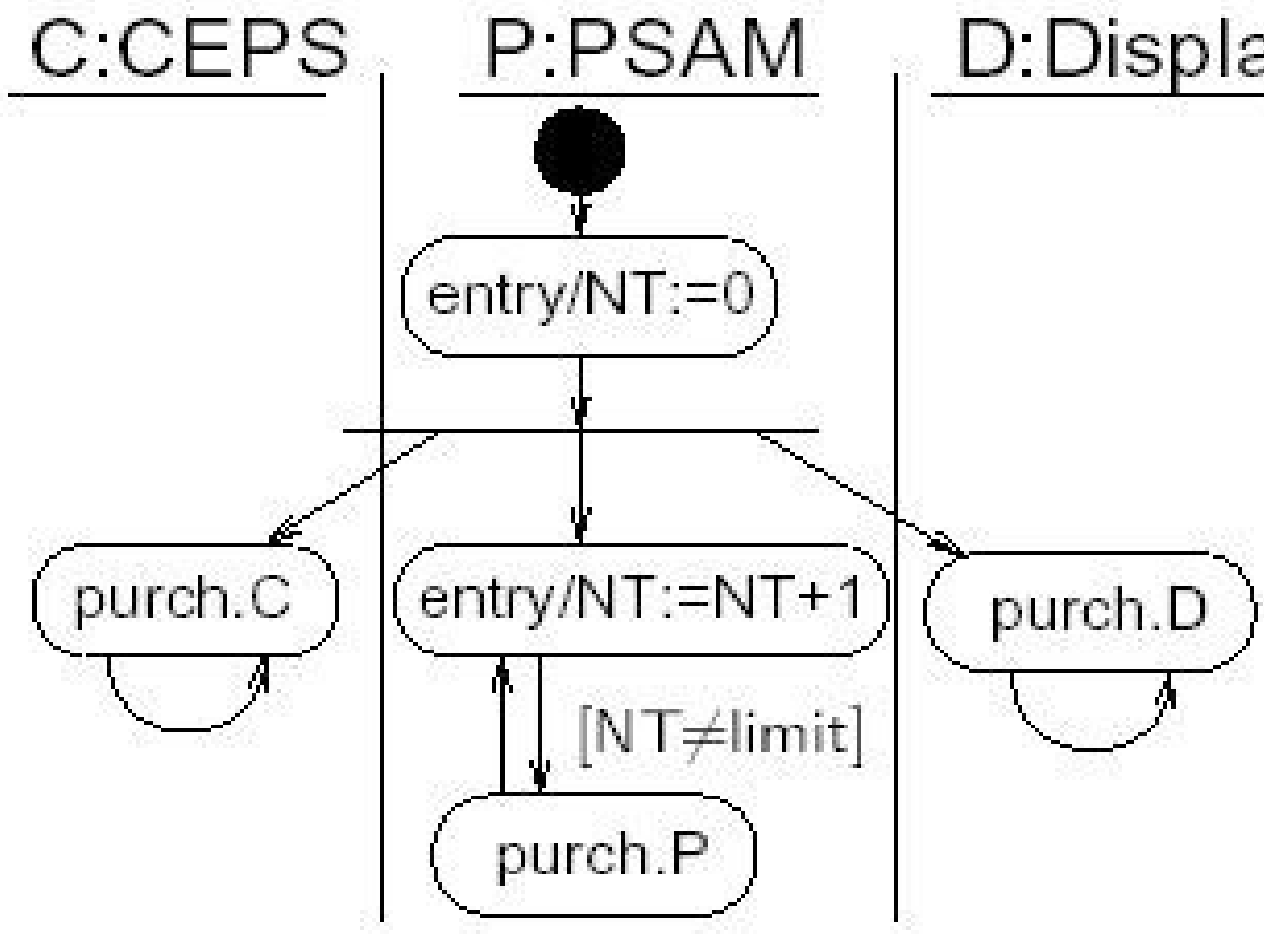


Stereotype	Threats
wire	{delete, read, insert}
smartcard	∅

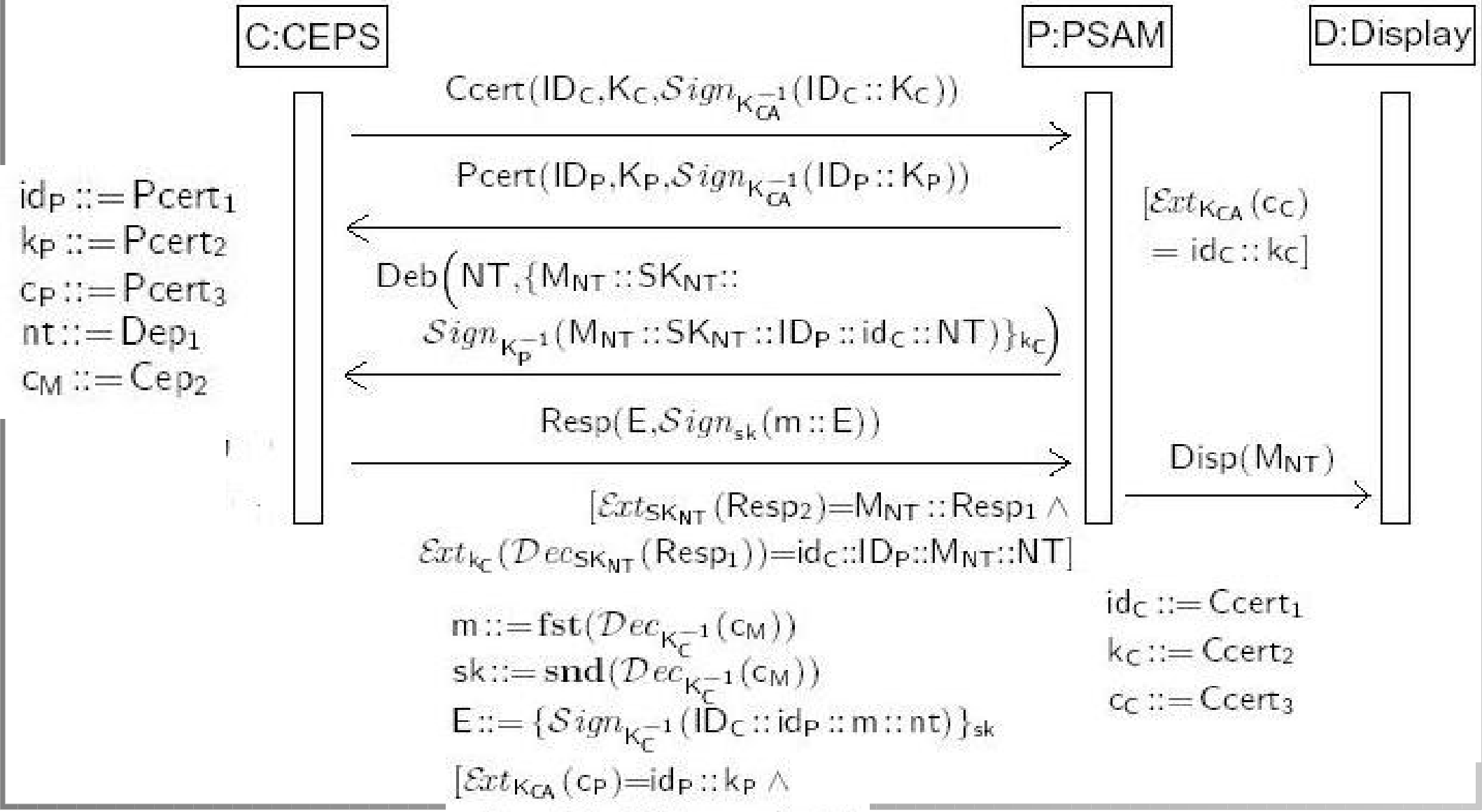
Klassendiagramm



Aktivitätsdiagramm



Interaktion



Sicherheitsbedrohungsmodell

Soll Karten-Authentisierung zwischen Station und Karte liefern.

Annahme: Karte und PSAM sind manipulationssicher.

Manipulieren von Kommunikationsverbindungen, Ersetzen von Komponenten.

Mögliche Angriffsmotivationen (Beispiele):

- **(Kein-)Karteninhaber**: Kauf ohne Bezahlung.
- **Angestellter des Geschäfts**: Kaufen von digitalem Inhalt mit der Karte des Kunden.
- **Angestellter des Kartenbetreibers**: Geldbetrag auf eigenes Konto umleiten.

Die Rollen können jeweils zusammenarbeiten oder sogar in einer Person übereinstimmen.

Sicherheitsanalyse

Keine direkte Kommunikation zwischen Karte und Inhaber. Manipulation der Aufladestation möglich.

➔ Post-Transaktions-Abrechnungsystem.

➔ Gespeicherte Transaktionsdaten sicherheitskritisch.

➔ Modell-basierte Analyse dieses System-Teiles.

Sicherheitsbedingungen (informell)

Kartenbesitzer-Sicherheit: Verkäufer hat nur Anspruch auf den Geldbetrag, der auf der Karte nach der Transaktion registriert ist.

Verkäufer-Sicherheit. Verkäufer bekommt Bestätigung der Transaktion im Austausch für verkaufte Waren (um Geld zurückfordern zu können).

Kartenemittent-Sicherheit. Summe des Kontostandes der gültigen Karten und PSAMs unverändert durch Transaktion.

Verkäufer-Sicherheit: Technisch

Spezifikation der Verkäufer-Sicherheit mit Bezug auf Protokollnachrichten:

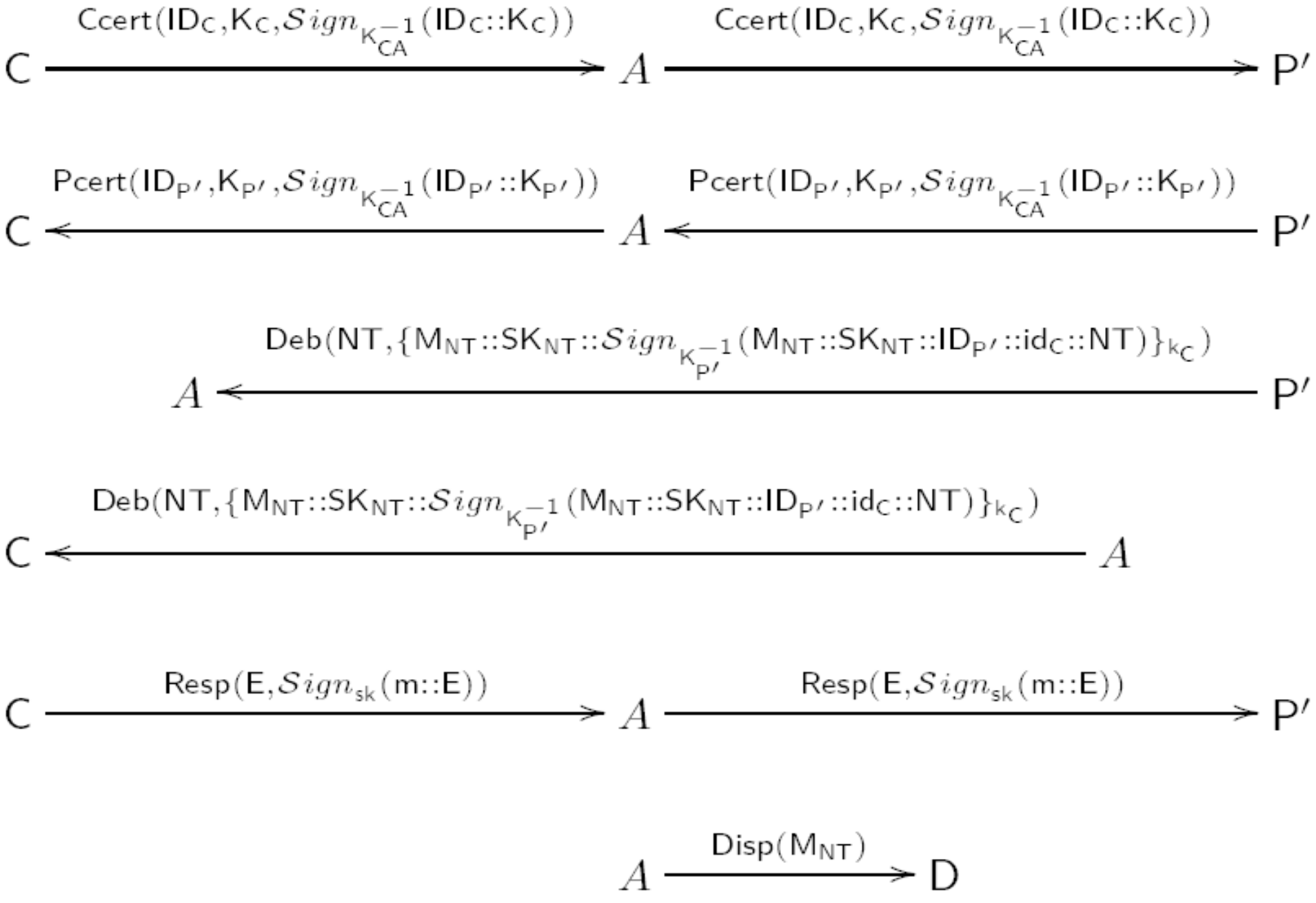
Jedes Mal, wenn das Display einen Wert M_{NT}, erhält, ist P in Besitz der zugehörigen Signaturen $Sign_{K_{CA}}{}^{-1}(ID_C::K_C)$ und $Sign_{K_C}{}^{-1}(ID_C::ID_P::M_{NT}::NT)$ für die relevanten Werte ID_C, $K_C{}^{-1}$ und einen bislang unbenutzten Wert NT.

Analyse ergibt: Eigenschaft nicht erfüllt (!).

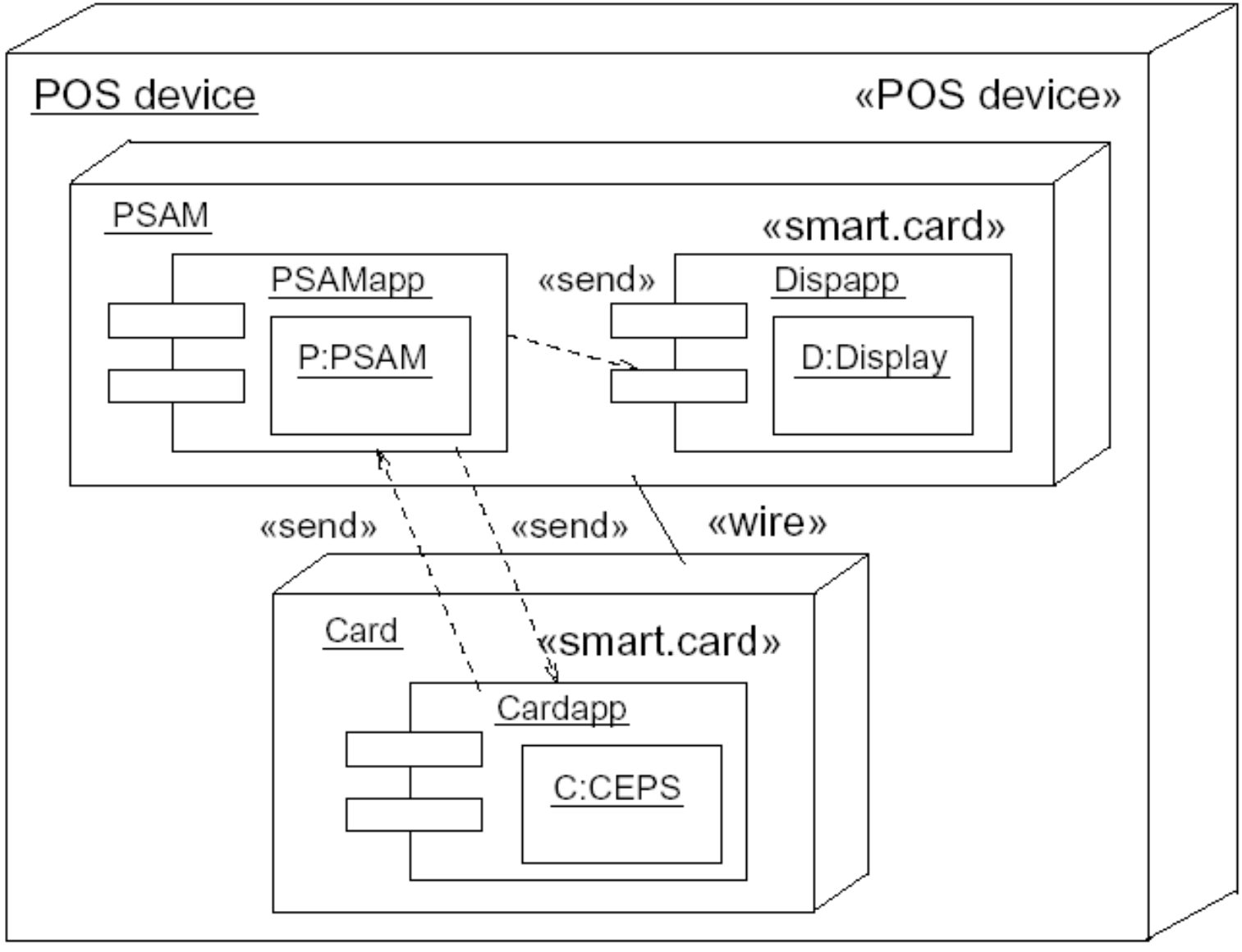
Angriff nutzt die Tatsache aus, dass das POS Gerät nicht manipulationssicher ist:

Leite Nachrichten zwischen Karten und PSAM zu einem anderen PSAM um (z.B. zum Kauf von digitalen Inhalt seitens eines Angestellten, auf Kosten des Kartenbesitzers).

Angriffsszenario



Verbesserung: Kommunikationsverbindung zwischen PSAM und Display absichern



Ladeprotokoll (Load Protocol)

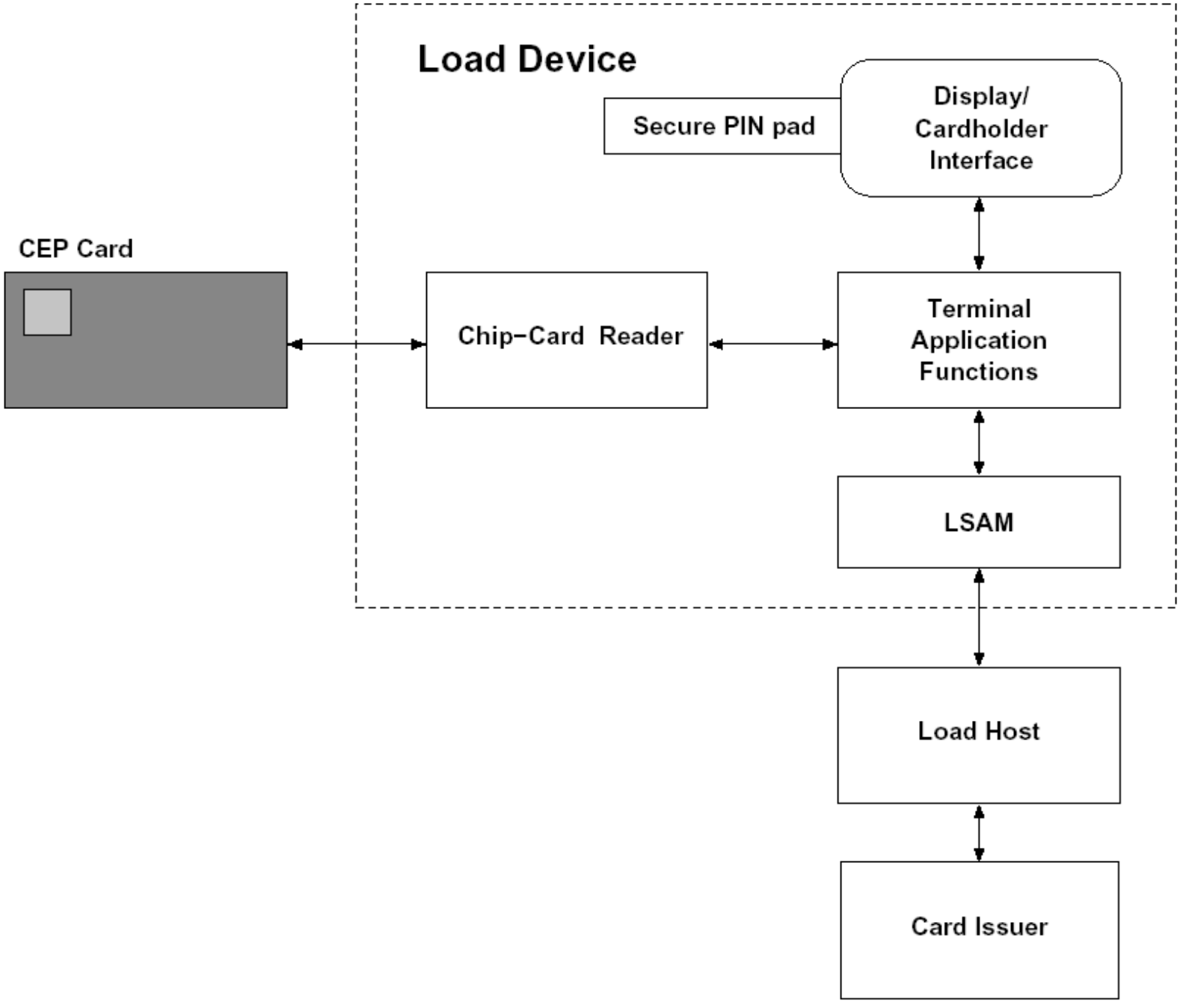
Karte mit Bargeld an Aufladestation laden (on-line).

Load Security Application Module (LSAM) speichert Transaktionsdaten.

Schickt Daten an Kartenemittent, der finanzielle Abwicklung übernimmt.

Symmetrische Verschlüsselung / Signatur.

CEPS Ladegerät



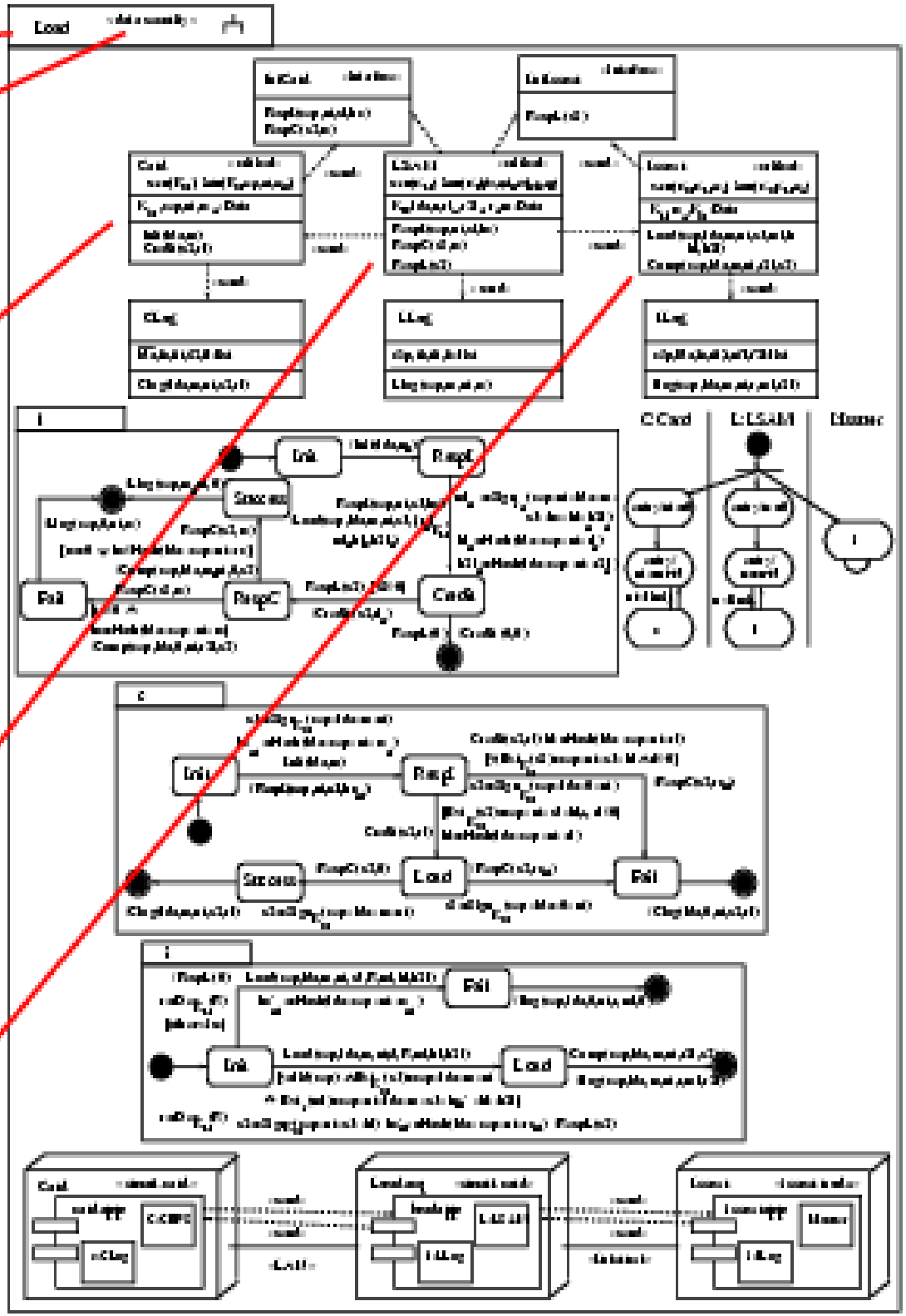
CEPS Lade-Protokoll: UMLsec-Spezifikation

Load
«data security»

Card «critical» {secrecy={K_{CI}}} {integrity={K_{CI},cep,nt,rc_{nt}}}
cep, nt, rc_{nt} : Data; K_{CI} : Keys
Init(lda,m) Credit(s2,rl)

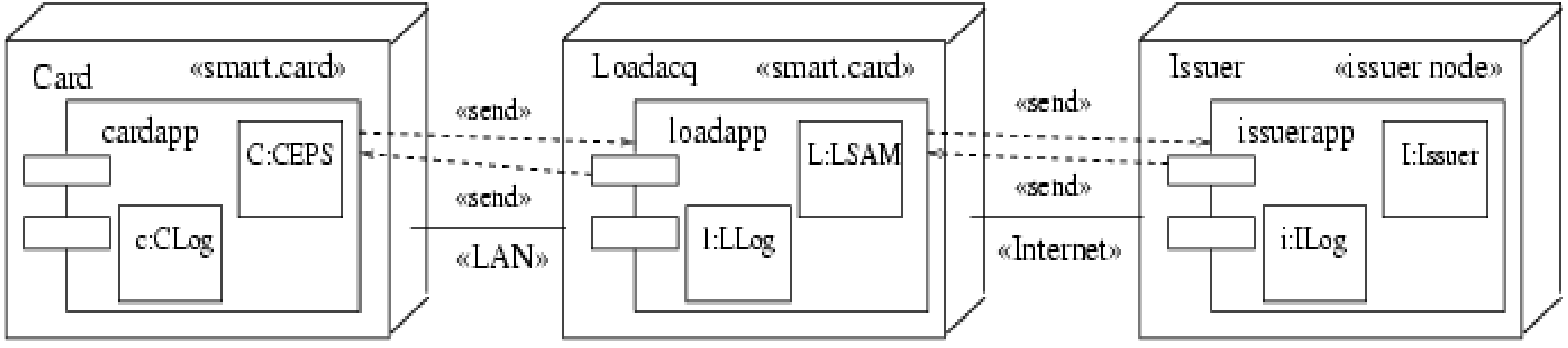
LSAM «critical» {secrecy={K_{LI}}} {integrity={K_{LI},lda,n,rl_n,$r2l_n$,r_n,m_n}}
lda, n, rl_n, $r2l_n$, m_n : Data K_{LI}, r_n : Keys
RespI(cep,nt,sl,hc) RespC(s3,rc) RespL(s2)

Issuer «critical» {secrecy={K_{CI},K_{LI},rc_{nt}}} {integrity={K_{CI},K_{LI},rc_{nt}}}
rc_{nt} : Data; K_{LI}, K_{CI} : Keys
Load(cep,lda,m,nt,s1,ml,h hl,h2l) Comp(cep,lda,m,nt,r2l,s3)

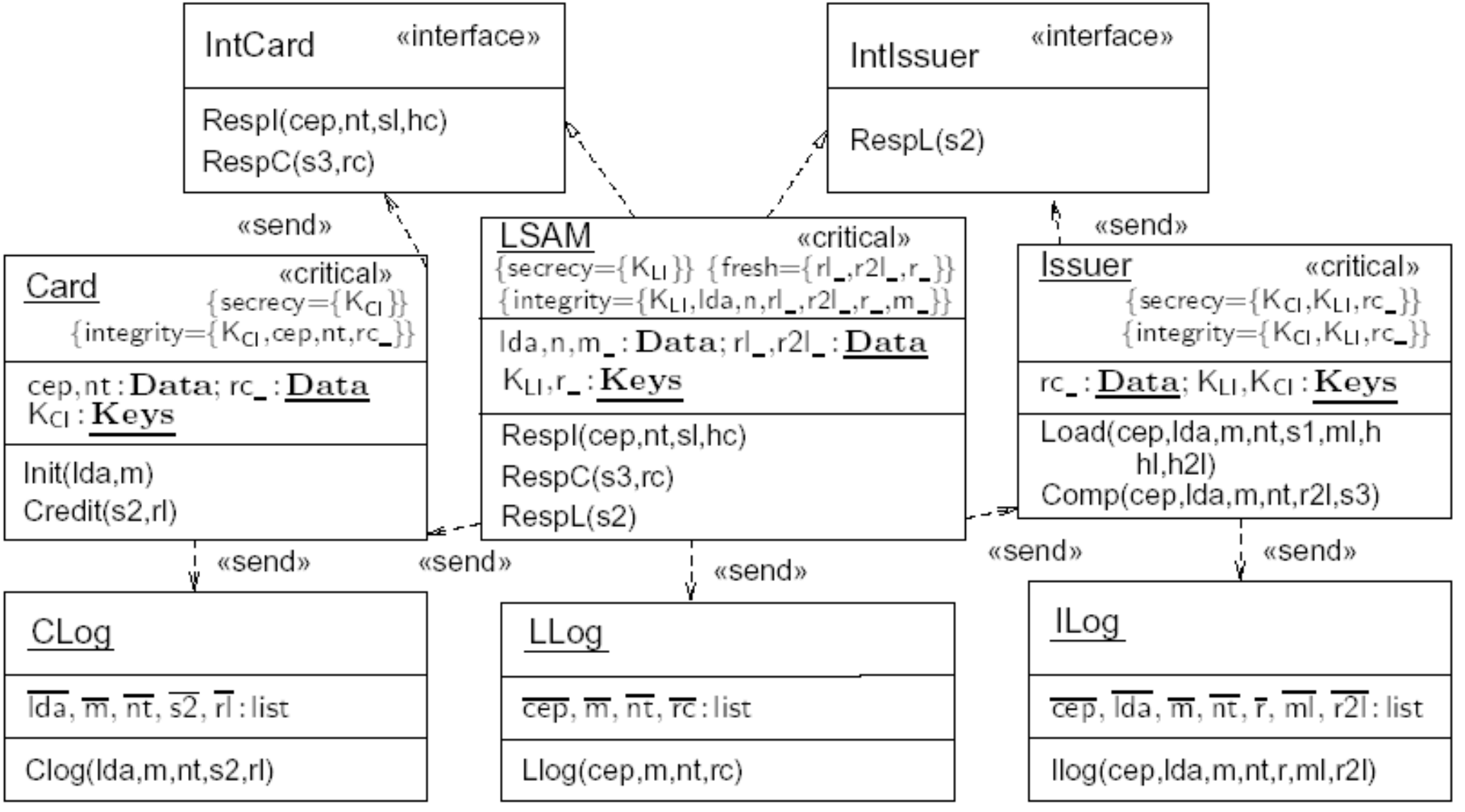


technische univ
dortmund

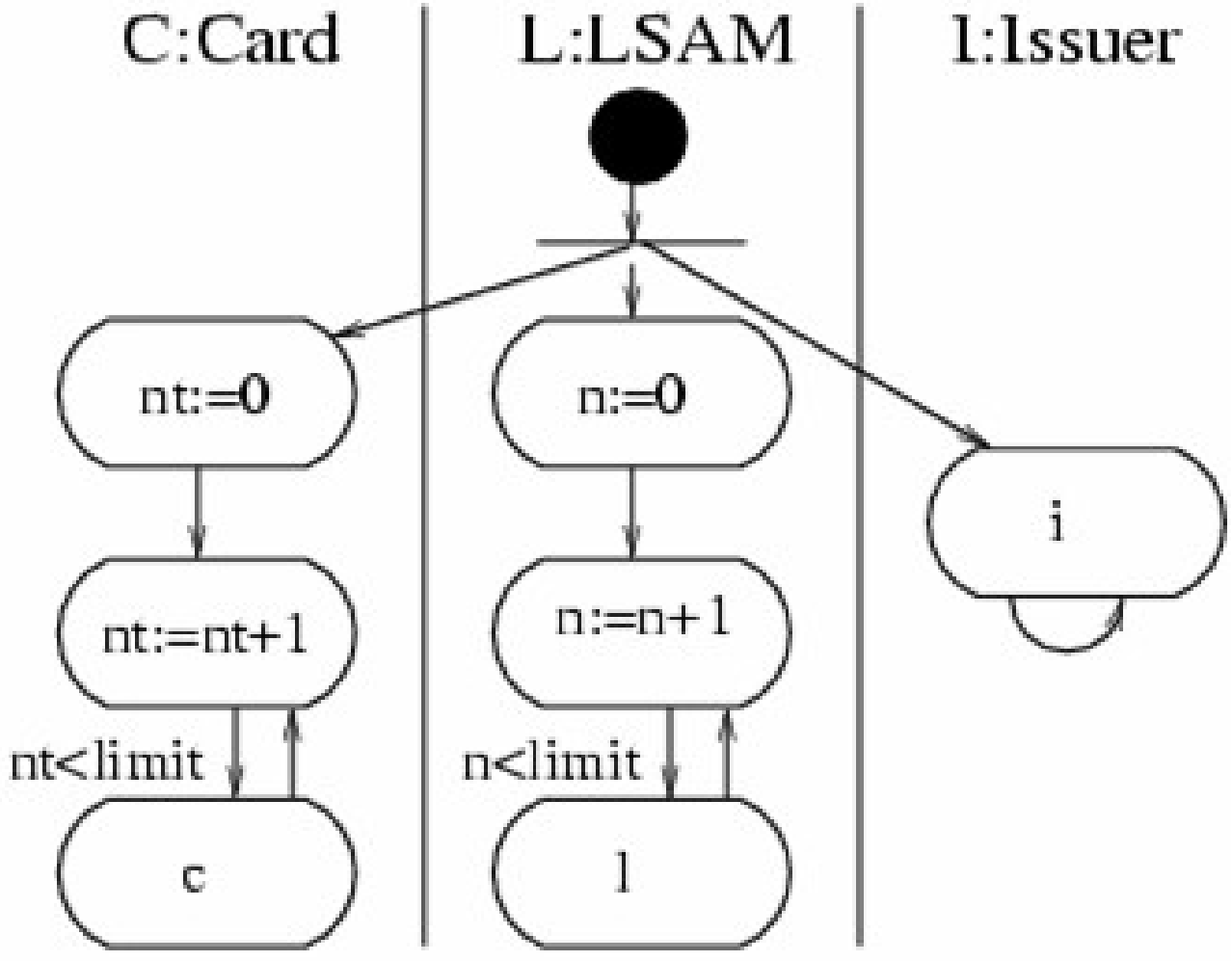
Lade-Protokoll: Verteilungsdiagramm



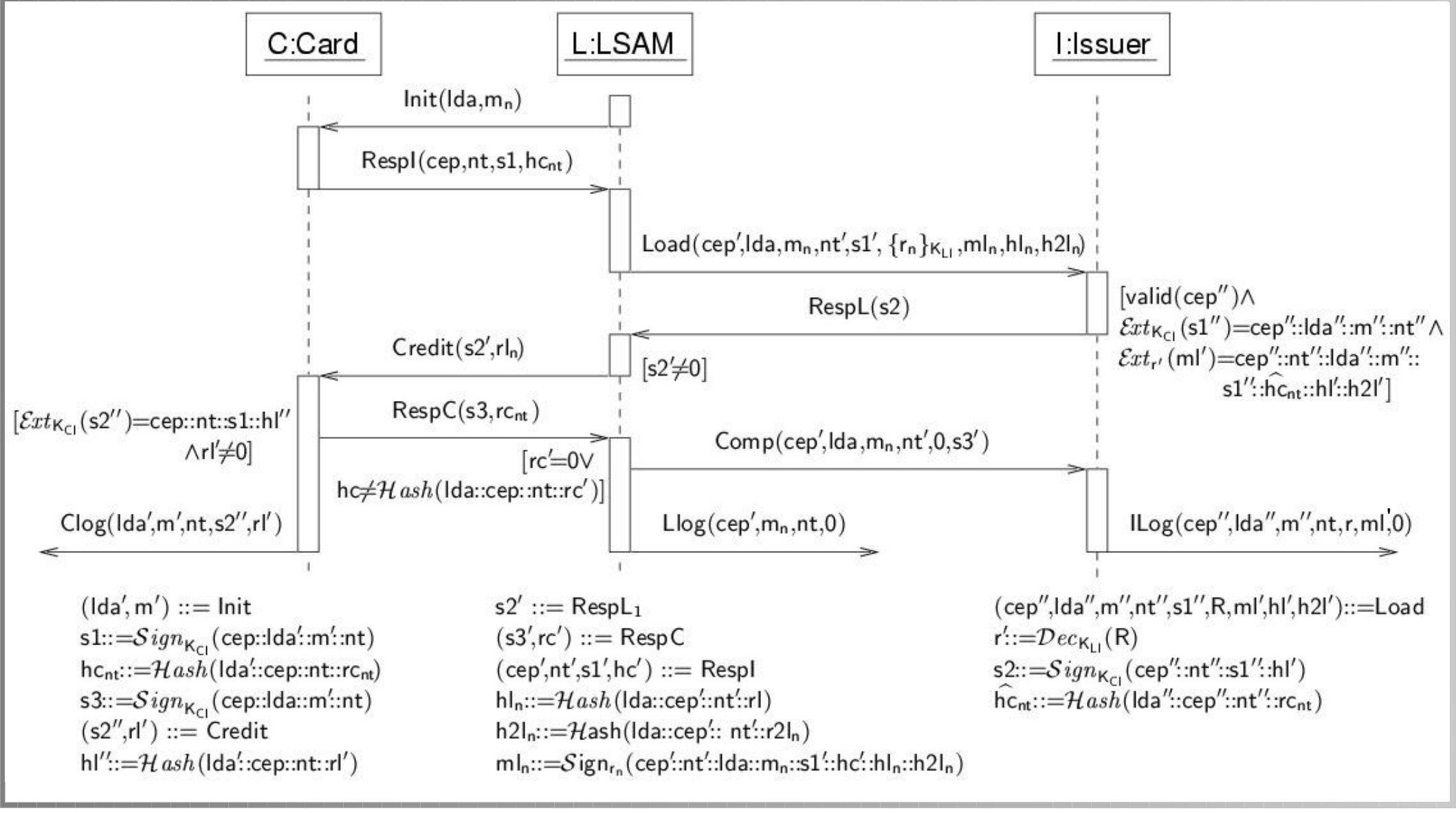
Lade-Protokoll: Klassendiagramm



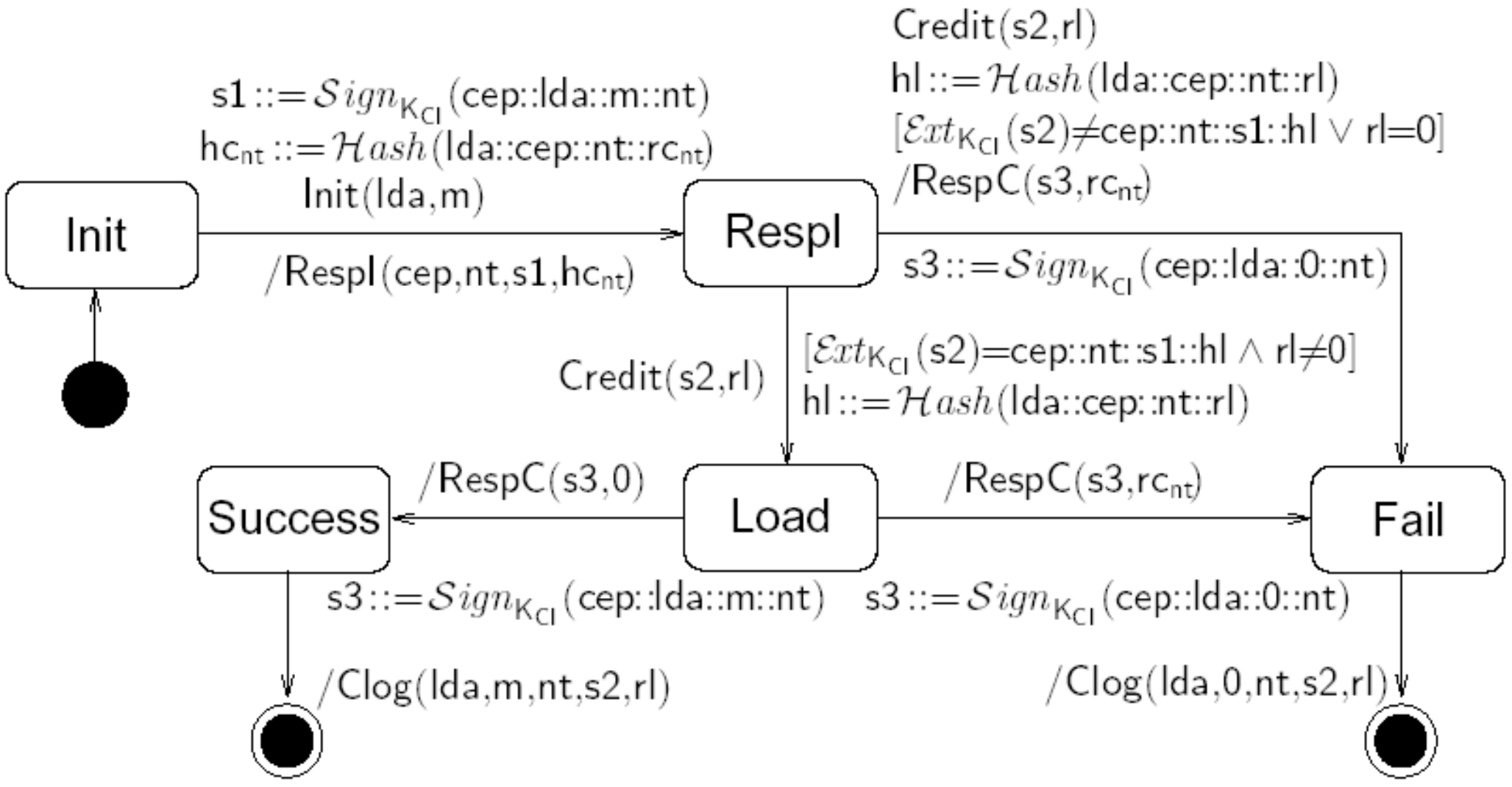
Lade-Protokoll: Koordination



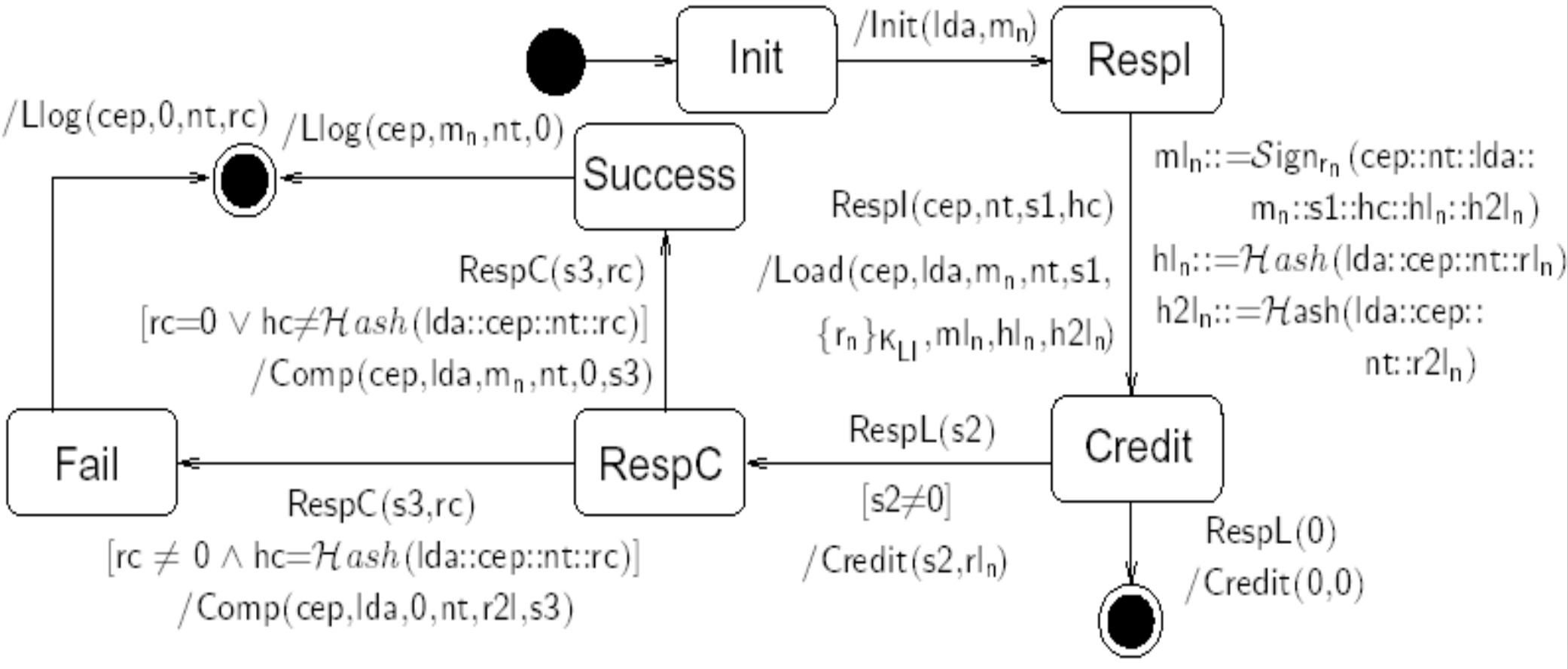
Lade-Protokoll: Interaktion



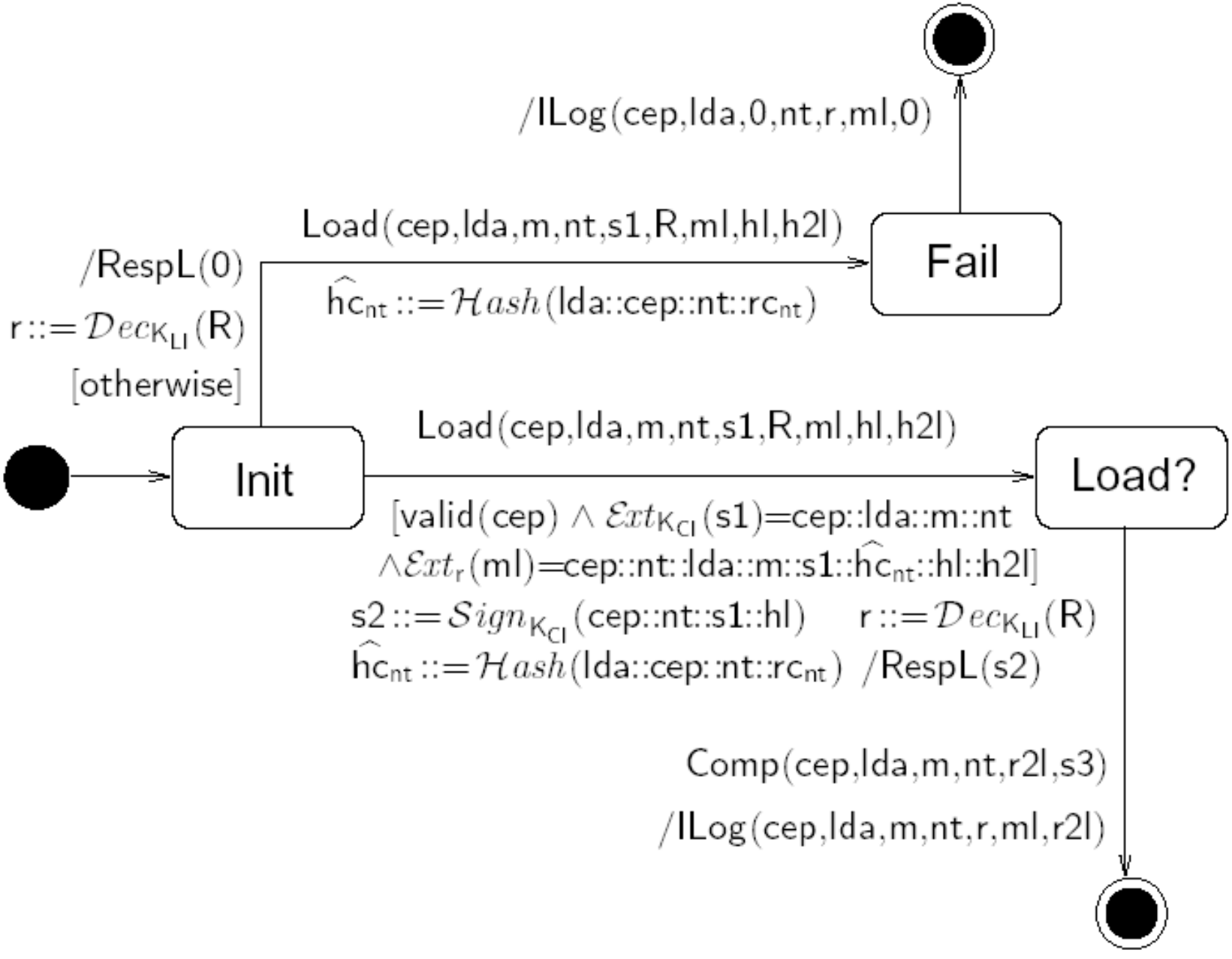
CEPS-Karte: Statechart



CEPS-LSAM: Statechart



CEPS-Kartenemittent: Statechart



Übersicht Daten-werte

Variable	Explanation
C	card
L	LSAM
I	card issuer
rc_{nt}	secret random values shared between card and issuer
rl_n, $r2l_n$	random numbers of LSAM
r_n	symmetric keys of LSAM
m_n	transaction amounts
m, rl, hl	m_n, rl_n, hl_n as received at card issuer
nt	card transaction number
n	acquirer-generated identification number
lda	load device identifier
cep	card identifier
s1	card signature: $\mathcal{S}ign_{K_{CI}}(\mathsf{cep}::\mathsf{lda}::\mathsf{m}::\mathsf{nt})$
hc_{nt}	card hash value: $\mathcal{H}ash(\mathsf{lda}::\mathsf{cep}::\mathsf{nt}::rc_{nt})$
$\widehat{hc}_{nt}$	hc_{nt} as created at issuer
rc, hc	rc_{nt}, hc_{nt} as received at load acquirer
K_{CI}	key shared between card and issuer
K_{LI}	key shared between LSAM and issuer
ml_n	$\mathcal{S}ign_{r_n}(\mathsf{cep}::\mathsf{nt}::\mathsf{lda}::m_n::\mathsf{s1}::\mathsf{hc}::hl_n::h2l_n)$ (signed by LSAM)
hl_n	hash of transaction data: $\mathcal{H}ash(\mathsf{lda}::\mathsf{cep}::\mathsf{nt}::\mathsf{rl})$
$h2l_n$	hash of transaction data: $\mathcal{H}ash(\mathsf{lda}::\mathsf{cep}::\mathsf{nt}::\mathsf{r2l})$
s2	issuer signature: $\mathcal{S}ign_{K_{CI}}(\mathsf{cep}::\mathsf{nt}::\mathsf{s1}::\mathsf{hl})$
s3	card signature of the form $\mathcal{S}ign_{K_{CI}}(\mathsf{cep}::\mathsf{lda}::\mathsf{m}::\mathsf{nt})$

Bedrohungsszenarien

Annahme: Karte und LSAM manipulationssicher.

Mögliche Angreiferaktionen: Kommunikation abhören, Komponenten ersetzen.

Mögliche Motive (Beispiele):

Kartenbesitzer: Aufladen, ohne zu bezahlen.

Ladestation Betreiber: Geld des Kartenbesitzers einbehalten.

Kartenemittent: Unberechtigt Geld vom Ladestation-Betreiber verlangen.

Gemeinsamer Angriffsversuch denkbar.

Sicherheitsanforderungen (informell)

Kartenbesitzer: Wenn Karte laut Log-Daten mit dem Betrag *m* aufgeladen wurde, kann der Kartenbesitzer dem Karten-Emittenten beweisen, dass der Ladestation-Betreiber ihm *m* schuldet.

Ladestation-Betreiber: Ladestation-Betreiber muss Betrag *m* dem Kartenemittenten nur zahlen, nachdem er den Betrag vom Kartenbesitzer erhalten hat.

Karten-Emittent: Summe der Guthaben von Karten-inhaber und Ladestation-Betreiber nach Transaktion unverändert.

Ladestationbetreiber-Sicherheit: Technisch

Definiere Sicherheitsanforderung des Ladestationsbetreibers mit Bezug auf die Protokollnachrichten:
Nehme an, dass Kartenemittent *I* die Signatur $ml_n = Sign_{rn}(cep::nt::lda::m_n::s1::hc_{nt}::hl_n::h2ln)$ besitzt und dass Karte *C* die Zufallszahl rl_n besitzt, wobei $hl_n = Hash\ (lda::cep::nt::rl_n)$.

Dann gilt nach der Transaktion eine der folgenden Aussagen:

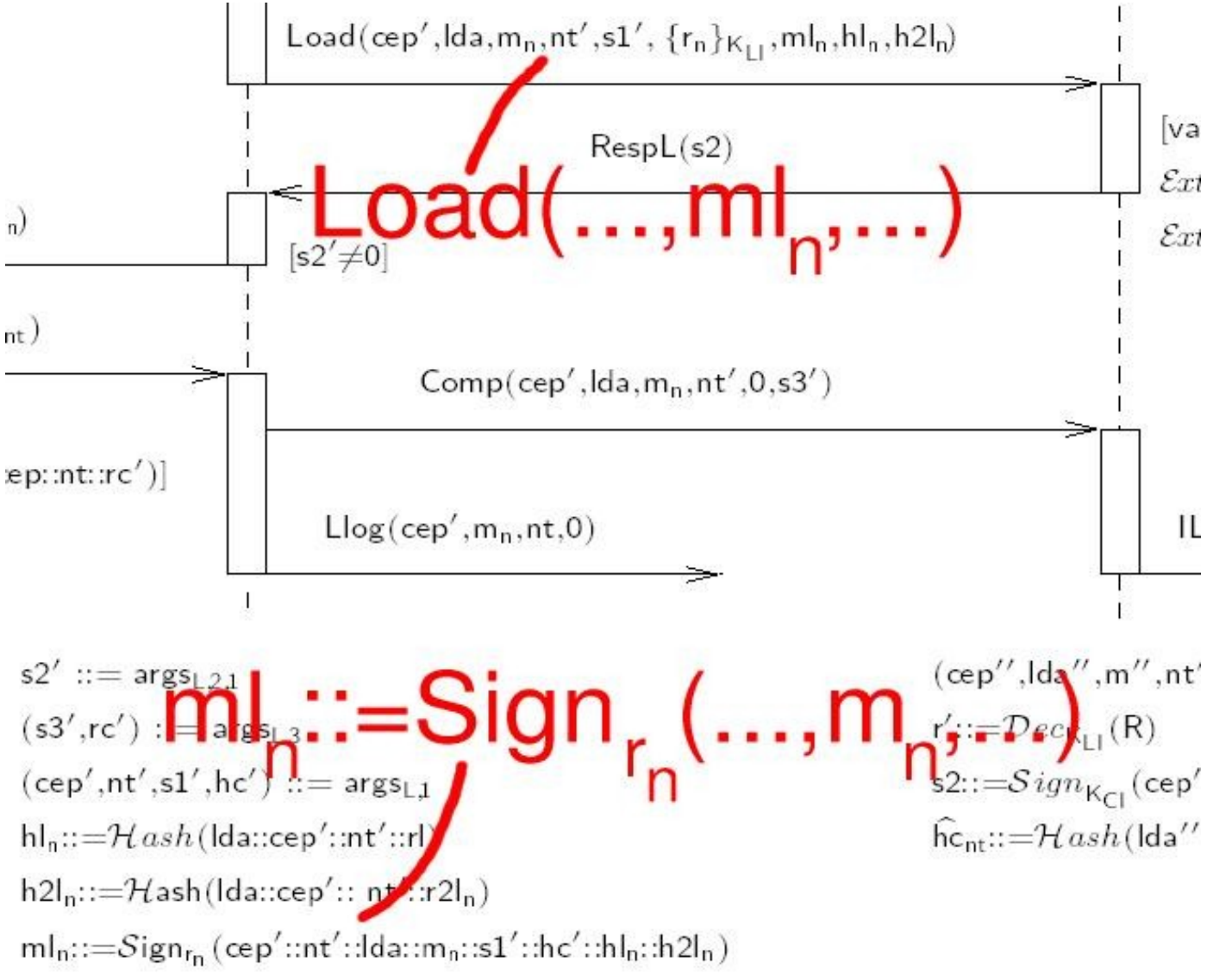
- Llog(cep,lda,m_n,nt) wurde zu I:LLog gesendet (also hat der Ladegerätbetreiber L den Betrag m_n in bar bekommen) oder
- Llog $(cep, lda, 0, nt)$ wurde zu I:LLog gesendet (also hat der Ladegerätbetreiber L den Betrag m_n dem Kartenbesitzer zurückgegeben) und L hat die Zufallszahl rc_{nt} erhalten (die den Wert m_{ln} negiert), wobei $hc_{nt} = Hash(lda::cep::nt::rc_{nt})$.

Ladegerätbetrieber-Sicherheit

"m_{ln} gewährt die Garantie, dass der Ladegerätbetreiber den Transaktionsbetrag dem Kartenemittenten schuldet"
(Zitat CEPS-Spezifikation)

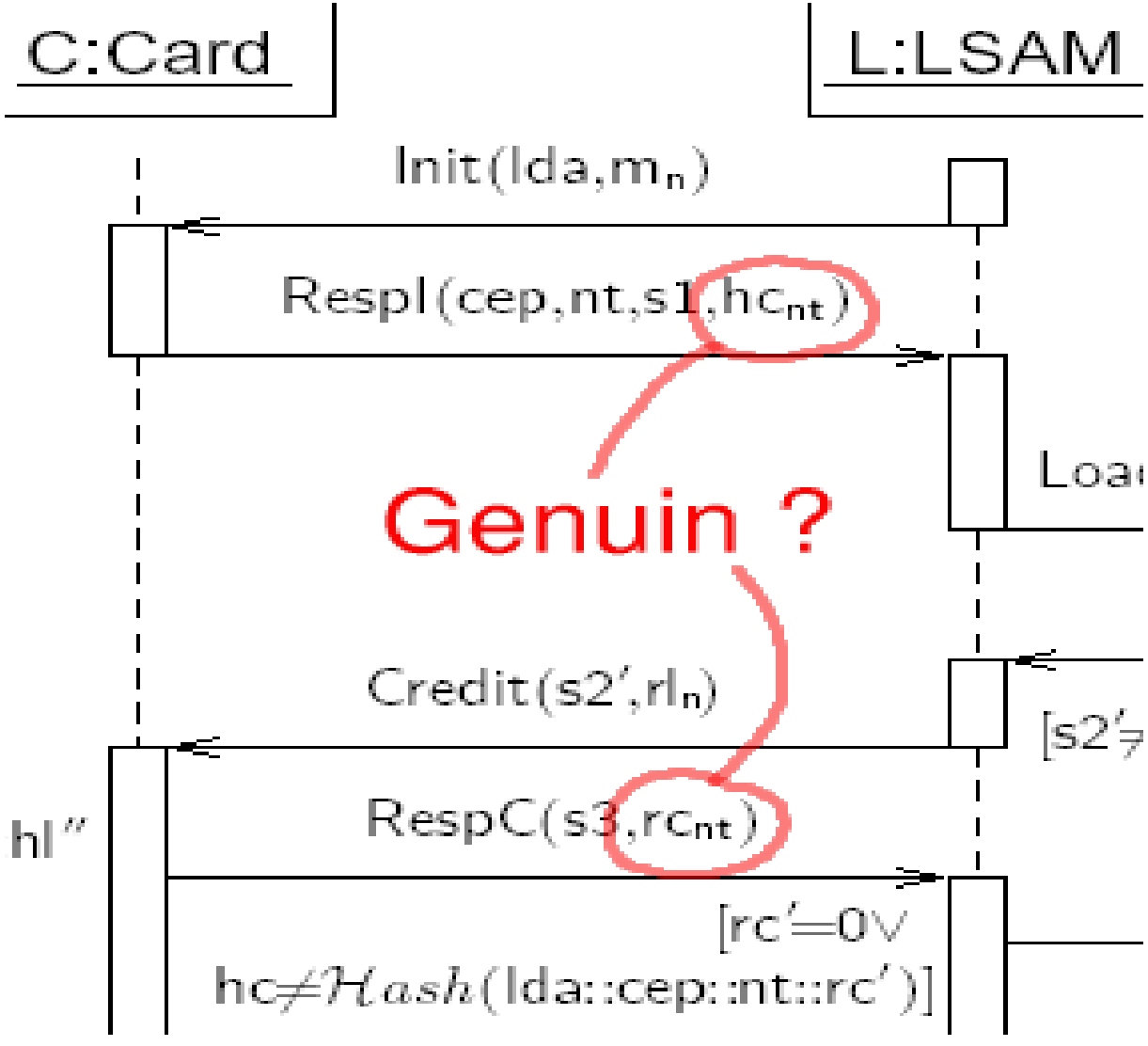
Überraschung

- ml_n: „Beweis“ für Bank, dass Lade-gerät Geld erhielt.
- Aber: r_n geteilt zwischen Bank und Ladegerät (symmetrisch).



Überraschung (2)

rc_{nt}: „Beweis“ für LSAM, dass Ladegerät nur Betrag m_n erhielt.
Aber: LSAM kann Validität von rc_{nt} nicht beweisen.



Schwachstelle

Analyse: Keine Sicherheit für Ladestation gegen interne Angreifer.

Änderung: asymmetrischer Schlüssel in ml_n , Signatur für hc_{nt}.

Modifizierte Version sicher laut Analyse.

Kartenbesitzer-Sicherheit

Kartenbesitzer-Sicherheit:

1) Für jede Nachricht Clog*(lda,m,nt,s2,rl)*, die an c : Clog gesendet wird, wenn $m \neq 0$ (d.h. wenn es scheint, dass Karte mit m geladen wurde), dann $rl \neq 0$ und es gilt:

$$Ext_{KCl}(s2) = cep :: nt :: Sign_{KCl}(cep :: lda :: m :: nt) :: Hash(lda :: cep :: nt :: rl)$$

(wobei der Kartenemittent bestätigt, dass *rl* ein geprüfter Nachweis der Transaktion ist). Und:

2) Für jede zwei Nachrichten Clog*(lda,m,nt,s2,rl)* und *Clog(lda',m',nt',s2',rl')* die zu c : Clog gesendet wurden, haben wir nt ≠ nt'.

Kartenemittent-Sicherheit:

Für jede Nachricht Clog*(lda,m,nt,s2,rl)*, die an c : Clog gesendet wird, wenn $m \neq 0$ und

$$Ext_{KCl}(s2) = cep :: nt :: Sign_{KCl}(cep :: lda :: m :: nt) :: Hash(lda :: cep :: nt :: rl)$$

für einen Wert lda gilt, dann hat der Kartenemittent eine gültige Signatur m_{ln} gemäß der Transaktion.

Aktuelles zum Thema Geldkarten

SPIEGEL ONLINE

13. Juni 2012, 13:52 Uhr

"Girogo" der Sparkassen

Datenschützer fürchten Missbrauch bei neuer Funk-Geldkarte

Von Hilmar Schmundt und Ole Reißmann

Die Sparkassen feiern die neuen funkenden Girokarten als tollen Service. Doch die Kritik am Drahtlos-Cash "Girogo" wächst. Das Plastikgeld verrät, wo der Besitzer zuletzt eingekauft hat - und für wie viel. Datenschützer sind alarmiert, der Sparkassenverband findet das nicht weiter schlimm.

Hamburg - Die Sparkassen wollen ihre 45 Millionen Kunden mit neuem Plastikgeld ausstatten. Drahtloses Bezahlen per NFC-Kurzstreckenfunk (Near Field Communication) sollen die Karten künftig ermöglichen. Mit einem Wisch vor einem Lesegerät lässt sich Geld übertragen. Im Raum Hannover startet "Girogo" mit 1,5 Millionen Nutzern, in drei Jahren soll ganz Deutschland Cash funken können.

Schnell soll es jetzt gehen, damit nicht internationale Firmen wie Visa, Mastercard oder, schlimmer noch, die Internetriesen Google und Paypal das Geschäft mit dem drahtlosen Bezahlen machen. Doch womöglich wird die neue Bezahltechnik überhastet eingeführt, mit Funktionen, die nicht besonders ausgereift sind.

Denn beim Einsatz der neuen Sparkassen-Karte könnten viele Informationen über ihren Besitzer verraten werden, warnen Datenschützer. Die Funkkarten haben eine eindeutige Kennung, lassen sich unbemerkt auslesen und damit zur Überwachung missbrauchen. Nicht nur das: Die Karten speichern die letzten 15 Bezahlvorgänge und die letzten drei Ladevorgänge - unverschlüsselt und drahtlos auslesbar, wie der Programmierer Andreas Schiermeier herausgefunden hat.

Software zum Auslesen der Karten gibt es im Netz

"Zu jeder dieser Transaktionen ist ein Datums- und Zeitstempel, der Betrag und die Kennung des Händlers oder des Ladeterminals hinterlegt", sagt Schiermeier, der zum Frankfurter Chaos Computer Club gehört. Dabei sei es egal, ob die Geldkarte drahtlos oder auf herkömmliche Weise eingesetzt werde. Ausgelesen werden konnten solche Daten mit entsprechenden Lesegeräten bisher auch schon. Aber: "Der drahtlose Zugriff auf diese Daten ist neu."

Das Auslesen sei äußerst trivial, sagt Schiermeier. Benötigt werde nur ein handelsübliches RFID-Lesegerät und eine Software. Passende Lesegeräte wurden zum Beispiel zum Start des elektronischen Personalausweises ausgegeben, Software für Windows gibt es kostenlos im Netz. Dabei könnten die Daten auch verschlüsselt auf der Karte gespeichert werden, um sie vor unberechtigtem Zugriff zu schützen.

Die Sparkasse findet das nicht weiter schlimm, weil auf der Karte "keinerlei personenbezogene Daten" abgelegt seien, wie Michael Schlier vom Sparkassenverband Hannover sagt. "Weder der Ort des Einkaufs noch die gekaufte Ware noch der Händlername ist nachvollziehbar." Kunden könnten so einen Überblick über ihre Finanzen behalten. "Für jeden anderen sind diese Informationen jedoch ohne Wert."

Zusammenfassung

- Aufbau Common Electronic Purse Specifications
- Protokoll
- Schwachstellen-Analyse
- Verbesserung