Micropayments with Controlled Privacy Using Existing Infrastructure

Network Manifold Associates, Inc.

Ed Gerck (egerck@nma.com)
Larry Suto (lsuto@nma.com
Thomas Blood (tblood@nma.com)
Einar Stefferud (stef@nma.com)

Rump Session
6th International Financial Cryptography Conference
Southampton, Bermuda
March 12 2002

Micropayments: Positioning

- Many micropayments and Internet payment systems have been proposed and developed: FirstVirtual, Payword, Micromint, Paypal, …
- Lessons learned from FirstVirtual and others:
  - Needs an accumulator somewhere, that must be honest, auditable, preserve customer privacy, have low cost and offer high security
  - Needs to use a payment infrastructure
  - Banks are not always accessible for a transaction in real-time
  - Needs customers
  - Simple, direct and immediate
  - Needs to induce trust among the parties; requires multiple channels of information
  - Trust paradox: the least you need to trust, the more you can trust

Goals & Challenges

The goals are:

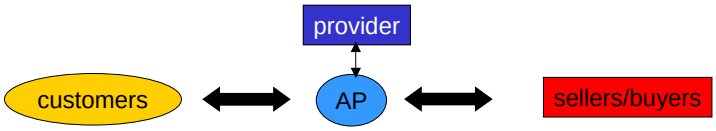
- Easy to apply: for example, as a portal for wireless and Web payments
- Appeal to telcos (NTT, Sprint, Nextel, …) because:
  - telcos already know how to handle micro-payments
  - telcos already work with a large payment range: $0.01 to $1,000s
  - telcos have payment infrastructure
  - telcos have large customer base
  - customers already trust the telco
  - telcos need to regain market leverage at the user's end
  - real-time access requirement is OK for a telco
- Allow customers to buy/sell even if the bank is not accessible

The challenges are:

- Require the least need to trust the service
- Create a pass-through service
- Flexible protection of user privacy
- Allow impulse buying
- Provide non-repudiation

NMA

Paradigm: Authorization Portal



Authorization Portals: electronic marketplaces where providers are able to connect their customers to sellers and buyers.

> An Authorization Portal is the XXI century version of the practice of selling one's customer list, with all its upsides and none of its downsides.

Example: an Authorization Portal controls access to a seller's offer, verifies credit and charges the customers without disclosing the customers' financial data to the seller.

Value added by provider: customer privacy, financial data, authentication, authorization, administration, session control, non-repudiation, trust, transaction security, reliability, integrity, auditing and availability.

NMA

Problem: Implementation

- **PKI:** digital certificates are too large; does not authenticate users, just machines to machines; costly; large revocation liability; lack of trust; does not scale.
- **SSO:** password-based; shared secret liability; costly; lack of trust; does not scale.
- **ECC PKI:** ECC compact PKI digital certificates are still too large (4,800 bits); same PKI problems
- **Passport:** Password-based, globally centralized authorization; large liability; Microsoft knows all (no customer privacy to Microsoft); lack of trust; does not scale; cost?

Main Road Blocks: lack of trust, large liability, lack of scale, cost

NMA

 5

Solution: APEX

- APEX is a network service
- APEX is an authorization portal engine
- APEX is built as a secure four-party protocol with stateless servers
- APEX is designed for wireless

Authorization Portal Exchange (APEX): Uses very compact digital certificates (30~160 bits), provides user authentication, multi-channel trust, integrated authorization, integrated SSO, integrated optimized routing, scales to any number of users.

APEX uses three NMA tools:

- DTC
- DTCA
- 3TNet

NMA

 6

First Tool: DTC

Digital Transaction Certificate (DTC) objects:

K, K' = keys	Pwd = private password
AI = Authorization Information	RC = Return Code

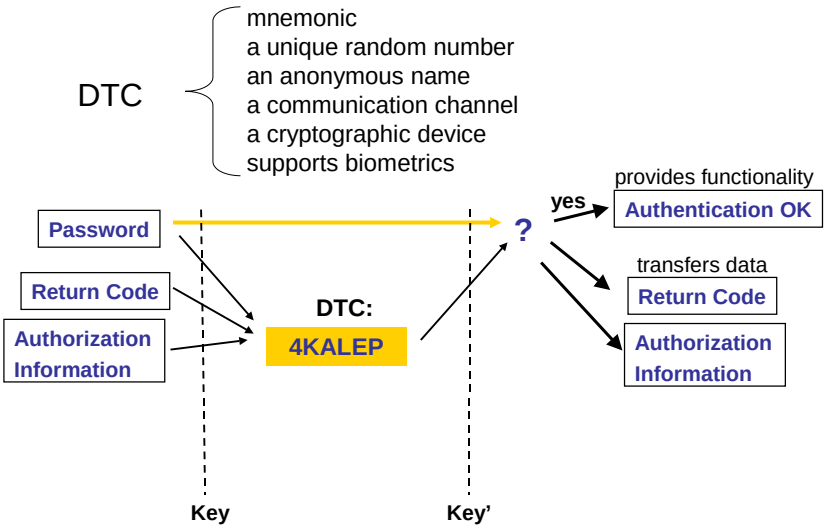
A DTC is a nonce, representing a signature with appendix of the password and a signature without appendix of AI and RC.

To verify a DTC, a verifier needs both the key and the password.

Dictionary attacks can be made infeasible (need to guess both the DVC and the Pwd). Brute-force attacks can be prevented by using sufficiently large keys. There is no password list to protect because users hold the passwords; there are no shared secrets for user data.

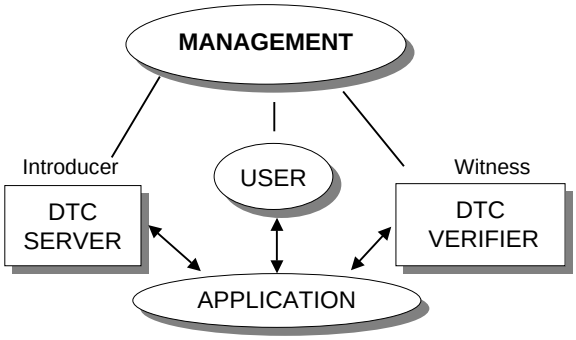
Stateless (no memory): DTCs are issued for random inputs of H[Pwd], AI and RC, and verified for random inputs of DTC and Pwd.

First Tool: DTC



Second Tool: DTCA

The DTCA is a network service that manages DTCs.

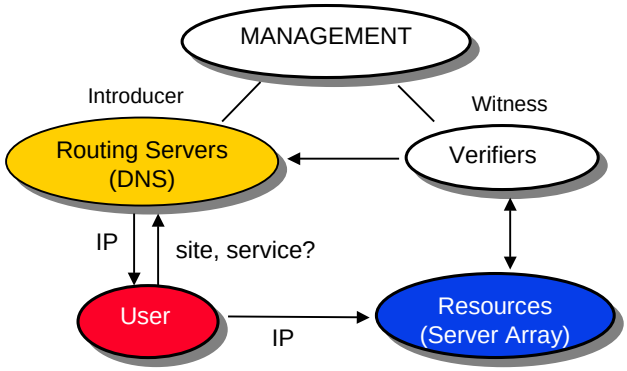


 9

Third Tool: 3TNET

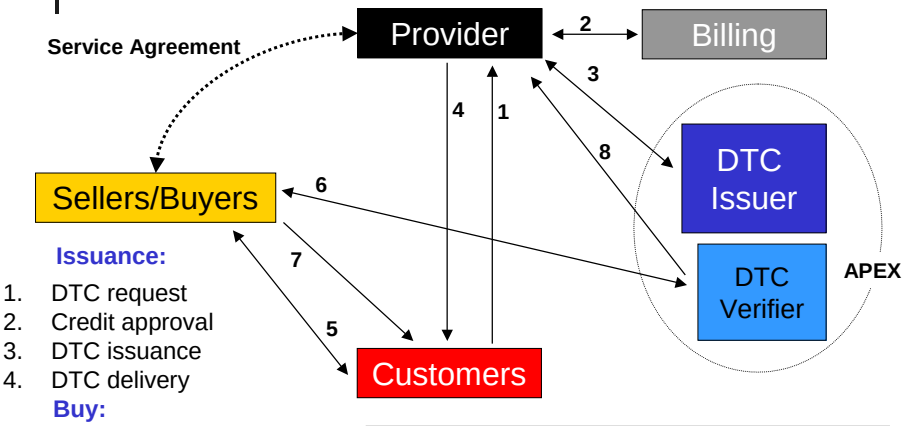
- improves throughput speed
- improves reliability
- provides dynamic routing
- immediate error feedback
- supports split horizon
- screens access to resources
- provides E2E high QoS with low QoS components

NMA's 3-Tier Network (3TNet) is a service implemented with DTCAs and DTCs.



 10

Type I APEX Authorization Dynamics



Issuance:

1. DTC request
2. Credit approval
3. DTC issuance
4. DTC delivery

Buy:

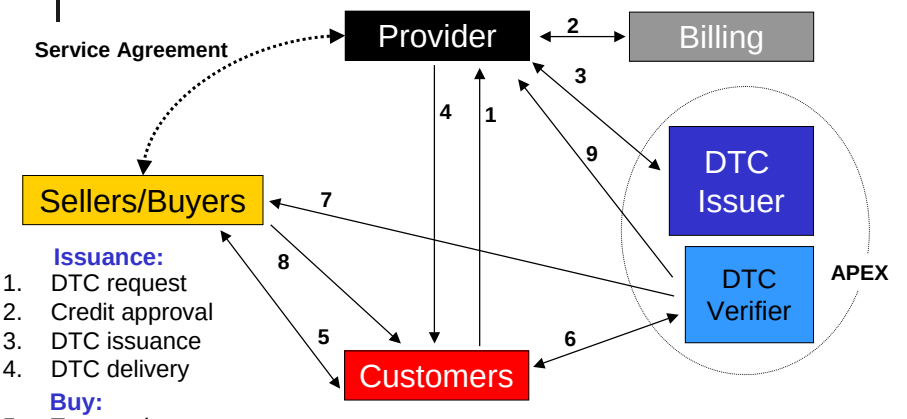
5. Transaction request
6. DTC approval
7. Transaction delivery
8. Notification

Caveats:
Sellers/Buyers may replay or disclose the DTC!
Customers need to trust sellers/buyers not to disclose DTC.

NMA

 11

Type II APEX Authorization Dynamics



Issuance:

1. DTC request
2. Credit approval
3. DTC issuance
4. DTC delivery

Buy:

5. Transaction request
6. DTC approval
7. Transaction approval
8. Transaction delivery
9. Notification

Sellers/Buyers never learn the DTC or password!
Customer can reuse the DTC (multiple-payments).

NMA

 12

APEX Demos

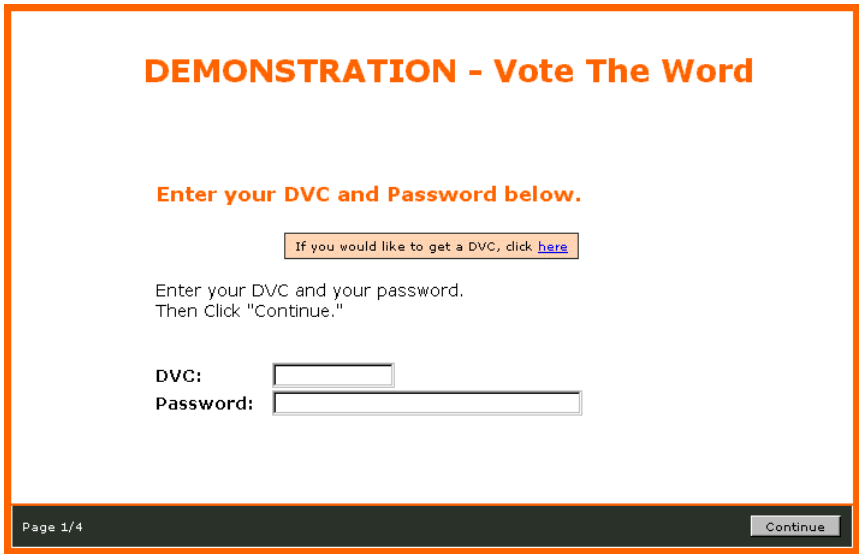
- Game: Vote The Word (*)
  - allows multiple payments; prevents double spending
  - prevents spoofing
  - fully auditable
  - publicly verifiable
  - users define their own private passwords
  - users define the winning result by anonymous voting
- Auction: Toy Auction
  (upon request)
- Wireless Banking: M-Cash
  (upon request)

(*) demo in cooperation with Safevote, Inc.

NMA

 13

Vote the Word: Seller

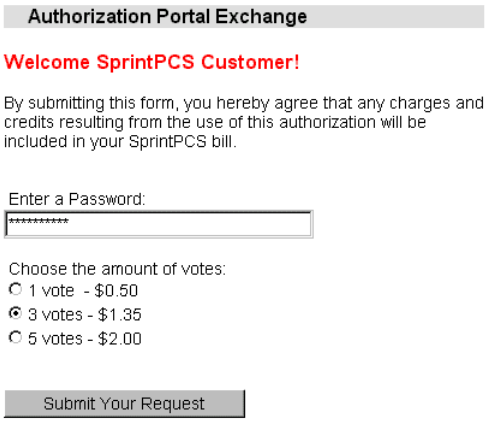


NMA

 14

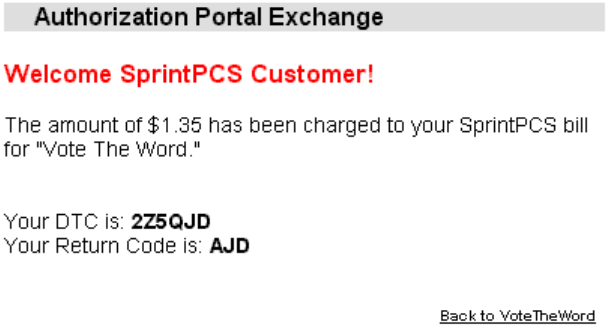
Vote the Word: APEX

Demonstration



Vote the Word: APEX

Demonstration



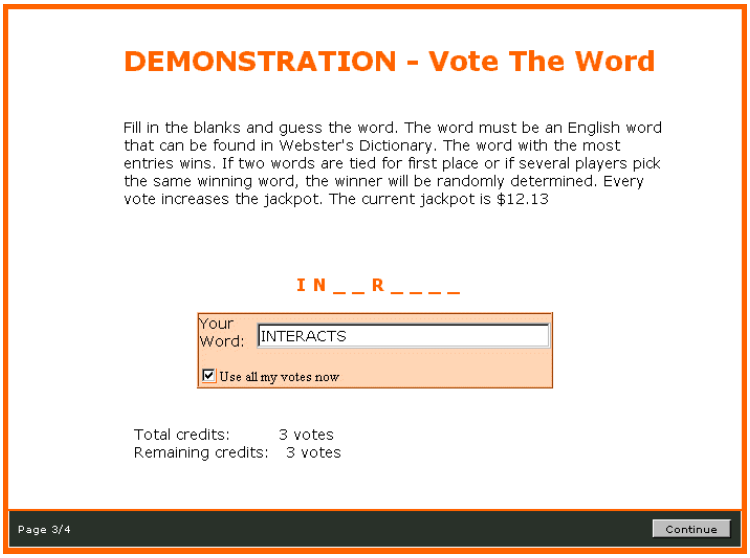
Vote the Word: Seller

 17

Vote the Word: Seller

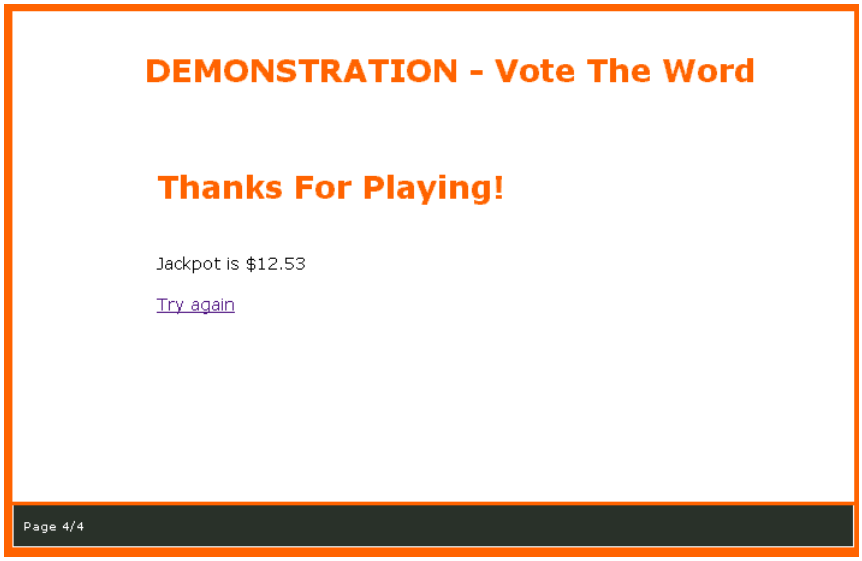
 18

Vote the Word: Seller



 19

Vote the Word: Seller



 20

Summary of Features

- connects *desire to purchase* with *ability to supply products or services*
- leverages large customer base
- allows micropayments as well as medium to large transactions
- supports impulse/spontaneous purchasing
- shares billing infrastructure to reduce overhead
- connects customers to sellers without asking for or disclosing customers' private data
- avoids shared risks
- easily monetizes transactions; easy for sellers/buyers to join
- there is no requirement for banks to be accessible during the transaction
- win-win-win for customer, provider, seller/buyer
- supports BOBO (Bill On Behalf Of): http://www.developer.sprintpcs.com/news/index.jsp?action=wam_overview

Micropayments with Controlled Privacy Using Existing Infrastructure

Network Manifold Associates, Inc.

Ed Gerck (egerck@nma.com)
Larry Suto (lsuto@nma.com
Thomas Blood (tblood@nma.com)
Einar Stefferud (stef@nma.com)

Rump Session
6th International Financial Cryptography Conference
Southampton, Bermuda
March 12 2002