

Exhibit A13

Carl Meyer, S. M. Matyas, *Cryptography: A New Dimension in Computer Data Security* (John Wiley & Sons 1982) (“Matyas 1982”)

MATYAS 1982 qualifies as prior art to U.S. Patent No. 5,793,302 (“the ’302 patent”) under at least 35 U.S.C. § 102(b) and, particularly in view of Stambler’s infringement contentions, invalidates at least claims 51, 53, 55, and 56 of the ’302 patent. To the extent that Stambler contends that MATYAS 1982 does not disclose one or more limitations of the asserted claims, and further contends that the given limitation is not inherent in MATYAS 1982 as practiced, then it would have been obvious to combine the teachings of MATYAS 1982 with the knowledge of a person having ordinary skill in the art to show all the limitations of the asserted claims. Such knowledge includes (but is not limited to) the uses of public key cryptography, *see e.g.*, Rivest, Shamir, and Adelman, “A Method for Obtaining Digital Signatures and Public Key Cryptosystems,” *Communications of the ACM* (Vol. 21. No. 2, Feb. 1978). That article shows, for example, that it had been obvious for more than a decade to use digital signatures and public key cryptography to authenticate electronic funds transfers. *Id.* at 1 (“This has obvious applications in ... ‘electronic funds transfer’ systems.”). It would also have been obvious, as a design choice, to use the bootstrapping technique identified in that reference to use public key encryption techniques to securely exchange symmetric keys which could then be used for further messages. *Id.* at 122 (“A public key cryptosystem can be used to ‘bootstrap’ into a standard encryption scheme such as the NBS [National Bureau of Standards] method. Once secure communications have been established, the first message transmitted can be a key to use in the NBS scheme to encode all following messages.”).

MasterCard reserves the right to supplement and/or amend this claim chart depending on the Court’s claim constructions and how Stambler is construing the patent claims in an attempt to assert infringement.

These claim charts show exemplary citations to the prior art relative to the asserted claims of the ’302 patent. The determination of invalidity should be based on the entirety of each prior art document and not isolated portions of the document. Thus, the exemplary citations are merely intended to be illustrative.

Asserted '302 Claims	Matyas 1982
Claim 51	
<p>51. A method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, a credential being previously issued to at least one of the parties by a trusted party,</p>	<p>Matyas 1982 discloses a method for authenticating the transfer of funds from an account associated with a first party to an account associated with a second party, a credential being previously issued to at least one of the parties by a trusted party, the information stored in the credential being non-secret, as claimed.</p> <p><u>Example 1</u></p> <p>An example of methods of message authentication are methods for authenticating the transfer of funds. <i>See</i> p. 429-473.</p> <p><u>Example 2</u></p> <p>An example of a method of checking digital signatures is the method of authentication. <i>See</i> p. 477.</p>
<p>the information stored in the credential being non-secret, the method comprising:</p>	<p><u>Example 1</u></p> <p>The example of p. 457 shows message authentication in an interchange system.</p>

Asserted '302 Claims	Matyas 1982
	<p style="text-align: center;">Data Modification</p> <p>Many active fraud threats involve the modification of data in real time. These threats can be countered by either of two techniques, message encryption or message authentication. Message encryption, as the name implies, is simply the encryption of all, or at least most, of the message which conveys the transaction. This technique has the advantage of providing privacy as well as security. The disadvantage, however, is that the encrypted message cannot be comprehended or processed by the EDP systems (acquirer's, switch's, issuer's) through which the transaction passes. Thus, the message must be decrypted prior to being processed, but once decrypted, it loses its cryptographic protection, and therefore is susceptible to fraudulent modification within the EDP system.</p> <p>Message authentication is a technique which produces cryptographic check digits which are appended to the message. These digits are analogous to a parity check or cyclic redundancy check, except that in this case the check digits are cryptographically generated, using DES and a secret key. These digits, called the message authentication code or MAC, are generated by the originator, appended to the transmitted message, and then checked by the recipient, who also holds the same secret key used in the generation process. Should anyone attempt to modify the message between the time the MAC is generated and the time it is checked, he would be detected. Not knowing the secret key, he would be unable to generate the correct MAC for his modified message. Similarly, no one can successfully introduce a spurious message because he could not generate the proper MAC for this message.</p> <p>The suggested technique for MAC generation is as follows: The first 64 bits of that portion of the transaction to be protected are block encrypted using DES and the secret key. Then the next 64 transaction bits to be thus protected are Exclusive-ORed (modulo 2 added) with the just produced cipher. The result is then block encrypted using the same key, producing a new 64 bits of cipher. This procedure is continued until all critical transaction fields have been included. (The final data block will likely be less than 64 bits, so it is padded with zeros to make a full 64 bits prior to being Exclusive-ORed with the just produced cipher.) Some subset of the final cipher, at least six decimal digits or five hexadecimal digits, serves as the MAC.</p> <p>As a minimum, the following fields should be included in the MAC generation for a transaction request message:</p> <ol style="list-style-type: none"> 1. Transaction type (debit, credit, etc.). 2. Cardholder's account number. 3. Amount.

Asserted '302 Claims	Matyas 1982
	<p>(p. 457).</p> <p>The message authentication technique thus includes a transmitted transaction request message that is non-secret, along with a message authentication code appended thereto. The transaction request message includes the account number (a “credential”) issued to the cardholder (a “first party”) by a bank (a “trusted party”). The account number is non-secret. <i>See, e.g.</i> p. 458 (“the MAC approach does not provide privacy”).</p> <p><u>Example 2</u></p> <p>The example of p. 477 shows the transfer of funds from an account associated with a first party (customer) to the account associated with a second party (grocer/merchant).</p>

Asserted '302 Claims	Matyas 1982
	<p>A customer wishes to use a bank card to pay a grocery bill of \$35.00 and to receive an additional \$50.00 in cash. Assume that the grocer's account is with institution X and the customer's account is with institution Y. The customer's card is inserted into the EFT terminal, either by the customer or by an employee of the retailer attending the EFT terminal, and the customer enters his PIN via a suitable entry device such as a keyboard or a PIN pad, which looks and operates much like a hand-held calculator. Similarly, the grocer enters a transfer request for \$85.00 to be transferred from the customer's account to the grocer's account (\$35.00 for the groceries plus the \$50.00 to be given to the customer).</p> <p>The information entered at the EFT terminal is assembled into a <i>debit request</i> message. This message or <i>transaction request</i>, which includes the customer's PIN, his account number (PAN), and suitable routing information, is then sent via the acquirer (HPC X) and switch to the issuer (HPC Y).</p> <p>Upon receiving the debit request, HPC Y verifies that the PIN correlates properly with the customer's PAN, and that the customer's account balance is sufficient to cover the \$85.00 transfer. If the PIN check fails, the user is normally given at least two more chances to enter the correct PIN. If after the additional trials the PIN is still rejected, HPC Y sends a negative reply to HPC X. If the PIN is correct but the account balance is insufficient to cover the transfer, HPC Y denies the debit request by sending a negative reply or <i>debit refusal</i> (insufficient funds) message to HPC X. A message is then sent via the network to the grocer's EFT terminal indicating to the grocer that the funds transfer has been disapproved.</p> <p>If the debit request is approved, HPC Y records the debit request, reduces the customer's account balance by \$85.00, and transmits a positive reply or <i>debit authorization</i> message back to HPC X. Upon receiving the debit authorization HPC X takes two actions. A message is sent to the grocer's EFT terminal, indicating to the grocer that the funds transfer has been approved. Then HPC X credits the grocer's account with \$85.00. This completes the transaction. (Although other protocols are possible, the one described above will be assumed throughout the present discussion.)</p> <p>(p. 477).</p> <p>A credential (comprising identifier (IDc), public key (PKc), and signature of the identifier and public key (DSKb (CE (IDc, PKc))) has been previously issued to the customer by the issuer bank</p>

Asserted '302 Claims	Matyas 1982
	<div data-bbox="583 321 1312 836" data-label="Diagram"> <p>IDc: PKc, D_{SKb} [CE (IDc, PKc)]</p> <p>Customer's identifier, public key, and digital signature on IDc and PKc computed with the bank's private key</p> <p>IDb: PKb, D_{SKu} [CE (IDb, PKb)]</p> <p>Issuing bank's identifier, public key, and digital signature on IDb and PKb computed with the private interchange key</p> <p>SKc* = SKc ⊕ PIN</p> <p>Customer's Private Card Key</p> <p>Public-Key Algorithm</p> </div> <p data-bbox="583 841 1260 868">Figure 11-41. Information Stored on the Intelligent Secure Card</p> <p data-bbox="573 917 684 954">(p. 593).</p> <p data-bbox="573 979 1436 1076">promised, the security of the entire system is lost. The described public key approach depends, therefore, on one node or key distribution center which is trusted by everyone in the system, and that one party controls and manages the universal secret key.</p> <p data-bbox="573 1117 684 1154">(p. 597).</p> <p data-bbox="573 1187 1778 1256">The credential information (IDc, PKc, and the signature of that identity and public key data) is public.</p>

Asserted '302 Claims	Matyas 1982
<p>receiving funds transfer information, including at least information for identifying the account of the first party and information for identifying the account of the second party, and a transfer amount;</p>	<p>Matyas 1982 discloses receiving funds transfer information, including at least information for identifying the account of the first party and information for identifying the account of the second party, and a transfer amount, as claimed.</p> <p><u>Example 1</u></p> <p>The transaction request message includes the cardholder's account number ("information for identifying the account of the first party") and an amount. <i>See</i> p. 457, reproduced above. It is inherent that an interchange transaction would include information for identifying the account of a second party to a funds transfer. <i>See, e.g.</i>, p. 461-462.</p> <p><u>Example 2</u></p> <p>For example, the customer sends to the issuer a funds transfer request in Fig. 11-44, p. 596:</p>

Asserted '302 Claims

Matyas 1982

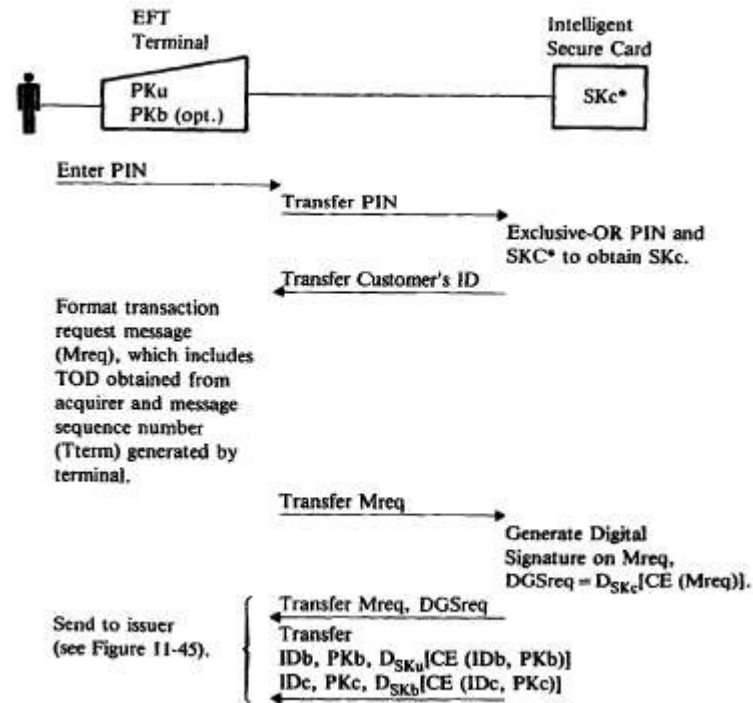


Figure 11-44. On-Line Use—EFT Terminal

(p 596).

The transfer request message, Mreq, contains at least the information of the example transaction of p. 477, which includes at least information for identifying the account of the first party, and information for identifying the account of the second party, and a transfer amount:

Asserted '302 Claims	Matyas 1982
	<p>For example, consider a simple transaction in which cryptography is not employed. A customer wishes to use a bank card to pay a grocery bill of \$35.00 and to receive an additional \$50.00 in cash. Assume that the grocer's account is with institution X and the customer's account is with institution Y. The customer's card is inserted into the EFT terminal, either by the customer or by an employee of the retailer attending the EFT terminal, and the customer enters his PIN via a suitable entry device such as a keyboard or a PIN pad, which looks and operates much like a hand-held calculator. Similarly, the grocer enters a transfer request for \$85.00 to be transferred from the customer's account to the grocer's account (\$35.00 for the groceries plus the \$50.00 to be given to the customer).</p> <p>The information entered at the EFT terminal is assembled into a <i>debit request</i> message. This message or <i>transaction request</i>, which includes the customer's PIN, his account number (PAN), and suitable routing information, is then sent via the acquirer (HPC X) and switch to the issuer (HPC Y).</p> <p>(p. 477).</p> <p>See also description of transaction request message at p. 456-57.</p>
<p>generating a variable authentication number (VAN) using at least a portion of the received funds transfer information;</p>	<p>Matyas 1982 discloses generating a variable authentication number (VAN) using at least a portion of the received funds transfer information, as claimed.</p> <p><u>Example 1</u></p> <p>A MAC (a “variable authentication number” or “VAN”) is generated using, among other information, at least the cardholder's account number and amount. See p. 457, reproduced above.</p> <p><u>Example 2</u></p> <p>For example, the digital signature (DGSreq)</p> <p>----- A secret user key (SK_c, where c stands for customer) is used to generate a quantity (DGSreq) which will enable the issuer to authenticate the transaction</p>

Asserted '302 Claims	Matyas 1982
	<p>request message, Mreq. In the conventional approach this quantity was called a MAC. Since a public-key approach provides a digital signature capability, the term DGS is used instead of MAC. To demonstrate the parallelism between the public-key and conventional algorithm approaches, assume that (Mreq, DGSreq) is routed to the issuer and define DGSreq as</p> $DGSreq = D_{SKc}[CE(Mreq)]$ <p>where CE(Mreq) represents the compressed encoding of Mreq. As discussed in Chapter 9, CE(M) is a one-way function of M and can be generated with publicly known keys for symmetric as well as asymmetric algorithms. In the implementation discussed here it suffices to specify one public key for generating CE(M) without, at the same time, specifying the corresponding secret key. This is so because the sender and receiver use the same procedure for generating CE(M). To check the signature, the issuer generates the compressed encoding of the received message and compares it with $E_{PKc}(DGSreq)$ (i.e., the received DGSreq encrypted under PKc). If both quantities agree Mreq is accepted; otherwise, not.</p> <p>(p. 590)</p>
<p>determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information; and</p>	<p>Matyas 1982 discloses determining whether the at least a portion of the received funds transfer information is authentic by using the VAN and the credential information, as claimed.</p> <p><u>Example 1</u></p> <p>The MAC is used by the recipient to authenticate the transaction request message. The recipient performs a parity check or cyclic redundancy check. <i>See</i>, p. 457, reproduced above. That is, the recipient uses the transaction request message, including the cardholder's account number ("credential information") and a secret key to determine that the MAC ("VAN") corresponds to the transaction request message.</p> <p><u>Example 2</u></p> <p>For example, the digital signature DGSreq is used to validate the transfer request message (Mreq):</p>

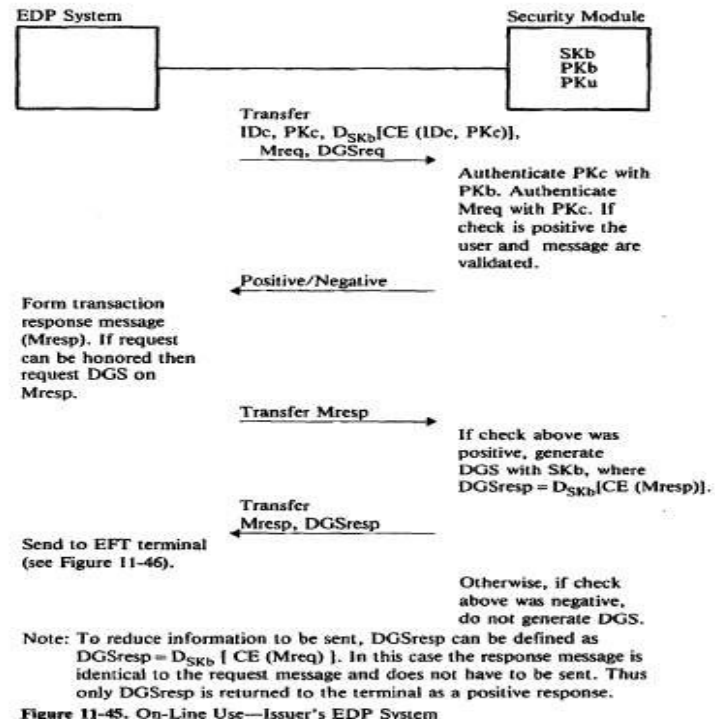
Asserted '302 Claims	Matyas 1982
	<p>generating CE(M). To check the signature, the issuer generates the compressed encoding of the received message and compares it with $E_{PK_c}(DGSreq)$ (i.e., the received DGSreq encrypted under PK_c). If both quantities agree Mreq is accepted; otherwise, not.</p> <p>This check on DGSreq can be used also to verify the user (e.g., if SK_c is defined as $SK_c = SK_c^* \otimes PIN$, where SK_c^* is a secret parameter stored on the card). Since the digital signature (DGS) is now also a function of PIN, personal verification as well as message authentication are combined in one procedure. [The same idea was used in the hybrid key management approach by defining $KTR = D_{KP \otimes PIN}(ID)$ and is repeated here for the sake of uniformity in the discussion.]</p> <p>(p. 590).</p> <p>The credential information is used to identify the customer (ID_c) in order to obtain the correct public key PK_c for performing the digital signature authentication.</p> <p>At the issuer, the corresponding PK_c of reference, which is filed under the user's identifier, is read from the EDP system's data base⁴³ and used to</p> <p>(p. 592)</p> <p>encrypt the received DGSreq. This result is compared for equality with the compressed encoding calculated on the received message Mreq. Furthermore, the received TOD is checked for currency against a TOD of reference stored in the issuer's EDP system. If both tests succeed, the issuer concludes that the content of the message is correct, the message is not a stale message, and the secret information entered by the customer at the entry point (SK_c^* and PIN) is properly related to the claimed ID.</p> <p>(p. 593).</p> <p>The credential is stored on the customer intelligent secure card and included in the transfer request.</p>

Asserted '302 Claims	Matyas 1982
	<div data-bbox="590 310 1266 894"><p>$IDc: PKc, D_{SKb} [CE (IDc, PKc)]$</p><p>Customer's identifier, public key, and digital signature on IDc and PKc computed with the bank's private key</p><p>$IDb: PKb, D_{SKu} [CE (IDb, PKb)]$</p><p>Issuing bank's identifier, public key, and digital signature on IDb and PKb computed with the private interchange key</p><p>$SKc^* = SKc \oplus PIN$</p><p>Customer's Private Card Key</p><div data-bbox="611 797 858 873">Public-Key Algorithm</div></div> <p data-bbox="590 899 1215 932">Figure 11-41. Information Stored on the Intelligent Secure Card</p> <p data-bbox="573 980 676 1013">(p. 593)</p> <div data-bbox="600 1040 1167 1175"><p data-bbox="1058 1040 1167 1062">$DGSreq = D$</p><p data-bbox="600 1078 768 1127">Send to issuer (see Figure 11-45).</p><p data-bbox="800 1062 1125 1175">{ Transfer Mreq, DGSreq Transfer IDb, PKb, $D_{SKu} [CE (IDb, PKb)]$ IDc, PKc, $D_{SKb} [CE (IDc, PKc)]$ }</p></div> <p data-bbox="600 1192 978 1224">Figure 11-44. On-Line Use—EFT Terminal</p> <p data-bbox="573 1273 781 1305">(p. 596, partial).</p> <p data-bbox="176 1338 527 1411">transferring funds from the account of the first party to</p> <p data-bbox="573 1338 1898 1411">Matyas 1982 discloses transferring funds from the account of the first party to the account of the second party if the at least a portion of the received funds transfer information and the VAN are determined to</p>

Asserted '302 Claims	Matyas 1982
<p>the account of the second party if the at least a portion of the received funds transfer information and the VAN are determined to be authentic.</p>	<p>be authentic, as claimed.</p> <p><u>Example 1</u></p> <p>The transaction is approved if the MAC is determined to be correct based on the transaction request message and the secret key. <i>See</i> pp. 457-458. It is inherent that the approved interchange transaction involves a transfer of funds from the account of the first party to the account of the second party.</p> <p><u>Example 2</u></p> <p>For example, Fig. 11-45, p. 598 shows that the issuer validates the VAN and at least a portion of the funds transfer information (user and message are validated), <i>See</i> also Fig. 11-46 (“Honor Transaction Request”).</p>

Asserted '302 Claims

Matyas 1982



(p. 598).

If the debit request is approved, the funds are transferred. See, e.g., Fig. 11-46; see also p. 477:

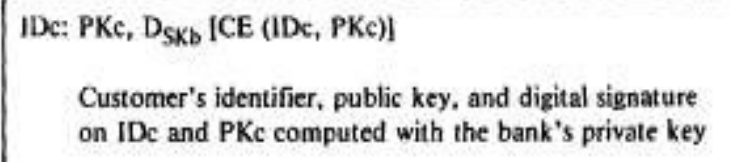
If the debit request is approved, HPC Y records the debit request, reduces the customer's account balance by \$85.00, and transmits a positive reply or *debit authorization* message back to HPC X. Upon receiving the debit authorization HPC X takes two actions. A message is sent to the grocer's EFT terminal, indicating to the grocer that the funds transfer has been approved. Then HPC X credits the grocer's account with \$85.00. This completes the transaction. (Although other protocols are possible, the one described above will be assumed throughout the present discussion.)

Asserted '302 Claims	Matyas 1982
Claim 53	
<p>53. The method of claims 51 wherein the funds transfer comprises a payment made by the first party to the second party.</p>	<p>Matyas 1982 discloses the method of claim 51 wherein the funds transfer comprises a payment made by the first party to the second party, as claimed.</p> <p><u>Example 1</u></p> <p>It is inherent that the cardholder (the “first party”) in an interchange transaction would involve a funds transfer from the cardholder to a second party (e.g., a merchant).</p> <p><u>Example 2</u></p> <p>For example, the transaction request Mreq may be used to make a payment is indicated by the example of p. 477. <i>See also</i> Fig. 11-46.</p> <p style="padding-left: 40px;">If the debit request is approved, HPC Y records the debit request, reduces the customer's account balance by \$85.00, and transmits a positive reply or <i>debit authorization</i> message back to HPC X. Upon receiving the debit authorization HPC X takes two actions. A message is sent to the grocer's EFT terminal, indicating to the grocer that the funds transfer has been approved. Then HPC X credits the grocer's account with \$85.00. This completes the transaction. (Although other protocols are possible, the one described above will be assumed throughout the present discussion.)</p> <p>(p. 477).</p>

Asserted '302 Claims	Matyas 1982
Claim 55	
<p>55. The method of claim 51 wherein the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information.</p>	<p>Matyas 1982 discloses the method of claim 51 wherein the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information, as claimed.</p> <p><u>Example 1</u></p> <p>The MAC is generated using, among other information, at least the cardholder's account number and amount. <i>See</i> p. 457, reproduced above. The MAC is generated to permit error detection of the transaction request message. <i>See, e.g.,</i> p. 458 (e.g., "protecting the transaction against fraudulent modifications").</p> <p><u>Example 2</u></p> <p>For example, the digital signature is generated using an error detection code (compressed representation) of the transaction request Mreq</p> <p style="padding-left: 40px;">Since a public-key approach provides a digital signature capability, the term DGS is used instead of MAC. To demonstrate the parallelism between the public-key and conventional algorithm approaches, assume that (Mreq, DGSreq) is routed to the issuer and define DGSreq as</p> $\text{DGSreq} = \text{D}_{\text{SK}_e}[\text{CE}(\text{Mreq})]$ <p style="padding-left: 40px;">where CE(Mreq) represents the compressed encoding of Mreq. As discussed in Chapter 9, CE(M) is a one-way function of M and can be generated with publicly known keys for symmetric as well as asymmetric algorithms. In the implementation discussed here it suffices to specify one public key for generating CE(M) without, at the same time, specifying the corresponding secret key. This is so because the sender and receiver use the same procedure for generating CE(M). To check the signature, the issuer generates the compressed encoding of the received message and compares it with $\text{E}_{\text{PK}_e}(\text{DGSreq})$ (i.e., the received DGSreq encrypted under PK_e). If both quantities agree Mreq is accepted; otherwise, not.</p> <p>(p. 590).</p> <p>This describes a 1-way function that serves to generate an error detection code. <i>See</i> p. 469 (MAC</p>

Asserted '302 Claims	Matyas 1982
	Generation paragraph). E.g., “Should anyone attempt to modify such a message while in transit he would be unable to do so without detection.”)
Claim 56	
<p>56. The method of claim 51 for further securing the transfer of funds, at least one party being previously issued a credential by a trusted party, the credential information including information associated with the at least one party and a second variable authentication number (VAN1), the VAN1 being used to secure at least a portion of the credential information to the at least one party, authentication and the transfer of funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN1.</p>	<p>Matyas 1982 discloses the method of claim 51 for further securing the transfer of funds, at least one party being previously issued a credential by a trusted party, the credential information including information associated with the at least one party and a second variable authentication number (VAN1), the VAN1 being used to secure at least a portion of the credential information to the at least one party, authentication and the transfer of funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN1, as claimed.</p> <p><u>Example 2</u></p> <p>For example, the credential (including Customer’s identifier, Public Key, and signature of those) is issued to the customer by the issuer bank and stored on the customer's bank card.</p>

Asserted '302 Claims	Matyas 1982
	<div data-bbox="590 310 1266 894"> <p> $ID_c: PK_c, D_{SK_b} [CE (ID_c, PK_c)]$ Customer's identifier, public key, and digital signature on ID_c and PK_c computed with the bank's private key </p> <p> $ID_b: PK_b, D_{SK_u} [CE (ID_b, PK_b)]$ Issuing bank's identifier, public key, and digital signature on ID_b and PK_b computed with the private interchange key </p> <p> $SK_c^* = SK_c \oplus PIN$ Customer's Private Card Key </p> <div data-bbox="611 797 858 875">Public-Key Algorithm</div> </div> <p data-bbox="590 899 1218 932">Figure 11-41. Information Stored on the Intelligent Secure Card</p> <p data-bbox="569 951 684 984">(p. 593).</p> <p data-bbox="569 1019 1862 1127">promised, the security of the entire system is lost. The described public key approach depends, therefore, on one node or key distribution center which is trusted by everyone in the system, and that one party controls and manages the universal secret key.</p> <p data-bbox="569 1131 684 1164">(p. 597).</p> <p data-bbox="569 1200 1866 1268">The credential contains information associated with the customer. The second variable authentication number (VAN1) is the signature part of the credential:</p>

Asserted '302 Claims	Matyas 1982
	 <p>(Fig 11-41, p, 593, partial).</p> <p>The credential information is “secured” to the customer by the digital signature (VAN1), because authentication fails if that digital signature cannot be verified.</p>