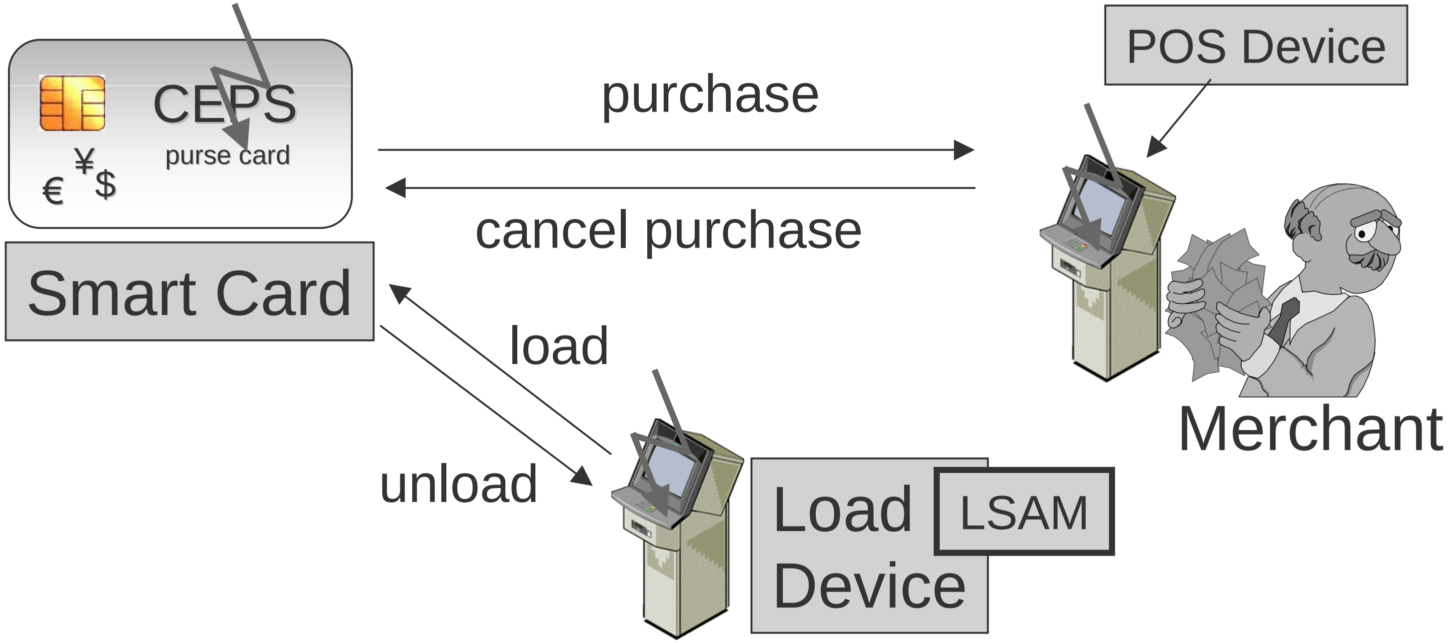
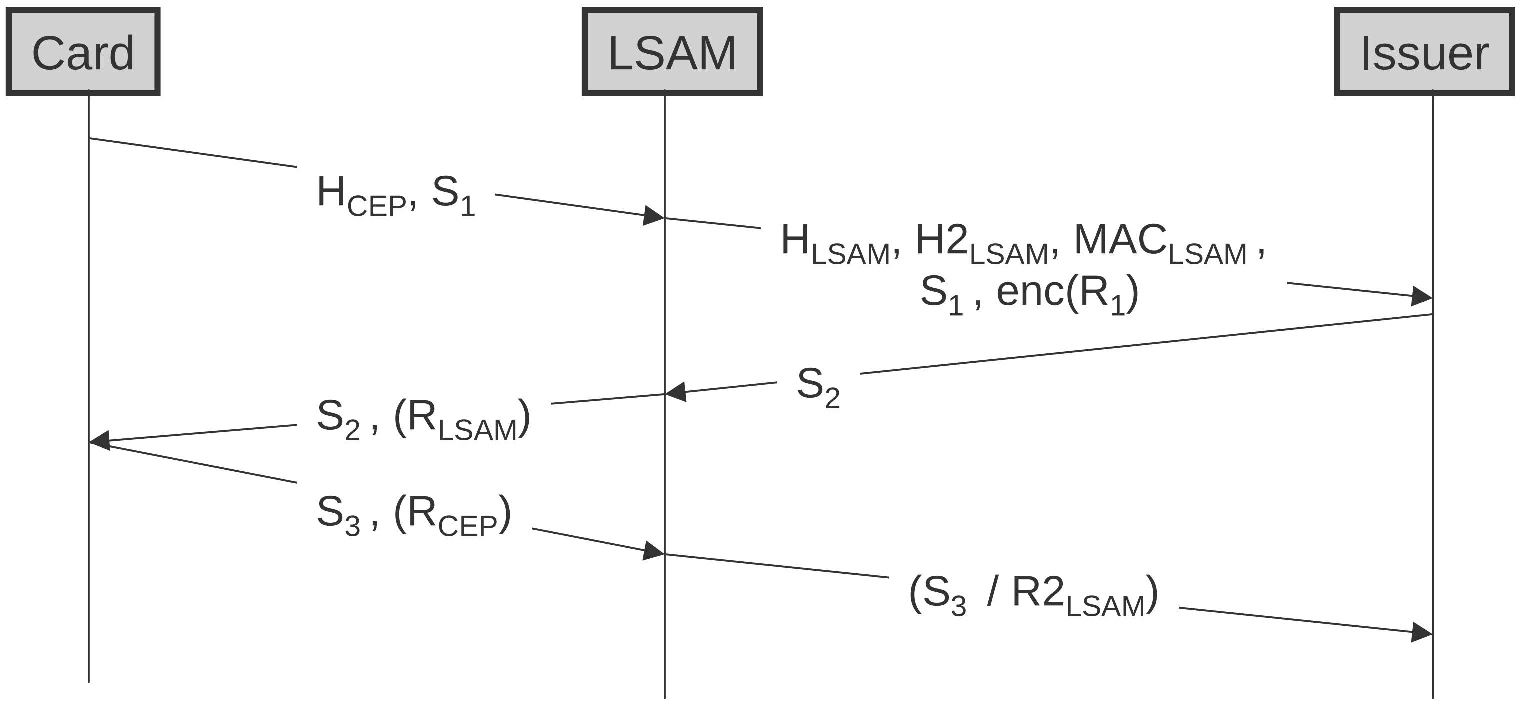
Electronic Purse Systems



- ... will become globally interoperable (CEPS standard)
- ... are complex distributed e-commerce applications
- ... are highly security critical

CEPS: Load Transaction

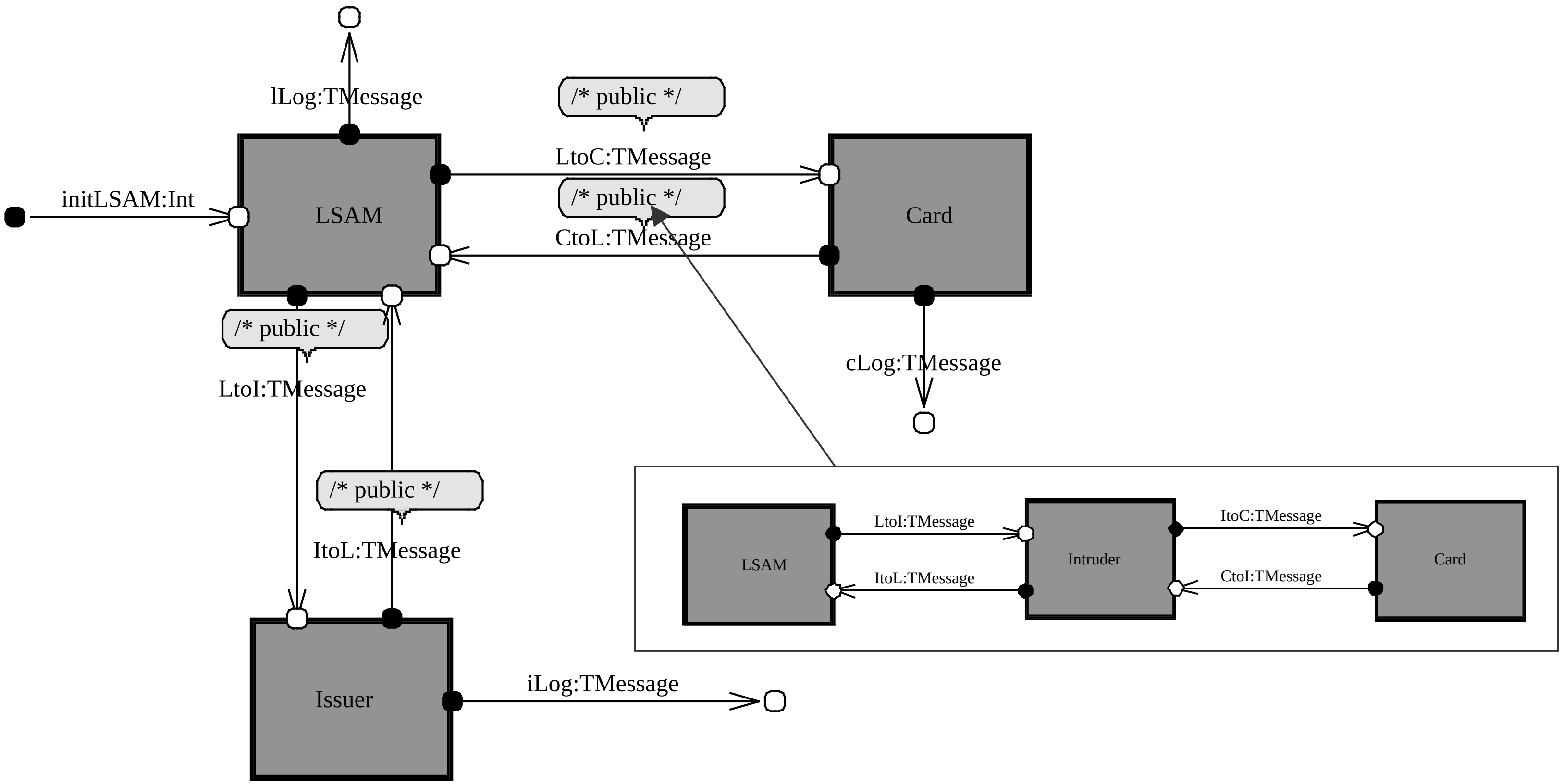


- Protection against fraud using (symmetric key) signatures
- Security requirements provide fail-safety:
  - R_{CEP} is sent by the card if it experiences an error
  - If the LSAM experiences an error, either S_3 or $R2_{LSAM}$ are sent to Issuer
  - The LSAM either sends S_2 and R_{LSAM} to the Card, or $R2_{LSAM}$ to the Issuer
  - ...

AutoFocus

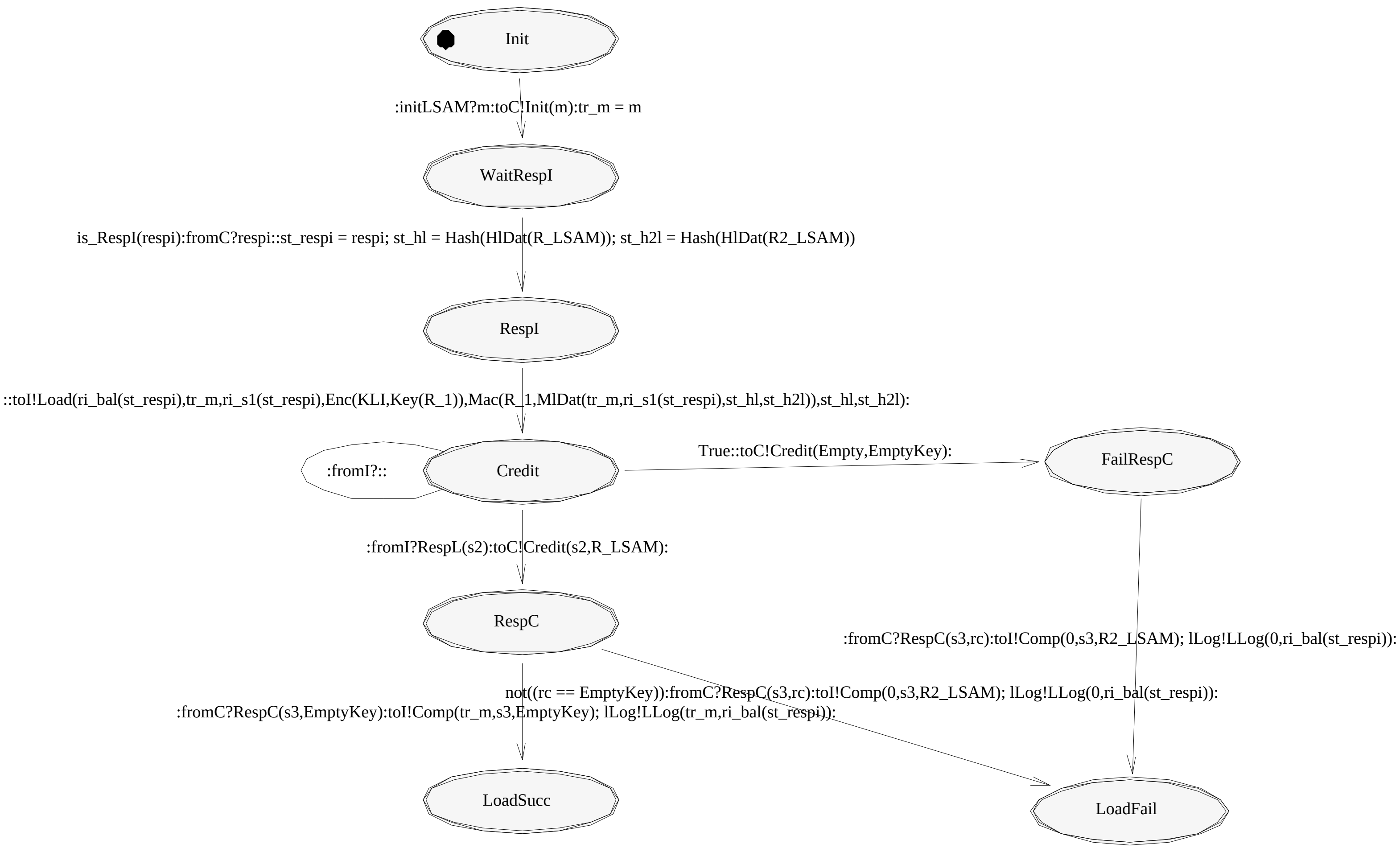
- CASE tool, based on formal background (FOCUS)
- Graphical, view oriented modelling
  - System Structure Diagrams
  - State Transition Diagrams
  - Message Sequence Charts
  - Data Type Definitions
- Views related to UML-RT, support hierarchy
- Features:
  - Simulation
  - Validation (Consistency, Testing, Model Checking)
  - Code Generation (e.g. Java, C)

CEPS Load Transaction in AutoFocus



- Protocol participants as AutoFocus components
- Unreliable Channels (public): „Intruder“ component can
  - Drop messages
  - Replace messages (Invalid inputs, etc.) without guessing secrets

State Chart for LSAM

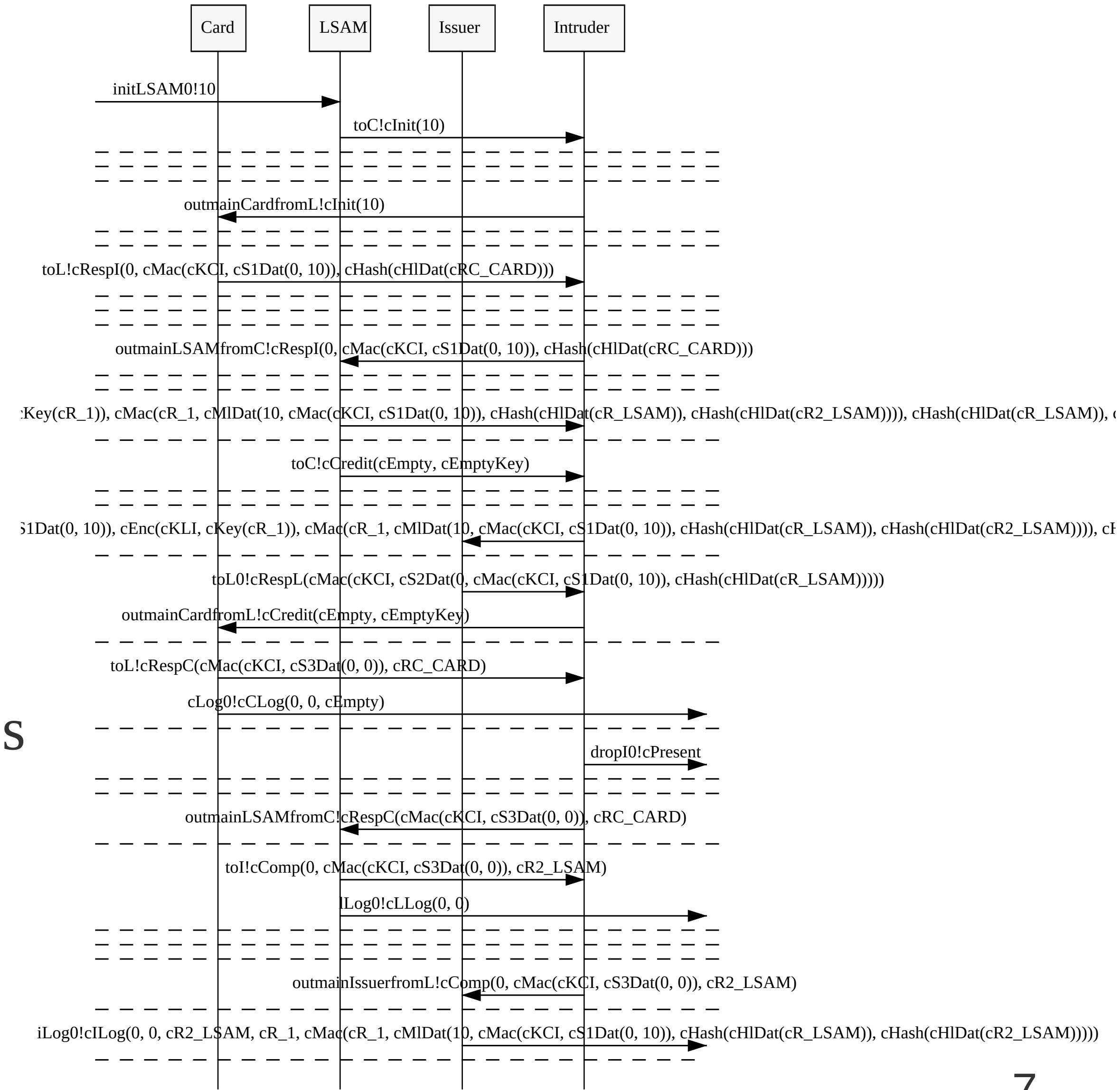


Test Case Specifications

- Based on security requirements
  - RC_{CARD} sent by Card
  - $R2_{LSAM}$ sent by LSAM
  - S_2 sent by LSAM
  - ...
- Based on model structure
  - Success/Failure States
  - Coverage of critical transactions
  - Coverage of critical intruder activities

Test Sequence Generation

- Runs fulfilling the test case specifications
  - Computed using a constraint logic solver
  - Describe possible vulnerabilities
  - Use as test sequences for implementation



Contributions

- Formal specification of CEPS Load Transaction
  - Using graphical description techniques of the CASE-Tool AutoFocus
- Specification-based test sequence generation
  - Based on the AutoFocus model
  - Focused on security properties, such as fail-safety
  - To test the implementation for vulnerabilities
  - Using Constraint Logic Programming
- $\Rightarrow$ Integrated treatment of security aspects

Formally Testing Fail-Safety of Electronic Purse Protocols

Guido Wimmel
Software & Systems Engineering
Technische Universität München

(with Jan Jürjens)