EAP State Machine

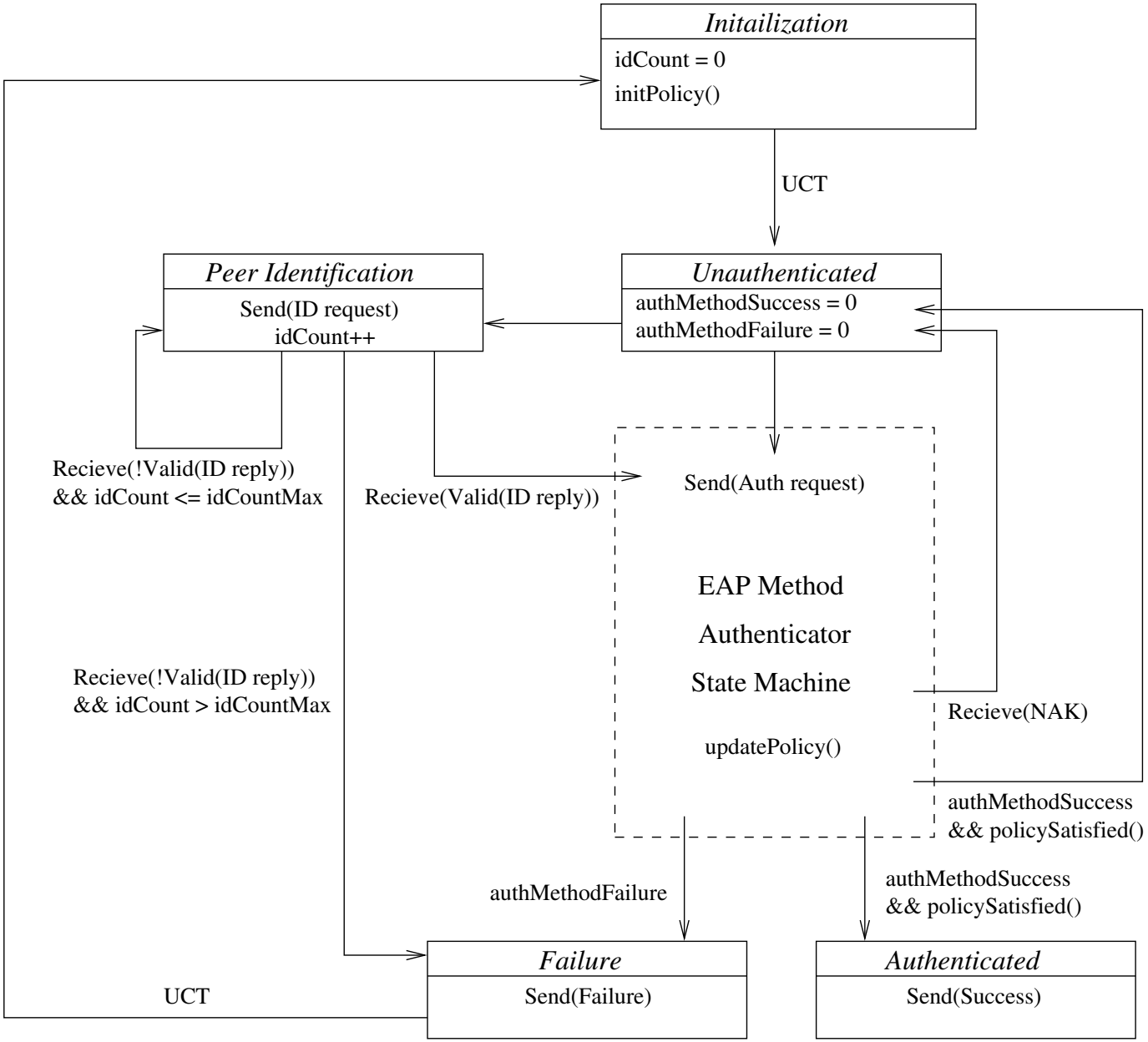
Bryan D. Payne & Nick L. Petroni, Jr.

53rd IETF March 2002

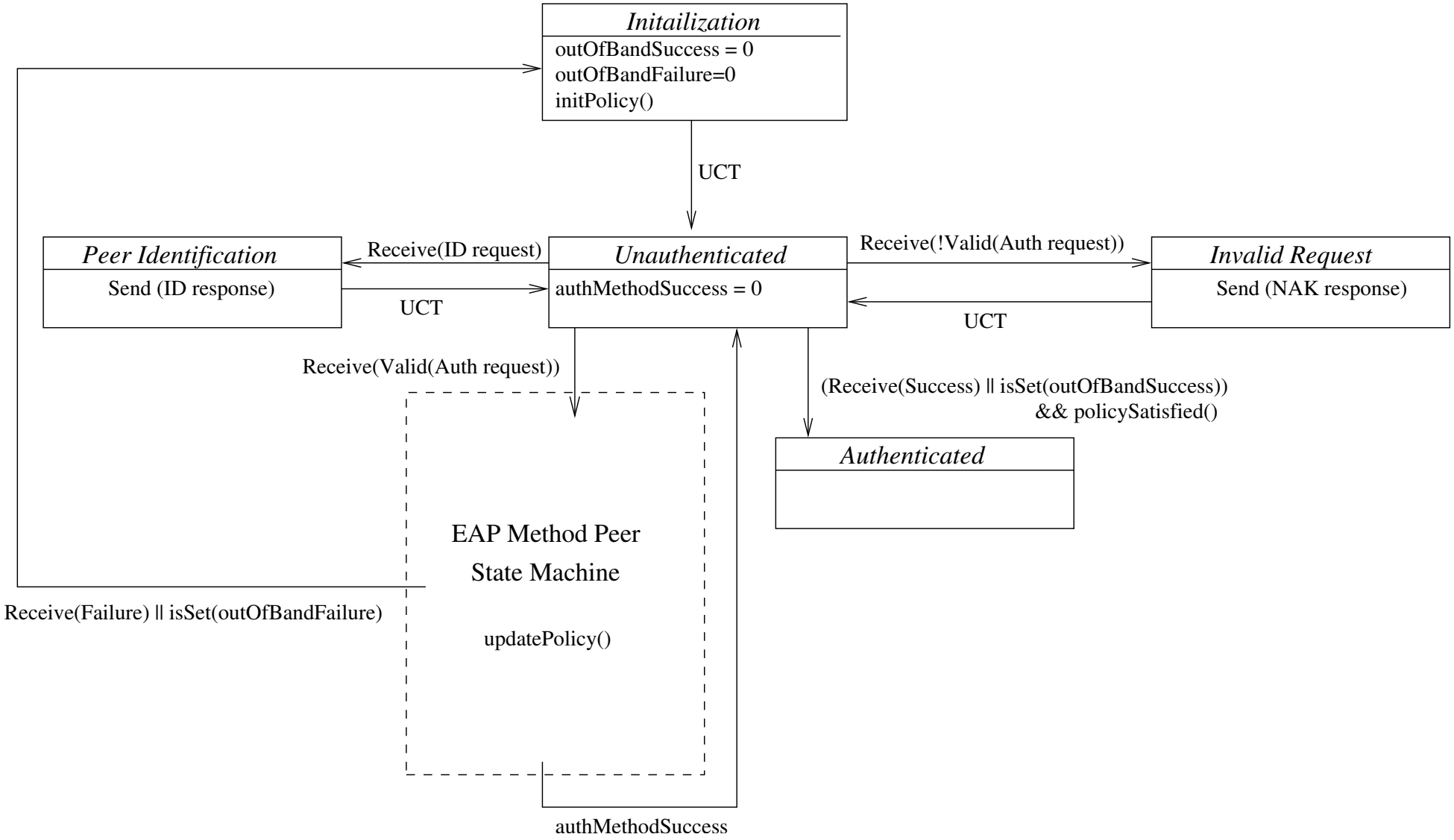
Contents

- EAP Authenticator State Machine
  - *Discuss state machine design decisions*
  - *Explain weaknesses in the EAP specification*
- EAP Peer State Machine
  - *Same as above*
- Issues and Concerns
  - *Discuss security issues encountered*
  - *Discuss potential protocol problems*

EAP Authenticator State Machine



EAP Peer State Machine



Issues and Concerns

- What is policy?
  - *Significantly affects security*
  - *Specification should define policy*
- Peer's control over state machine
  - *Does EAP really support mutual authentication?*
  - *Inconsistent states reachable*
- Formal state machines still needed for each authentication type
  - *MD5-challenge*
  - *One-time password (OTP)*
  - *Generic token card*
  - *and others...*

Conclusions

- State machines proposed
- Open for discussion

- http://www.cs.umd.edu/∼bdpayne/papers/eap-state-machine.pdf
- http://www.cs.umd.edu/∼bdpayne/papers/eap-pres.pdf