iKP

Internet Keyed Payment Protocols

Mihir Bellare, Juan Garay,
Amir Herzberg, Hugo Krawczyk, Mark Linehan

IBM T. J. Watson Research Center
P. O. Box 218, Yorktown Heights, NY 10598, USA

email {mihir, garay, amir, hugo, linehan}@watson.ibm.com

Ralf Hauser, Phil Janson, Michael Steiner,
Gene Tsudik, Michael Waidner

IBM Zurich Research Laboratory
Säumerstrasse 4, CH8803 Rüschlikon, Switzerland

email {rah, pj, sti, gts, wmi}@zurich.ibm.com

Ph. +41 1 724 8 488 / Fax. +41 1 710 3608

Security Requirements

Issuer/Acquirer Requirements

[REQ A1] Proof of Transaction Authorization by Buyer.

- [a.] Weak Proof --- authentication but no non-repudiation
- [b.] Strong Proof --- provides non-repudiation to resolve disputes between Buyer and payment system provider.

[REQ A2] Proof of Transaction Authorization by Seller

- [a.] Weak proof
- [b.] Strong proof

Seller Requirements

[REQ S1] Proof of Transaction Authorization by Acquirer

[a.] Weak proof

[b.] Strong proof

[REQ S2] Proof of Transaction Authorization by Buyer

[a.] Weak proof

[b.] Strong proof

[REQ S3] Impossibility of Unauthorized Payment

[a.] Impossibility: Unauthorized payments impossible provided acquirer *not* compromised

[b.] Disputability: Even if acquirer is compromised, Seller can prove not having authorized payment

Buyer Requirements

[REQ B1] Impossibility of Unauthorized Payment.

[a.] Impossibility: unauthorized payments are impossible provided acquirer is not compromised.

[b.] Disputability: even if acquirer is compromised, Buyer can prove not having authorized the payment.

[REQ B2] Proof of Transaction Authorization by Acquirer

[REQ B3] Certification and Authentication of Seller

[REQ B4] Receipt from Seller.

[a.] Weak proof
[b.] Strong proof

[REQ B5] Transaction/Order Privacy

[a.] Buyer and Seller want to protect privacy of ordering information from eavesdroppers.

[b.] Buyer and Seller want to hide description of goods/services from acquirer.

[REQ B6] Anonymity: Buyer want to protect identity from eavesdroppers & Sellers

Non-Requirements

[NREQ 1] Untraceability of payment with respect to the payment system provider:

In iKP acquirer can identify both Buyer or Seller.

[NREQ 2] Real-time (small payment) capability

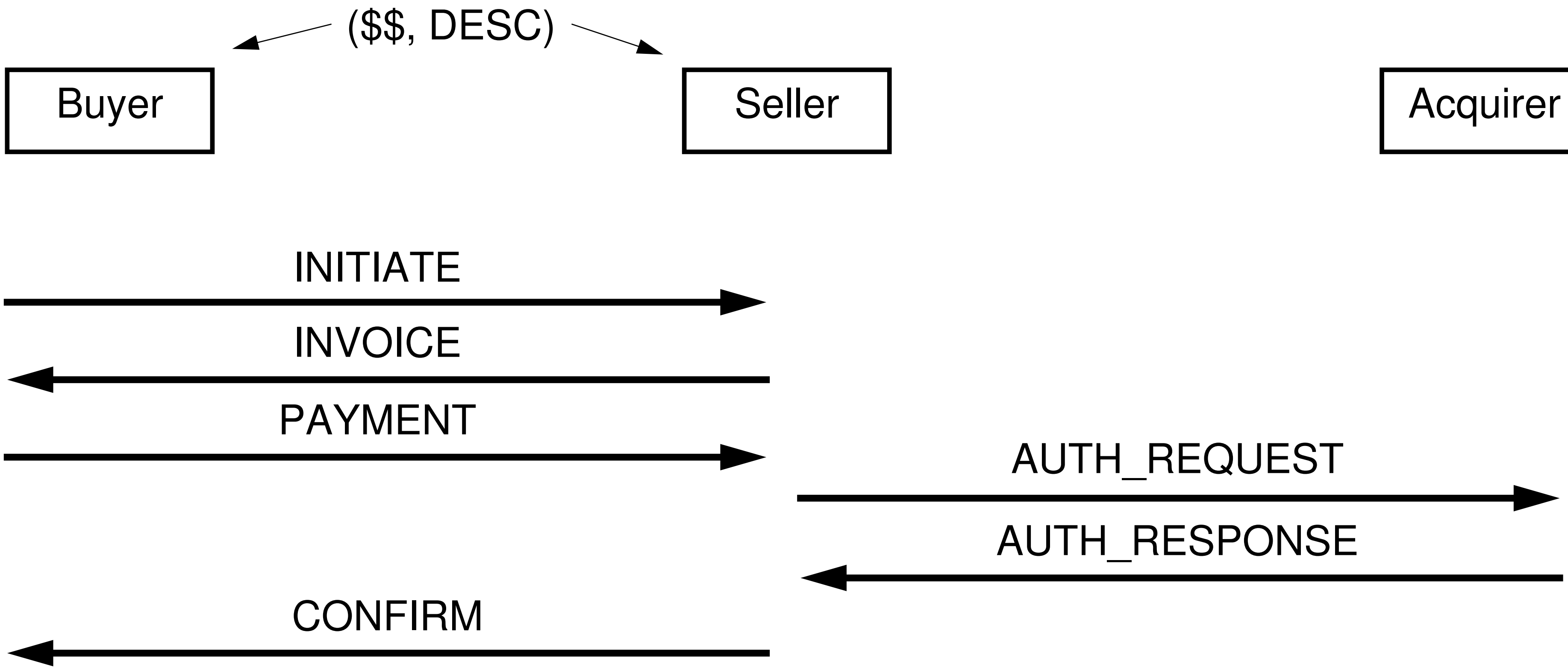
[NREQ 3] Secure Delivery of goods/services

[NREQ 4] Negotiations of payment amount (price) and other contractual details.

[NREQ 5] Protection from traffic analysis protection and covert channels

iKP Protocol Description

High-Level Flows



Notation

A, S, B	Protocol Participants: Acquirer, Seller, Buyer
[...]	Optional fields
PK_Z/SK_Z	Z's public/private key-pair; Z in {A,S,B}
E_A	Randomized encryption with integrity under PK_A
$S_Z(TXT)$	Signature under Z's private key SK_Z; Z in {A,S,B}
$SALT_B$	Random number generated by B
V	Random number generated by Seller
$$	Amount and currency
DATE	Seller's date/time stamp
$NONCE_S$	Seller's nonce (counter or random number)
ID_S	Seller’s id
TID_S	Transaction ID chosen by Seller
H(.)	Strong one-way hash function
DESC	Description of purchase/goods, opaque string
BAN	Buyer's Account Number, e.g., credit card number or account number
PIN	Buyer's PIN
R_B	Random number chosen by Buyer to form B_{ID}
B_{ID}	One-time Buyer ID, $B_{ID}=H(R_B,BAN)$
Y/N	Response from the clearing network

Detailed Flows

Buyer ← ($$, DESC) → Seller   Acquirer

Buyer → Seller: $SALT_B$, B_{ID} {= $H(R_B, BAN)$}

Seller → Buyer:

ID_S, TID_S, DATE, $NONCE_S$, H(DESC, $SALT_B$),
H($$, B_{ID}, ID_S, TID_S, DATE, $NONCE_S$, H(DESC,$SALT_B$), [H(V)]),
[S_S(H(*COMMON*)), [H(V)], [$CERT_S$]], [$CERT_A$]

CLEAR
COMMON
SIG_S

Buyer → Seller:

TID_S, E_A($$, R_B, BAN, H(*COMMON*), [PIN]),
[S_B(E_A(*SLIP*),H(*COMMON*)), [$CERT_B$]]

SLIP
SIG_B

Seller → Acquirer: CLEAR, E_A(*SLIP*), [*SIG_B*], [*SIG_S*]

SIG_A

Acquirer → Seller: TID_S, Y/N, S_A(Y/N, H(*COMMON*))

Seller → Buyer: [TID_S, Y/N, [SIG_A], [[*SIG_S*], V]]

Protocol Options

($$, DESC) → Buyer, Seller

Buyer | Seller | Acquirer

$SALT_B$, B_{ID} {= $H(R_B$,BAN)} →

ID_S, TID_S, DATE, $NONCE_S$, H(DESC, $SALT_B$),
H($$, B_{ID}, ID_S, TID_S, DATE, $NONCE_S$, H(DESC,$SALT_B$), [H(~~V~~)]),
~~[S_S(H(*COMMON*)), [H(V)], [$CERT_S$]], [$CERT_A$]~~

CLEAR
COMMON
SIG_S

TID_S, E_A($$, R_B, BAN, H(*COMMON*), [~~PIN~~]),
~~[S_B(E_A(*SLIP*),H(*COMMON*)), [$CERT_B$]]~~ →

SLIP
SIG_B

CLEAR, E_A(*SLIP*), [~~*SIG_B*~~], [~~*SIG_S*~~] →

SIG_A

← TID_S, Y/N, S_A(Y/N, H(*COMMON*))

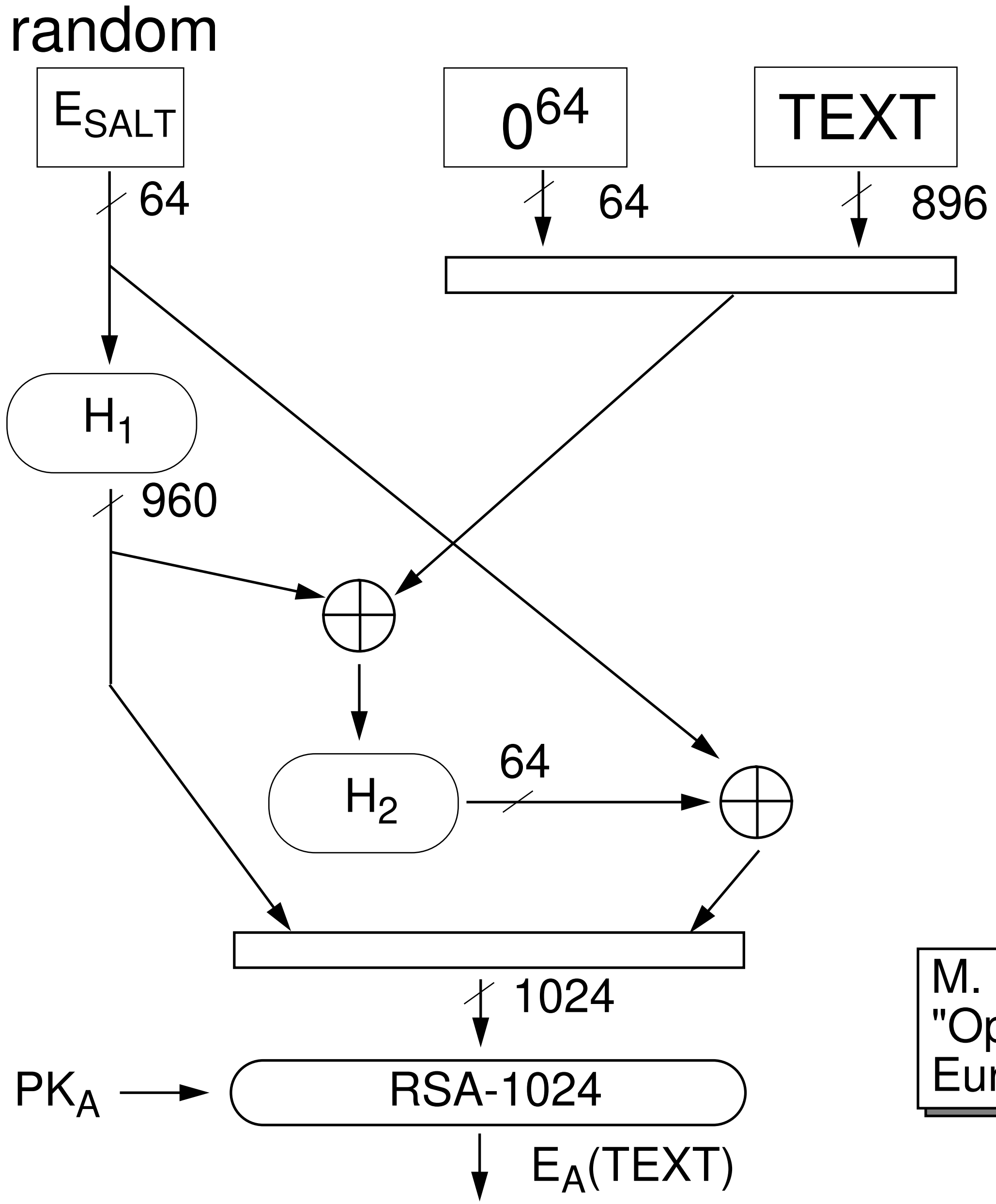
← ~~[TID_S, Y/N, [SIG_A], [[*SIG_S*], V]]~~

Encryption in iKP

- Limited to protecting the Buyer's PIN and Buyer Account Number
- All protocols require the Buyer to compute E_A(TEXT)
  - E_A RSA encryption, 1024 bits key length
  - TEXT = (VNO, $$, HASH, BAN, R_B, PIN, SALT)

VNO	Protocol Version number -- 32 bits
$$	Payment amount and currency -- 64 bits
HASH	H(COMMON) -- 128 bits
BAN	Buyer Account Number -- 0-128 bits
R_B	128 bits
PIN	Buyer PIN -- 0-64 bits
SALT	Random salt / padding -- at least 64 bits

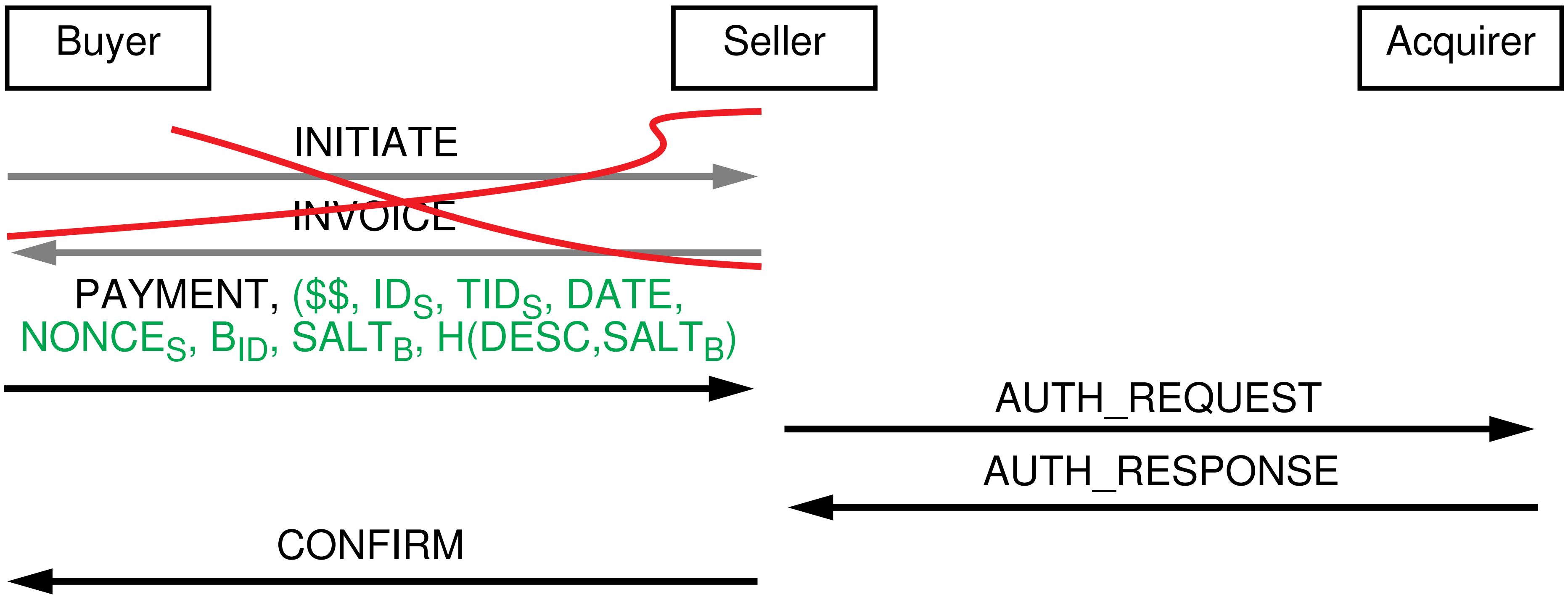
Encryption E_A(TEXT)



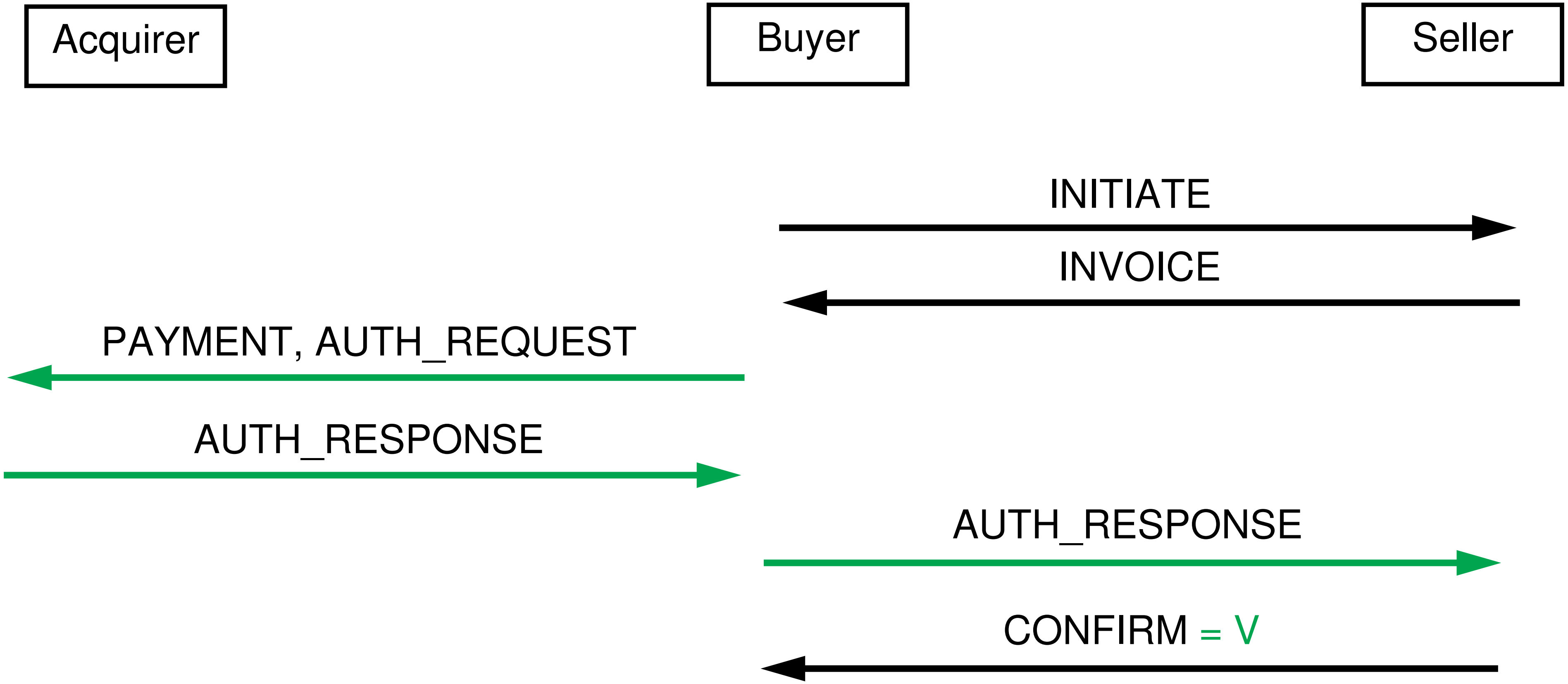
M. Bellare and P. Rogaway:
"Optimal Asymmetric Encryption";
Eurocrypt 94

Protocol Variations

Protocol without initial flows



Protocol with Buyer-Acquirer Link



References

[1] Phil Janson:
Internet Keyed Payment Protocols (iKP) -- Overview;
IBM Research Division, Zürich, May 1995.

[2] Mihir Bellare, Juan A. Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Michael Waidner:
iKP -- A Family of Secure Electronic Payment Protocols;
USENIX Workshop on Electronic Commerce '95.

[3] Mark Linehan, Gene Tsudik:
Internet Keyed Payments Protocol (iKP);
Internet Draft <draft-tsudik-ikp-00.txt>, July, 1995.

<http://www.zurich.ibm.com:80/Technology/Security/extern/ecommerce/iKP.html>