TAPI: Transactions for Accessing Public Infrastructure

Pekka Nikander

HIIT & Ericsson

Joint work with Angelos Keromytis, Matt Blaze,
John Ioannidis, Sotiris Ioannidis, and Vassilis Prevelakis

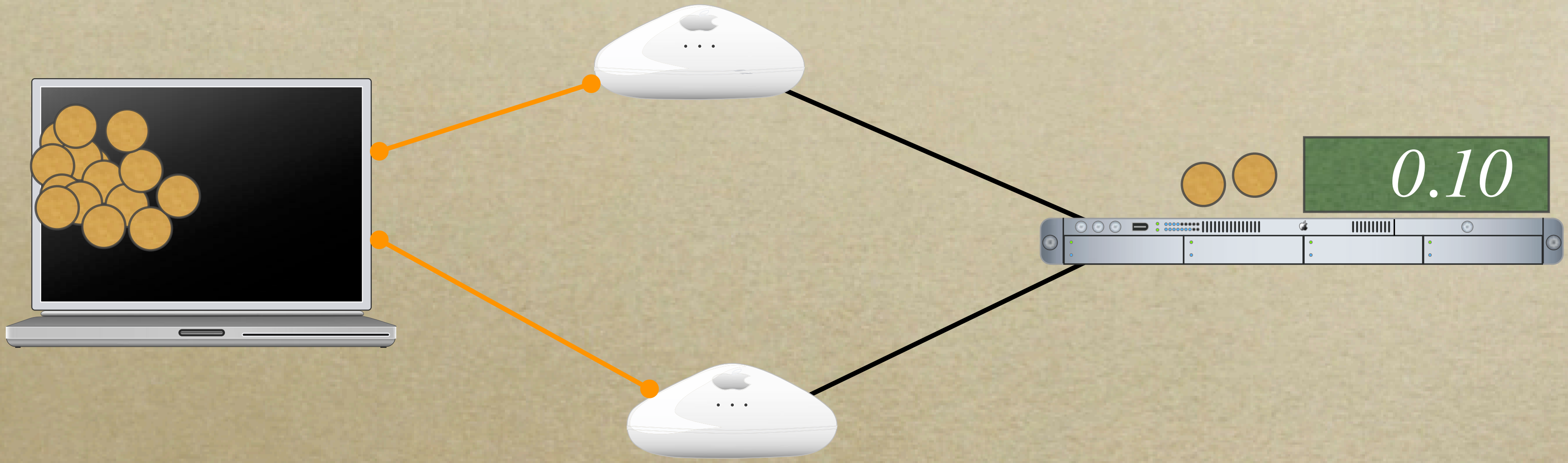
Presentation outline

- *Overview*
- *Conceptual idea*
- *Protocol view*
- *KeyNote2 Micro-checks*
- *OTP Coins*
- *Putting the details together*
- *Summary*

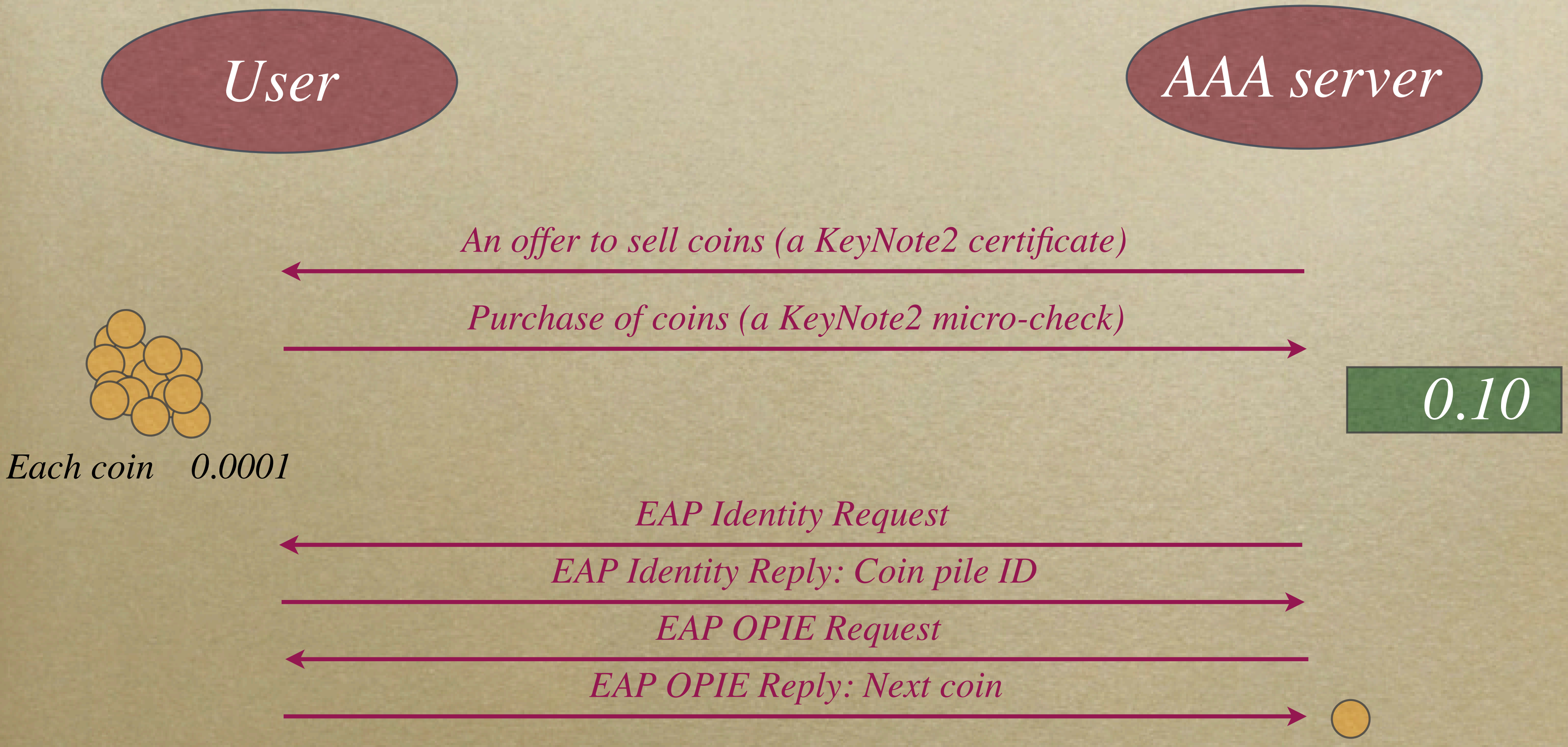
Overview

- *General, off-line, micro-payment system*
- *Amortizes cost of expensive crypto over many small, cheap-to-verify transactions*
  - *No probabilistic schemes*
- *Includes explicit risk management and dispute handling mechanisms*
- *Based on KeyNote2 and OTPCoins*
- *Especially suitable for Internet access*

Conceptual idea (for access)



Protocol point-of-view



User

AAA server

An offer to sell coins (a KeyNote2 certificate)

Purchase of coins (a KeyNote2 micro-check)

0.10

Each coin 0.0001

EAP Identity Request

EAP Identity Reply: Coin pile ID

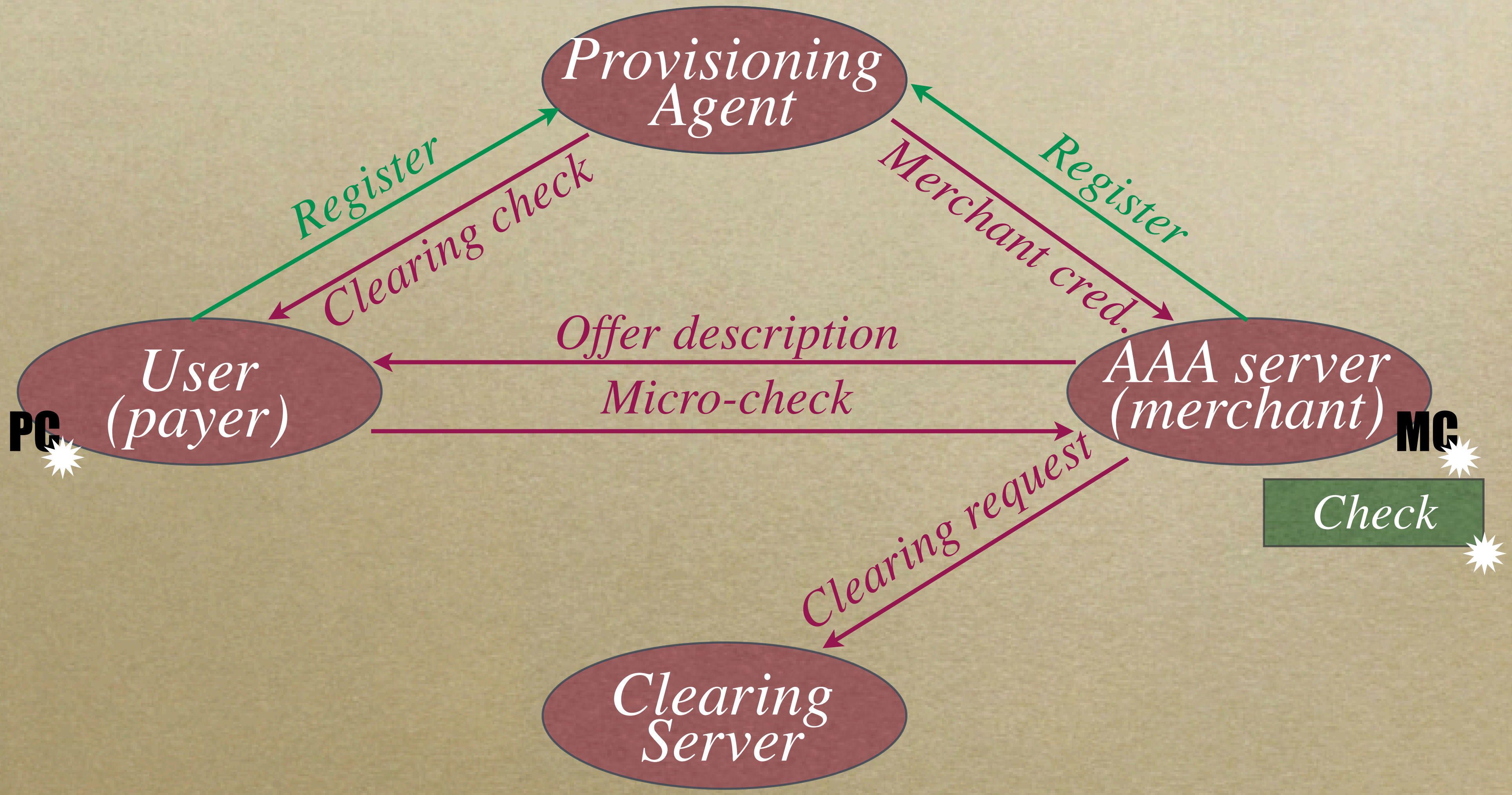
EAP OPIE Request

EAP OPIE Reply: Next coin

KeyNote2 Micro-checks

- *Presented & revised in FC2001 & FC2002*
- *Based on KeyNote2 trust management system, introduced in 1998 [RFC2704]*
  - *Assumes that each party has a public key*
  - *Keys sign credentials, delegating trust*
- *Each check encodes* conditions *for its validity*

Roles and Credentials



OTP Coins

- *A reverse hash chain of a given length <n>*
  - $H_0=hash(H_1)=hash(hash(H_2))=hash^n(H_n)$
- *Revealed one-by-one, first* H_0 *then* H_1 *etc*
  - *Receiver can verify that* $H_{n-1} = hash(H_n)$, *thereby verifying that* H_n is *the next value*
- *Compatible with EAP OPIE [RFC2289]*

Putting details together

- *Initial hash value H_0 stored in the check*
- *Subsequent hash values very cheap to verify*
- *Merchant shows last received value H_k*
    - *Clearing checks that $H_0 = hash^k(H_k)$*
    - *User charged only for <k> coins*

Summary

- *A cheap, practical micro-payment approach*
  - *Based on existing, proven technology*
  - *No new, fancy crypto*
- *Splits a KeyNote2 micro-check into coins*
- *Suitable for wireless Internet access*
  - *Designed to work with IEEE 802.1x*
- *Supports off-line and on-line verification*