Willkommen zur Vorlesung

# *Softwarearchitekturen im Finanz- und Versicherungsbereich*

im Sommersemester 2010

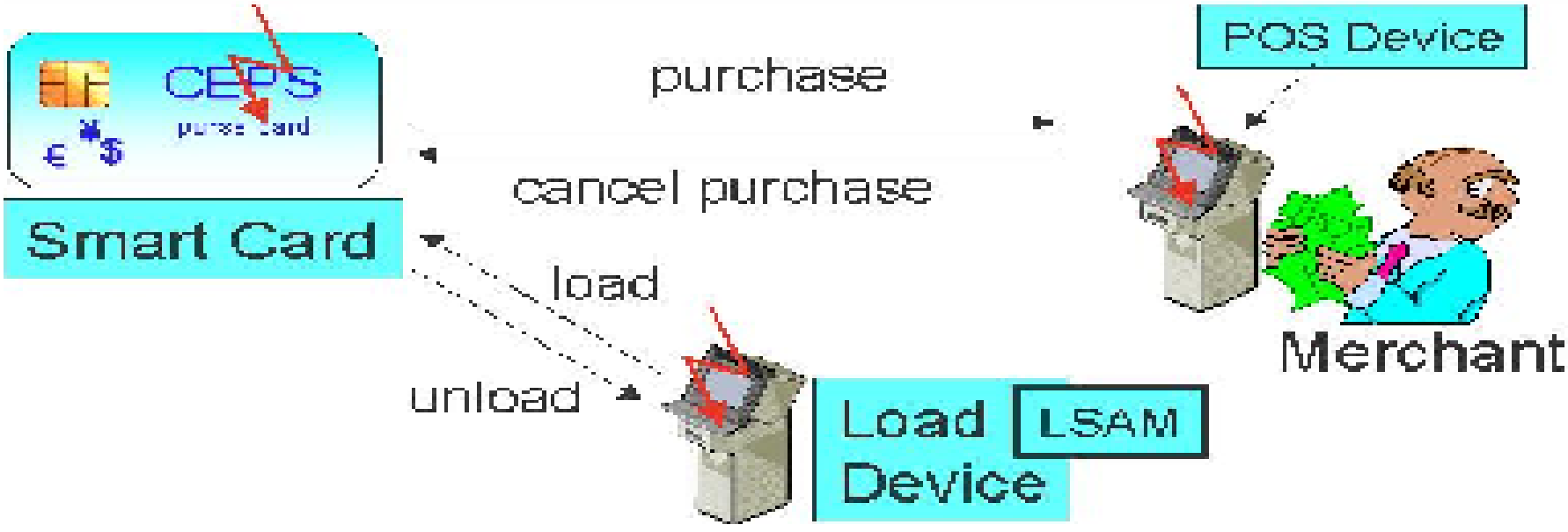
Prof. Dr. Jan Jürjens

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

# 7.Elektronische Geldbörsen

# Common Electronic Purse Specifications



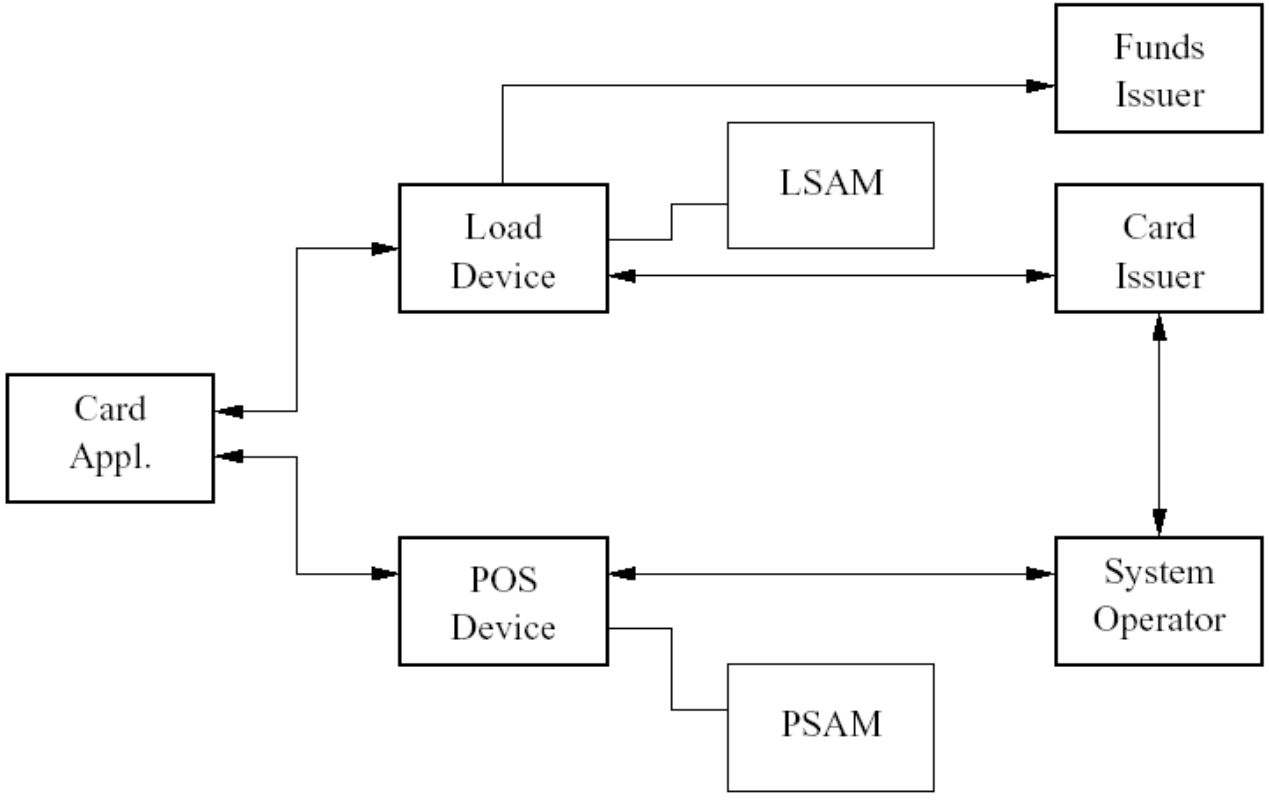



Globaler Standard (90% des Marktes).

Smart card speichert Kontostand. Kryptographie auf Chip sichert Transaktionen.

Sicherer als Kreditkarten (transaktionsgebundene Autorisierung).

# CEPS Überblick



# Aufgabe 7.1

- Zeichne einen Bedrohungsbaum für das CEPS System. [3 P.]

# Purchase Protocol

Offline transaction to pay for goods with money previously loaded on card.

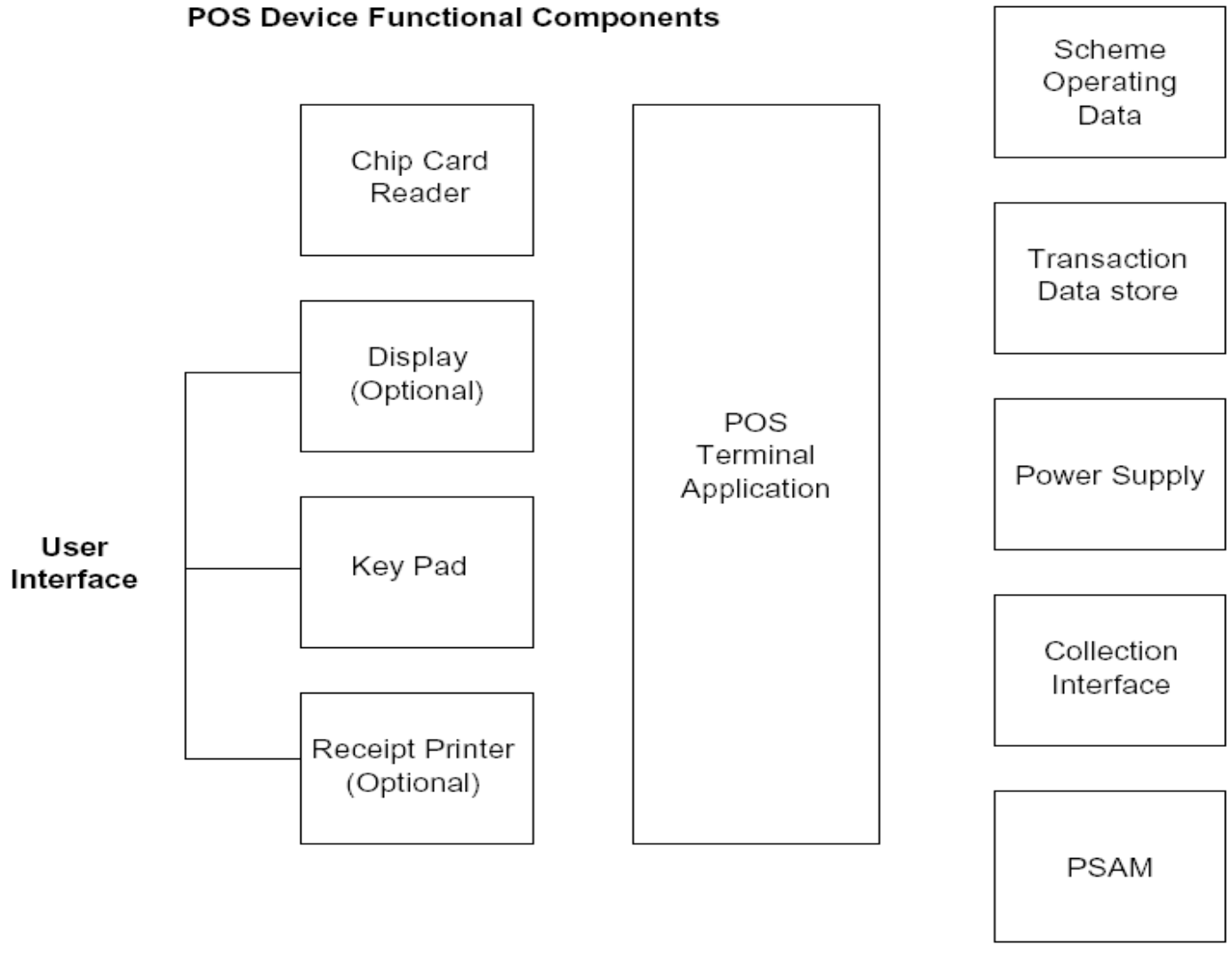
Protocol participants: customer's card, merchant's POS device.

POS device contains Purchase Security Application Module (PSAM): all security-critical data processing and storage for POS device.

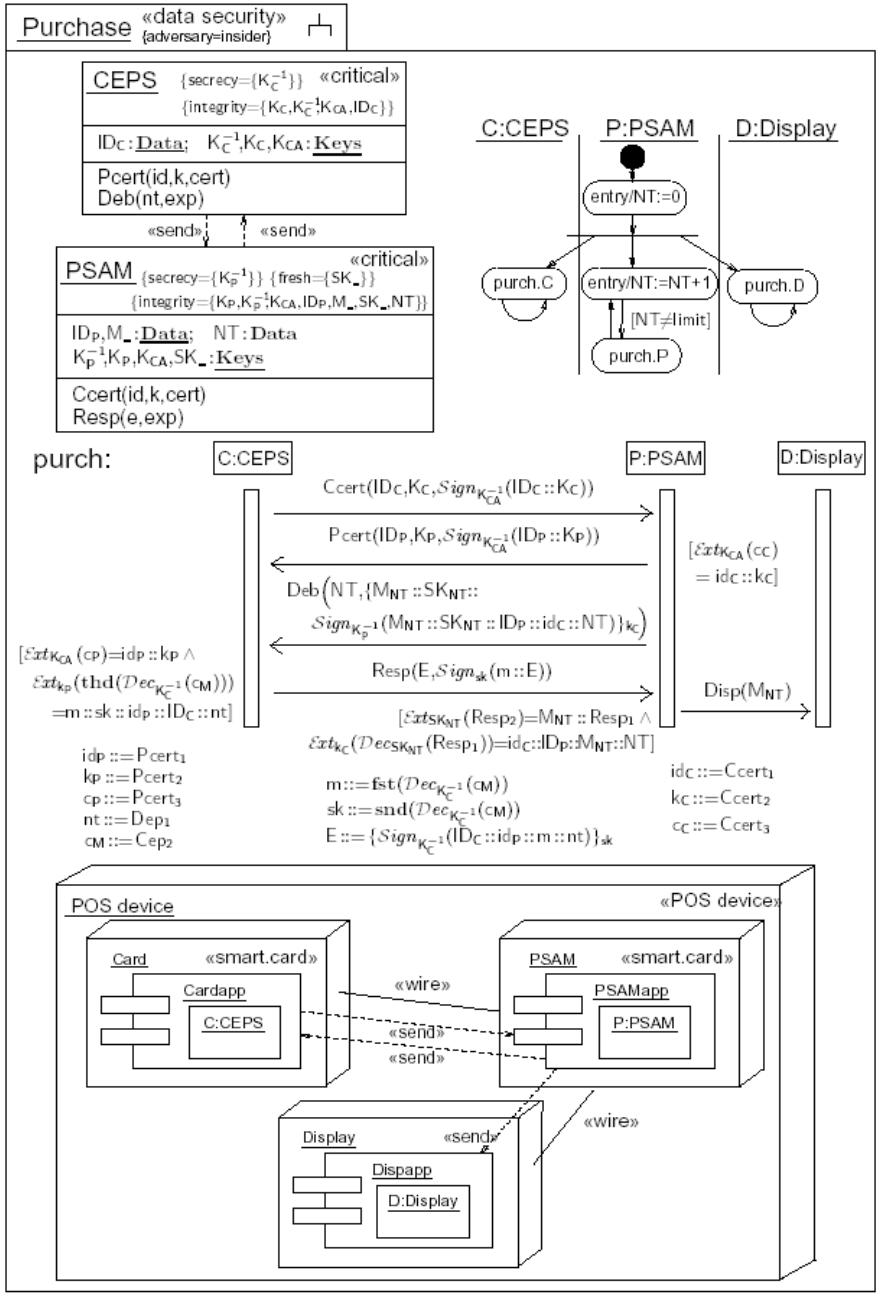
Card account balance adjusted; transaction data logged and later sent to issuer for financial settlement.

Use at public terminals; Internet use envisaged.

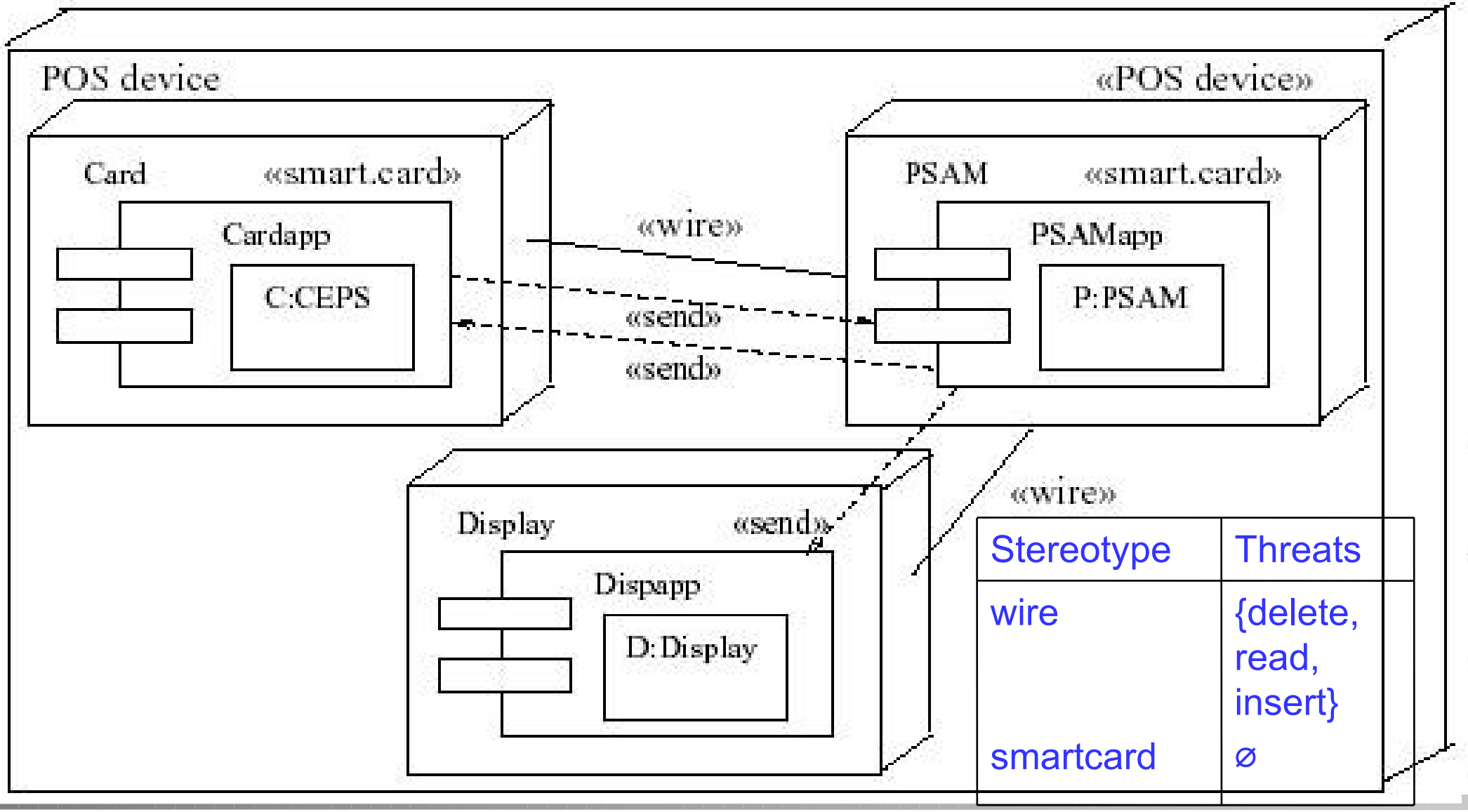
# POS Device


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

# UMLsec Spec.

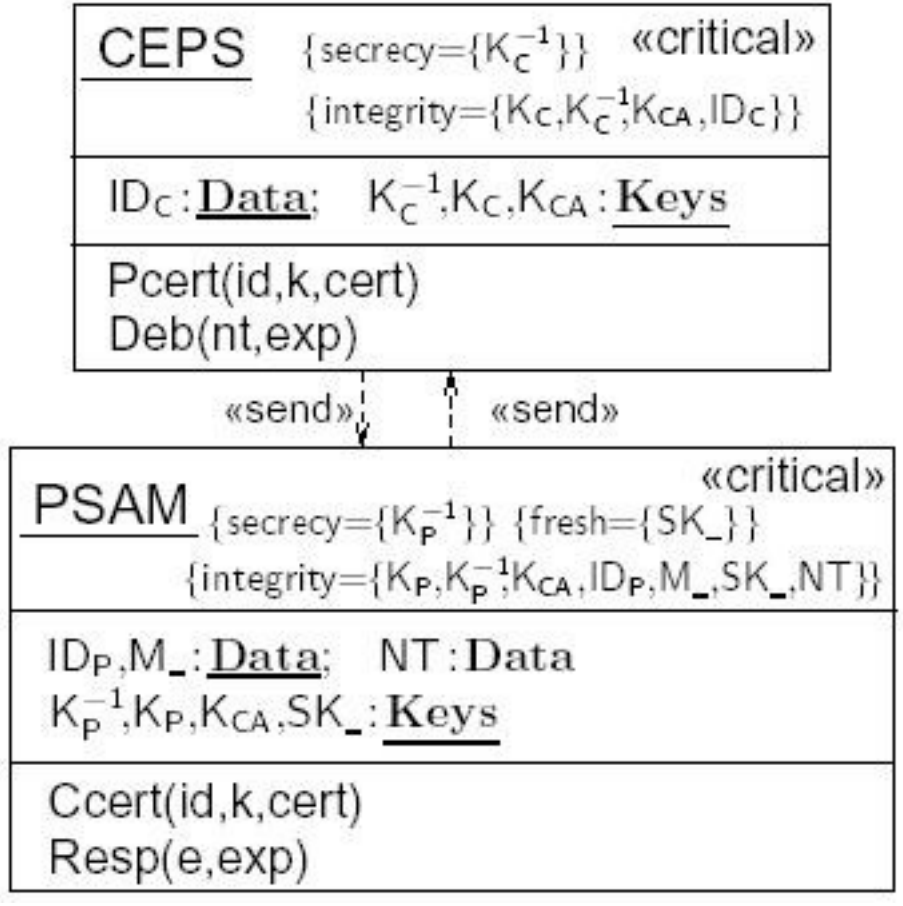

Purchase «data security» {adversary=insider}
CEPS {secrecy={K_C^-1}} «critical» {integrity={K_C,K_C^-1,K_CA,ID_C}}
ID_C:Data; K_C^-1,K_C,K_CA:Keys
Pcert(id,k,cert)
Deb(nt,exp)
«send» «send»
PSAM {secrecy={K_P^-1}} {fresh={SK_}} «critical» {integrity={K_P,K_P^-1,K_CA,ID_P,M_,SK_,NT}}
ID_P,M_:Data; NT:Data
K_P^-1,K_P,K_CA,SK_:Keys
Ccert(id,k,cert)
Resp(e,exp)
C:CEPS
P:PSAM
D:Display
entry/NT:=0
purch.C
entry/NT:=NT+1
purch.D
[NT≠limit]
purch.P
purch:
Ccert(ID_C,K_C,Sign_{K_CA^-1}(ID_C::K_C))
Pcert(ID_P,K_P,Sign_{K_CA^-1}(ID_P::K_P))
[Ext_{K_CA}(cc) = id_C::k_C]
Deb(NT,{M_NT::SK_NT:: Sign_{K_P^-1}(M_NT::SK_NT::ID_P::id_C::NT)}_{k_C})
[Ext_{K_CA}(c_P)=id_P::k_P ∧ Ext_{k_P}(thd(Dec_{K_C^-1}(c_M))) =m::sk::id_P::ID_C::nt]
Resp(E,Sign_sk(m::E))
Disp(M_NT)
[Ext_{SK_NT}(Resp_2)=M_NT::Resp_1 ∧ Ext_{k_C}(Dec_{SK_NT}(Resp_1))=id_C::ID_P::M_NT::NT]
id_P::=Pcert_1
k_P::=Pcert_2
c_P::=Pcert_3
nt::=Dep_1
c_M::=Cep_2
m::=fst(Dec_{K_C^-1}(c_M))
sk::=snd(Dec_{K_C^-1}(c_M))
E::={Sign_{K_C^-1}(ID_C::id_P::m::nt)}_sk
id_C::=Ccert_1
k_C::=Ccert_2
c_C::=Ccert_3
POS device
«POS device»
Card «smart.card»
Cardapp
C:CEPS
«wire»
«send»
«send»
PSAM «smart.card»
PSAMapp
P:PSAM
«wire»
Display «send»
Dispapp
D:Display

# Purchase Protocol: Architecture

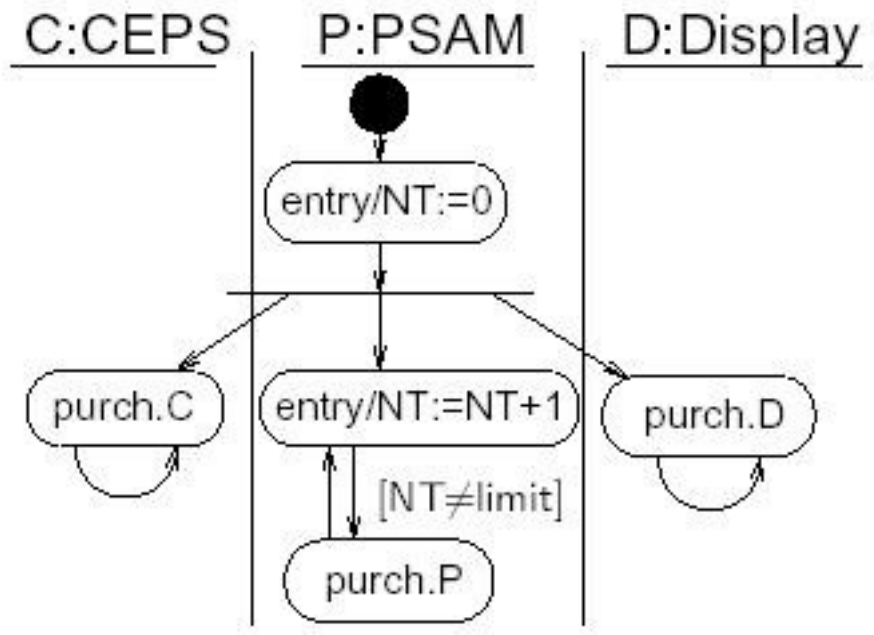



| Stereotype | Threats |
|---|---|
| wire | {delete, read, insert} |
| smartcard | ⌀ |

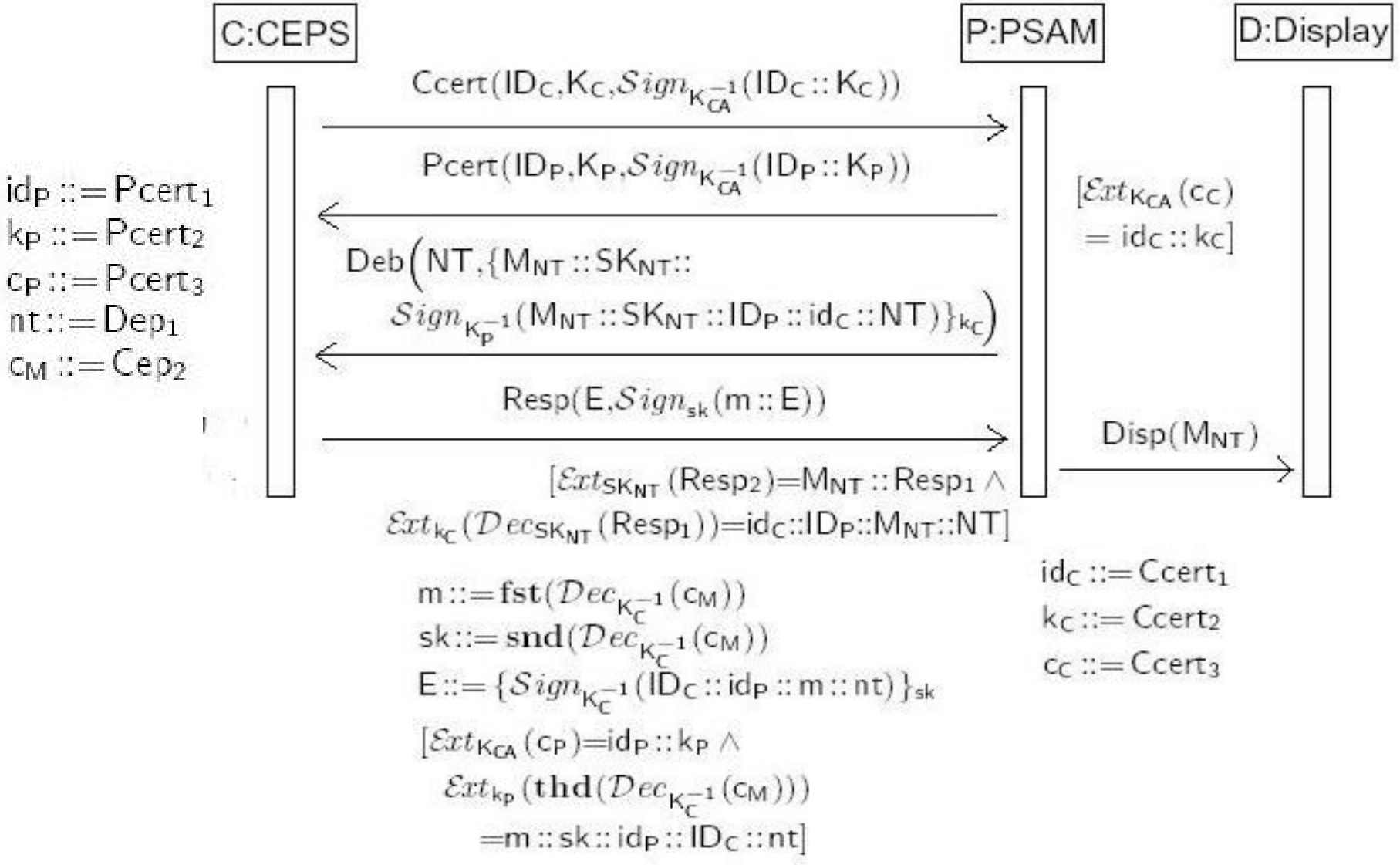
# Class Diagram



# Activity diagram



# Interaction



# Security Threat Model

Supposed to provide mutual authentication between terminal and card.

Card, PSAM assumed tamper-resistant.

Intercept communication links, replace components.

Possible attack motivations:

- **(Non-)Cardholder**: purchase without pay.
- **Merchant employee**: buy digital content with customer's card.
- **Card issuer employee**: credit transactions to own (cover-up) business.

May coincide or collude.

# Sicherheitsanalyse

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

➔ Post-Transaktions-Abrechnungsystem.

➔ Gespeicherte Transaktionsdaten sicherheitskritisch.

➔ Modell-basierte Analyse dieses Teiles.

# Aufgabe 7.2

- Welche Sicherheitseigenschaft, die für Bargeldnutzer im Allgemeinen erfüllt ist, wird durch das Post-Transaktions-Abrechnungssystem eingeschränkt (insbesondere wenn die Karte über ein Bankkonto aufgeladen wird) ? [2 P.]

# Security conditions (informal)

Cardholder security. Merchant can only claim amount registered on card after transaction.

Merchant security. Merchant receives proof of transaction in exchange for sold good.

Card issuer security. Sum of balances of valid cards and PSAMs unchanged by transaction.

# Merchant security

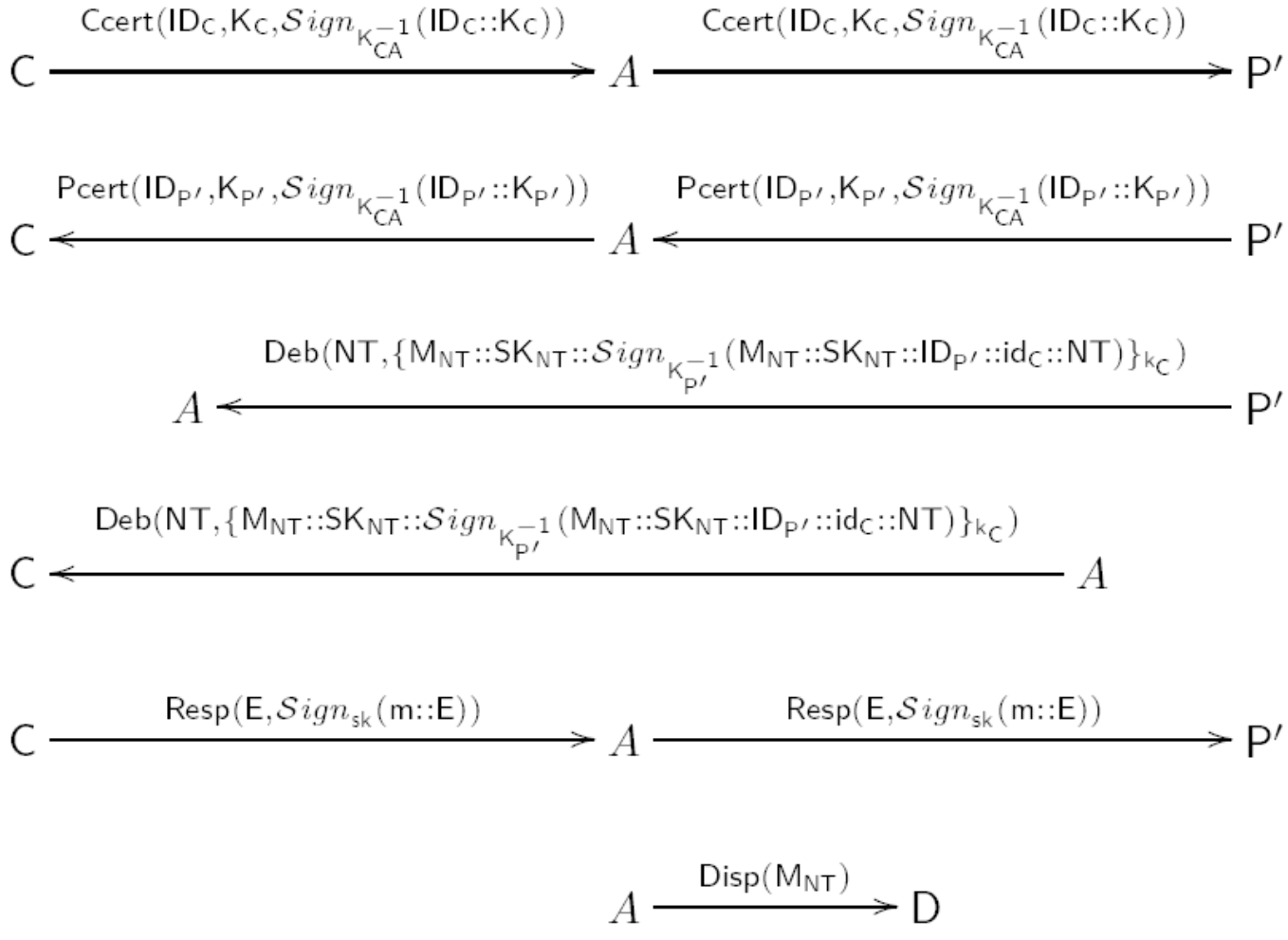
Each time display $D$ receives value $M_{NT}$, $P$ is in possession of $Sign_{K_{CA}}{}^{-1}(ID_C::K_C)$ and $Sign_{K_C}{}^{-1}(ID_C::ID_P::M_{NT}::NT)$ for some $ID_C$, $K_C{}^{-1}$ and new value $NT$.

Not satisfied. Attack automatically computed.

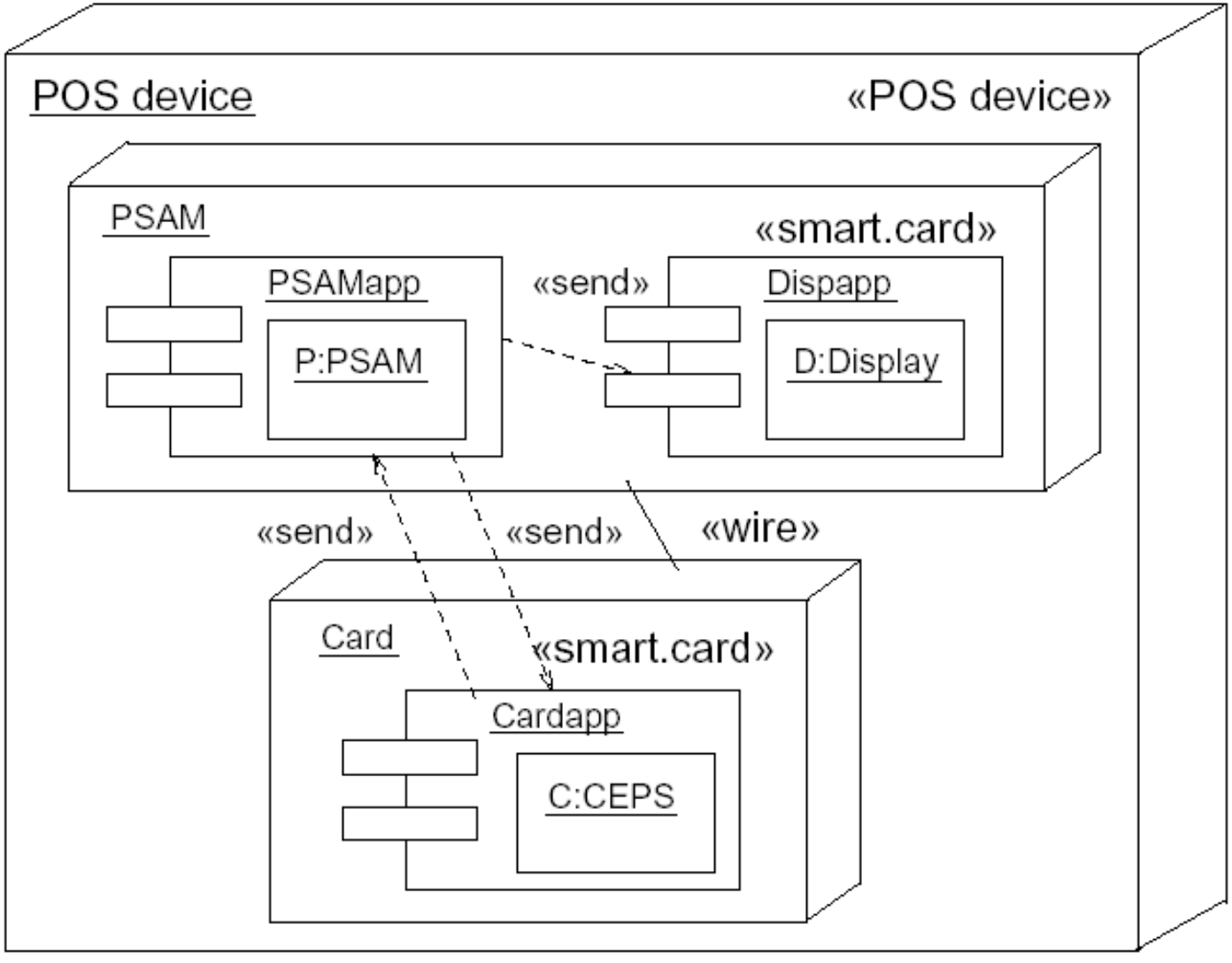
Attack exploits the fact that POS device is not tamper-proof.

Redirect messages between card and PSAM to another PSAM (e.g. to buy digital content, on the cost of the cardholder).

# Attack


Ccert(IDC,KC,$Sign_{K_{CA}^{-1}}$(IDC::KC))
C
A
Ccert(IDC,KC,$Sign_{K_{CA}^{-1}}$(IDC::KC))
P′
Pcert(IDP′,KP′,$Sign_{K_{CA}^{-1}}$(IDP′::KP′))
C
A
Pcert(IDP′,KP′,$Sign_{K_{CA}^{-1}}$(IDP′::KP′))
P′
Deb(NT,{MNT::SKNT::$Sign_{K_{P'}^{-1}}$(MNT::SKNT::IDP′::idC::NT)}kC)
A
P′
Deb(NT,{MNT::SKNT::$Sign_{K_{P'}^{-1}}$(MNT::SKNT::IDP′::idC::NT)}kC)
C
A
Resp(E,$Sign_{sk}$(m::E))
C
A
Resp(E,$Sign_{sk}$(m::E))
P′
Disp(MNT)
A
D

# Fix: Protect PSAM-device link



# Aufgabe 7.3

- Welcher Angriff wäre möglich, wenn es den Transaktionszähler *NT* nicht geben würde ? (Pfeildiagramm des Angriffablaufes zeichnen) [4 P.]

# Ladeprotokoll

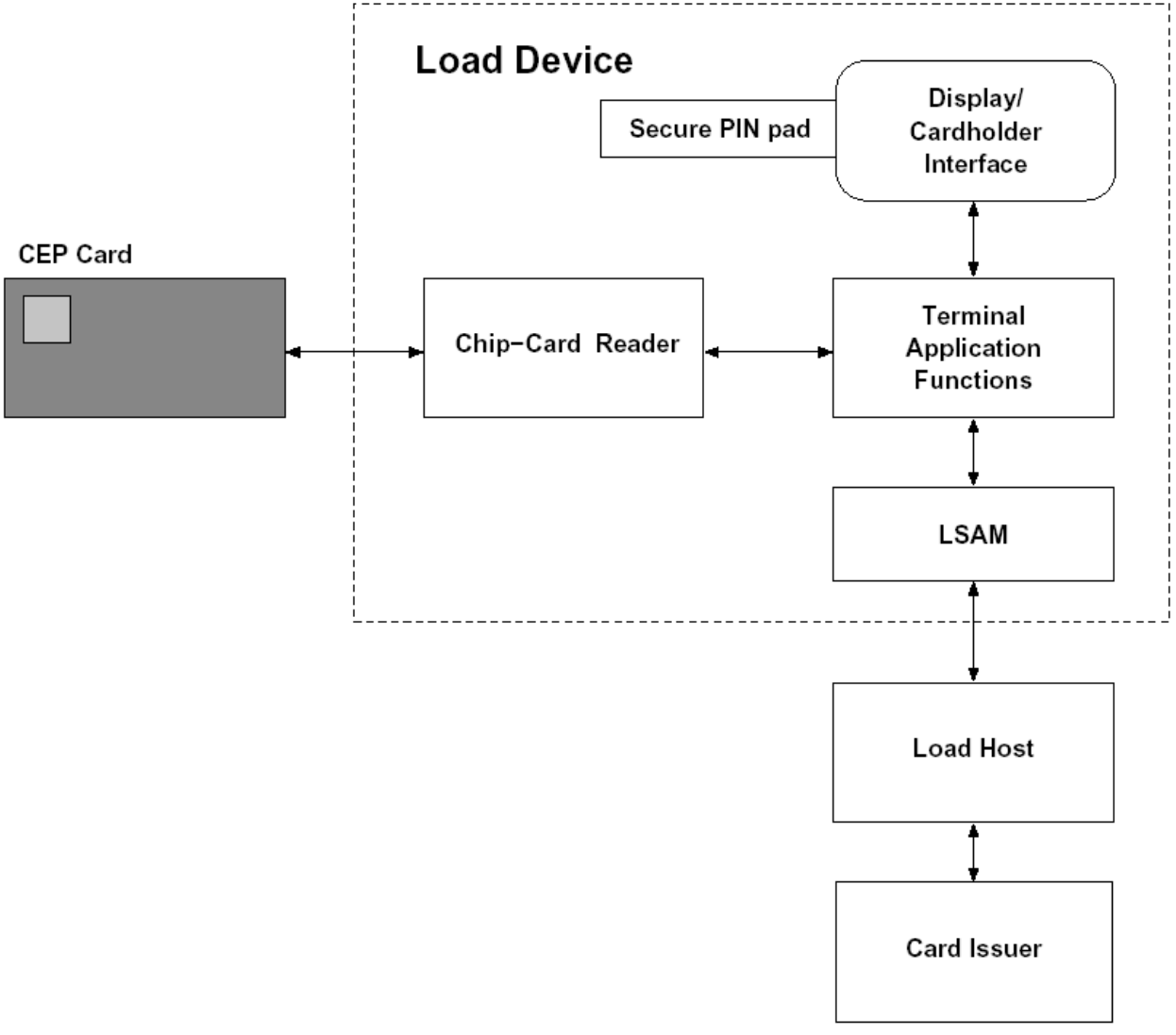
Karte mit Bargeld an Aufladestation laden (on-line).

Load Security Application Module (LSAM) speichert Transaktionsdaten.

Schickt Daten an Kartenemittent, der finanzielle Abwicklung übernimmt.

Symmetrische Verschlüsselung/Signatur.

# CEPS load device



# CEPS load device

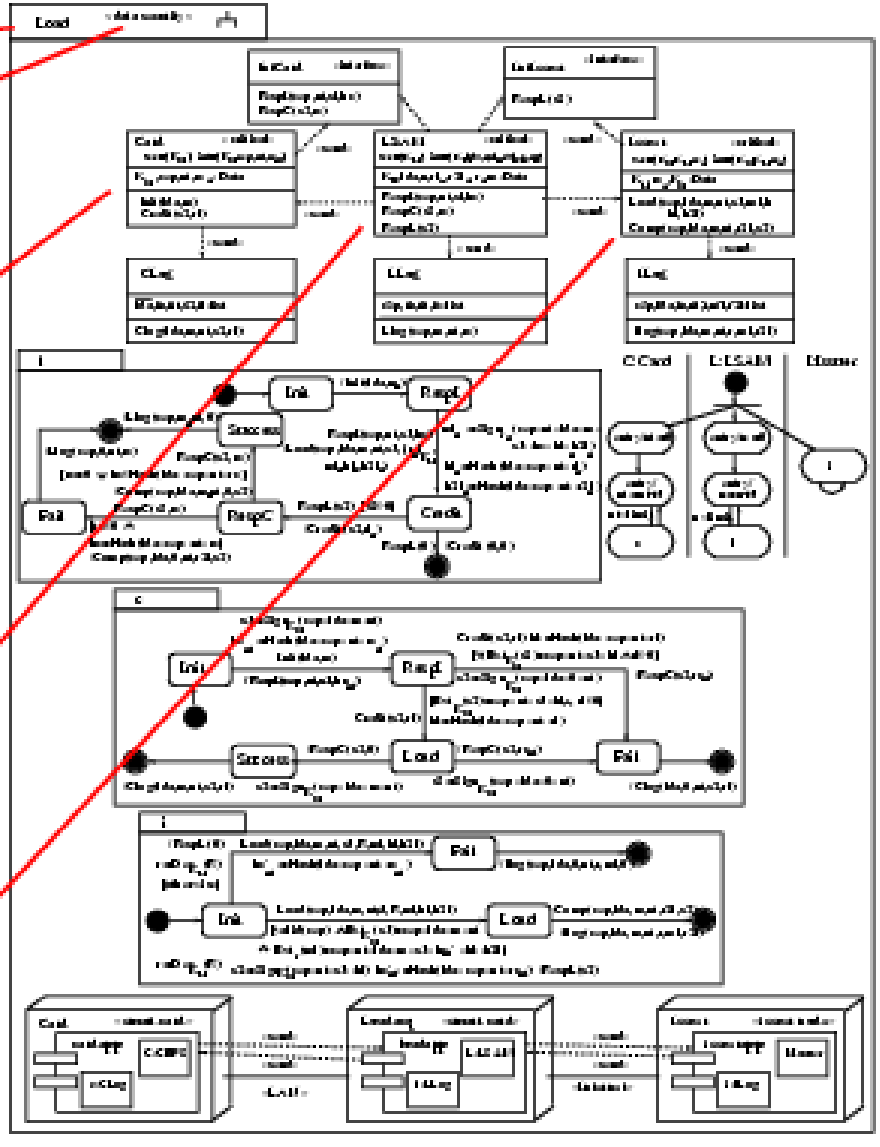
Load

«data security»

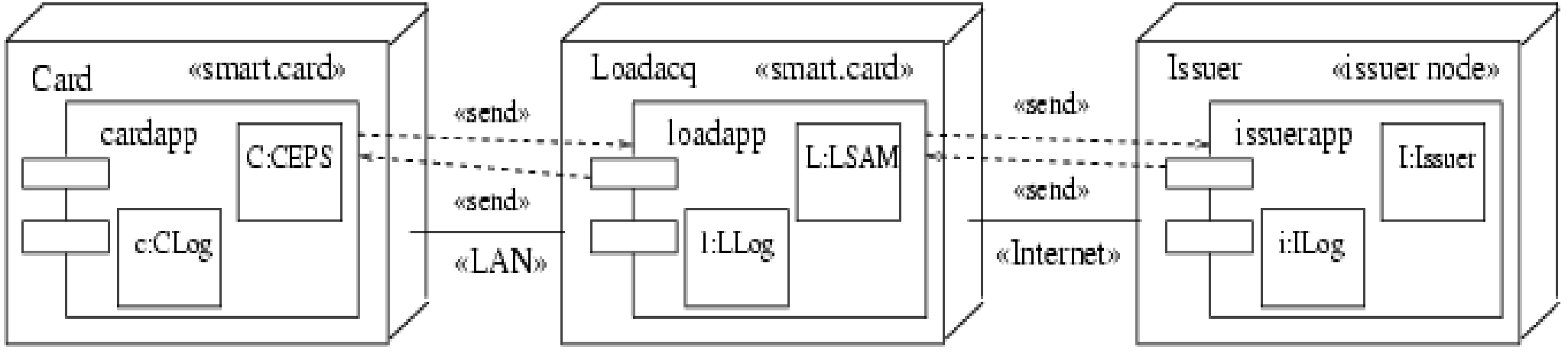
| Card «critical» {secrecy={$K_{CI}$}} {integrity={$K_{CI}$,cep,mt,$rc_{nt}$}} |
|---|
| cep, nt, $rc_{nt}$ : Data; $K_{CI}$ : Keys |
| Init(lda,m)<br>Credit(s2,rl) |

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

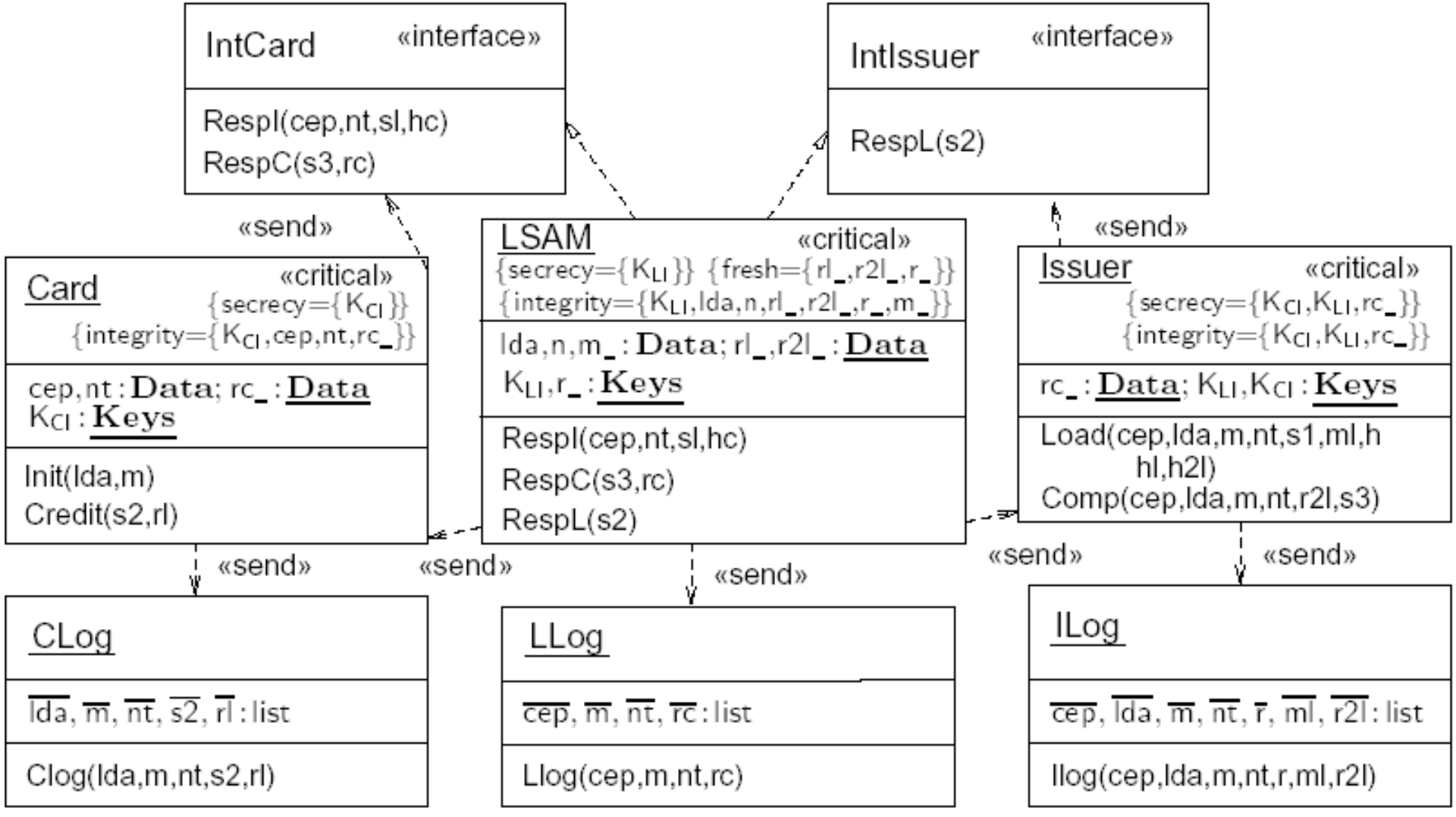
| Issuer «critical» {secrecy={$K_{CI}$,$K_{LI}$,$rc_{nt}$}} {integrity={$K_{CI}$,$K_{LI}$,$rc_{nt}$}} |
|---|
| $rc_{nt}$ : Data; $K_{LI}$, $K_{CI}$ : Keys |
| Load(cep,lda,m,nt,s1,ml,h hl,h2l)<br>Comp(cep,lda,m,nt,r2l,s3) |



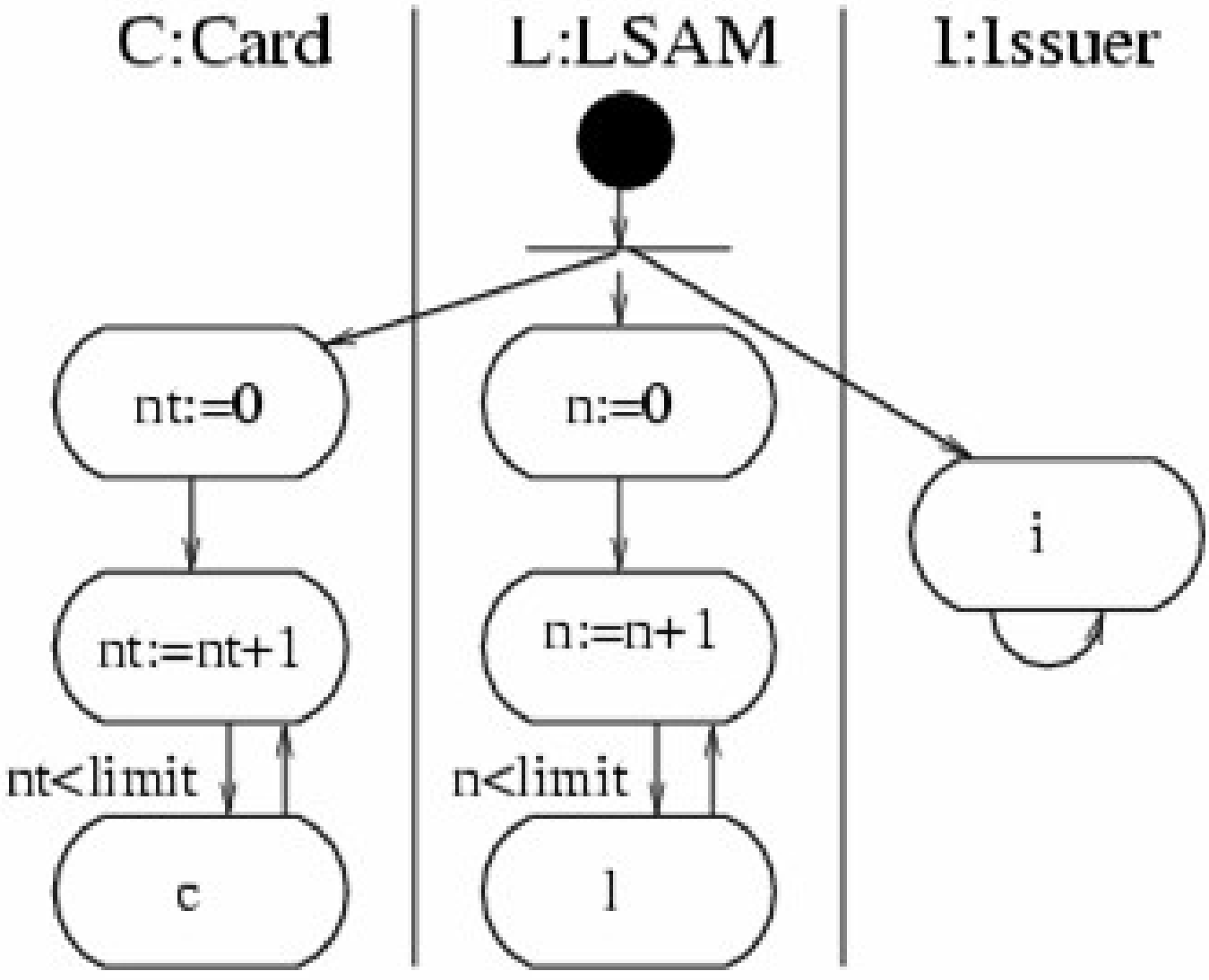
# Load Protocol: Physical View



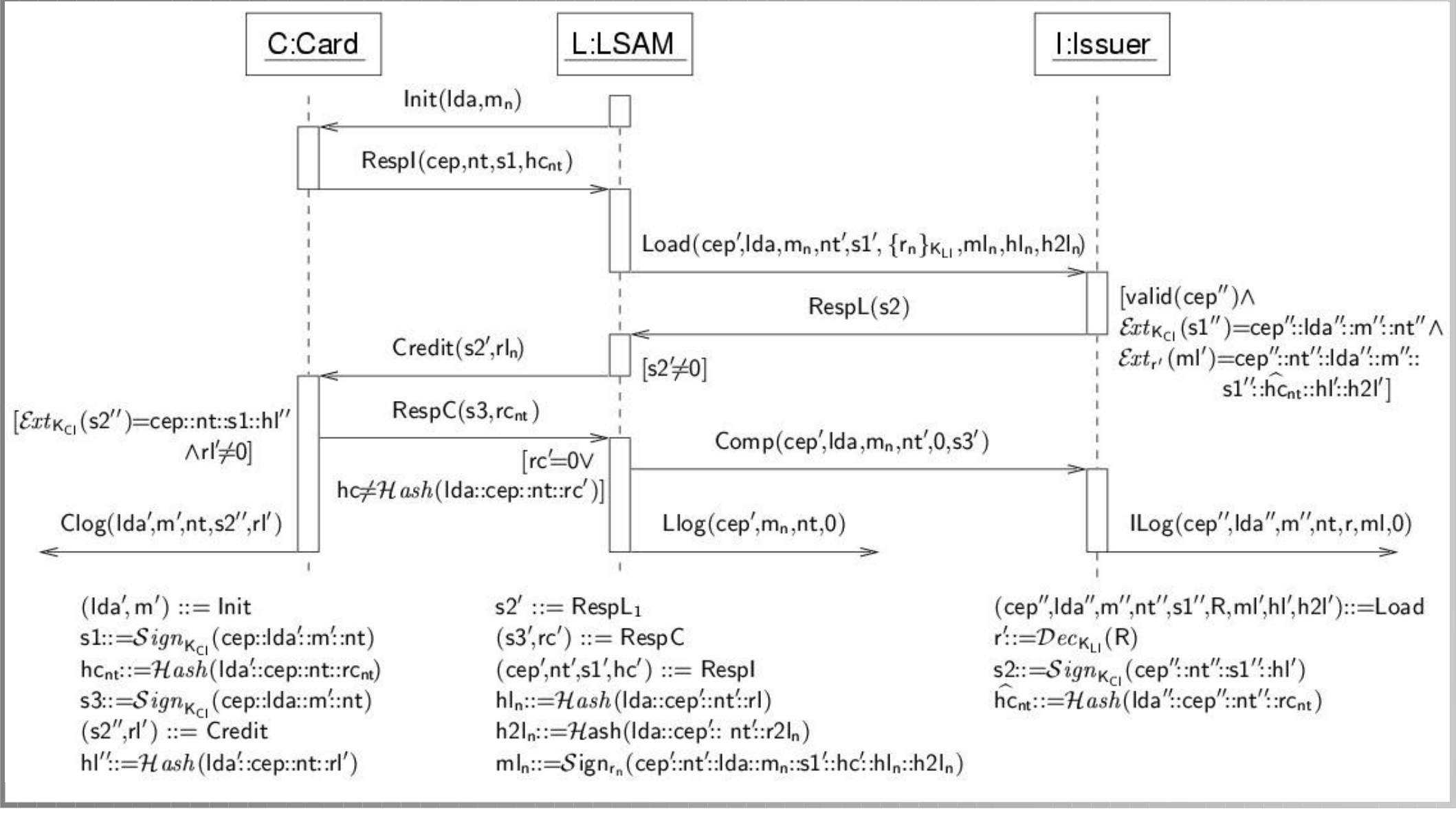
# Load Protocol: Structural View



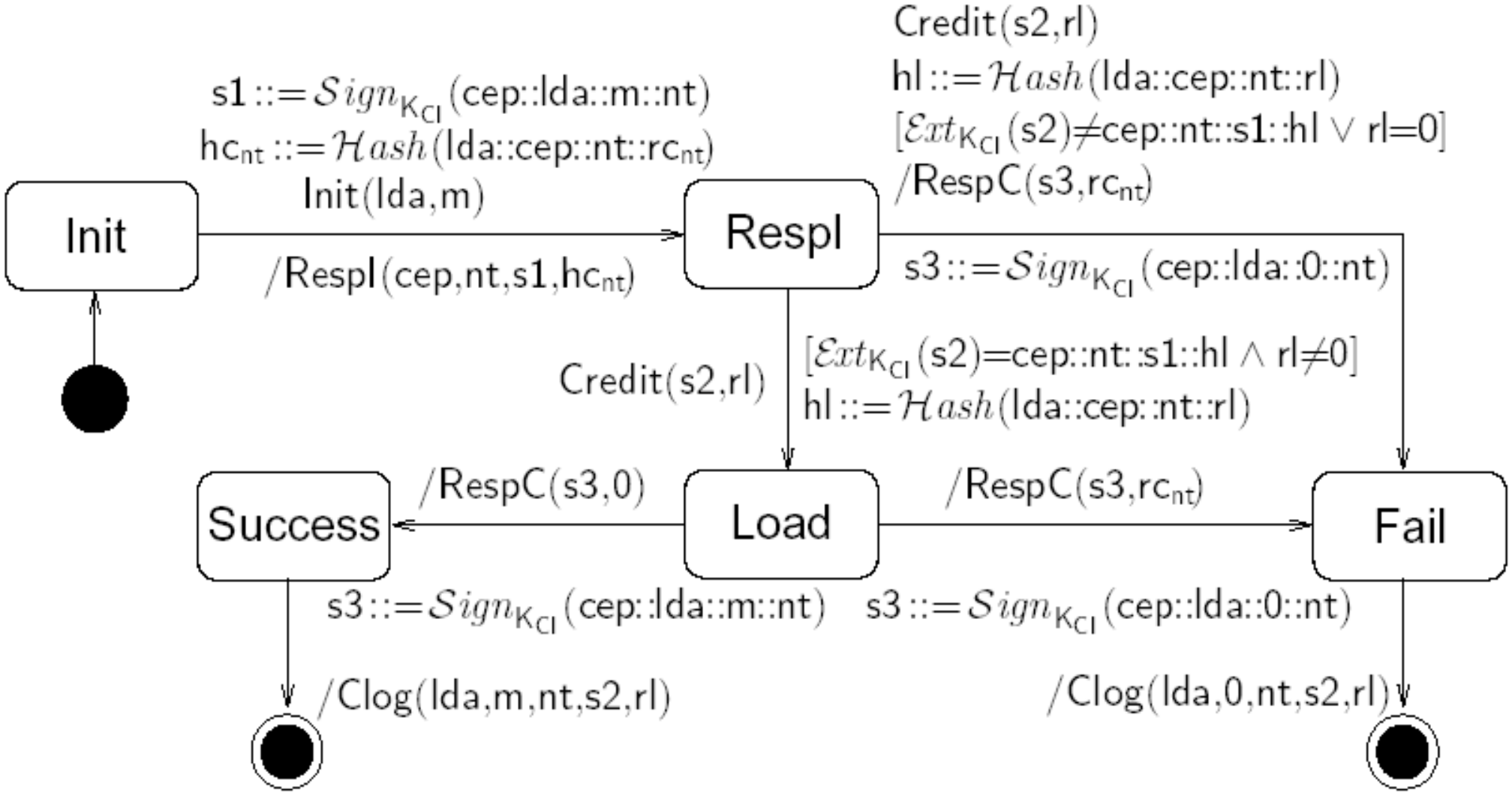
# Load Protocol: Coordination View



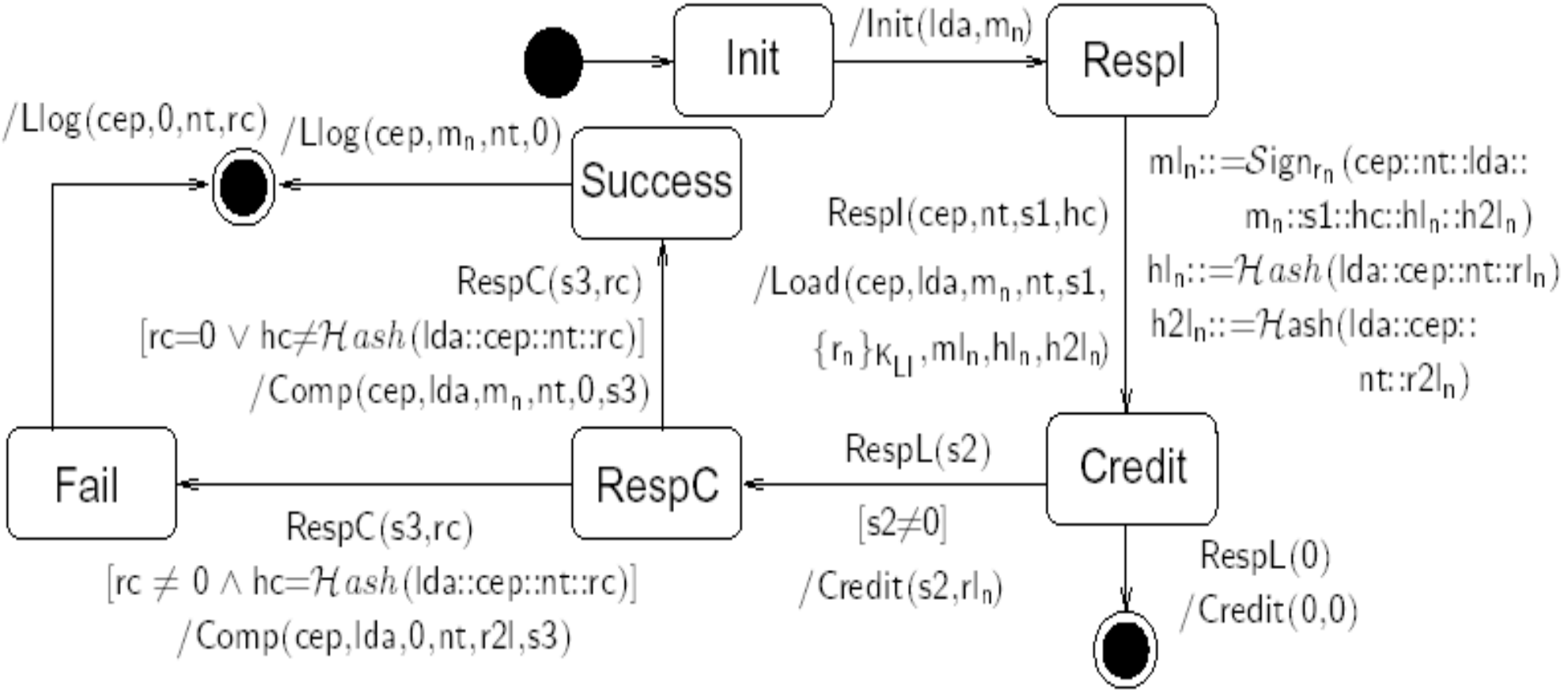
# Load Protocol: Interaction View



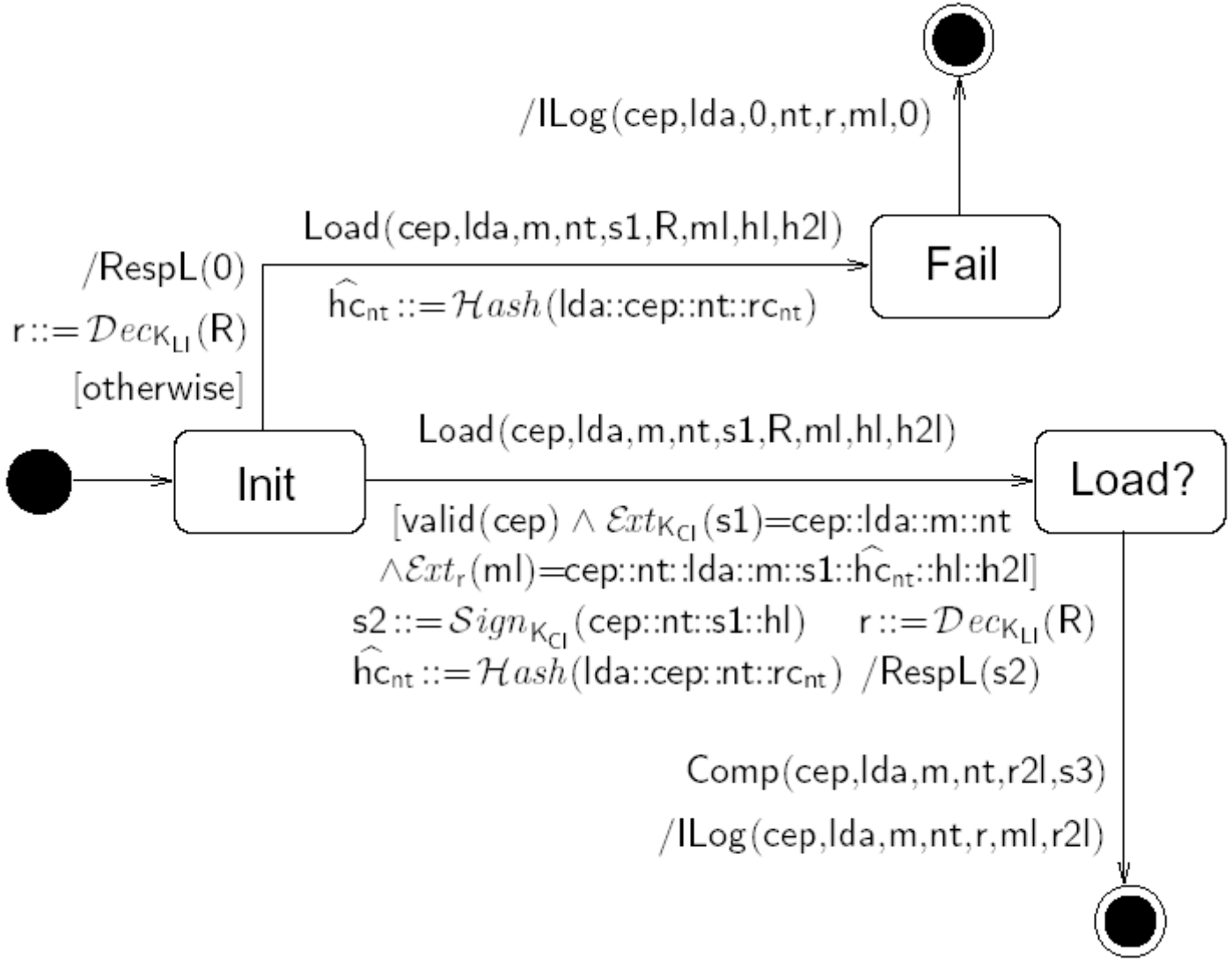
# CEPS Card Statechart



# CEPS LSAM Statechart



# CEPS Card Issuer Statechart



# CEPS Card Issuer Statechart

| 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: $\mathcal{S}ign_{K_{CI}}(cep :: lda :: m :: nt)$ |
| $hc_{nt}$ | card hash value: $\mathcal{H}ash(lda :: cep :: nt :: rc_{nt})$ |
| $\widehat{hc}_{nt}$ | $hc_{nt}$ 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 |
| $ml_n$ | $\mathcal{S}ign_{r_n}(cep :: nt :: lda :: m_n :: s1 :: hc :: hl_n :: h2l_n)$ (signed by LSAM) |
| $hl_n$ | hash of transaction data: $\mathcal{H}ash(lda :: cep :: nt :: rl)$ |
| $h2l_n$ | hash of transaction data: $\mathcal{H}ash(lda :: cep :: nt :: r2l)$ |
| s2 | issuer signature: $\mathcal{S}ign_{K_{CI}}(cep :: nt :: s1 :: hl)$ |
| s3 | card signature of the form $\mathcal{S}ign_{K_{CI}}(cep :: lda :: m :: nt)$ |

# Bedrohungsszenarien

Annahme: Card, LSAM manipulationssicher.

Mögliche Angreiferaktionen: Kommunikation abhören, Komponenten ersetzen.

Mögliche Motive:

**Kartenbesitzer**: Aufladen ohne zu bezahlen

**Ladestation Betreiber**: Geld des Kartenbesitzers einbehalten

**Kartenausgeber**: Geld vom Ladestation Betreiber verlangen

Gemeinsamer Angriffsversuch denkbar.

# Sicherheitsanforderungen (informell)

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

**Ladestation-Betreiber:** Ladestation-Betreiber muss Betrag *m* dem Kartenausgeber nur zahlen, nachdem vom Kartenbesitzer erhalten.

**Emittenten:** Summe der Guthaben von Karten-inhaber und Ladestation Betreiber unverändert.

# Load Acquirer Security

Suppose card issuer *I* possesses $ml_n = Sign_{rn}(cep::nt::lda::m_n::s1::hc_{nt}::hl_n::h2ln)$ and card *C* possesses $rl_n$, where $hl_n = Hash\ (lda::cep::nt::rl_n)$.

Then after execution either of following hold:

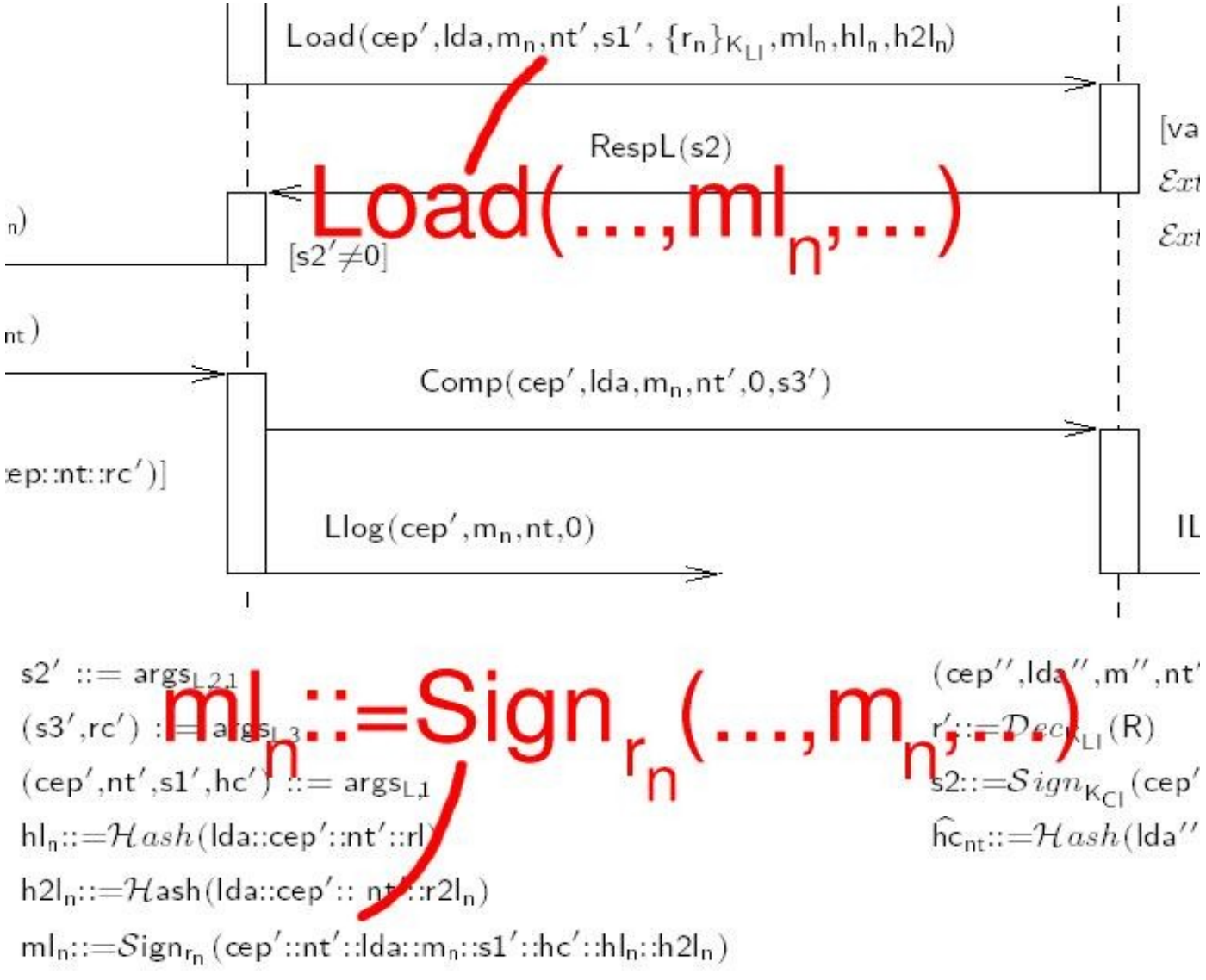
- Llog*(cep,lda,*$m_n$*,nt)* has been sent to I:LLog (so load acquirer L has received and retains $m_n$ in cash) or
- Llog *(cep, lda, 0, nt)* has been sent to I : LLog (so L returns $m_n$ to cardholder) and L has received $rc_{nt}$ with $hc_{nt} = Hash(lda::cep::nt::rc_{nt})$ (negating $m_{ln}$).

"$m_{ln}$ provides guarantee that load acquirer owes transaction amount to card issuer" (CEPS)

# Überraschung

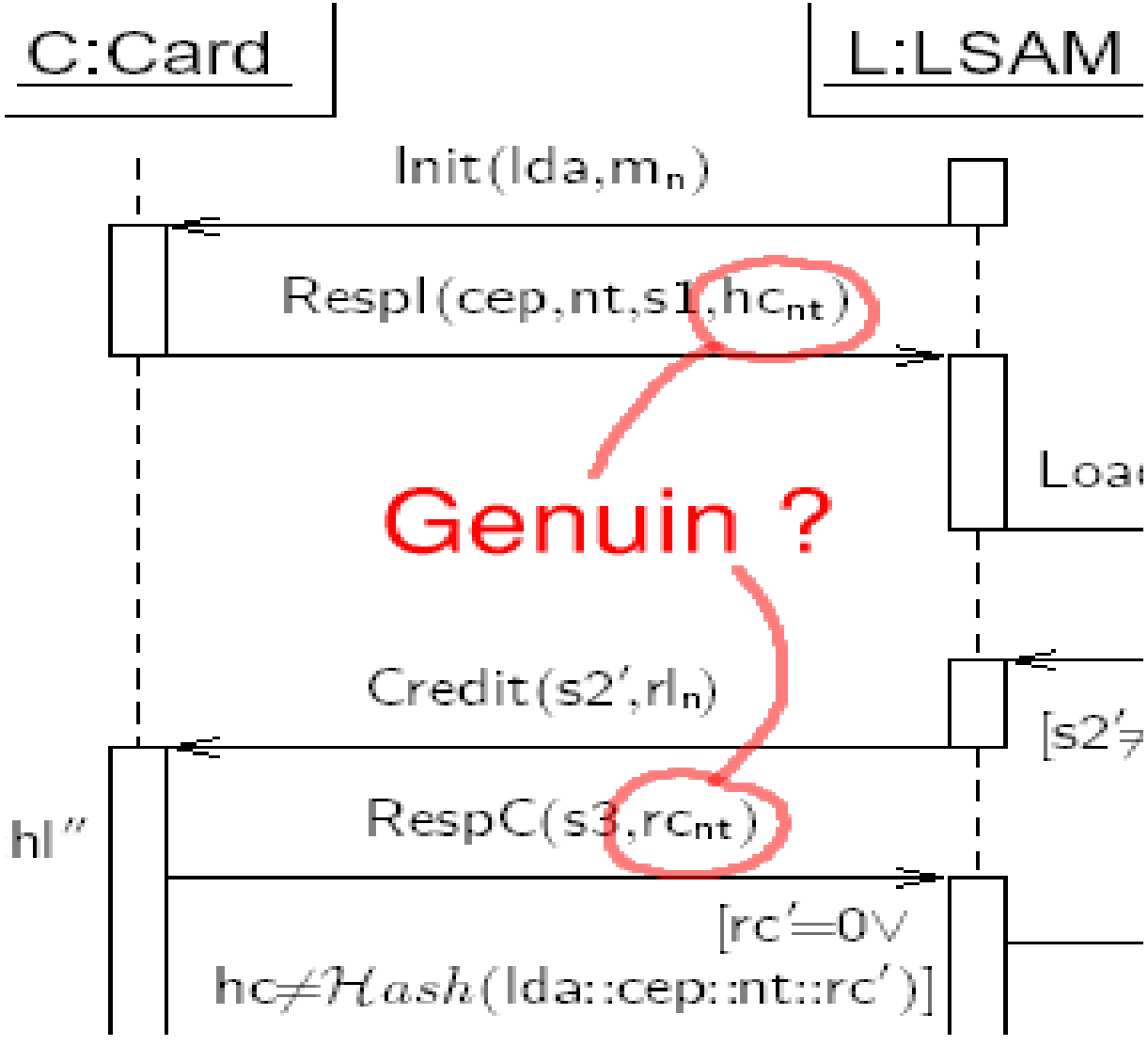
$ml_n$: „Beweis“ für Bank, dass Lade-gerät Geld erhielt.

Aber: $r_n$ geteilt zwischen Bank und Ladegerät.



# 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.

# Aufgabe 7.4

- Modifiziere das Sequenzdiagramm gemäß der genannten Änderung. [4 P.]

# Cardholder Security

*Cardholder security: For any message* $\mathsf{Clog}(\mathsf{lda}, \mathsf{m}, \mathsf{nt}, \mathsf{s2}, \mathsf{rl})$ *sent to* $\mathsf{c} : \mathsf{CLog}$, *if* $\mathsf{m} \neq 0$ *(that is, the card seems to have been loaded with* m*) then* $\mathsf{rl} \neq 0$ *and*

$$\mathcal{E}xt_{\mathsf{K_{CI}}}(\mathsf{s2}) = \mathsf{cep} :: \mathsf{nt} :: \mathcal{S}ign_{\mathsf{K_{CI}}}(\mathsf{cep} :: \mathsf{lda} :: \mathsf{m} :: \mathsf{nt}) :: \mathcal{H}ash(\mathsf{lda} :: \mathsf{cep} :: \mathsf{nt} :: \mathsf{rl})$$

*holds (that is, the card issuer certifies* rl *to be a valid proof for the transaction). For any two messages* $\mathsf{Clog}(\mathsf{lda}, \mathsf{m}, \mathsf{nt}, \mathsf{s2}, \mathsf{rl})$ *and* $\mathsf{Clog}(\mathsf{lda}', \mathsf{m}', \mathsf{nt}', \mathsf{s2}', \mathsf{rl}')$ *sent to* $\mathsf{c} : \mathsf{CLog}$, *we have* $\mathsf{nt} \neq \mathsf{nt}'$.

# Load Acquirer Security

*Card issuer security: For each message* $\mathsf{Clog}(\mathsf{lda}, \mathsf{m}, \mathsf{nt}, \mathsf{s2}, \mathsf{rl})$ *sent to* $\mathsf{c} : \mathsf{CLog}$, *if* $\mathsf{m} \neq 0$ *and*

$$\mathcal{E}xt_{\mathsf{K_{CI}}}(\mathsf{s2}) = \mathsf{cep} :: \mathsf{nt} :: \mathcal{S}ign_{\mathsf{K_{CI}}}(\mathsf{cep} :: \mathsf{lda} :: \mathsf{m} :: \mathsf{nt}) :: \mathcal{H}ash(\mathsf{lda} :: \mathsf{cep} :: \mathsf{nt} :: \mathsf{rl})$$

*holds for some* lda, *then the card issuer has a valid signature* $\mathsf{ml}_\mathsf{n}$ *corresponding to this transaction.*

# Card Issuer Security

*Card issuer security: For each message* $\mathsf{Clog}(\mathsf{lda}, \mathsf{m}, \mathsf{nt}, \mathsf{s2}, \mathsf{rl})$ *sent to* $\mathsf{c} : \mathsf{CLog}$, *if* $\mathsf{m} \neq 0$ *and*

$$\mathcal{E}xt_{\mathsf{K_{cl}}}(\mathsf{s2}) = \mathsf{cep} :: \mathsf{nt} :: \mathcal{S}ign_{\mathsf{K_{cl}}}(\mathsf{cep} :: \mathsf{lda} :: \mathsf{m} :: \mathsf{nt}) :: \mathcal{H}ash(\mathsf{lda} :: \mathsf{cep} :: \mathsf{nt} :: \mathsf{rl})$$

*holds for some* $\mathsf{lda}$, *then the card issuer has a valid signature* $\mathsf{ml}_\mathsf{n}$ *corresponding to this transaction.*

# Aufgabe 7.5

- Welcher Angriff wäre möglich, wenn es den Transaktionszähler *nt* nicht geben würde ? (Pfeildiagramm des Angriffablaufes) [4 P.]