MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA TUTELA DELLA PROPRIETA' INDUSTRIALE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

DOMANDA NUMERO	**101996900532796**
Data Deposito	**19/07/1996**
Data Pubblicazione	**19/01/1998**

Priorità	08/503984
Nazione Priorità	US
Data Deposito Priorità	

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	K		

Titolo

PROCEDIMENTO E SISTEMA PER FORNIRE INTERSCAMBI DI DOCUMENTI E DATI ELETTRONICI SICURI (EDI) SU UNA RETE APERTA

PREMENOS CORP.,

con sede a Concord, California (U.S.A.)

MI 96 A 1519

* * * * * * * *

19 LUG. 1996

D E S C R I Z I O N E

La presente invenzione riguarda procedimenti e sistemi per fornire EDI sicuro su una rete aperta del sistema, come ad esempio la rete INTERNET e, particolarmente, riguarda un perfezionato procedimento e sistema per fornire una trasmissione di tipo postale EDI sicura su una rete aperta che impiega uno schema di crittografia o crittografico a chiavi o indicativi pubbliche/private di tipo RSA, al fine di fornire autentificazione sicura, e non-ripudio sia dell'origine che della ricezione.

Sistemi di comunicazione sicuri a chiavi pubbliche/private su una rete aperta sono ben noti, come ad esempio descritto nei brevetti statunitensi Nn. 4.578.531; 4.471.164; 5.268.962; 5.142.577; 4.893.338; 5.222.140; 5.261.002; 5.073.934; 5.303.303; 5.297.208; 5.369.705; 5.351.293; 5.375.169; 5.224.166; 5.253.294; e 5.237.611. Il sistema crittografico a chiavi pubbliche/private RSA è un ben noto sistema a chiavi pubbliche per fornire messaggi sicuri su una rete aperta, come la rete INTERNET, ed è descritto in vari brevetti statunitensi concessi come per esempio i brevetti statunitensi Nn. 4.405.829; 4.424.414; 4.200.770; 4.218.582; 5.073.935; e 4.723.284, il cui contenuto è qui incluso a titolo di riferimento. In aggiunta, è noto il concetto di non-ripudio dell'origine, come descritto nei brevetti statunitensi Nn. 5.226.709; e 5.367.573; e sono pure noti sistemi in cui segnature digitali sono impiegate i sistemi a chiavi pubbliche/private come descritto nei brevetti statunitensi

ASSOCIATI

Nn. 5.311.591; 5.214.702; 5.337.360; 4.868.877; 5.001.752; 5.005.200; 5.136.643; 5.018.196; 4.885.777; 4.267.782; 5.351.302; 5.208.858; 5.299.263; 5.142.578; 4.987.593; 4.991.210; 5.339.361; 5.373.558; 4.625.076; ed è noto il sistema Entrust commerciato dalla Northern Telecom. In aggiunta, vari altri sistemi di trasmissioni sicuri sono stati sviluppati con gli anni in un tentativo di tentare di fornire comunicazioni commerciali sicure su reti pubbliche o private, come descritto nei brevetti statunitensi Nn. 5.369.702; 4.876.716; 5.199.074; 4.823.388; 5.268.962; 5.022.080; 5.136.646; e 5.204.961. Inoltre, l'impiego di interscambio di dati o documenti elettronici o per trasmettere comunicazioni commerciali da pari a pari è noto nella tecnica, come ad esempio descritto nel brevetto statunitense No. 5.202.977 posseduto dalla presente Assegnataria o nel summenzionato brevetto statunitense No. 5.337.360. Tuttavia, i Richiedenti non sono a conoscenza di alcun tentativo riuscito della tecnica nota di impiegare la rete INTERNET, o qualsiasi altra rete aperta ampiamente accessibile come linee telefoniche od un qualsiasi sistema TCP/IP in cui un sistema a chiavi pubbliche/chiavi private sicuro, come ad esempio un sistema RSA, sia stato combinato con successo con EDI per fornire autentificazione e non-ripudio sia di origine che di ricezione in una transazione privata da pari a pari sicura suscettibile di aver luogo in qualsiasi momento sulla rete aperta senza richiedere controllo di parole d'ordine o di codice, ed al tempo stesso fornendo pure verifica dell'integrità dei messaggi. Un simile sistema elimina la necessità di avere reti a valore-aggiunto private ed altre reti private di terze parti come pure garantire la possibilità di realizzare commercialmente transazioni commer-

ASSOCIATI

ciali private tra pari e pari su una rete aperta largamente disponibile impiegando EDI. La certezza di non-ripudio ed autentificazione elimina la capacità dell'una o dell'altra parte relativamente al negare che la transazione sia stata approvata ed elimina dubbi relativi al contenuto del documento EDI determinante l'esecuzione della transazione. La capacità del procedimento e del sistema della presente invenzione relativa al fornire comunicazione tipo postale EDI sicura in combinazione con un sistema a chiavi pubbliche/private di tipo RSA, elimina gli inconvenienti della tecnica nota.

Il procedimento ed il sistema della presente invenzione comprendono l'impiegare il messaggio di riconoscimento AUTACK o EDI come un documento per fornire la segnatura o "firma" digitale in un sistema a chiavi pubbliche/private in cui l'AUTACK è segnato da un codice di totale di quadratura (hash) crittografato, dalla comunicazione di interscambio EDI che è stata crittografata con la chiave privata del trasmettitore, come ad esempio in un sistema a chiave pubblica/privata di tipo RSA, e costituisce un perfezionamento di questi sistemi. Poichè l'AUTACK o riconoscimento funzionale è sigillato con la chiave privata del trasmettitore del riconoscimento funzionale, il ricevitore del messaggio originale, quando il trasmettitore originale decripta il messaggio AUTACK di risposta con la chiave pubblica del ricevitore, il trasmettitore avrà garanzia che il ricevitore desiderato abbia effettivamente a trasmettere l'AUTACK di risposta o riconoscimento di risposta e sarà garantito dell'integrità della ricezione grazie al fatto che viene rivelato il codice di totale di quadratura o "hash" corretto.

ASSOCIATI MODIANO

Il messaggio EDI AUTACK, come il messaggio EDIFACT AUTACK, che è uno standard internazionale generico di EDI per scopi amministrativi, commerciali e per transazioni, è preferibilmente impiegato per fornire l'autentificazione o autentica sicura desiderata, il desiderato sicuro non-ripudio dell'origine o ricezione, e riconoscimento o diniego di riconoscimento per una o più "buste" EDI, come ad esempio le buste X.12 o EDIFACT, a titolo esemplificativo. Nel procedimento e sistema attualmente preferiti della presente invenzione, nel processo di autentificazione e non-ripudio d'origine, la parte trasmittente calcola un desiderato totale di quadratura o sommario dei messaggi da EDI, come il MD5 per l'intera comunicazione di interscambio EDI ed inserisce il valore nel messaggio AUTACK. La parte trasmittente o trasmettitore calcola quindi preferibilmente il MD5 (message digest versione 5 o versione di sommario di messaggio 5) del messaggio AUTACK e segna in modo digitale il messaggio AUTACK crittografando il MD5 calcolato con la chiave privata del trasmettitore, ed inserisce questo valore nel messaggio AUTACK. Così, il messaggio AUTACK o di riconoscimento EDI, è preferibilmente impiegato per fornire la segnatura. La parte ricevente o ricevitore, dopo ricezione del messaggio, decripta o decrittografa quindi la comunicazione di interscambio EDI, se essa è crittografata, e calcola il MD5 per la comunicazione di interscambio EDI ricevuta. Se è desiderato non-ripudio dell'origine, allora il ricevitore decripta quindi il messaggio AUTACK con la chiave pubblica del trasmettitore. Il valore ottenuto mediante tale decriptazione in questo esempio è il MD5 del messaggio AUTACK. Il MD5 del messaggio AUTACK è quindi calcolato e comparato con il valore decriptato. Se entrambi i valori sono uguali,

MODIANO & ASSOCIATI

sere dedotto provando il codice di sicurezza nel messaggio AUTACK, allora quanto segue risulta implicito per stabilire non-ripudio della ricezione: la comunicazione di interscambio EDI in questione è nota sia al trasmettitore che al ricevitore poichè il MD5 della comunicazione di interscambio EDI ed il numero di interscambio sono contenuti nel messaggio AUTACK e sono stati debitamente riconosciuti, l'integrità e l'autenticità della comunicazione di interscambio EDI in seguito a ricezione sono state verificate, ed il ricevitore non nega di aver ricevuto la comunicazione di interscambio EDI in questione.

La capacità di commerciare o condurre affari su una base da pari-a-pari su una rete pubblica aperta, come ad esempio la rete INTERNET, senza la necessità di controllo di parole d'ordine o di codice, può essere controllata, nel grado desiderato, dai partecipanti alla transazione commerciale tramite l'impiego di accordi o contratti tra partner commerciali per fornire certificazione di scambio delle chiavi, o facendo affidamento su una autorità certificata che rilascia e verifica i percorsi delle chiavi pubbliche/private. Così, transazioni private e sicure, soggette ad autentificazione e a non-ripudio sia dell'origine che della ricezione, unitamente a verifica dell'integrità dei messaggi, impiegando EDI, possono esser eseguite su una rete di comunicazione aperta.

Nei disegni:

la figura 1 è uno schema di flusso funzionale del procedimento e del sistema attualmente preferiti secondo la presente invenzione per fornire EDI sicuro su una rete aperta, come ad esempio la rete INTERNET, al fine di fornire integrità, autentificazione, non-ripudio di origine e di rice-

ASSOCIATI MODIANO

allora l'integrità del messaggio AUTACK è verificata ed è stabilito non-ripudio dell'origine. Il MD5 della comunicazione di interscambio EDI è quindi comparato con il MD5 dell'interscambio EDI che è stato inserito nel messaggio AUTACK e, se i due sono uguali, allora l'integrità dell'interscambio EDI è verificata, ed è stabilito non-ripudio dell'origine.

Per stabilire quindi non-ripudio della ricezione, dopo aver verificato l'integrità e l'autenticità della comunicazione di interscambio EDI ricevuta nel modo descritto precedentemente, un nuovo AUTACK o AUTACK di risposta è creato popolando tutti i segmenti ed elementi come appropriato, il MD5 calcolato è segnalato in digitale con la chiave privata del ricevitore, il MD5 segnato in digitale è inserito nell'AUTACK di risposta, segmenti appropriati del messaggio AUTACK di risposta sono popolati, ed il messaggio AUTACK di risposta preparato è trasmesso al trasmettitore. Il trasmettitore originale, alla ricezione di questo messaggio AUTACK di risposta verifica quindi la segnatura digitale dal ricevitore del suo messaggio originale medinte decriptazione di esso con la chiave pubblica del ricevitore. Il valore ottenuto mediante tale decriptazione o decriptografazione, è il MD5 dell'AUTACK di risposta ricevuto. Un trasmettitore originale, che ha ricevuto l'AUTACK di risposta dal ricevitore del suo messaggio, calcola quindi il MD5 dell'AUTACK di risposta ricevuto e, se il MD5 calcolato è uguale all'MD5 descriptato, allora l'integrità dell'AUTACK è preservata ed è stabilito non-ripudio dell'origine dell'AUTACK. Inoltre, se il MD5 contenuto nel segmento particolare dell'AUTACK ricevuto ove esso è stato inserito dal trasmettitore è uguale all'MD5 dell'interscambio EDI precedentemente trasmesso ed il riconoscimento è positivo, il che può es-

GIUDIANO & ASSOCIATI

zione, ed EDI impiegante segretezza;

la figura 2 è un diagramma di flusso funzionale della porzione del procedimento e del sistema di figura 1, che fornisce autentificazione o autentica e non-ripudio di origine impiegando il messaggio EDIFACT AUTACK;

la figura 3 è un diagramma di flusso funzionale, simile a figura 2, della porzione del procedimento e del sistema di figura 1, che fornisce non-ripudio del ricevitore impiegando il messaggio EDIFACT AUTACK;

la figura 4 è un diagramma di flusso funzionale della ricezione di "posta" sicura sulla rete INTERNET secondo il procedimento ed il sistema attualmente preferiti della presente invenzione;

la figura 5 è un diagramma di flusso funzionale, simile a figura 4 della trasmissione della posta sicura o segreta sulla rete INTERNET secondo il procedimento ed il sistema attualmente preferiti della presente invenzione;

la figura 6 è un diagramma di flusso funzionale simile a figura 4 del controllo di partner commerciali secondo il procedimento ed il sistema attualmente preferiti della presente invenzione;

la figura 7 è un diagramma di flusso funzionale, simile a figura 4, di gestione di giornali o "log" di controllo amministrativo o di "audit" secondo il procedimento ed il sistema attualmente preferiti della presente invenzione;

la figura 8 è un diagramma di flusso funzionale, simile alla figura 4, di gestione di tracciatura o "tracking" secondo il procedimento ed il sistema attualmente preferiti della presente invenzione;

la figura 9 è un diagramma di flusso funzionale, simile a figura 4,

MODIANO & ASSOCIATI

di monitoraggio dei compiti o "job" secondo il procedimento e sistema attualmente preferiti della presente invenzione;

la figura 10 è un diagramma funzionale dell'organizzazione del sistema impiegato nell'attuare il procedimento attualmente preferito della presente invenzione;

le figure 11-13 costituiscono un digramma di flusso funzionale, simile a figura 4, del procedimento e sistema attualmente preferiti complessivi delle figure 1-10, la figura 11 illustrando verifica di certificazioni, la figura 12 illustrando elaborazione TPA e la figura 13 illustrando elaborazione di chiavi pubbliche/chiavi private;

la figura 14 è una illustrazione schematica di una tipica visualizzazione sullo schermo di un calcolatore conformemente al procedimento ed al sistema attualmente preferiti della presente invenzione, illustrante le varie opzioni funzionali che devono essere controllate dagli utenti per garantire comunicazione postale sicura o segreta sulla rete INTERNET secondo il procedimento ed il sistema attualmente preferiti della presente invenzione;

le figure da 15 a 21 sono illustrazioni schematiche, simili a figura 14, di tipiche visualizzazioni di schermo di calcolatore conformemente alla opzione "TRADING PARTNERS PROFILE o DEL PROFILO DEI PARTNER COMMERCIALI" nella visualizzazione di schermo di figura 14;

le figure da 22 a 28 sono illustrazioni schematiche, simili a figura 14, di tipiche visualizzazioni di schermo di calcolatore secondo l'opzione "TRADING PARTNERS AGREEMENTS o DI ACCORDI DI PARTNER COMMERCIALI" nella visualizzazione di schermo di figura 14, e la figura 28 illu-

MODIANO & ASSOCIATI

strando la visualizzazione di schermo di OUTBOUND RETRANSMISSION o di RI-TRASMISSIONE USCENTE" per trasmettere posta elettronica o E-mail sicura o segreta secondo il procedimento ed il sistema attualmente preferiti della presente invenzione;

le figure da 29 a 33 sono illustrazioni schematiche, simili a figura 14, di tipiche visualizzazioni di schermo di calcolatore conformemente alla opzione "KEY MANAGEMENT o di GESTIONE CHIAVI" o indicativi nella visualizzazione di schermo di figura 14; e

le figure da 34-41 sono illustrazioni schematiche, simili a figura 14, delle tipiche visualizzazioni di schermo di calcolatore secondo l'opzione "TRACKING o di TRACCIATURA" nella visualizzazione di schermo di figura 14, le figure da 35 a 38 illustrando interscambi di tracciatura e le figure da 39 a 41 illustrando tracciatura di una "rete giornale" di controllo amministrativo o "audit log".

Facendo ora riferimento dettagliato ai disegni, ed inizialmente alla figura 1, in essa è illustrato un diagramma di flusso funzionale del sistema 100 attualmente preferito secondo la presente invenzione per fornire EDI sicura o segreta su una rete aperta convenzionale come ad esempio la rete INTERNET 102 commercialmente disponibile. Il procedimento ed il sistema preferiti secondo la presente invenzione sono implementati in un sistema che è fornito con il marchio di fabbrica di TEMPLAR, posseduto dalla presente Assegnataria. Come sarà illustrato più dettagliatamente in seguito, facendo riferimento alle figure da 2 a 41, il procedimento ed il sistema attualmente preferiti della presente invenzione forniscono integrità, autentica o autentificazione, non-ripudio o non rigetto sia di origine

che di ricezione, ed EDI impiegante segretezza. Ciò è preferibilmente utilizzato impiegando il messaggio di riconoscimento AUTACK o EDI (Electronic Data Interchange o di Interscambio di Dati Elettronico) come un documento per fornire una segnatura o firma digitale in un sistema a chiavi o indicativi pubblici/privati che è preferibilmente un sistema impiegante il convenzionale schema di criptografia o criptatura a chiavi o indicativi pubblici/privati RSA convenzionale come il sistema criptografico descritto nei brevetti statunitensi Nn. 4.405.828; 4.424.414; 4.200.770; e 4.218.582, il cui contenuto è qui incorporato nella propria completezza a titolo di riferimento. Come sarà descritto più dettagliatamente in seguito, l'AUTACK è preferibilmente sigillato o "segnato" con una segnatura o firma digitale che è preferibilmente creata mediante crittografia dell'MD5 (message digest versione 5 o versione di sommario messaggi 5) del messaggio AUTACK con l'elemento originatore della chiave privata di AUTACK come ad esempio la chiave privata del trasmettitore nel processo preferito di autentificazione e non-ripudio dell'origine illustrato in figura 2, o con la chiave privata del ricevitore nel processo preferito di non-ripudio di ricezione illustrato in figura 3. La segnatura digitale è quindi preferibilmente inserita in una posizione predeterminata nell'AUTACK e trasmessa all'altra parte partecipante alla transazione. Poichè l'AUTACK è sigillato con la chiave privata del trasmettitore dell'AUTACK, quando il ricevitore di tale AUTACK decripta l'AUTACK con la chiave pubblica del trasmettitore di tale AUTACK, egli avrà garanzia che il ricevitore previsto del suo messaggio trasmetta effettivamente tale AUTACK, ed avrà pure garanzia dell'integrità della ricezione grazie al fatto che il corretto codice "hash"

MODIANO & ASSOCIATI

o dei totali di quadratura viene rivelato nel modo che sarà descritto successivamente. Secondo la presente invenzione, la chiave segreta crittografata o criptata, usata per criptare il messaggio, come pure il messaggio di per se stesso, sono contenuti nel messaggio PKCS.

Il MD5 è un valore convenzionale che può essere ottenuto in un messaggio EDI mediante quadratura o suddivisione convenzionale di una quantità, come un interscambio EDI. Vi è una bassissima probabilità che il MD5 di qualsiasi due documenti diversi abbia ad essere il medesimo e, perciò, il MD5 è preferibilmente impiegato per stabilire l'integrità di interscambi EDI conformemente la procedimento attualmente preferito della presente invenzione.

Come è ben noto dagli utenti di EDI, un messaggio AUTACK è uno standard UN/EDIFACT per l'autentificazione ed il riconoscimento. Secondo il procedimento ed il sistema attualmente preferiti della presente invenzione, l'AUTACK è preferibilmente costituito dal USH o titolo-intestazione di sicurezza, USB, USX per identificare il messaggio, USY per mantenere informazione di sicurezza o segretezza sul messaggio riportato, USR, e qualche altro segmento convenzionale normalmente presente in un AUTACK. Preferibilmente, informazione come tipo di risposta, applicazione di ambito di sicurezza, e funzione di sicurezza. Sono codificati nel segmento di USH. A titolo esemplificativo, il secondo elemento del segmento di USH può preferibilmente contenere il valore 2, o un qualche altro valore designato, se l'AUTACK dovesse servire come un documento verificante non-ripudio dell'origine con, ad esempio, il quinto campo avente il valore di 2, o un qualche altro valore designato, se dovesse essere richiesto un riconosci-

ODIANO & ASSOCIATI

mento. Il segmento di USX contiene preferibilmente il numero di interscambio dell'interscambio EDI in questione, concatenando così il messaggio riportato all'AUTACK, ed il segmento USR preferibilmente è un supporto di risultato di sicurezza e contiene il MD5 segnato in digitale dell'AUTACK secondo la presente invenzione.

Come è ulteriormente illustrato in figura 1 e preferito, supponendo di avere una transazione commerciale tra solamente due parti, cioè tra due parti che si sono impegnate in un accordo di soci o partner commerciali, ciascuna delle parti ha una stazione di lavoro a calcolatore convenzionale 104, 106, come ad esempio RS/6000, HP/9000 e un SOLARIS; un convenzionale traslatore o traduttore EDI 108, 110; un convenzionale elemento servitore software/hardware integrato 112, 114 che è stato programmato per operare conformemente al procedimento ed al sistema preferiti della presente invenzione e che include convenzionali terminali di visualizzazione 116, 118 per calcolatori in grado di operare in un ambiente di tipo Microsoft WINDOWS o UNIX X-WINDOWS, per visualizzare messaggi e selezioni conformemente al procedimento preferito della presente invenzione come pure messaggi e documenti trasmessi tramite EDI sulla rete INTERNET 102 nell'attuare il procedimento della presente invenzione, i servitori 112, 114 essendo atti a fornire le desiderate autentificazioni, integrità, non-ripudio di origine e ricezione, e segretezza conformemente alla presente invenzione. Come è illustrato e preferito, i servitori 112, 114 comunicano convenzionalmente sulla rete aperta, come la rete INTERNET 102, attraverso un ambiente postale eterogeneo 120, 122, come ad esempio un ambiente impiegante SMPT/MIME, X400/X435, LOTUS NOTES/cc:MAIL, e/o MICROSOFT

MEDIANO & ASSOCIATI

MAIL/EXCHANGE. I servitori 112, 114 sono preferibilmente convenzionali calcolatori o elaboratori che sono stati convenzionalmente programmati in C++, per attuare il procedimento attualmente preferito della presente invenzione e sono preferibilmente orientati a operare su una delle seguenti piattaforme UNIX: AIX, HPUX, SUN OS, o SOLARIS.

Nella seguente TABELLA A sono elencati i vari scritti che possono essere facilmente impiegati da un programmatore di ordinaria esperienza nel campo per creare la necessaria programmazione in C++, che è un linguaggio di programmazione orientato algi oggetti, per l'esecuzione sui servitori 112, 114 per attuare il procedimento attualmente preferito della presente invenzione. Come si noterà, i vari scritti o documenti originali si riferiscono alla trasmissione di un documento EDI, ritrasmissione di un documento EDI, ricezione di un documento EDI valido, ricezione di un messaggio di riconoscimento AUTACK, ricezione di una nuova chiave pubblica di un partner commerciale, distribuzione della propria nuova chiave pubblica a partner commerciali affiliati, attivazione del menù principale di gestione di certificazione, creazione della propria coppia di chiave privata/pubblica, cambiamento di un certificato (la propria coppia di chiavi pubblica/privata), rimozione della propria coppia di chiavi privata/pubblica, copiatura della propria chiave pubblica in archivi a dischi, stampa del proprio certificato della propria chiave pubblica, preservazione della propria chiave privata/pubblica in archivi a dischi, recupero della propria chiave privata/pubblica dall'archivio a dischi per sostituire la chiave privata/pubblica esistente, recupero della propria chiave privata/pubblica dall'archivio a dischi ad una chiave nuova, attivazione del

MODIANO & ASSOCIATI

menù principale di gestione della chiave pubblica dei partner commerciali, aggiunta di una chiave pubblica dei partner commerciali, cambiamento della chiave pubblica dei partner commerciali, rimozione della chiave pubblica dei partner commerciali, copiatura della chiave pubblica dei partner commerciali dall'archivio a dischi per sostituire la chiave pubblica dei partner commerciali, copiatura della chiave pubblica dei partner commerciali dall'archivio a dischi ad una chiave nuova, attivazione del menù principale di gestione degli accordi o contratti dei partner commerciali, aggiunta di contratti dei partner commerciali, cambiamento dei contratti o accordi dei partner commerciali, rimozione dei contratti o accordi dei partner commerciali, copiatura dei contratti o accordi dei partner commerciali, copiatura dei contratti o accordi dei partner commerciali nell'archivio a dischi, copiatura dei contratti o accordi dei partner commerciali dall'archivio a dischi, imballaggio MIME (convenzione dispositivo di imballaggio postale MIME), disimballaggio MIME, imballaggio PKCS (PKCS convenzionale), disimballaggio PKCS, lavoro con il record di tracciatura, monitoraggio dei compiti dei servitori, ricezione di un documento EDI non valido con un problema di integrità, ricezione di un AUTACK con un problema di integrità, ricezione di posta non supportata, ricezione di un interscambio EDI senza AUTACK mentre è atteso non-ripudio dell'origine, e ricezione di un AUTACK imprevisto.

MODIANO & ASSOCIATI

TABELLA A

SCRITTI

TRASMISSIONE DI UN DOCUMENTO EDI

Iniziatore	Azione	Partecipante
Traduttore EDI	Richiesta di trasmettere un lotto EDI	Agente autentificazione
Agente di autentificazione	Ottenimento ID trasmettitore e ricevitore	Busta interscambio EDI
Agente di autentificazione	Creazione registrazione di tracciatura	Registrazione tracciatura
Agente di autentificazione	Creazione di una voce del giornale di inizio eventi	Giornale controllo amminis.
Agente di autentificazione	Richiesta metodo di calcolo di sommario e indirizzo destinazione di partner commerciali, indirizzo di sorgente, procedimento di non ripudio ricezione (NRR), non ripudio di origine (NRO); segretezza e trasferimento	Accordo dei partner commerciali
Agente di autentificazione	Ottenimento sommario identificazioni	Interscambio EDI
Interscambio EDI	Ottenimento metodo sommario identificazioni	Configurazione
Interscambio EDI	Calcolo sommario di interscambio EDI	Calcolatore sommario
Agente di autentificazione	Verifica che il numero di controllo e del sommario di identificazione è unico	Lista tracciatura
Agente di autentificazione	Creazione AUTACK	AUTACK
AUTACK	Ottenimento ID, NRR, NRO chiave privata, controllo integrità, metodo sommario	Contratto partner commerciali
AUTACK	Ottenimento chiave privata	Elenco chiavi
AUTACK	Ottenimento sommario integrità	Interscambio EDI
AUTACK	Calcolo proprio sommario	Calcolatore sommario
AUTACK	Segnatura del sommario di AUTACK	BSAFE
Agente di autentificazione	Creazione busta AUTACK	Busta UNB
Agente di autentificazione	Criptazione interscambio EDI	PKCS
Agente di autentificazione	Combinazione interscambio EDI e AUTACK in un corpo postale codificato MIME (parziali MIME multipli)	Imballatore MIME
Agente di autentificazione	Trasmissione interscambio codificato a partner commerciale	Trasmissione posta
Agente di autentificazione	Aggiornamento registrazione tracciatura con data trasmissione e tempo trasmissione, locazione del corpo postale, ID trasmettitore e ricevitore, NRO e sommario integrità, ID chiave privata, ID chiave pubblica, sommario identificazioni	Registrazione tracciatura
Agente di autentificazione	Creazione di una voce giornale trasmissione postale	Giornale controllo amm.
Agente di autentificazione	Rinvio codice di ritorno di successo e ID registrazione tracciatura a traduttore EDI	Agente autentificazione
Monitor di ritrasmis.	Richiesta dello stato di riconoscimento	Registrazione tracciatura
Monitor di ritrasmissione	Richiesta azione di trasmissione	Contratto partner commerciali
Monitor di ritrasmis.	Richiesta ritrasmissione interscambio EDI	Agente autentificazione
Agente di autentific.	Richiesta locazione corpo postale	Registrazione tracciatura
Agente di autentific.	Trasmissione interscambio codificato a partner com.	Trasmissione posta
Agente di autentificazione	Aggiornamento registrazione tracciature con data e tempo ritrasmissione	Registrazione tracciatura
Agente di autentific.	Creazione di una voce di giornale posta ritrasmessa	Giornale controllo amm.

ASSOCIATI

RICEZIONE DI UN DOCUMENTO EDI VALIDO

Iniziatore	Azione	Partecipante
Imballatore MIME	Informazione arrivo posta	Imballatore MIME
Agente di autentificazione	Creazione voce giornale posta ricevuta con successo	Giornale controllo amm.
Agente di autentificazione	Convalidazione della posta ricevuta che conteneva un interscambio EDI	Interscambio EDI
Agente di autentificazione	Creazione registrazione tracciature	Registrazione tracciature
Agente di autentificazione	Ottenimento ID trasmettitore e ricevitore	Busta interscambio EDI
Agente di autentificazione	Ottenimento contratto partner commerciali con ID trasmettitore e ricevitore	Contratto partner commerciale
Agente di autentificazione	Ottenimento del sommario di interscambio e del sommario segnato e metodo di calcolo del sommario	AUTACK
AUTACK	Ottenimento ID chiave pubblica	Contratto partner commerciale
AUTACK	Ottenimento della chiave pubblica del partner comm.	Elenco chiavi
Elenco chiavi	Lettura della chiave pubblica efficace più recente	Elenco chiavi
AUTACK	Decriptazione del sommario segnato	BSAFE
Agente di autentificazione	Calcolo sommario dell'interscambio EDI	Interscambio EDI
Agente di autentificazione	Comparazione sommario calcolato di EDI Interscambio con il sommario nell'AUTACK Verifica del sommario dell'AUTACK parziale uguale al sommario segnato decriptato nell'AUTACK	AUTACK
Agente di autentificazione	Ottenimento sommario identificazione	Intersambio EDI
Interscambio EDI	Ottenimento metodo sommario di identificazione	Configurazione
Interscambio EDI	Calcolo sommario dell'interscambio EDI	Calcolatore sommari
Agente di autentificazione	Verifica che il numero di controllo e del sommario di identificazione è unico	Lista tracciature
Agente di autentificazione	Creazione di una voce del giornale di interscambio EDI ricevuto con successo	Giornale controllo amministrativo
Agente di autentificazione	Ottenimento del non ripudio di identificatore ricezione	Contratto partner commerciali
Agente di autentificazione	Creazione di un numero di controllo di AUTACK di ricon.	AUTACK
AUTACK	Ottenimento ID chiave privata	Contratto partner commerciale
AUTACK	Ottenimento chiave privata	Elenco chiavi
AUTACK	Segnatura sommario	BSAFE
Agente di autentificazione	Creazione di una voce del giornale di richieste di trasmissione AUTACK	Giornale controllo amm.
Agente di autentificazione	Creazione di un corpo postale codificato MIME AUTACK	Imballatore MIME
Agente di autentificazione	Trasmissione dell'AUTACK codificato a partner comm.	Trasmissione posta
Agente di autentificazione	Aggiornamento registrazione tracciature con data e tempo trasmissione AUTACK, posizione del corpo postale, ID trasmettitore e ricevitore, sommario	Registrazione tracciature
Agente di autentificazione	Creazione di una voce del giornale di AUTACK trasmesso	Giornale controllo amm.
Agente di autentificazione	Ottenimento azione post-elaborazione di instradamento verso l'interno	Contratto partner commerciali
Agente di autentificazione	Scrittura dati EDI a archivio o elenco specificato	Agente di autentificazione
Agente di autentificazione	Esecuzione comando post-elaborazione (ad esempio richiesta traduttore EDI)	Agente di autentificazione

ASSOCIAZIONE MODIANO

RICEZIONE DI UN RICONOSCIMENTO AUTACK

Iniziatore	Azione	Partecipante
Imballatore MIME	Avviso arrivo posta	Imballatore MIME
Agente di autentificazione	Ottenimento lista di parti di corpo MIME	Imballatore MIME
Agente di autentificazione	Convalida della posta ricevuta che conteneva un AUTACK	Interscambio AUTACK
Agente di autentificazione	Ottenimento ID trasmettitore ricevitore	Busta interscambio AUTACK
Agente di autentificazione	Ottenimento identificatore NRR, ID chiave pubblica	Contratto partner commerciali
Agente di autentificazione	Verifica segnatura trasmettitore	BSAFE
Agente di autentificazione	Ottenimento numero controllo interscambio e sommario integrità	AUTACK
Agente di autentificazione	Aggiornamento data e tempo riconoscimento ricevuto dell'interscambio trasmesso	Registrazione tracciature

RICEZIONE DI UNA CHIAVE PUBBLICA NUOVA DEI PARTNER COMMERCIALI

Iniziatore	Azione	Partecipante
Imballatore MIME	Avviso arrivo posta	Imballatore MIME
Agente di autentificazione	Ottenimento lista di parti di corpo MIME	Imballatore MIME
Agente di autentificazione	Convalida che la posta ricevuta conteneva un certificato	Certificato
Agente di autentificazione	Ottenimento nome distinzione, qualificatore e ID del partner commerciale	Certificato
Agente di autentificazione	Ottenimento indirizzo di posta-E di staff di gestione certificati, chiave pubblica	Elenco chiavi
Agente di autentificazione	Verifica della segnatura	BSAFE
Agente di autentificazione	Arrivo certificato giornale	Giornale cont. amm.
Agente di autentificazione	Creazione di una registrazione di tracciature con tipo certificato	Regis. tracciature
Agente di autentificazione	Informazione utente dell'arrivo del certificato	Agente autentific.
Utente	Verifica con il partner commerciale che il certificato è corretto	Utente
Utente	Selezione per aggiornamento del certificato dalla registrazione di tracciature	Utente
UI	Ottenimento del certificato	Regist. tracciature
UI	Aggiunta al certificato del nuovo numero seriale	Elenco chiavi
UI	Cambiamento della data scaduta del certificato preced.	Elenco chiavi
UI	Aggiornamento certificati giornale	Giornale cont. amm.
UI	Cambiamento dello stato della registrazione di tracciature ad aggiornato	Registrazione tracciature

DISTRIBUZIONE NUOVA PROPRIA CHIAVE PUBBLICA A PARTNER COMMERCIALI CORRELATI

Iniziatore	Azione	Partecipante
Utente	Richiesta pulsante gestione certificati	Utente
UI	Ottenimento lista coppia-chiavi/ID chiavi	Elenco chiavi
UI	Visualizzazione della lista della coppia delle chiavi sullo schermo	UI
Utente	Selezione del certificato da distribuire	Utente
Utente	Richiesta funzione di distribuzione	Utente
UI	Ottenimento lista di partner commerciali impieganti quel certificato	Contratto partner commerciali
UI	Ottenimento dell'indirizzo di posta-E del partner commer.	Partner commerciali
UI	Visualizzazione della lista degli indirizzi dei partner commerciali e di posta-E	UI
Utente	Selezione o deselezione partner commerciale	Utente
Utente	Cambiamento indirizzo posta-E	Utente
Utente	Aggiunta nuovo indirizzo posta-E	Utente
Utente	Richiesta processo di distribuzione	Utente
UI	Creazione del certificato (X.509 o PKCS?)	Elenco chiavi
UI	Codificazione del certificato in formato MIME	Imballatore MIME
UI	Trasmissione del certificato di codificazione MIME	Trasmissione posta
UI	Creazione di una voce del giornale di chiavi trasmesse	Giornale controllo amm.

MODIANO & ASSOCIATI

ATTIVAZIONE MENU' PRINCIPALE GESTIONE CERTIFICATI

Iniziatore	Azione	Partecipante
Utene	Richiesta bottone gestione certificati	Utente
UI	Ottenimento lista coppia chiavi-ID chiavi	Elenco chiavi
UI	Visualizzazione lista di coppia chiavi su schermo	UI

CREAZIONE PROPRIA COPPIA CHIAVI PRIVATA/PUBBLICA

L'utente richiede di registrare e attivare il menù principale di gestione dei certificati prima di passare a questa funzione.

Iniziatore	Azione	Partecipante
Utente	Richiesta pulsante creazione coppia chiavi	Utente
UI	Visualizzazione di uno schermo per accettare ID chiavi, data effettiva, nome distinto e indirizzo posta-E	UI
Utente	Tastierazione ID della chiave, data effettiva, nome e indirizzo posta-E	Utente
UI	Creazione coppia chiavi	Elenco chiavi
Elenco chiavi	Ottenimento lunghezza della chiave	Configurazione
Elenco chiavi	Ottenimento seme di generazione chiave	Generatore semi
Elenco chiavi	Generazione coppia di chiavi privata e pubblica	BSAFE
Elenco chiavi	Assicurazione non esistenza chiave pubblica	Base dati elenco chiavi
Elenco chiavi	Ottenimento chiave criptatura interna	Configurazione
Elenco chiavi	Criptatura chiave privata	BSAFE
Elenco chiavi	Assegnazione 1 a numero seriale	Elenco chiavi
Elenco chiavi	Scrittura coppia chiavi	Base dati
Elenco chiavi	Ritorno coppia chiavi	Elenco chiavi
UI	Aggiornamento elenco chiavi	UI

CAMBIAMENTO CERTIFICATO (PROPRIA COPPIA CHIAVI PRIVATA/PUBBLICA)

L'utente chiede di registrare e attivare il menù principale di gestione dei certificati prima di passare a questa funzione.

Iniziatore	Azione	Partecipante
Utente	Selezione di una coppia di chiavi per il cambiamento	Utente
Utente	Richiesta pulsante variazione certificato	Utente
UI	Visualizzazione di uno schermo per variare la data, il nome e l'indirizzo di posta-E effettivi	Utente
Utente	Cambiamento campi	Utente
Utente	Richiesta di creare un nuovo pulsante di chiavi	Utente
UI	Rigenerazione della coppia di chiavi	Elenco chiavi
Elenco chiavi	Assegnazione nuovo numero seriale	Elenco chiavi
Elenco chiavi	Ottenimento di un seme di generazione chiave	Generatore semi
Elenco chiavi	Ottenimento lunghezza della chiave	Configurazione
Elenco chiavi	Generazione coppia di chiavi privata e pubblica	BSAFE
Elenco chiavi	Assicurazione non esistenza della chiave pubblica	Base dati elenco chiavi
Elenco chiavi	Ottenimento chiave criptatura interna	Configurazione
Elenco chiavi	Criptatura chiave privata	BSAFE
Elenco chiavi	Scrittura nuova coppia di chiavi	Base dati elenco chiavi
Elenco chiavi	Ritorno della coppia di chiavi	Elenco chiavi
UI	Aggiornamento lista chiavi	UI

ODMAN & ASSOCIATI

RIMOZIONE PROPRIA COPPIA CHIAVI PRIVATA/PUBBLICA

L'utente richiede registrazione e attivazione menù principale gestione certificati prima di passare a questa funzione

Iniziatore	Azione	Partecipante
Utente	Selezione di una coppia di chiavi per la rimozione	Utente
Utente	Richiesta pulsante rimozione coppia chiavi	Utente
UI	Controllo se coppia chiavi è impiegata in un qualsiasi contratto di partner commerciali	Contratto partner commerciali
UI	Visualizzazione del messaggio di conferma	UI
Utente	Conferma per rimuovere la coppia di chiavi	Utente
UI	Rimozione della coppia di chiavi	Elenco chiavi
Elenco chiavi	Disattivazione della coppia di chiavi	Base dati elenco chiavi
UI	Marcatura della coppia di chiavi come disattivata sullo schermo	UI

COPIATURA PROPRIA CHIAVE PUBBLICA SU ARCHIVIO A DISCHI

L'utente richiede di registrare e attivare il menù principale di gestione dei certificati prima di passare a questa funzione.

Iniziatore	Azione	Partecipante
Utente	Selezione di una chiave	Utente
Utente	Richiesta della funzione copiatura su disco	Utente
UI	Visualizzazione di uno schermo per segnalare il nome dell'archivio di uscita	UI
Utente	Tastieratura nome archivio	Utente
UI	Visualizzazione di uno schermo di conferma di sostituzione	UI
Utente	Selezione per ricoprire l'archivio esistente	Utente
UI	Emissione in uscita del cert.in formato X.509 a archivio a dischi	Elenco chiavi
UI	Visualizzazione di un messaggio completo	UI
UI	Rivisualizzazione lista	UI

STAMPA CERTIFICATO PROPRIA CHIAVE PUBBLICA

L'utente richiede di registrare e attivare il menù principale di gestione dei certificati prima di passare a questa funzione.

Iniziatore	Azione	Partecipante
Utente	Selezione di una chiave	Utente
Utente	Richiesta funzione stampa certificati	Utente
UI	Ottenimento certificato formattato in modo umanamente leggibile	Elenco chiavi
Elenco chiavi	Formattazione dei distinti nome, chiave pubblica, data effettiva, riferimento (ID chiave), numero seriale, algoritmo di segnatura, segnatura certificati, versione, trasmettitore e indirizzo posta-E	Elenco chiavi
UI	Emissione in uscita del certif. a stampante difetti sistema	UI
UI	Rivisualizzazione della lista	UI

PRESERVAZIONE PROPRIA CHIAVE PRIVATA/PUBBLICA A ARCHIVIO A DISCHI

L'utente richiede di registrare e attivare il menù principale di gestione dei certificati prima di passare a questa funzione.

Iniziatore	Azione	Partecipante
Utente	Selezione di una chiave	Utente
Utente	Richiesta della funzione di preservazione su disco	Utente
UI	Visualizzazione di uno schermo per segnalare il nome dell'archivio di uscita	UI
Utente	Tastierazione nome dell'archivio	Utente
UI	Visualizzazione di uno schermo di conferma di sostituzione	UI
Utente	Selezione di ricopertura dell'archivio esistente	Utente
UI	Fornitura in uscita della coppia di chiavi- nome distinto, chiave privata/pubblica, data effettiva, numero seriale di riferimento (ID della chiave), algoritmo sommari, sommario, versione, trasmettitore e indirizzo posta-E ad archivio	Elenco chiavi
UI	Visualizzazione di un messaggio di completamento	UI
UI	Rivisualizzazione della lista	UI

ASSOCIATI

RECUPERO PROPRIA CHIAVE PRIVATA/PUBBLICA DA ARCHIVIO A DISCHI PER SOSTITUIRE QUELLA ESISTENTE

L'utente richiede di registrare e attivare il menù principale di gestione di certificati prima di passare a questa funzione.

Iniziatore	Azione	Partecipante
Utente	Selezione di una chiave	Utente
Utente	Richiesta della funzione di recupero da disco	Utente
UI	Visualiz. di uno schermo per segnalare il nome dell'archivio d'ingresso	UI
Utente	Tastierazione del nome dell'archivio	Utente
UI	Visualizzazione di una conferma di sostituzione e preservazione dello schermo delle coppie delle chiavi	UI
Utente	Selezione di ricopertura della chiave esistente e tastierazione del nome dell'archivio di preservazione	Utente
UI	Creazione di una voce del giornale	Giornale controllo amm.
UI	Fornitura in uscita della coppia di chiavi esistente - nome distinto, chiave privata, pubblica, data effettiva, riferimento (ID della chiave), numero seriale, algoritmo sommari, sommario, versione indirizzo trasmettitore e posta-E allo archivio di preservazione	Elenco chiavi
UI	Sostituzione della coppia di chiavi	Elenco chiavi
Elenco chiavi	Lettura della informazione delle chiavi dall'archivio	Elenco chiavi
Elenco chiavi	Aggiornamento della informazione delle chiavi	Base di dati
UI	Visualizzazione di un messaggio di completamento	UI
UI	Rivisualizzazione della lista	UI

RECUPERO PROPRIA CHIAVE PRIVATA/PUBBLICA DA ARCHIVIO A DISCHI AD UNA CHIAVE NUOVA

L'utente richiede di registrare e attivare il menù principale di gestione dei certificati prima di passare a questa funzione.

Iniziatore	Azione	Partecipante
Utente	Richiesta della funzione di recupero da disco	Utente
UI	Visualizzazione di uno schermo per segnalare il ID della chiave e il nome dell'archivio d'ingresso	UI
Utente	Tastierazione di ID della chiave e del nome d'archivio	Utente
Elenco chiavi	Lettura della informazione di chiave dall'archivio	Elenco chiavi
Elenco chiavi	Calcolo del sommario certificato	Calcolatore sommari
Elenco chiavi	Verifica d'adattamento del sommario	Elenco chiavi
Elenco chiavi	Scrittura della informazione nuova	Base dati
UI	Aggiunta della coppia di chiavi alla lista	UI
UI	Rivisualizzazione della lista	UI

CHIANO & ASSOCIATI

ATTIVAZIONE MENU' PRINCIPALE GESTIONE CHIAVI PUBBLICHE PARTNER COMMERCIALI

Iniziatore	Azione	Partecipante
Utente	Richiesta pulsante chiavi partner commerciali	Utente
UI	Ottenimento di una lista di chiavi pubbliche partner comm.	Elenco chiavi
UI	Visualizzazione della lista di chiavi pubbliche dei partner commerciali su schermo	UI

AGGIUNTA CHIAVE PUBBLICA PARTNER COMMERCIALI

L'utente richiede di registrare e attivare il menù principale di gestione certificati pubblici partner commerciali prima di passare a questa funzione.

Iniziatore	Azione	Partecipante
Utente	Richiesta pulsante aggiunta chiave pubblica partner comm.	Utente
UI	Visualizzazione schermo aggiunta chiave pubblica partner comm.	UI
Utente	Selezione di aggiungere la chiave da un archivio a dischi	Utente
UI	Visualizzazione di uno schermo per tastierare il nome dell'archivio	UI
Utente	Tastierazione nome archivio	Utente
UI	Lettura indirizzo posta-E, data effettiva, chiave pubblica, numero telefonico, indirizzo stradale	Archivio chiavi pubbliche
UI	Visualizzazione della chiave pubblica	UI
Utente	Tastierazione del nome della società del partner comm.	Utente
UI	Visualizzazione della chiave pubblica nuova nella lista sullo schermo	UI

CAMBIAMENTO CHIAVE PUBBLICA PARTNER COMMERCIALE

L'utente richiede di registrare e attivare il menù principale di gestione dei certificati pubblici del partner commerciale prima di passare a questa funzione.

Iniziatore	Azione	Partecipante
Utente	Selezione di una chiave pubblica per cambiamento	Utente
Utente	Richiesta del pulsante di cambiamento chiave pubblica	Utente
UI	Ottenimento della informazione sulla chiave pubblica	Elenco chiavi
UI	Visualizzazione chiave pubblica partner commerciale su schermo	UI
Utente	Variazione della data effettiva e della chiave pubblica	Utente
UI	Aggiornamento della chiave pubblica	Elenco chiavi
UI	Aggiunta alla chiave pubblica nuova del nuovo numero seriale	Elenco chiavi
UI	Visualizzazione della chiave pubblica nuova nella lista sullo schermo	UI

RIMOZIONE CHIAVE PUBBLICA PARTNER COMMERCIALI

L'utente richiede di registrare e attivare il menù principale di gestione dei certificati pubblici dei partner commerciali prima di passare a questa funzione.

Iniziatore	Azione	Partecipante
Utente	Selezione di una chiave pubblica per la rimozione	Utente
Utente	Richiesta del pulsante rimozione chiave pubblica	Utente
UI	Ottenimento informazione della chiave pubblica	Elenco chiavi
UI	Visualizzazione schermo aggiunta chiave pubblica partner comm.	UI
UI	Visualizzazione schermo di conferma	UI
Utente	Conferma della rimozione	Utente
UI	Disattivazione della chiave pubblica	Elenco chiavi
UI	Rimozione della chiave pubblica dalla lista sullo schermo	UI

COPIATURA CHIAVE PUBBLICA PARTNER COMMERCIALE DA ARCHIVIO A DISCHI PER SOSTITUIRE QUELLA ESISTENTE

L'utente richiede di registrare e attivare il menù principale di gestione dei certificati prima di passare a questa funzione.
Si supponga che l'archivio sia nel formato X.509.

Iniziatore	Azione	Partecipante
Utente	Selezione di una chiave pubblica	Utente
Utente	Richiesta della funzione recupero da disco	Utente
UI	Visualizzazione di uno schermo per segnalare il nome dell'archivio d'ingresso	UI
Utente	Tastierazione del nome dell'archivio	Utente
UI	Visualizzazione di una conferma di sostituzione e preservare lo schermo della coppia di chiavi	UI
Utente	Selezione di ricoprire la chiave esistente e tastierazione del nome dell'archivio di preservazione	Utente
UI	Creazione di una voce del giornale	Giornale controllo amm.
UI	Emissione in uscita della chiave esistente - nome distinto, chiave pubblica, data effettiva, riferimento (ID della chiave), numero seriale, algoritmo sommari, sommario, versione, trasmettitore e indirizzo posta-E ad archivio di preservazione	Elenco chiavi
UI	Sostituzione della chiave	Elenco chiavi
Elenco chiavi	Lettura della informazione della chiave dall'archivio	Elenco chiavi
Elenco chiavi	Aggiornamento dell'informazione della chiave	Base dati
UI	Visualizzazione di un messaggio di completamento	UI
UI	Rivisualizzazione della lista	UI

MODIANO & ASSOCIATI

COPIATURA CHIAVE PUBBLICA PARTNER COMMERCIALI DA ARCHIVIO A DISCHI A CHIAVE NUOVA

L'utente deve registrare e attivare il menù principale di gestione dei certificati prima di passare a questa funzione.

Si supponga che l'archivio sia nel formato X.509.

Iniziatore	Azione	Partecipante
Utente	Richiesta della funzione recupero da disco	Utente
UI	Visualizzazione di uno schermo per segnalare ID della chiave e il nome dell'archivio d'ingresso	UI
Utente	Tastierazione ID della chiave e nome d'archivio	Utente
Elenco chiavi	Lettura informazione della chiave dall'archivio	Elenco chiavi
Elenco chiavi	Calcolo sommario certificato	Calcolatore sommari
Elenco chiavi	Verifica adattamento sommario	Elenco chiavi
Elenco chiavi	Scrittura informazione della chiave	Base dati
UI	Aggiunta della chiave alla lista	UI
UI	Rivisualizzazione della chiave	UI

ASSOCIATI

ATTIVAZIONE MENU' PRINCIPALE GESTIONE CONTRATTI PARTNER COMMERCIALI

Iniziatore	Azione	Partecipante
Utente	Richiesta pulsante contratto partner commerciali	Utente
UI	Ottenimento di una lista dei contratti dei partner commerciali	Lista dei contratti dei partner comm.
UI	Visualizzazione della lista di contratti dei partner commerciali su schermo	UI

AGGIUNTA CONTRATTO PARTNER COMMERCIALI

L'utente deve registrare e attivare il menù principale di gestione dei partner commerciali prima di ottenere questa funzione.

Iniziatore	Azione	Partecipante
Utente	Richiesta pulsante aggiunta contratto partner comm.	Utente
UI	Visualizzazione schermo contratto partner commerciale per accettare partner commerciale locale e ID certificato; partner commerciale distante e ID certificato	UI
Utente	Richiesta aggiunta partner comm. locale nuovo	Utente
UI	Visualizzazione di uno schermo di aggiunta partner comm.	UI
Utente	Tastierazione nome, contatto, indirizzo di posta-E di contatto, telefono, fax, indirizzo, nome completo, commenti	Utente
UI	Verifica non esistenza partner commerciale	Elenco partner comm.
UI	Aggiunta del partner commerciale	Elenco partner comm.
UI	Visualizzazione del partner comm. locale sullo schermo	UI
Utente	Tastierazione tipo busta, separatori,qualificatore e ID	Utente
Utente	Richiesta aggiunta partner commerciale lontano nuovo	Utente
UI	Visualizzazione di uno schermo aggiunta partner comm.	UI
Utente	Tastierazione nome, contatto, indirizzo posta-E contatto, telefono, fax, indirizzo, nome completo, commento	Utente
UI	Verifica non esistenza partner commerciale	Elenco partner comm.
UI	Aggiunta del partner commerciale	Elenco partner comm.
UI	Visualizzazione del partner comm. distante sullo schermo	UI
Utente	Richiesta pulsante instradamento verso l'interno	Utente
UI	Visualizzazione schermo di informazione instradamento verso l'interno	UI
Utente	Tastierazione informazione verso l'interno-stato; sicurezza-NRO, NRR e confidenziale; archiviazione per ricevere dati EDI: comando di elaborazione dopo ricezione	Utente
UI	Verifica informazione di instradamento verso l'interno	Instradamento verso l'interno
UI	Aggiunta instradamento verso l'interno	Instradamento verso l'interno
Utente	Richiesta pulsante di instradamento in uscita	Utente
UI	Visualizzazione schermo di informazione instradamento in uscita	UI
Utente	Tastierazione informazione di trasporto - ricevitore MIME e indirizzo posta-E trasmettitore, dimensioni messaggio massime, gruppo caratteri	Utente
Utente	Tastierazione sicurezza-NRO, NRR confidenziale	Utente
Utente	Tastierazione intervallo di ritrasmissione e azione	Utente
UI	Verifica informazione di instradamento in uscita	Instrad. in uscita
UI	Aggiunta instradamento in uscita	Instrad. in uscita
UI	Rivisualizzazione dello schermo principale dei contratti dei partner commerciali	UI

Utente	Selezione per preservare il contratto dei partner commerciali	Utente
UI	Aggiunta del contratto dei partner commerciali	Lista contratti partner commerciali

CAMBIAMENTO CONTRATTO PARTNER COMMERCIALI

L'utente deve registrare e attivare il menù principale di gestione dei partner commerciali prima di passare a questa funzione.

Iniziatore	Azione	Partecipante
Utente	Selezione contratto partner commerciale per cambiamento	Utente
Utente	Richiesta pulsante cambiamento contratto partner commerciali	Utente
UI	Ottenimento contratto partner commerciali selezionato	Lista dei contratti dei partner commerciali
UI	Ottenimento informazione - partner commerciale locale e distante, informazione entrante e uscente	Contratto dei partner commerciali
UI	Visualizzazione informazione contratto partner commerciali su schermo e non ammissione cambiamento partner commerciale locale e distante	UI
Utente	Richiesta di cambiamento della informazione del partner commerciale locale	Utente
UI	Ottenimento informazione relativa al partner commerciale locale	Partner commerciale
UI	Visualizzazione della informazione del partner comm. su schermo	UI
Utente	Cambiamento indirizzo posta-E del partner commerciale	Utente
UI	Aggiornamento partner commerciale	Partner commerciale
UI	Visualizzazione dello schermo dei contratti dei partner comm.	UI
Utente	Selezione di cambiamento del partner commerciale distante	UI
UI	Ottenimento informazione relativa al partner comm. distante	Partner commerciale
UI	Visualizzazione della informazione del partner comm. su schermo	UI
UI	Visualizzazione dello schermo contratti dei partner comm.	UI
Utente	Cambiamento dell'indirizzo del partner commerciale	Utente
UI	Aggiornamento del partner commerciale	Partner commerciale
UI	Visualizzazione dello schermo contratti del partner commerciale	UI
Utente	Cambiamento della informazione di instradamento entrante e uscente	Utente
Utente	Selezione di aggiornare il contratto dei partner commerciali	Utente
UI	Aggiornamento del contratto del partner commerciale	Lista dei partner comm.

RIMOZIONE DEL CONTRATTO DEI PARTNER COMMERCIALI

L'utente deve registrare e attivare il menù principale di gestione dei partner commerciali prima di passare a questa funzione.

Iniziatore	Azione	Partecipante
Utente	Selezione di un contratto di partner comm. per la rimozione	Utente
Utente	Richiesta del pulsante di rimozione del contratto del partner commerciale	Utente
UI	Ottenimento del contratto del partner commerciale selezionato	Lista dei contratti dei partner commerciali
UI	Ottenimento informazione - partner commerciale locale e distante	Lista dei contratti dei partner commerciali
UI	Visualizzazione informazione di contratto partner commerciale su schermo	UI
UI	Visualizzazione dello schermo di conferma	UI
Utente	Conferma rimozione	Utente
UI	Rimozione contratto partner commerciale	Lista dei contratti dei partner commerciali
UI	Rimozione contratto dalla lista sullo schermo	UI
UI	Rivisualizzazione della nuova lista sullo schermo	UI

COPIATURA CONTRATTO PARTNER COMMERCIALI SU ARCHIVIO A DISCHI

L'utente deve registrare e attivare il menù principale di contratti dei partner commerciali prima di passare a questa funzione

Iniziatore	Azione	Partecipante
Utente	Selezione di un contratto di partner commerciali	Utente
Utente	Richiestadella funzione di copiatura su disco	Utente
UI	Visualizzazione di uno schermo per segnalare il nome dell'archivio di uscita	UI
Utente	Tastierazione nome dell'archivio	Utente
UI	Visualizzazione di uno schermo di conferma di sostituzione	UI
Utente	Selezione di ricoprire l'archivio esistente	Utente
UI	Emissione in uscita del contratto del partner commerciali ad archivio come un archivio piano	Contratto dei partner commerciali
UI	Visualizzazione di un messaggio di completamento	UI
UI	Rivisualizzazione della lista	UI
Utente	Richiesta funzione copiatura da disco	Utente
UI	Visualizzazione di uno schermo per segnalare il nome dell'archivio d'ingresso	UI
Utente	Tastierazione nome d'archivio	Utente
UI	Visualizzazione di uno schermo di conferma di sostituzione	UI
Utente	Selezione di sovrascrivere il contratto dei partner commerciali esistente	Utente
UI	Sostituzione del contratto dei partner commerciali	Contratto dei partner commerciali
Contratto di partner commerciali	Lettura della informazione dei contratti dei partner commerciali dall'archivio	Contratto dei partner commerciali
Contratto di partner commerciali	Aggiornamento della informazione dei contratti dei partner commerciali	Base di dati
UI	Visualizzazione di un messaggio di completamento	UI
UI	Rivisualizzazione della lista	UI

MODIANO & ASSOCIATI

IMBALLAGGIO MIME

Iniziatore	Azione	Partecipante
Agente di autentificazione	Creazione di un oggetto MIME con interscambio EDI, AUTACK, contratto partner commerciali	Imballatore MIME
Imballatore MIME	Ottenimento qualificatore e ID del trasmettitore e del ricev.	Interscambio EDI
Imballatore MIME	Ottenimento da e a indirizzo posta-E di dimensioni parziali MIME massime	Contratto partner commerciali
Imballatore MIME	Ottenimento di sicurezza - metodo di criptatura partner commerciali (ad esempio DES o RC4), ID chiave pubblica partner commerciali, identificatore di confidenzialità	Contratto partner commerciali
Imballatore MIME	Imbustare interscambio EDI in busta PKCS	Imbustatore PKCS
Imballatore MIME	Creazione parte di corpo EDI per interscambio PKCS e EDI	Parte di corpo MIME
Imballatore MIME	Creazione parte di corpo AUTACK	Parte di corpo MIME
Imballatore MIME	Creazione titolo MIME a e da indirizzo posta-E	Titolo MIME
Imballatore MIME	Creazione parziali MIME da titolo MIME e parti di corpo	Messaggio MIME
Imballatore MIME	Ritorno del messaggio MIME a agente autentificazione	Imballatore MIME

DISIMBALLAGGIO MIME

Iniziatore	Azione	Partecipante
Trasmiss. posta	Creazione caso parziale MIME	Imballatore MIME
Imballatore MIME	Registrazione arrivo parziale	Giornale controllo amm.
Imballatore MIME	Assemblaggio parziali	Imballatore MIME
Imballatore MIME	Registrazione di tutti i parziali ricevuti	Giornale controllo amm.
Imballatore MIME	Disimballaggio parte di corpo imballata	Disimbustatore PKCS
Imballatore MIME	Informazione arrivo posta agente autentificazione	Imballatore MIME
Agente autentif.	Ottenimento da e a indirizzo posta-E	Imballatore MIME
Imballatore MIME	Ottenimento sicurezza TP	Contratto partner commerciali
Agente autentif.	Ottenimento lista parti di corpo	Messaggio MIME
Agente autentif.	Ottenimento parte di corpo AUTACK	Messaggio MIME
Agente autentif.	Ottenimento interscambio EDI	Messaggio MIME
Agente autentif.	Continuazione con altra elaborazione	Agente autentificazione

MODIANO & ASSOCIATI

IMBALLAGGIO PKCS

Iniziatore	Azione	Partecipante
Imballatore MIME	Creazione di un interscambio EDI imballato	Imballatore PKCS
Imballatore PKCS	Ottenimento qualificatore e ID trasmettitore e ricevitore	Interscambiatore EDI
Imballatore PKCS	Ottenimento ID chiave pubblica partner commerciali e metodo di criptatura (ad esempio DES o RC4)	Contratto partner commerciali
Imballatore PKCS	Ottenimento chiave pubblica partner commerciale	Elenco chiavi
Imballatore PKCS	Ottenimento chiave DES casuale	Criptatore DES
Imballatore PKCS	Criptatura interscambio EDI	Criptatore DES
Imballatore PKCS	Criptatura chiave DES	BSAFE
Imballatore PKCS	Creazione parte di corpo MIME imballata con la chiave DES criptata e interscambio EDI	Parte di corpo MIME
Imballatore PKCS	Ritorno interscambio EDI imballato	Imballatore PKCS

DISIMBALLAGGIO PKCS

Iniziatore	Azione	Partecipante
Imballatore MIME	Svolgimento di una parte di corpo imballata	Imballatore PKCS
Imballatore PKCS	Ottenimento ID chiave pubblica partner commerciale	Contratto partner commerciali
Imballatore PKCS	Ottenimento chiave pubblica partner commerciale	Elenco chiavi
Imballatore PKCS	Adattamento del certificato nella busta al certificato nell'elenco chiavi	Chiave pubblica partner commerciale
Imballatore PKCS	Ottenimento interscambiatore EDI imballato	Parte di corpo imballata
Imballatore PKCS	Decriptatura chiave DES	BSAFE
Imballatore PKCS	Decriptatura interscambio EDI criptato	Criptatore DES
Imballatore PKCS	Rinvio interscmabiatore EDI a imballatore MIME	Imballatore PKCS

ASSOCIATI & MOLINO

LAVORO CON REGISTRAZIONE TRACCIATURE

Iniziatore	Azione	Partecipante
Utente	Richiesta funzione lavoro con registrazione tracciature	Utente
UI	Segnalazione criteri di selezione, intervallo di date, trasmettitore/ricevitore, ID registrazione tracciatura, stato, tipo di dati, numero di controllo di interscambio (tipo di dati, sensibile e solo applicazione a dati EDI)	UI
Utente	Tastierazione criteri, ad esempio intervallo date	Utente
UI	Ottenimento di una lista di registrazione di tracciatura che rientrano entro l'intervallo di date specificato	Registrazione tracciature
Reg. tracciature	Richiesta base dati	Base dati
UI	Visualizzazione di una lista di registrazione tracciatura	UI
Utente	Richiesta dettaglio visione di un lotto EDI	Utente
UI	Ottenimento dettaglio	Reg. tracciature
UI	Visualizzazione del dettaglio del lotto EDI	UI
Utente	Richiesta della ritrasmissione di un interscambio	Utente
UI	Ritrasmissione dell'interscambio	Agente di autentific.
UI	Rivisualizzazione al dettaglio	UI
Utente	Chiusura	Utente
UI	Rivisualizzazione della lista della registrazione di tracciature	UI
Utente	Selezione di ritrasmettere un lotto EDI	Utente
UI	Ritrasmissione del lotto	Agente di autentific.
UI	Rivisualizzazione della lista di registrazioni di tracciatura	UI
Utente	Rielaborazione di un lotto uscente	Utente
UI	Rielaborazione di un lotto uscente (iniziando dal principio)	Agente di autentificazione
UI	Rivisualizzazione della lista della registrazione di tracciatura	UI
Utente	Rielaborazione di un lotto entrante	Utente
UI	Rielaborazione di un lotto entrante (inizio dal principio)	Agente di autentific.
UI	Rivisualizzazione della lista della registrazione di tracciature	UI
Utente	Continuazione dall'ultima azione	Utente
UI	Continuazione dall'ultima azione	Agente di autentific.
Agente autentif.	Ottenimento stato	Reg. tracciature
Agente autentif.	Continuazione elaborazione conformemente allo stato	Agente di autentific.
UI	Rivisualizzazione della lista della registrazione di tracciature	UI
Utente	Ripetizione ultima azione di un lotto entrante di successo cioè ritraduzione	utente
UI	Ripetizione ultima azione	Agente di autentific.
Agente autentif.	Ottenimento stato	Reg. tracciature
Agente autentif.	Ripetizione ultima azione	Agente di autentific.
UI	Rivisualizzazione della lista della registrazione di tracciature	UI
Utente	Selezione di stampare un gruppo di registrazioni di tracciatura	Utente
UI	Ottenimento informazione sommari registrazioni tracciatura	Reg. tracciature
UI	Formattazione rapporto	UI
UI	Stampa rapporto	Stampante
UI	Rivisualizzazione della lista della registrazione delle tracciature	UI
Utente	Rilascio di un mantenimento lotto EDI	Utente
UI	Cambiamento dello stato della registrazione delle tracc. a rilascio	Reg. tracciature

& ASSOCIATI MODIANO

UI	Elaborazione del lotto EDI	Agente autentificazione
UI	Rivisualizzazione della lista di registrazioni di tracciatura	UI
Utente	Selezione di visualizzare il contenuto di una posta ricevuta	Utente
UI	Ottenimento contenuto posta	Reg. tracciature
Reg. tracciature	Ottenimento contenuto posta	Archivio postale
UI	Visualizzazione posta	UI
Utente	Chiusura	Utente
UI	Rivisualizzazione della lista di registrazioni di tracciatura	UI

MONITORAGGIO COMPITI SERVITORI

Iniziatore	Azione	Partecipante
utente	Richiesta funzione lavoro con monitoraggio compiti servitori	Utente
UI	Ottenimento informazione compiti dei servitori	Sistema operativo sul servitore
UI	Visualizzazione del nome, stato dei compiti dei servitori	UI
Utente	Selezione di rinfrescare lo stato	Utente
UI	Ottenimento di informazione dei compiti dei servitori	Sistema operativo sul servitore
UI	Visualizzazione del nome, stato dei compiti dei servitori	UI
Utente	Selezione di avviare un compito di servitore, ad es. guardiano	Utente
UI	Avviamento del compito del servitore	Conf. dei compiti
Configurazione dei compiti	Avviamento del compito	Sistema operativo sul servitore
UI	Ottenimento informazione sui compiti dei servitori	Sistema operativo sul servitore
UI	Visualizzazione del nome, stato dei compiti dei servitori	UI

ONAIDO & ASSOCIATI

RICEZIONE DI UN DOCUMENTO EDI NON VALIDO CON PROBLEMA DI INTEGRITA'

Si supponga che l'inizio dello scritto sia il medesimo della ricezione di un documento EDI valido. Dopo verifica del sommario dell'AUTACK parziale uguale al sommario segnato decriptato nell'AUTACK, l'agente di autentificazione trova che il sommario nell'AUTACK non si adatta al sommario dell'interscambio EDI.

Iniziatore	Azione	Partecipante
Agente di autentificazione	Creazione di una registrazione di errori di integrità di interscambio con informazione seguente: sommario in AUTACK, sommario dell'interscambio EDI, numero di controllo AUTACK, numero di controllo di interscambio, nome dei partner commerciali, ID di registrazione di tracciature	Giornale di controllo amministrativo
Agente di autentificazione	Aggiornamento dello stato della registrazione di tracciature a errore di integrità di interscambio	Registrazione di tracciature
Agente di autentificazione	Ottenimento indirizzo posta-E locale	Contratto dei partner commerciali
Agente di autentificazione	Formattazione di una posta-E di errori di integrità di interscambio con informazione seguente: stampa di tempo, sommario in AUTACK, sommario dell'interscambio EDI, numero di controllo AUTACK, numero di controllo di interscambio, nome del partner commerciale, ID di registrazione tracciature	Agente di autentificazione
Agente di auten.	Trasmissione posta-E	Trasmissione posta
Agente di auten.	Ottenimento data e tempo di creazione di interscambio EDI	Interscambio EDI
Agente di autentificazione	Formattazione di un AUTACK negativo - il sommario nell'AUTACK ricevuto	AUTACK
Agente di auten.	Creazione di un interscambio AUTACK	Interscambio AUTACK
Agente di auten.	Codificazione dell'AUTACK negativo in formato MIME	Imballatore MIME
Agente di autentificazione	Trasmissione dell'AUTACK negativo codificato a partner commerciale	Trasmissione posta
	Aggiornamento dello stato della registrazione di tracciature a errore di integrità di interscambio con AUTACK negativo trasmesso	Registrazione di tracciature
	Registrazione dell'evento di AUTACK negativo trasmesso	Giornale controllo amm.

ASSOCIATI

RICEZIONE DI UN AUTACK CON PROBLEMA DI INTEGRITA'

Si supponga che l'inizio dello scritto sia il medesimo di quello della ricezione di un documento EDI valido. L'agente di autentificazione trova che il sommario dell'AUTACK parziale non è uguale a quello del sommario del segnale decriptato nell'AUTACK

Iniziatore	Azione	Partecipante
Agente di autentificazione	Creazione di una registrazione di errori di integrità AUTACK con l'informazione seguente: sommario segnato dell'AUTACK parziale in AUTACK, sommario segnato decriptato dell'AUTACK parziale in AUTACK, sommario calcolato dell'AUTACK parziale, numero di controllo AUTACK, nome dei partner commerciali, tasto pubblico dei partner commerciali, ID di registrazione di tracciature	Giornale di controllo amministrativo
Agente di autentificazione	Aggiornamento dello stato della registrazione delle tracciature a errore di integrità AUTACK	Registrazione di tracciature
Agente di autentificazione	Ottenimento di un indirizzo di posta-E locale	Contratto dei partner commerciali
Agente di autentificazione	Formattazione di una posta-E di errori di integrità AUTACK con l'informazione seguente: stampa di tempo, sommario segnato dell'AUTACK parziale in AUTACK, sommario segnato decriptato dell'AUTACK parziale in AUTACK, sommario calcolato dell'AUTACK parziale, numero di controllo AUTACK, nome del partner commerciale, chiave pubblica del partner commerciale, ID di registrazione di tracciature	Agente di autentificazione
Agente di autentificazione	Trasmissione della posta-E	Trasmissione posta

RICEZIONE DI POSTA NON SUPPORTATA

Si supponga che l'inizio dello scritto sia uguale a quello della ricezione di un documento EDI valido. L'agente di autentificazione trova che la posta non è un documento EDI, non è un AUTACK e non è un certificato.

Iniziatore	Azione	Partecipante
Agente di autentificazione	Scaricare la posta non supportata in un archivio	Archivio di scarico
Scarico archivio	Ottenere l'elenco degli archivi di scarico	Configurazione
Scarico archivio	Generazione di un nome d'archivio di scarico unico	Archivio di scarico
Scarico archivio	Fornitura in uscita della posta non supportata all'archivio di scarico	Archivio di scarico
Agente di autentificazione	Creazione di una registrazione di errori di posta non supportata ricevuta con informazione seguente: indirizzo posta-E del trasmettitore e ricevitore, soggetto, ID dei messaggi della posta-E, nome dell'archivio di scarico	Giornale controllo amministrativo
Agente di autentificazione	Aggiornamento dello stato della registrazione delle tracciature a posta non supportata ricevuta, preservazione del nome dell'archivio di scarico	Errore di tracciatura
Agente di autentificazione	Ottenimento dell'indirizzo della posta-E	Contratto partner commerciali
Agente di autentificazione	Formattazione di una posta-E di errori di posta non supportata ricevuta con informazione seguente: indirizzo della posta-E del trasmettitore e del ricevitore, soggetto, ID messaggi della posta-E, nome dell'archivio di scarico	Agente di autentificazione
Agente di autentificazione	Trasmissione della posta-E	Trasmissione posta

MODIANO & ASSOCIATI

RICEZIONE DI UN INTERSCAMBIO EDI SENZA AUTACK MENTRE E' ATTESO NON RIPUDIO DELL'ORIGINE

Si supponga che l'inizio dello scritto sia uguale a quello della ricezione di un documento EDI valido. L'agente di autentificazione trova che non vi è AUTACK nella posta.

Iniziatore	Azione	Partecipante
Agente di autentificazione	Scarico dell'interscambio EDI in un archivio	Archivio di scarico
Scarico archivio	Ottenimento dell'elenco degli archivi di scarico	Configurazione
Scarico archivio	Generazione di un nome d'archivio di scarico unico	Archivio di scarico
Scarico archivio	Emissione in uscita dell'interscambio EDI all'arch. di scarico	Archivio di scarico
Agente di autentificazione	Creazione di una registrazione di errori di AUTACK non ricevuto con informazione seguente: stampa di tempo, interscambio, numero di controllo, nome del partner commerciale, ID di registrazione di tracciature, nome dello archivio di scarico	Giornale di controllo amministrativo
Agente di autentificazione	Aggiornamento dello stato della registrazione di tracciatura a AUTACK non ricevuto, preservazione del nome dell'archivio di scarico	Registrazione di tracciatura
Agente di autentificazione	Ottenimento indirizzo posta-E locale	Contratto dei partner commerciali
Agente di autentificazione	Formattazione di una posta-E di errori di AUTACK non ricevuto con l'informazione seguente: stampa di tempo, numero di controllo di interscambio, nome del partner commerciale, ID di registrazione di tracciature, nome dell'archivio di scarico	Agente di autenficazione
Agente di autentificazione	Trasmissione della posta-E	Trasmissione posta

RICEZIONE DI UN AUTACK IMPREVISTO

Si supponga che l'inizio dello scritto sia il medesimo di quello della ricezione di un documento EDI valido. L'agente di autentificazione trova che vi è un AUTACK nella posta ma il contratto del partner commerciale non specifica alcun non ripudio di origine

Iniziatore	Azione	Partecipante
Agente di autentif.	Scaricamento interscambio EDI in un archivio	Archivio di scarico
Scarico archivio	Ottenimento elenco degli archivi di scarico	Configurazione
Scarico archivio	Generazione di un nome di archivio di scarico unico	Archivio di scarico
Scarico archivo	Emissione in uscita di EDI all'archivio di scarico	Archivio di scarico
Agente di autentif.	Scaricamento interscambio AUTACK in un archivio	Archivo di scarico
Scarico archivio	Ottenimento elenco degli archivi di scarico	Configurazione
Scarico archivio	Generazione di un nome di archivio di scarico unico	Archivio di scarico
Scarico archivio	Emissione in uscita dell'AUTACK all'archivio di scarico	Archivio di scarico
Agente di autentificazione	Creazione di una registrazione di errori AUTACK imprevisti con l'informazione seguente: stampa di tempo, numero di controllo interscambi, nome del partner commerciale, ID della registrazione delle tracciature, nomi degli archivi di scarico	Giornale del controllo amministrativo
Agente di autentificazione	Aggiornamento dello stato della registrazione di tracciature a AUTACK imprevisto, preservazione dei nomi degli archivi di scarico	Registrazione delle tracciature
Agente di autentificazione	Ottenimento di un indirizzo di posta-E locale	Contratto dei partner commerciali
Agente di autentificazione	Formattazione di una posta-E di errori AUTACK imprevisti con l'informazione seguente: stampa di tempo, numero di controllo d'interscambi, nome dei partner commerciali, ID di registrazione di tracciature, nomi degli archivi di scarico	Agente di autentificazione
Agente di autentif.	Trasmissione della posta-E	Trasmissione posta

JACOBACCI & PERANI S.p.A.

Le figure 14-41 illustrano le varie visualizzazioni di schermo in un ambiente di tipo WINDOWS convenzionale, che sono suscettibili di essere preferibilmente fornite sui tipici schermi 116, 118 di calcolatori associati con i servitori 112, 114 nell'attuare il procedimento precedente sotto il controllo del programma che è basato sugli scritti della TABELLA A. A tale proposito, la figura 14 illustra la visualizzazione di schermo complessiva che è presentata alle parti sulla rete che sono eleggibili per partecipare in transazioni commerciali EDI da pari a pari, da calcolatore a calcolatore, attraverso la rete INTERNET. Come è illustrato a titolo esemplificativo in figura 14, all'utente può essere fornita, a titolo esemplificativo, la scelta di selezionare finestre per TRADING PARTNER PROFILES, TRADING PARTNER AGREEMENTS, KEY MANAGEMENT, e TRACKING (PROFILI DEL PARTNER COMMERCIALI, CONTRATTI O ACCORDI TRA I PARTNER COMMERCIALI, GESTIONE DELLE CHIAVI e TRACCIATURA) nel convenzionale ambiente WINDOWS che è preferibilmente impiegato.

Le figure 15-21 illustrano varie visualizzazioni di schermi di calcolatori che possono essere presentati all'utente dopo selezione della finestra TRADING PARTNER PROFILES nella visualizzazione di schermo di figura 14. La figura 15 rappresenta uno scenario di tre possibili partner commerciali identificati da CISCO, SEARS e ME, in cui ME rappresenta l'utente stesso. La figura 16 illustra un possibile blocco di dialogo per creare il profilo dei partner commerciali direttamente sullo schermo di calcolatore o videata 116, 118. Analogamente, la figura 17 illustra un possibile blocco di dialogo per creare informazione di contatto per il partner commerciali direttamente sullo schermo 116, 118 di calcolatore. La figura 18 illustra

MODIANO & ASSOCIATI

un possibile blocco di dialogo per creare informazione di qualificazione EDI direttamente sullo schermo 116, 118 di calcolatore. La figura 19 illustra un possibile blocco di dialogo per chiavi di vincolo di partner commerciali che sono visualizzati e possono essere cambiate direttamente sullo schermo 116, 118 di calcolatore, essendo illustrate due opzioni cioè BIND o LEGATO e UNBIND o NON LEGATO. La figura 20 illustra la visualizzazione 116, 118 di schermo di calcolatore quando è stata selezionata l'opzione BIND KEYS nella visualizzazione di figura 19 al fine di legare o vincolare una chiave particolare ad un partner commerciale particolare. La figura 21 illustra la visualizzazione 116, 118 di schermo di calcolatore per KEY ADDENDUM ad esempio per visualizzare un certificato formattato che può essere legato o vincolato al partner commerciale assieme alla chiave.

Le figure 22-28 illustrano varie visualizzazioni di schermo di calcolatore che possono essere presentate all'utente dopo selezionare della finestra TRADING PARTNER AGREEMENTS o di contratti-accordi tra partner commerciali nella visualizzazione dello schermo di figura 14. La figura 22 rappresenta uno scenario dei medesimi tre partner commerciali identificati in figura 15. La figura 23 illustra un blocco di dialogo per creare, nell'esempio precedente, un accordo tra partner commerciali tra il ME d'utente, che è l'ID locale, e SEARS, che è l'ID distante, direttamente sullo schermo di calcolatore 116, 118. La figura 24 illustra un blocco di dialogo per creare le istruzioni di inbound routing o instradamento verso l'interno per il contratto o accordo dei partner commerciali direttamente sullo schermo di calcolatore 116, 118. Analogamente, le figure 25-27 illustrano vari blocchi di dialogo per creare le istruzioni di outbound routing o in-

stradamento in uscita per il contratto o accordo dei partner commerciali direttamente sullo schermo di calcolatore 116, 118. La figura 28 illustra un blocco di dialogo per selezionare le ritrasmissione outbound o in uscita direttamente sullo schermo di calcolatore 116, 118.

Le figure 29-33 illustrano varie visualizzazioni di schermo di calcolatore che possono presentarsi all'utente dopo aver selezionato la finestra KEY MANAGEMENT o di GESTIONE DELLE CHIAVI nella visualizzazione di schermo di figura 14. La figura 29 rappresenta nuovamente uno scenario dei medesimi tre partner commerciali presentati in figura 15. La figura 30 illustra un possibile blocco di dialogo associato con l'ID della chiave locale, la figura 31 illustra un possibile blocco di dialogo associato con l'ID della chiave distante, la figura 32 illustra un possibile blocco di dialogo associato con i dettagli della chiave, e la figura 33 illustra un possibile blocco di dialogo associato con l'esporto della chiave pubblica ad un altro archivio.

Le figure 34-41 illustrano varie visualizzazioni di schermi di calcolatori che possono presentarsi all'utente dopo selezione della finestra TRACKING o DI TRACCIATURA nella visualizzazione di schermo di figura 14. La figura 34 illustra una visualizzazione di schermo sullo schermo 116, 118 del calcolatore in cui sono stati trasmessi due messaggi EDI, uno tra SEARS e CISCO, e uno tra ME e THEM a titolo esemplificativo. La figura 35 illustra una possibile visualizzazione sullo schermo di calcolatore 116, 118 degli interscambi tra i partner commerciali e mostra il non-ripudio del messaggio AUTACK di ricezione, illustrando lo stato di AUTACK sullo schermo di calcolatore 116, 118 secondo la presente invenzione. La figura 36 illustra una possibile visualizzazione sullo schermo di calcolatore 116, 118

MODIANO & ASSOCIATI

dei dati EDI dopo che è stato selezionato il blocco di dialogo VIEW EDI DATA o VISIONE DATI EDI nella visualizzazione di schermo di figura 35. Le figure 37-38 illustrano possibili visualizzazioni di schermo sullo schermo 116, 118 del calcolatore per selezionare criteri di tracciatura. La figura 39 illustra una possibile visualizzazione di schermo sullo schermo 116, 118 del calcolatore di un "giornale" o log di controllo amministrativo o di audit, le figure 40-41 illustrando possibili visualizzazioni di schermo sullo schermo 116, 118 di calcolatore per selezionare criteri di selezione degli audit-log.

Facendo ora riferimento alla figura 2, sarà ora descritto il procedimento preferito per l'autentificazione e il non-ripudio dell'origine secondo il procedimento attualmente preferito della presente invenzione. Come è illustrato in figura 2 e come è preferito, il blocco 200 rappresenta un tipico interscambio EDI secondo la presente invenzione. Il blocco 202 rappresenta l'azione preferita del servitore in corrispondenza della estremità trasmettitore rispetto a questo interscambio EDI conformemente al procedimento della presente invenzione. Come è illustrato e preferito, il servitore del trasmettitore calcola preferibilmente l'MD5 per l'intero interscambio EDI, come ad esempio da ISA all'ultimo carattere di IEA (chiamato MD5EDIINTERCHANGE). Questo valore è quindi preferibilmente inserito in una posizione predeterminata nel messaggio AUTACK, come lo è preferibilmente il secondo elemento del segmento USY nel messaggio AUTACK. Il servitore del trasmettitore calcola quindi preferibilmente l'MD5 del messaggio AUTACK, ad esempio preferibilmente dal primo carattere di USH al primo carattere di UST. Il servitore del trasmettitore segna quindi preferibilmente il messag-

MODIANO & ASSOCIATI

gio AUTACK criptografando o criptando l'MD5 con la chiave privata del trasmettitore. Questo valore calcolato è quindi preferibilmente inserito in una locazione predeterminata nel messaggio AUTACK, preferibilmente come il primo elemento del segmento USR nel messaggio AUTACK. Il blocco 204 rappresenta un tipico messaggio AUTACK secondo il procedimento preferito della presente invenzione, dopo che il servitore del trasmettitore ha preso l'azione illustrata nel blocco 202. L'AUTACK 204 è quindi preferibilmente trasmesso al servitore del ricevitore ove hanno preferibilmente luogo l'azione e la verifica del ricevitore illustrate nel blocco 206. Se l'interscambio è criptato, allora il servitore o calcolatore del ricevitore lo decripta preferibilmente e calcola l'MD5 dell'interscambio EDI ricevuto. Supponendo che sia desiderato o richiesto non-ripudio dell'origine, allora il servitore del ricevitore, impiegando la chiave pubblica del trasmettitore, preferibilmente, decripta il contenuto del primo elemento del segmento di USR nel messaggio AUTACK 204, che è la locazione ove il servitore del trasmettitore ha inserito l'MD5 del messaggio AUTACK. Il valore così ottenuto mediante la decriptatura o decriptografazione è l'MD5 del messaggio AUTACK nell'esempio precedente, dal primo carattere di USH al primo carattere di UST. Il servitore del ricevitore calcola quindi preferibilmente l'MD5 del messaggio AUTACK e comparare l'MD5 calcolato con il valore dell'MD5 ottenuto mediante decriptatura del contenuto del primo elemento del segmento USR nel messaggio AUTACK. Se entrambi i valori di MD5 sono uguali, allora il servitore del ricevitore conosce che l'integrità del messaggio AUTACK è preservata ed è stabilito non-ripudio dell'origine. Il servitore del ricevitore compara quindi preferibilmente l'MD5 dell'interscambio EDI

ASSOCIATI MODIANO

con l'MD5 nel segmento USY del messaggio AUTACK, che è la locazione ove il servitore del trasmettitore ha inserito l'MD5 dell'interscambio EDI e, se i due valori di MD5 sono uguali, allora il servitore del ricevitore conosce che l'integrità dell'interscambio EDI è preservata, l'autenticità è verificata, ed è stabilito non-ripudio dell'origine.

Facendo ora riferimento alla figura 3, sarà ora descritto il processo preferito di non-ripudio di ricezione secondo il procedimento attualmente preferito della presente invenzione. Come è rappresentato nel blocco 208 e come è preferito, l'azione del servitore del ricevitore nel verificare l'integrità e l'autenticità dell'interscambio EDI ricevuto è preferibilmente come è stato descritto precedentemente con riferimento al blocco 206 di figura 2. Successivamente, il servitore del ricevitore crea preferibilmente un nuovo AUTACK, come ad esempio il messaggio AUTACK rappresentato dal blocco 210, e trasmette il nuovo AUTACK 210 al servitore del trasmettitore per la verifica da parte del servitore del trasmettitore originale, come è rappresentato mediante il blocco 212. Come è illustrato in figura 3, e come è preferito, nel creare il nuovo AUTACK, il servitore del ricevitore popola preferibilmente tutti i segmenti ed elementi come è appropriato, ad esempio tutti i segmenti e tutti gli elementi sino a ed incluso UST. Il servitore del ricevitore calcola quindi preferibilmente l'MD5 del nuovo AUTACK, come ad esempio da USH al primo carattere di UST, e segna l'MD5 calcolato con la chiave privata del ricevitore. Il servitore del ricevitore inserisce quindi preferibilmente l'MD5 segnato in modo digitale in una locazione predeterminata nel nuovo AUTACK, come ad esempio il primo elemento del segmento USR. Il servitore del ricevitore popola quindi preferibilmente i segmenti UNT e

ASSOCIAZIONE TRADIZIONALE

UNZ del nuovo AUTACK, come appropriato, e trasmette il nuovo AUTACK preparato al servitore del trasmettitore originale. Il servitore del trasmettitore originale verifica quindi preferibilmente la segnatura digitale del nuovo AUTACK ricevuto mediante decriptatura di esso con la chiave pubblica del ricevitore, il valore ottenuto mediante tale decriptatura essendo l'MD5 del nuovo AUTACK ricevuto. Il servitore del trasmettitore originale calcola quindi l'MD5 del nuovo AUTACK ricevuto e lo compara rispetto al valore dell'MD5 ottenuto dal processo di decriptatura. Se i due valori di MD5 sono i medesimi, allora il servitore del trasmettitore originale conosce che l'integrità del nuovo AUTACK è preservata ed è stabilito non-ripudio dell'origine del nuovo AUTACK. Il servitore del trasmettitore originale conosce pure che se l'MD5 contenuto nel segmento di USY del nuovo AUTACK ricevuto nell'esempio precedente è uguale all'MD5 dell'interscambio EDI precedentemente trasmesso ed il riconoscimento è positivo (come preferibilmente ottenuto provando il codice di sicurezza nel nuovo messaggio AUTACK), allora l'interscambio EDI in questione è noto per entrambi il trasmettitore ed il ricevitore poichè l'MD5 dell'interscambio EDI ed il numero dell'interscambio sono contenuti nel messaggio AUTACK e sono stati debitamente riconosciuti. In aggiunta, l'integrità e l'autenticità dell'interscambio EDI in seguito a ricezione saranno state verificate ed il trasmettitore del ricevitore non negherà di aver ricevuto l'interscambio EDI in questione.

Facendo ora riferimento alle figure 4-5, in esse è illustrato un diagramma di flusso di processo o elaborazione del procedimento attualmente preferito per ricevere e trasmettere posta elettronica (E-mail), rispettivamente, secondo il procedimento attualmente preferito della presente in-

STUDIO MODIANO & ASSOCIATI

venzione. A tale proposito, TEMPLAR, che è l'unità di controllo per attuare il procedimento attualmente preferito della presente invenzione, preferibilmente è disposto tra il convenzionale trasmettitore postale e l'archivio piano EDI specificato dall'utente sui sistemi trasmittente e ricevente, con il convenzionale SENDMAIL alimentato con il sistema operativo UNIX X-WINDOWS O MICROSOFT WINDOWS che è preferibilmente impiegato per trasmettere e ricevere posta, la posta che è trasmessa e ricevuta essendo preferibilmente conforme a MIME e PKCS essendo preferibilmente impiegato per criptografare o criptare e decriptare parti di corpi codificate in MIME. Preferibilmente, gli identificatori MIME non sono criptati. Come si è osservato precedentemente, il messaggio EDIFACT AUTACK è preferibilmente impiegato per fornire autentificazione sicura, sicuro non-ripudio di origine e/o sicura ricezione, e riconoscimento o diniego di riconoscimento per uno o più buste X.12 o EDIFACT o INVILUPPI. Preferibilmente, buste EDI multiple sono considerate come un blocco di dati nel sistema della presente invenzione. Preferibilmente, se un messaggio AUTACK ricevuto fallisce l'integrità del messaggio, allora un riconoscimento di ricezione non viene rinviato al trasmettitore originale del messaggio benchè, se desiderato, il sistema possa essere facilmente modificato per realizzare ciò.

Facendo ora riferimento alle figure 6-9, questi sono diagrammi di flusso di processo rispetto al controllo o gestione dei partner commerciali, gestione dei giornali di controllo amministrativo, gestione di tracciatura, e monitoraggio dei compiti rispettivamente conformemente al procedimento attualmente preferito della presente invenzione. Questi diagrammi sono auto-esplicativi quando considerati in unione con la discussione precedente e non saranno successivamente descritti in ulteriori dettagli.

MEDIANO ASSOCIATI

La figura 10 è il diagramma funzionale dell'organizzazione del procedimento attualmente preferito della presente invenzione come rappresentato dallo scritto o documento originale della TABELLA A e nella precedente discussione, e non sarà ulteriormente in seguito descritto in ulteriori dettagli.

Da ultimo, le figure 11-13 costituiscono un diagramma di flusso di processo del procedimento attualmente preferito della presente invenzione conformemente alla descrizione precedente, la figura 11 illustrando varie fasi di verifica dell'integrità del messaggio AUTACK, dell'interscambio EDI, e di certificazione, NRO rappresentando non-ripudio di origine ed NRR rappresentando non-ripudio di ricezione. La figura 12 illustra la porzione del procedimento dedicata all'elaborazione di TPA. La figura 13 illustra la porzione del procedimento della presente invenzione dedicata all'elaborazione della chiavi pubblica e privata, come pure di TPA, nell'attuare il procedimento della presente invenzione come è stato descritto precedentemente.

Così, utilizzando il messaggio AUTACK come un documento per la segnatura digitale che è segnato in base al sistema di chiavi pubblica/privata come RSA, è fornito un dispositivo di trasmissione postale altamente sicuro per EDI su una rete aperta, come ad esempio la rete INTERNET, in cui partner commerciali possono facilmente ottenere verifica sicura e sicura autentificazione e non-ripudio sia dell'origine che della ricezione tutte le quali cose sono importanti in transazioni commerciali elettroniche a rapidi movimenti entro un'area geografica largamente dispersa in cui una rete aperta è il mezzo di comunicazione più valido.

ASSOCIAZIONE

RIVENDICAZIONI

1. Sistema di comunicazioni per intercollegare selettivamente una pluralità di calcolatori su una rete pubblica aperta su cui detti calcolatori scambiano messaggi digitali sicuri tra un calcolatore trasmettitore ed un calcolatore ricevitore in detta pluralità di calcolatori, detto calcolatore trasmettitore avendo una prima chiave pubblica associata ed una prima chiave privata associata, detto calcolatore ricevitore avendo una seconda chiave pubblica associata ed una seconda chiave privata associata, detti messaggi digitali comprendendo una comunicazione di interscambio EDI tra detto calcolatore trasmettitore e detto calcolatore ricevitore, detta comunicazione di interscambio EDI avendo un messaggio di riconoscimento EDI associato, includente il perfezionamento caratterizzato dal fatto di comprendere

mezzi per calcolare un primo totale di quadratura per detta comunicazione di interscambio EDI da detto calcolatore trasmettitore;

mezzi per inserire detto primo totale di quadratura in una locazione predeterminata in detto messaggio di riconoscimento EDI associato;

mezzi per calcolare un secondo totale di quadratura di detto messaggio di riconoscimento EDI associato;

mezzi per segnare in digitale detto messaggio di riconoscimento EDI associato, detti mezzi di segnatura digitale di detto messaggio comprendendo mezzi per criptografare detto secondo totale di quadratura con detta chiave privata di detto calcolatore trasmettitore;

mezzi per inserire detto secondo totale di quadratura in una locazione predeterminata in detto messaggio di riconoscimento EDI associato;

mezzi per trasmettere detta comunicazione di interscambio EDI assieme a detto messaggio di riconoscimento EDI associato segnato in digitale a detto calcolatore

ricevitore su detta rete pubblica aperta; e

mezzi associati con detto calcolatore ricevitore per ricevere ed elaborare detta comunicazione di interscambio EDI ricevuta e detto messaggio di riconoscimento EDI segnato in digitale per fornire autentificazione e non-ripudio di dette comunicazioni di interscambio EDI da detto calcolatore emettitore, detti mezzi comprendendo mezzi per decifrare detto secondo totale di quadratura cifrato con detta chiave pubblica del calcolatore emettitore; per cui possono avvenire comunicazioni di interscambio EDI private sicure su una rete pubblica aperta fornendo al contempo autentificazione e non-ripudio di dette comunicazioni EDI.

2. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 1, in cui detti mezzi associati con detto calcolatore ricevente comprendono inoltre mezzi per calcolare un terzo totale di quadratura di detto messaggio di riconoscimento EDI ricevuto; e mezzi per comparare detto terzo totale di quadratura con detto secondo totale di quadratura decriptografato da detto messaggio di riconoscimento EDI ricevuto, detti mezzi di comparazione comprendendo mezzi per formare un'indicazione di integrità di detto messaggio di riconoscimento EDI e non-ripudio di origine quando detto secondo totale di quadratura decriptografato e detto terzo totale di quadratura corrispondono o si pareggiano.

3. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 2, in cui detti mezzi associati con detto calco-

ASSOCIAZIONE MODIANO

latore ricevitore comprendono inoltre mezzi per calcolare un quarto totale di quadratura di detta comunicazione di interscambio EDI ricevuta; e mezzi per comparare detto quarto totale di quadratura di detta comunicazione di interscambio EDI ricevuta con detto primo totale di quadratura in detto messaggio di riconoscimento EDI ricevuto, detti mezzi di comparazione comprendendo mezzi per fornire un'indicazione di integrità e verifica di autenticità di detta comunicazione di interscambio EDI e non-ripudio di origine quando detti primo e quarto totali di quadratura corrispondono o si pareggiano.

4. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 3, in cui detti mezzi associati con detto calcolatore ricevitore comprendono inoltre mezzi per creare un messaggio di riconoscimento EDI di risposta e trasmettere detto messaggio di riconoscimento EDI di risposta a detto calcolatore trasmettitore su detta rete pubblica aperta, detti mezzi di creazione del messaggio di riconoscimento EDI di risposta comprendendo mezzi per calcolare un quinto totale di quadratura di detto messaggio di riconoscimento EDI di risposta e per segnare in digitale detto quinto totale di quadratura criptografando detto quinto totale di quadratura con detta chiave privata di detto calcolatore ricevente; e mezzi per inserire detto quinto totale di quadratura segnato in digitale in una locazione predeterminata in detto messaggio di riconoscimento EDI di risposta trasmesso.

5. Sistema di comunicazioni su reta aperta sicuro perfezionato secondo la rivendicazione 4, comprendente inoltre mezzi associati con detto calcolatore trasmettitore per ricevere detto messaggio di riconoscimento

EDI di risposta trasmesso e per decriptografare detto quinto totale di quadratura criptografato con detta chiave pubblica di detto calcolatore ricevente per verificare detta segnatura digitale di detto messaggio di riconoscimento EDI di risposta; e mezzi per calcolare un sesto totale di quadratura di detto messaggio di riconoscimento EDI di risposta ricevuto; e mezzi per comparare detto sesto totale di quadratura rispetto a detto quinto totale di quadratura decriptografato, detti mezzi di comparazione comprendendo mezzi per fornire un'indicazione di integrità di detto messaggio di riconoscimento EDI di risposta ricevuto e non-ripudio di origine di detto messaggio di riconoscimento EDI di risposta; per cui non-ripudio della ricezione di detta comunicazione di interscambio EDI è stabilito da detto calcolatore trasmettitore.

6. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 5, in cui detti mezzi per creare detto messaggio di riconoscimento EDI di risposta comprendono inoltre mezzi per inserire detto quarto totale di quadratura in una locazione predeterminato in detto messaggio di riconoscimento EDI di risposta trasmesso, e detti mezzi associati con detto calcolatore trasmettitore comprendono inoltre mezzi per comparare detto quarto totale di quadratura in detto messaggio di riconoscimento EDI di risposta ricevuto con detto primo totale di quadratura, detti mezzi di comparazione fornendo un'indicazione di integrità ed autenticità di detto interscambio EDI quando detti primo e quarto totali di quadratura corrispondono o si pareggiano.

7. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 6, in cui detto messaggio di riconoscimento EDI

MODIANO & ASSOCIATI

comprende un messaggio AUTACK.

8. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 7, in cui detto messaggio di riconoscimento EDI di risposta comprende un messaggio AUTACK.

9. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 8, in cui ciascuno di detti totali di quadratura comprende un MD5.

10. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 9, in cui dette chiavi pubblica e privata comprendono un sistema di comunicazioni criptografiche di tipo RSA.

11. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 10, in cui detta rete pubblica aperta comprende la rete Internet.

12. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 1, in cui detta rete pubblica aperta comprende la rete Internet.

13. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 1 in cui detti mezzi associati con detto calcolatore ricevente comprendono inoltre mezzi per creare un messaggio di riconoscimento EDI di risposta e trasmettere detto messaggio di riconoscimento EDI di risposta a detto calcolatore trasmettitore su detta rete pubblica aperta, detti mezzi di creazione del messaggio di riconoscimento EDI di risposta comprendendo mezzi per calcolare un terzo totale di quadratura di detto messaggio di riconoscimento EDI di risposta e per segnare in digitale detto terzo totale di quadratura criptografando detto terzo totale

MODIANO & ASSOCIATI

di quadratura con detta chiave privata di detto calcolatore ricevente; e mezzi per inserire detto terzo totale di quadratura segnato in digitale in una locazione predeterminata in detto messaggio di riconoscimento EDI di risposta trasmesso.

14. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 13, in cui detta rete pubblica aperta comprende la rete Internet.

15. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 14 comprendente inoltre mezzi associati con detto calcolatore trasmettitore per ricevere detto messaggio di riconoscimento EDI di risposta trasmesso e per decriptografare detto terzo totale di quadratura criptografato con detta chiave pubblica di detto calcolatore ricevente per verificare detta segnatura digitale di detto messaggio di riconoscimento EDI di risposta; e mezzi per calcolare un quarto totale di quadratura di detto messaggio di riconoscimento EDI di risposta ricevuto; e mezzi per comparare detto quarto totale di quadratura rispetto a detto terzo totale di quadratura decriptografato, detti mezzi di comparazione comprendendo mezzi per fornire un'indicazione di integrità di detto messaggio di riconoscimento EDI di risposta ricevuto e non-ripudio di origine di detto messaggio di riconoscimento EDI di risposta; per cui non-ripudio della ricezione di detta comunicazione di interscambio EDI è stabilito da detto calcolatore trasmettitore.

16. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 13 comprendente inoltre mezzi associati con detto calcolatore trasmettitore per ricevere detto messaggio di riconoscimen-

STUDIO MODIANO ASSOCIATI

to EDI di risposta trasmessa e per decriptografare detto terzo totale di quadratura criptografato con detta chiave pubblica di detto calcolatore ricevente per verificare detta segnatura digitale di detto messaggio di riconoscimento EDI di risposta; e mezzi per calcolare un quarto totale di quadratura di detto messaggio di riconoscimento EDI di risposta ricevuto; e mezzi per comparare detto quarto totale di quadratura rispetto a detto terzo totale di quadratura decriptografato, detti mezzi di comparazione comprendendo mezzi per fornire un'indicazione di integrità di detto messaggio di riconoscimento EDI di risposta ricevuto e non-ripudio di origine di detto messaggio di riconoscimento EDI di risposta; per cui non-ripudio della ricezione di detta comunicazione di interscambio EDI è stabilito da detto calcolatore trasmettitore.

17. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 4, in cui detti mezzi per creare detto messaggio di riconoscimento EDI di risposta comprendono inoltre mezzi per inserire detto quarto totale di quadratura in una locazione predeterminata in detto messaggio di riconoscimento EDI di risposta trasmesso e detti mezzi associati con detto calcolatore trasmettitore comprendono inoltre mezzi per comparare detto quarto totale di quadratura in detto messaggio di riconoscimento EDI di risposta ricevuto con detto primo totale di quadratura, detti mezzi di comparazione fornendo un'indicazione di integrità ed autenticità di detto interscambio EDI quando detti primo e quarto totali di quadratura si adattano.

18. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 1, in cui detto messaggio di riconoscimento EDI

comprende un messaggio AUTACK.

19. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 18, in cui detta rete pubblica aperta comprende la rete Internet.

20. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 19, in ciascuno di detti totali di quadratura comprende un MD5.

21. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 1, in cui ciascuno di detti totali di quadratura comprende un MD5.

22. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 21, in cui detta rete pubblicata aperta comprende la rete Internet.

23. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 21, in cui detto messaggio di riconoscimento EDI comprende un messaggio AUTACK.

24. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 23, in cui dette chiavi pubblica e privata comprendono un sistema di comunicazioni criptografiche di tipo RSA.

25. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 24, in cui detta rete pubblica aperta comprende la rete Internet.

26. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 1, in cui dette chiavi pubblica e privata comprendono un sistema di comunicazioni criptografiche di tipo RSA.

27. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 26, in cui detta rete pubblica aperta comprende la rete Internet.

28. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 13, in cui detto messaggio di riconoscimento EDI comprende un messaggio AUTACK.

29. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 28, in cui detto messaggio di riconoscimento EDI di risposta comprende un messaggio AUTACK.

30. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 13, in cui detto messaggio di riconoscimento EDI di risposta comprende un messaggio AUTACK.

31. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 1 comprendente inoltre mezzi per generare una comunicazione di accordo di partner commerciali tra detto calcolatore trasmettitore e detto calcolatore ricevitore, detto calcolatore trasmettitore e detto calcolatore ricevitore comprendendo partner commerciali, detta comunicazione di accordo dei partner commerciali comprendendo dette chiavi pubbliche in detta comunicazione di interscambio EDI per consentire a detti partner commerciali di fornire mutua certificazione.

32. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 31, in cui detta rete pubblica aperta comprende la rete Internet.

33. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 32, in cui detto messaggio di riconoscimento EDI

comprende un messaggio AUTACK.

34. Sistema di comunicazioni su una rete aperta sicuro perfezionato secondo la rivendicazione 31, in cui detto messaggio di riconoscimento EDI comprende un messaggio AUTACK.

35. Procedimento per intercollegare selettivamente una pluralità di calcolatori su una rete pubblica aperta per fornire uno scambio tra calcolatori di messaggi digitali sicuri privati tra un calcolatore trasmettitore ed un calcolatore ricevitore in detta pluralità di calcolatori, detto calcolatore trasmettitore avendo una prima chiave pubblica associata ed una prima chiave privata associata, detto calcolatore ricevitore avendo una seconda chiave pubblica associata ed una seconda chiave privata associata, detti messaggi digitali comprendendo una comunicazione di interscambio EDI tra detto calcolatore trasmettitore e detto calcolatore ricevitore, detta comunicazione di interscambio EDI avendo un messaggio di riconoscimento EDI associato, detto procedimento comprendendo le fasi di segnare in digitale detto messaggio di riconoscimento EDI associato con detta chiave privata di detto calcolatore trasmettitore; trasmettere detta comunicazione di interscambio EDI assieme a detto messaggio di riconoscimento EDI associato segnato in digitale a detto calcolatore ricevitore su detta rete pubblica aperta; ed elaborare detto messaggio di riconoscimento EDI segnato in digitale per fornire autentificazione e non-ripudio di detta comunicazione di detta comunicazione di interscambio da detto calcolatore trasmettitore, detta fase di elaborazione comprendendo la fase di elaborare detto messaggio di riconoscimento EDI associato segnato in digitale ricevuto con detta chiave pubblica di detto calcolatore trasmettito-

re; per cui comunicazioni di interscambio EDI private sicure possono aver luogo su una rete pubblica aperta fornendo al tempo stesso autentificazione e non-ripudio di dette comunicazioni EDI impiegando detto messaggio di riconoscimento EDI associato.

36. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 35, in cui detta rete pubblica aperta comprende la rete Internet.

37. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 36 comprendente inoltre le fasi di creare un messaggio di riconoscimento EDI di risposta per detto calcolatore ricevitore; segnare in digitale detto messaggio di riconoscimento EDI di risposta con detta chiave privata di detto calcolatore ricevitore; trasmettere detto messaggio di riconoscimento EDI di risposta segnato in digitale a detto calcolatore trasmettitore su detta rete pubblica aperta, detto calcolatore trasmettitore ricevendo detto messaggio di riconoscimento EDI di risposta segnato in digitale; ed elaborare detto messaggio di riconoscimento EDI di risposta segnato in digitale ricevuto per fornire non-ripudio della ricezione di detta comunicazione di interscambio EDI da parte di detto calcolatore trasmettitore, detta fase di elaborazione comprendendo la fase di elaborare detto messaggio di riconoscimento EDI di risposta segnato in digitale ricevuto con detta chiave pubblica di detto calcolatore ricevitore; per cui non-ripudio della ricezione di detta comunicazione di interscambio EDI è stabilito da detto calcolatore trasmettitore.

38. Procedimento per fornire comunicazioni private sicure su una rete

pubblica aperta secondo la rivendicazione 35 comprendente inoltre le fasi di creare un messaggio di riconoscimento EDI di risposta da detto calcolatore ricevitore; segnare in digitale detto messaggio di riconoscimento EDI di risposta con detta chiave privata di detto calcolatore ricevente; trasmettere detto messaggio di riconoscimento EDI di risposta segnato a detto calcolatore trasmettitore su detta rete pubblica aperta, detto calcolatore trasmettitore ricevendo detto messaggio di riconoscimento EDI di risposta segnato in digitale; ed elaborare detto messaggio di riconoscimento EDI di risposta segnato in digitale per fornire non-ripudio della ricezione di detta comunicazione di interscambio EDI da parte di detto calcolatore trasmettitore, detta fase di elaborazione comprendendo la fase di elaborare detto messaggio di riconoscimento EDI di risposta segnato in digitale con detta chiave pubblica di detto calcolatore ricevente; per cui non-ripudio della ricezione di detta comunicazione di interscambio EDI è stabilito da detto calcolatore trasmettitore.

39. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 38, in cui detta fase di elaborazione comprende inoltre la fase di fornire non-ripudio dell'origine in detto calcolatore ricevitore da detto messaggio di riconoscimento EDI ricevuto.

40. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 39, in cui detta rete pubblica aperta comprende la rete Internet.

41. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 35, in cui detta fase di elabo-

ASSOCIATI

razione comprende inoltre la fase di fornire non-ripudio di origine in detto calcolatore ricevitore da detto messaggio di riconoscimento EDI ricevuto.

42. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 35, in cui detto messaggio di riconoscimento EDI comprende un messaggio AUTACK.

43. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 38, in cui detto messaggio di riconoscimento EDI di risposta comprende un messaggio AUTACK.

44. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 43, in cui detto messaggio di riconoscimento EDI comprende un messaggio AUTACK.

45. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 35, in cui dette chiavi pubblica e privata comprendono un sistema di comunicazioni criptografiche di tipo RSA.

46. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 45, in cui detta rete pubblica aperta comprende la rete Internet.

47. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 45, in cui detto messaggio di riconoscimento EDI comprende un messaggio AUTACK.

48. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 47 comprendente inoltre le fasi di creare un messaggio di riconoscimento EDI di risposta da detto calcola-

tore ricevente; segnare in digitale detto messaggio di riconoscimento EDI di risposta con detta chiave privata del calcolatore ricevente; trasmettere detto messaggio di riconoscimento EDI di risposta segnato a detto calcolatore trasmettitore su detta rete pubblica aperta, detto calcolatore trasmettitore o trasmittente ricevendo detto messaggio di riconoscimento EDI di risposta segnato in digitale; ed elaborare detto messaggio di riconoscimento EDI di risposta segnato in digitale ricevuto per fornire non-ripudio di ricezione di detta comunicazione di interscambio EDI da parte di detto calcolatore trasmettitore, detta fase di elaborazione comprendendo la fase di elaborare detto messaggio di riconoscimento EDI di risposta segnato in digitale ricevuto con detta chiave pubblica di detto calcolatore ricevente; per cui non-ripudio di ricezione di detta comunicazione di interscambio EDI è stabilito da detto calcolatore trasmettitore.

49. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 48, in cui detto messaggio di riconoscimento EDI di risposta comprende un messaggio AUTACK.

50. Procedimento per fornire comunicazioni private sicure su una rete pubblica aperta secondo la rivendicazione 49, in cui detta rete pubblica aperta comprende la rete Internet.

Il Mandatario:

- Dr. Ing. Guido MODIANO -

MI96 A 004519

TAV. I

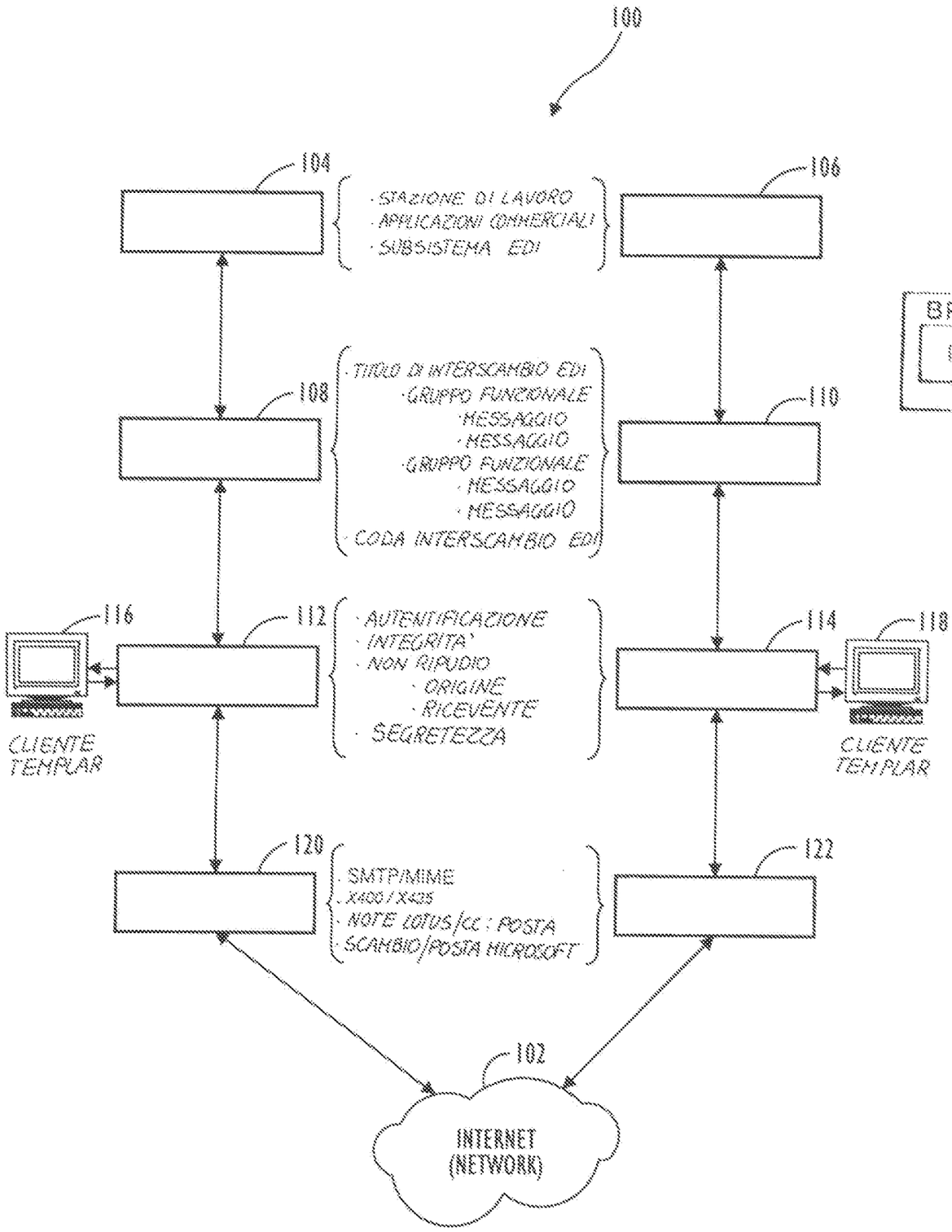


FIG. 1

BREV. MI-R
003072

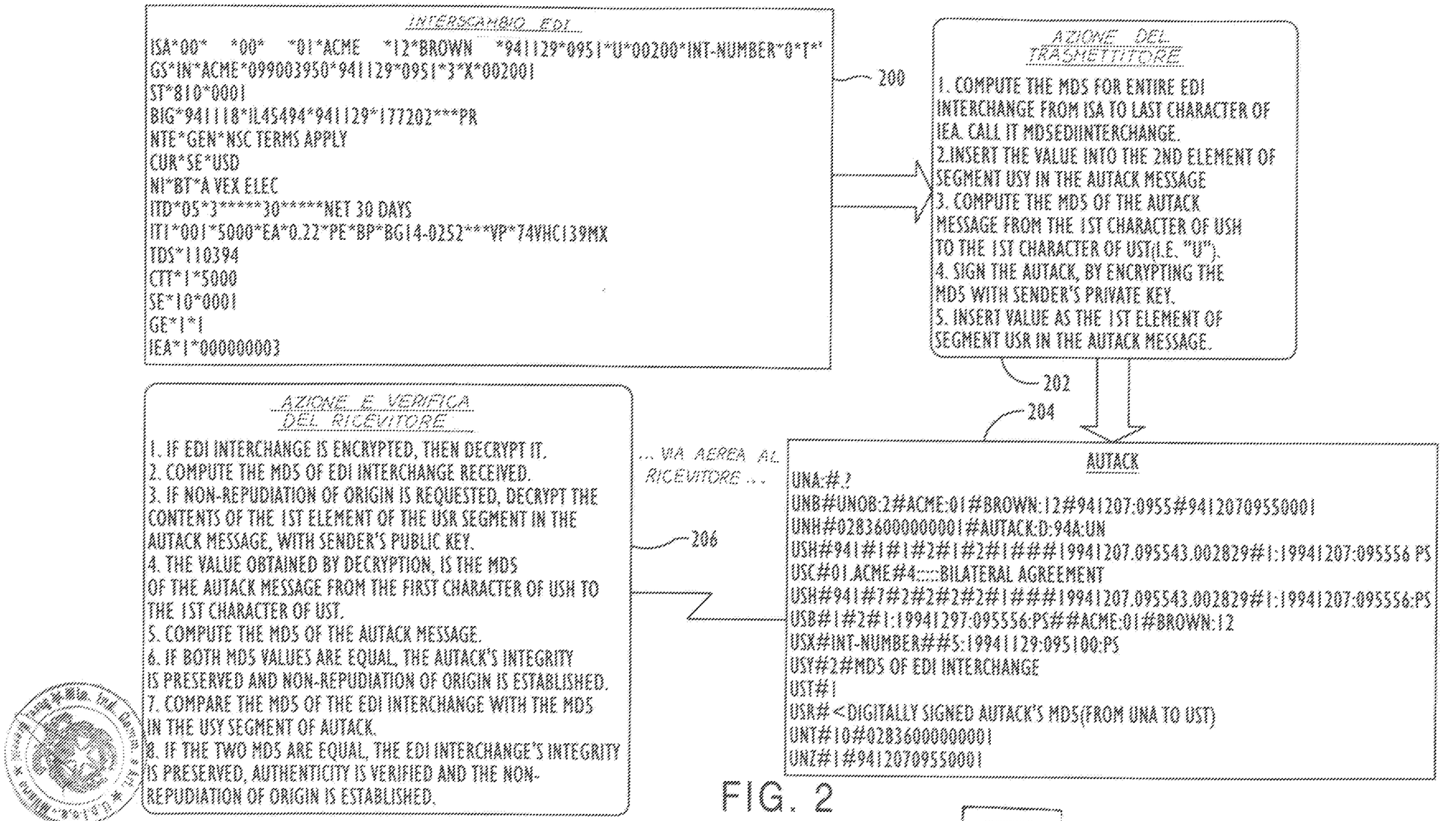


FIG. 2

U.S. Patent Nov. 28, 1995 Sheet 2 of 11 5,469,507

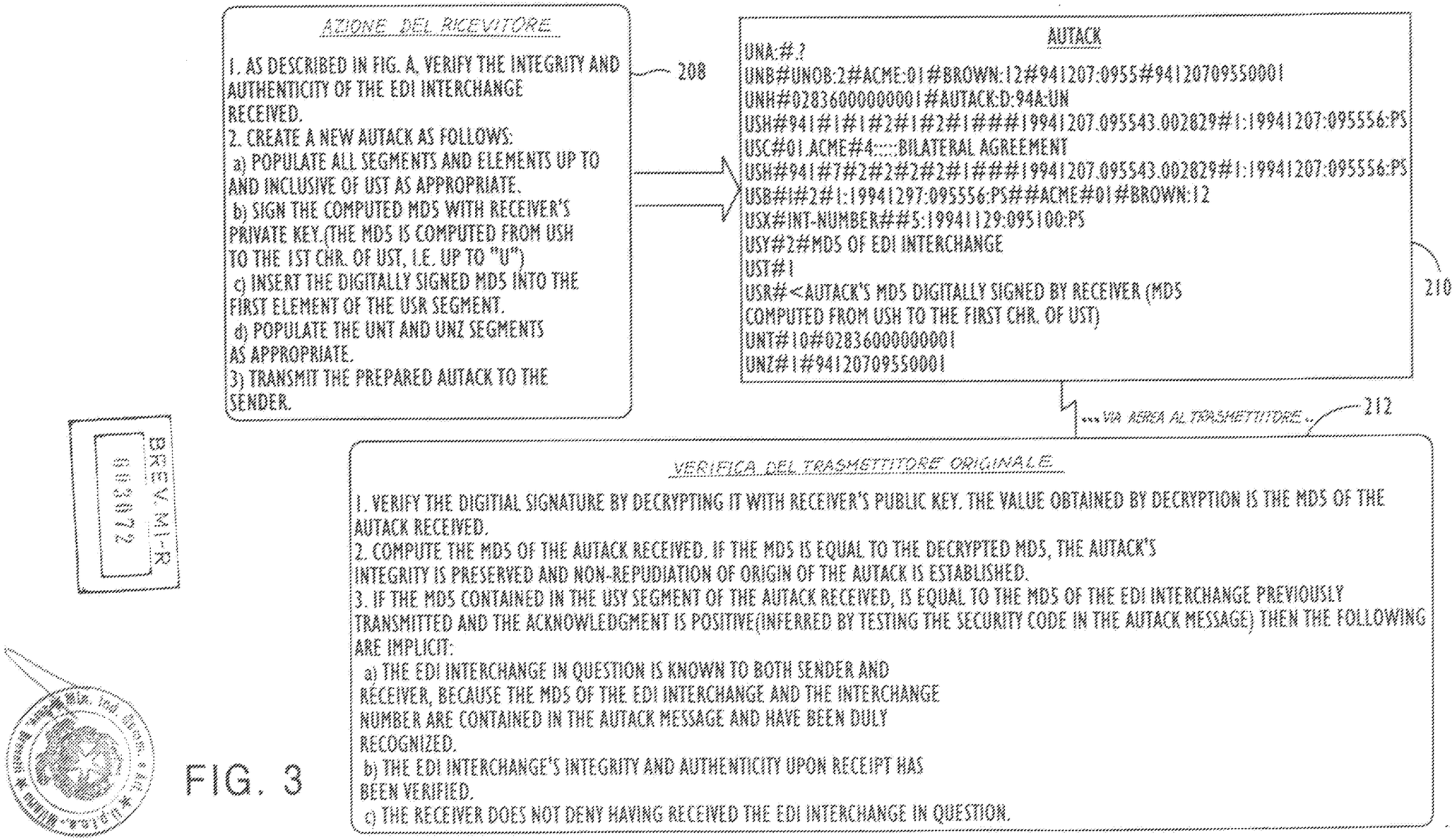


FIG. 3

BREVETTI-R
08 MI 92

TAV. III
VI 95 P-0015

TAV. IV

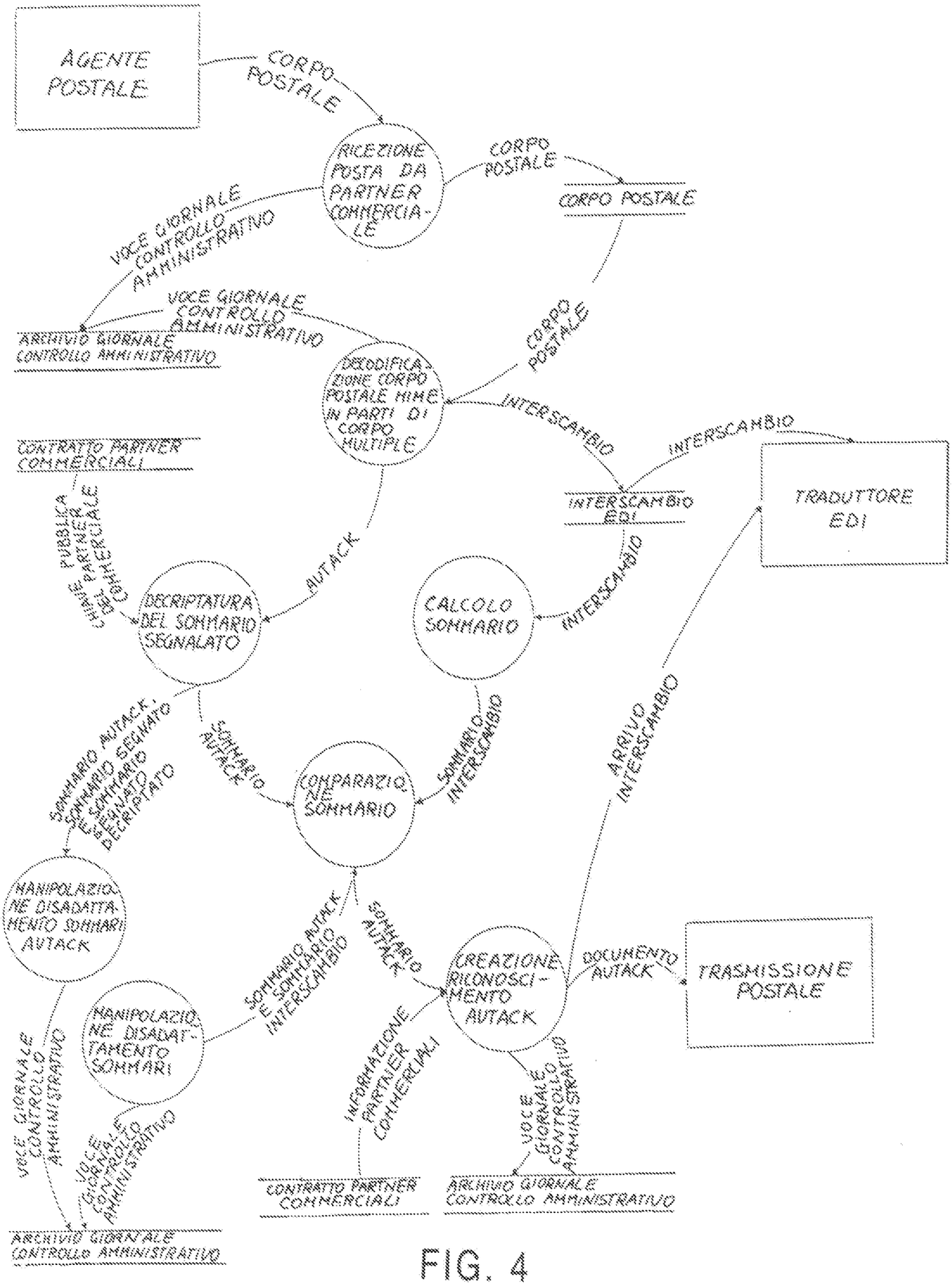


FIG. 4

BREV. MI-R
003072

MI 36 A 001519

TAV. V

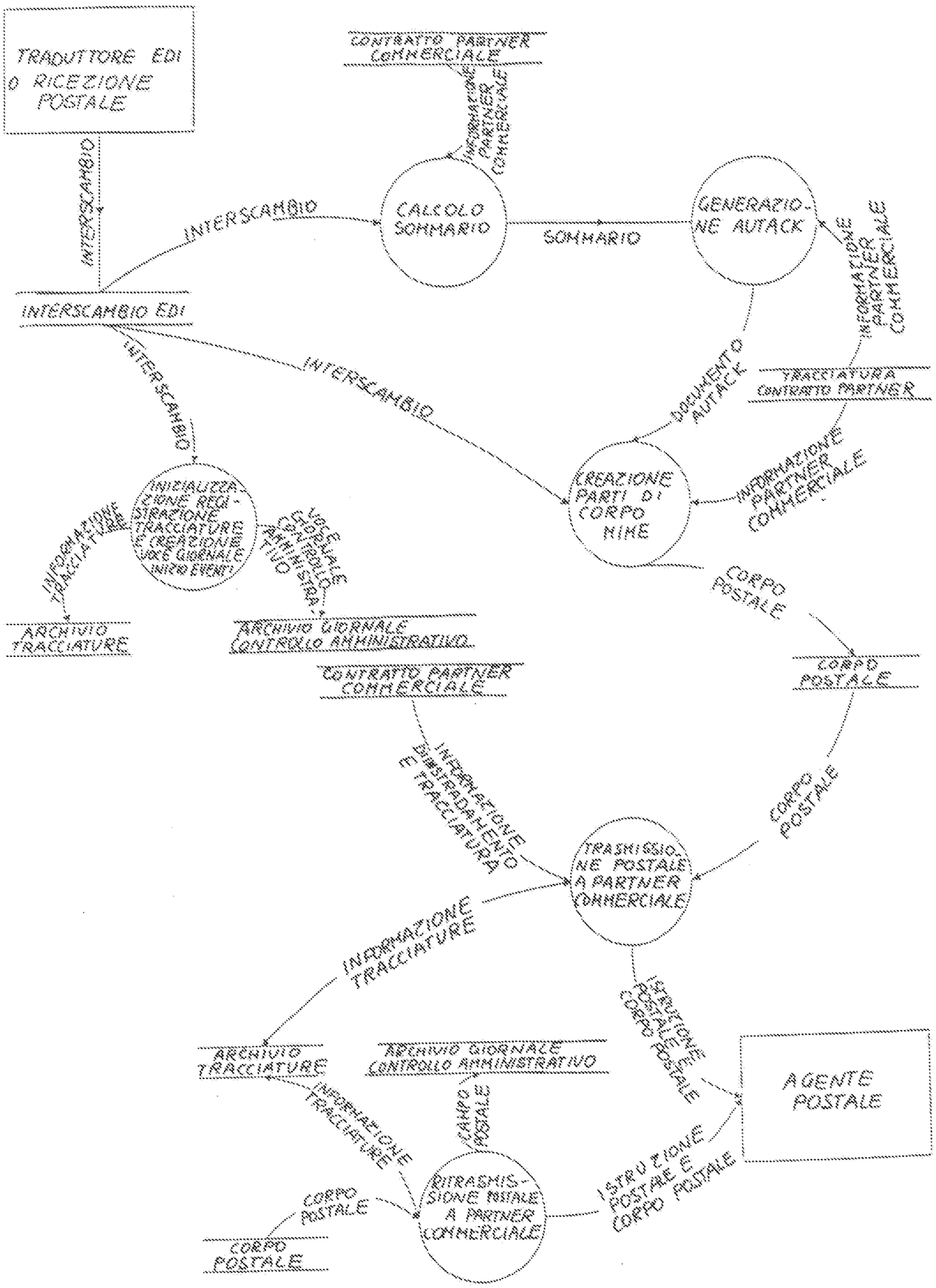


FIG. 5

BREV. MI-R
603872

MI 96 A 001519

TAV. VI

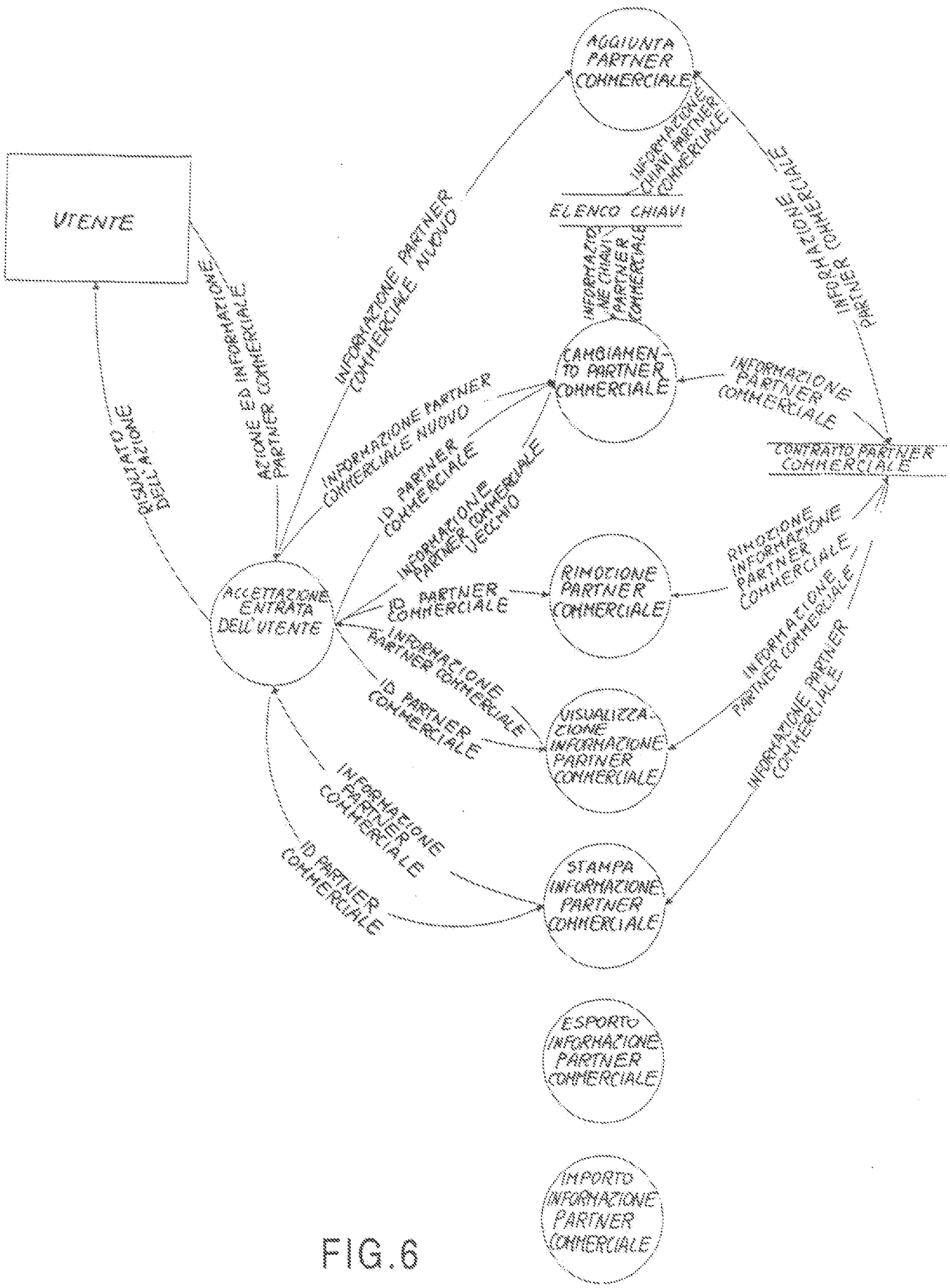
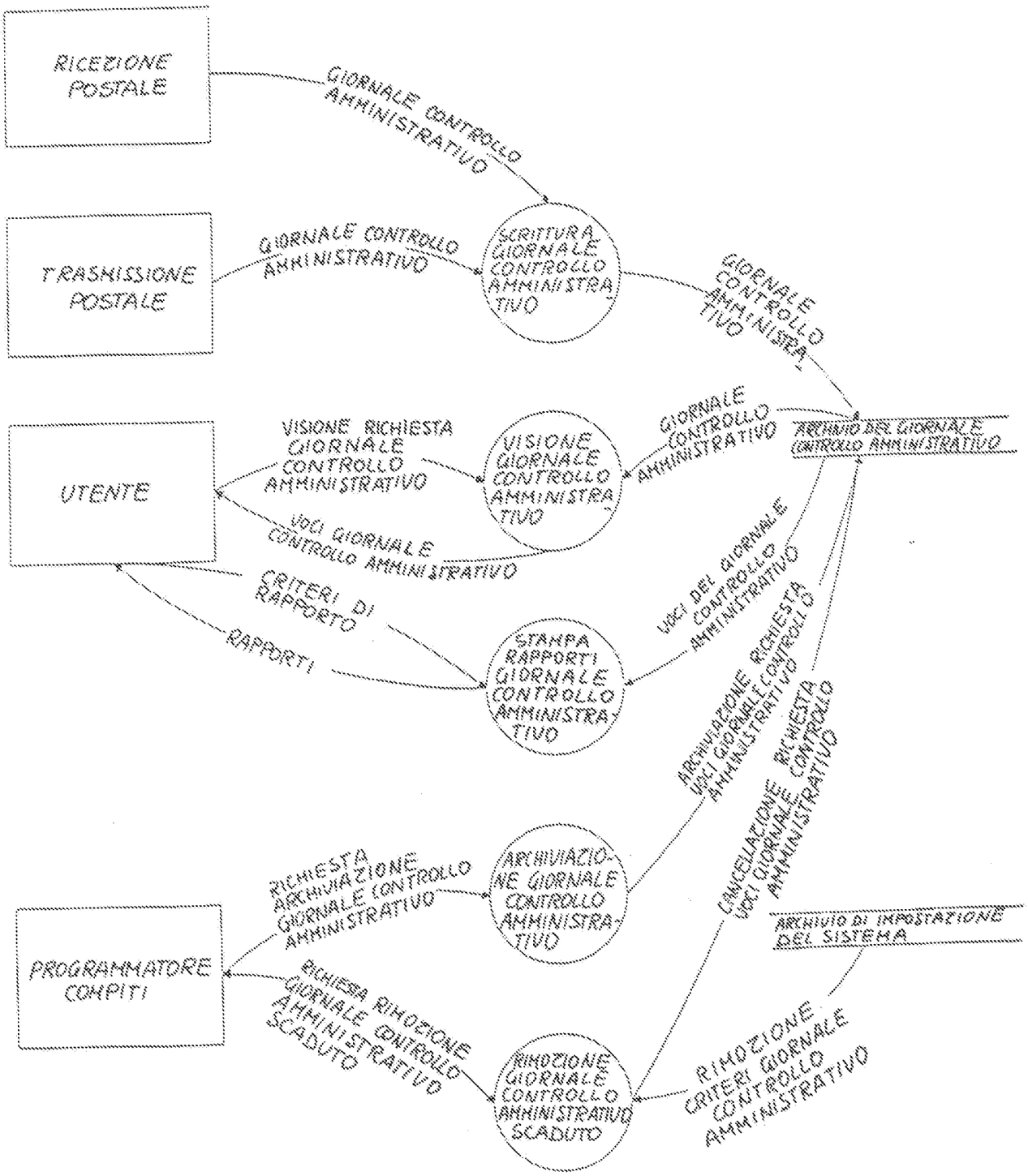


FIG.6

BREVMI-R
003072

MI 36 A 00159

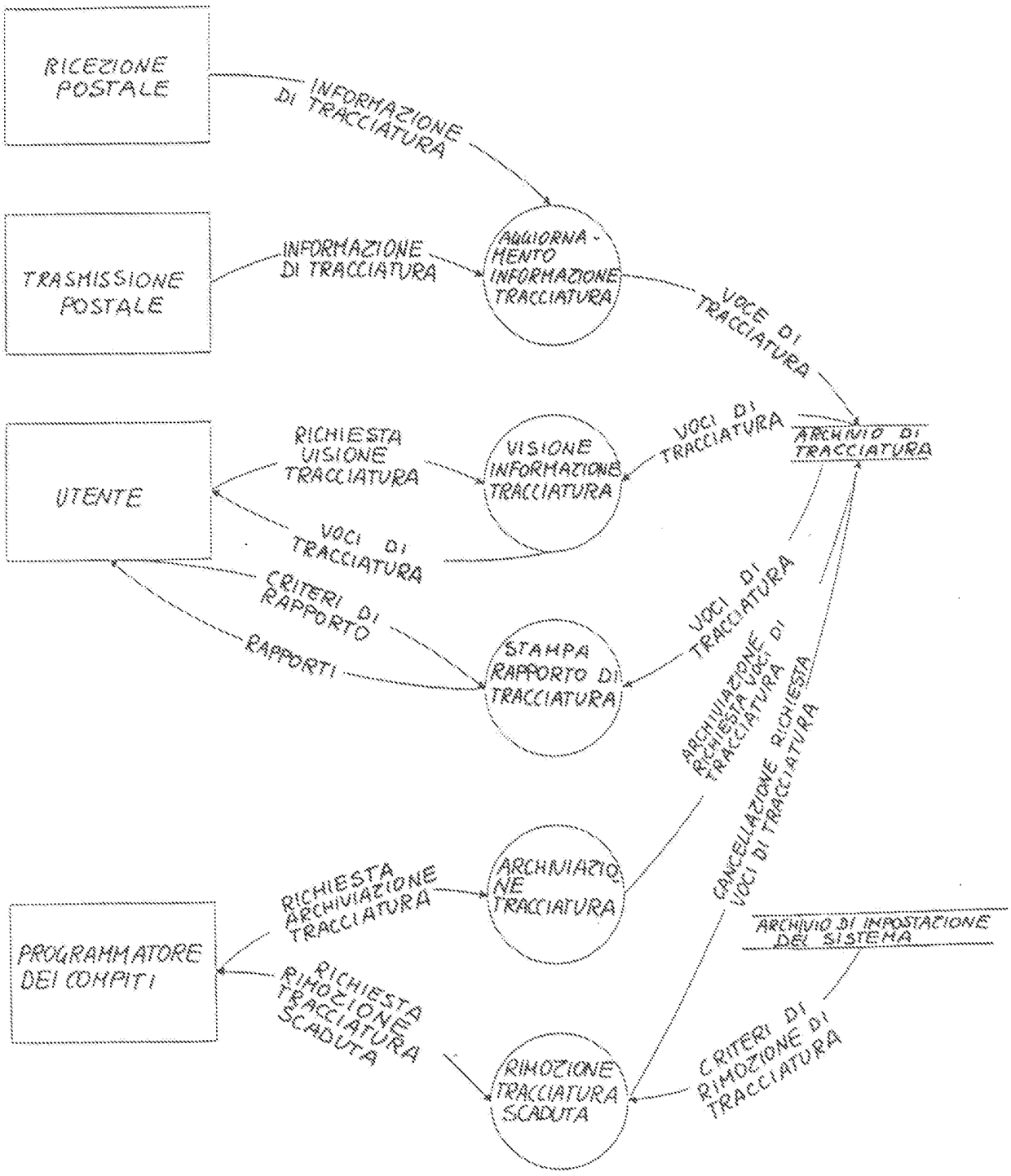
TAV. VII



BREV. MI-R
603172

FIG. 7

TAV. VIII



BREV. MI-R
003872

FIG.8

MI 96 A 00150

TAV. IX

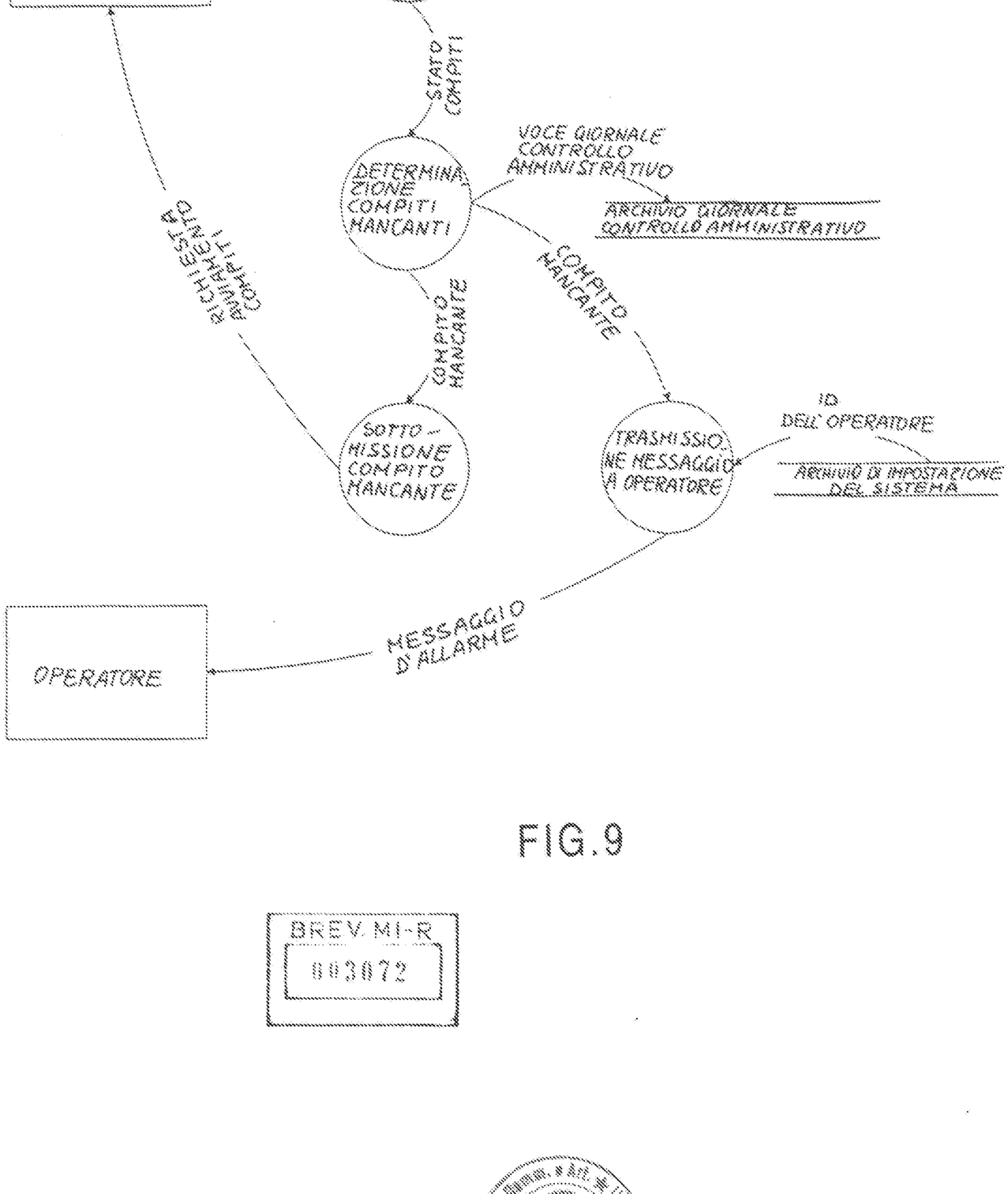


FIG.9

BREV. MI-R
003072

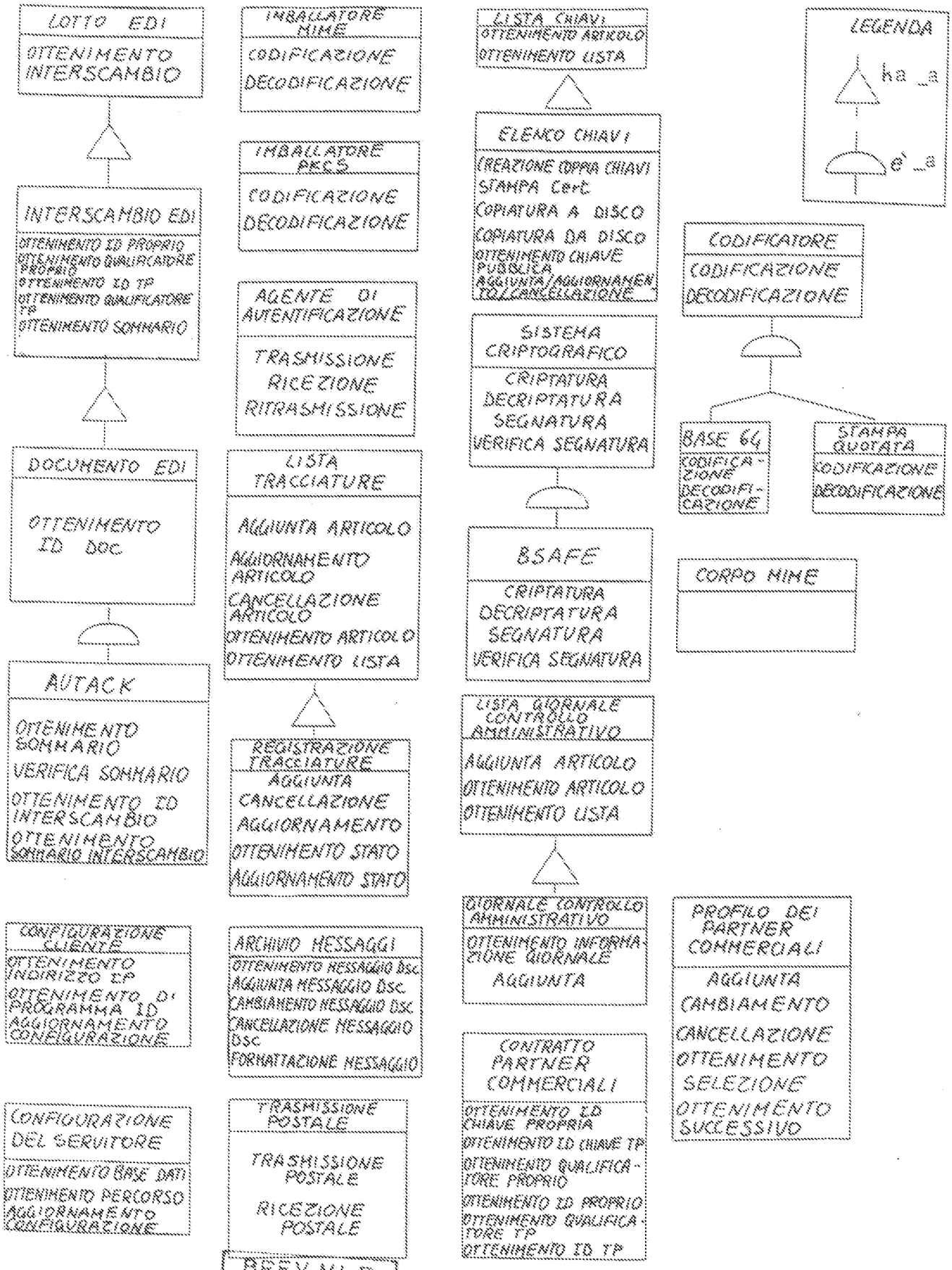


FIG. 10

BREV. MI-R
003072

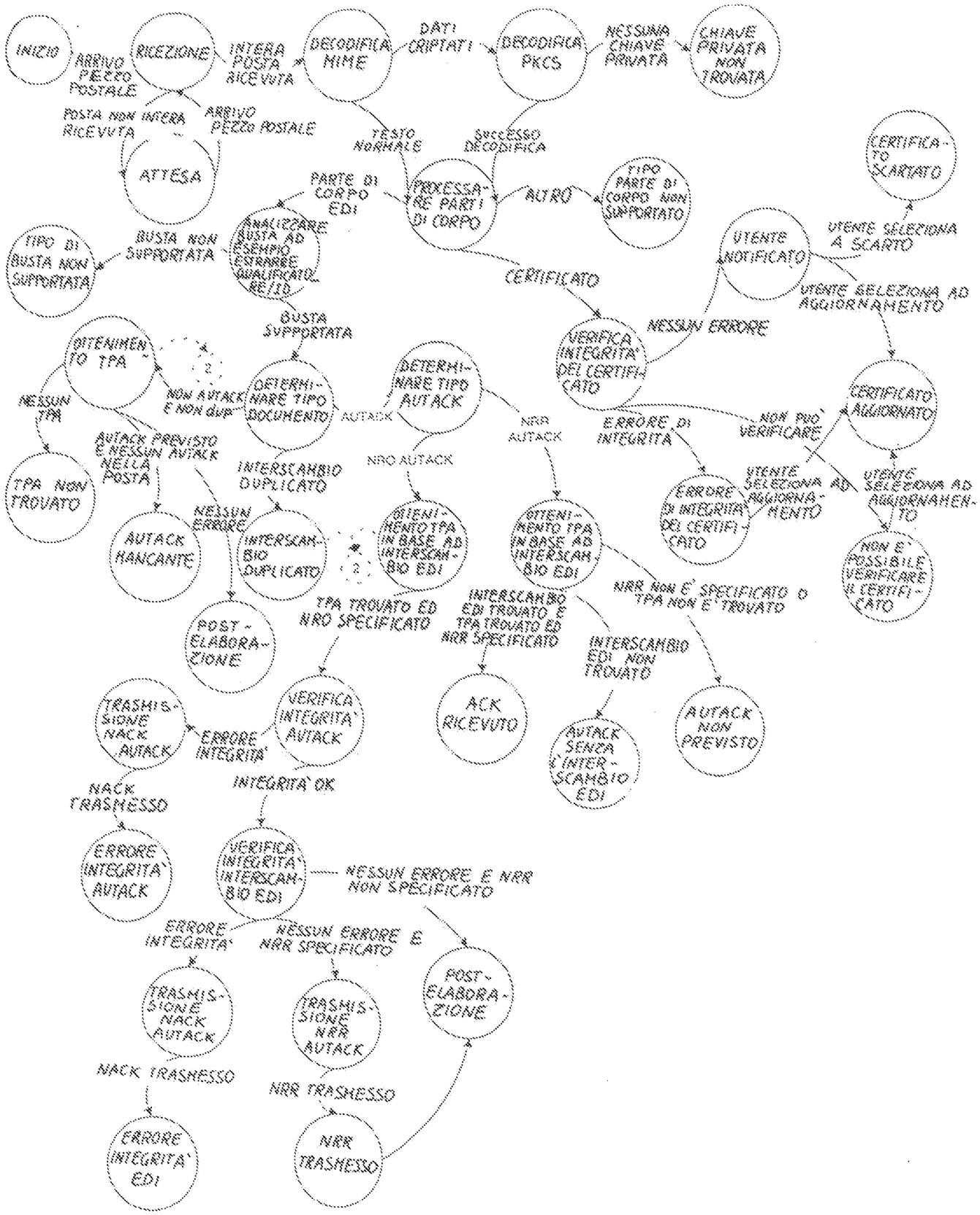


FIG. 11

BREV. MI-R
003872

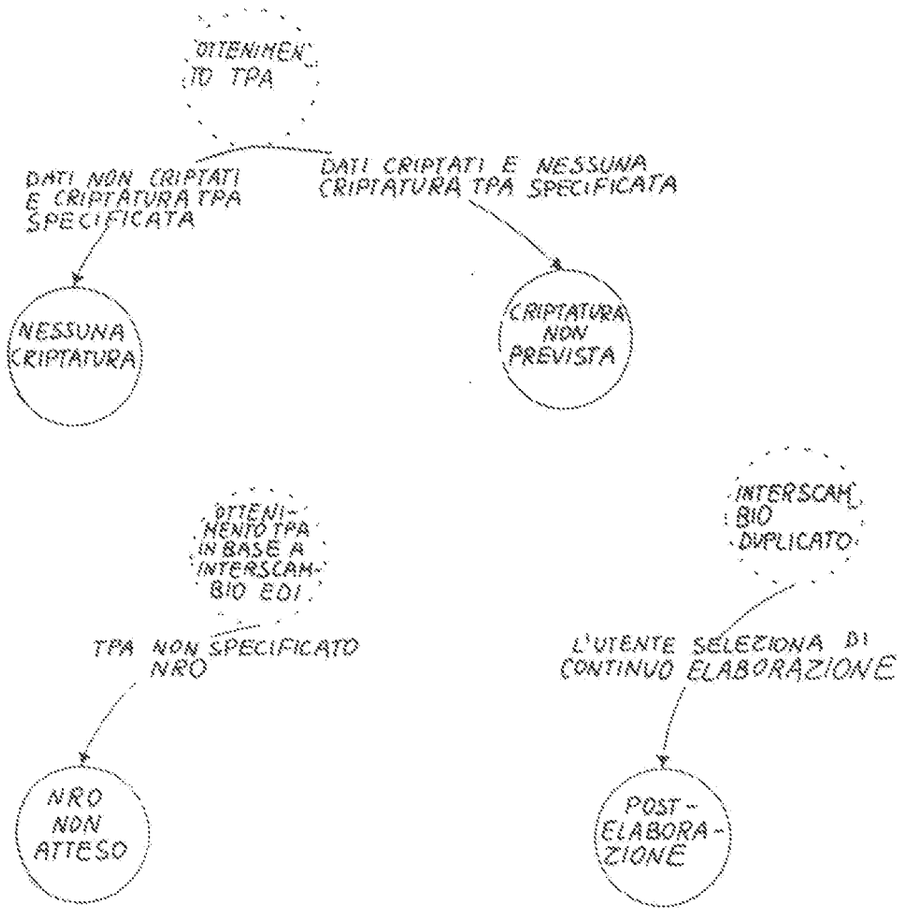


FIG. 12

BREV. MI-R
603072

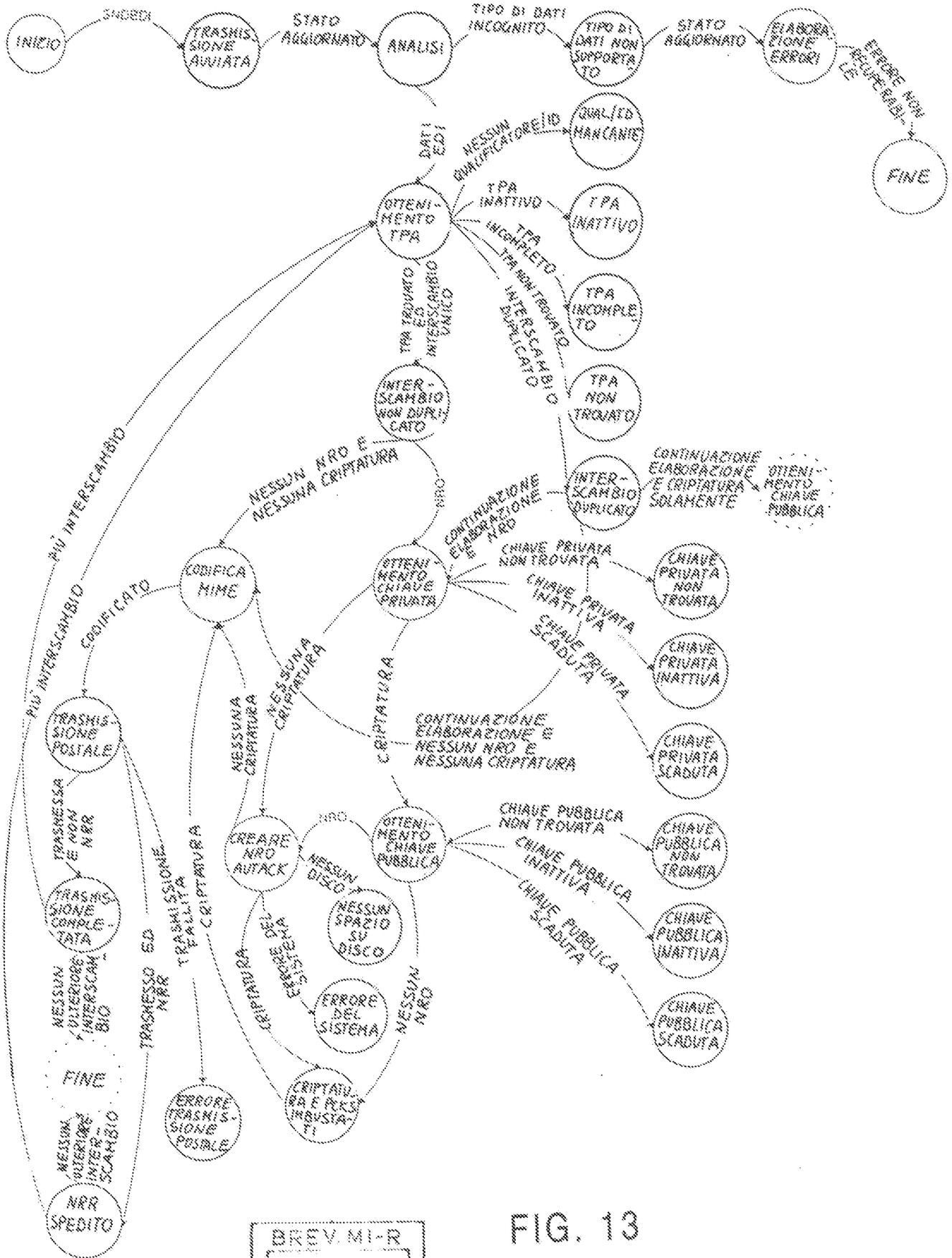


FIG. 13

BREV. MI-R
003072

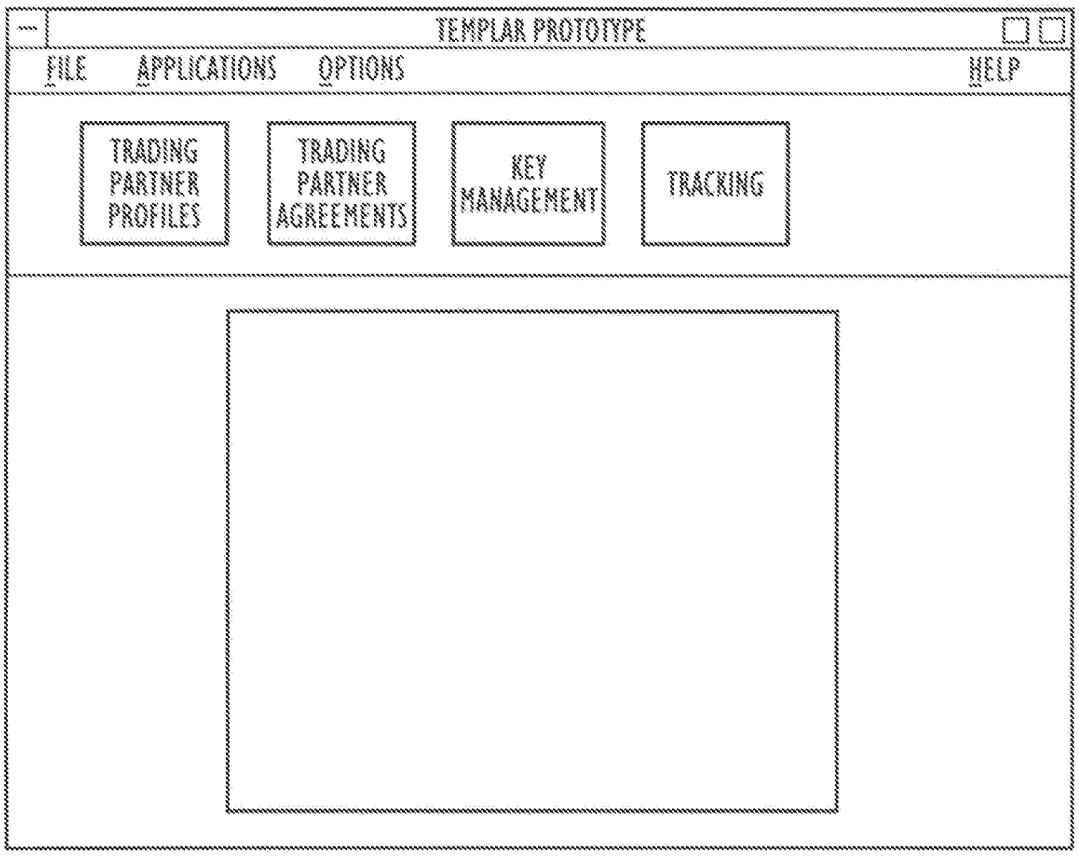


FIG. 14

BREV. MI-R
003072

HI 96 A-00 (5/9

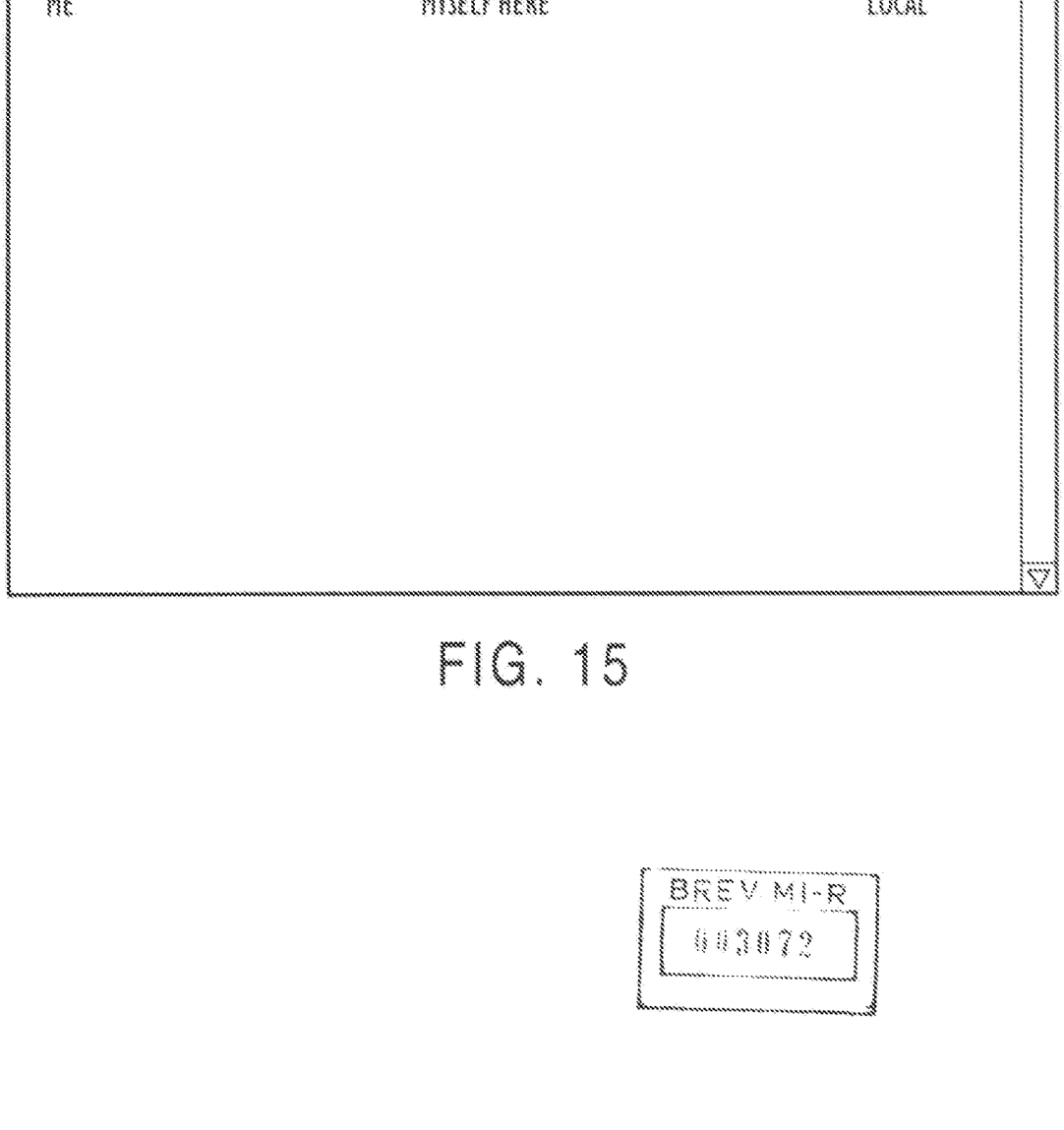


FIG. 15

BREVMI-R
003072

MI 96 A 001513

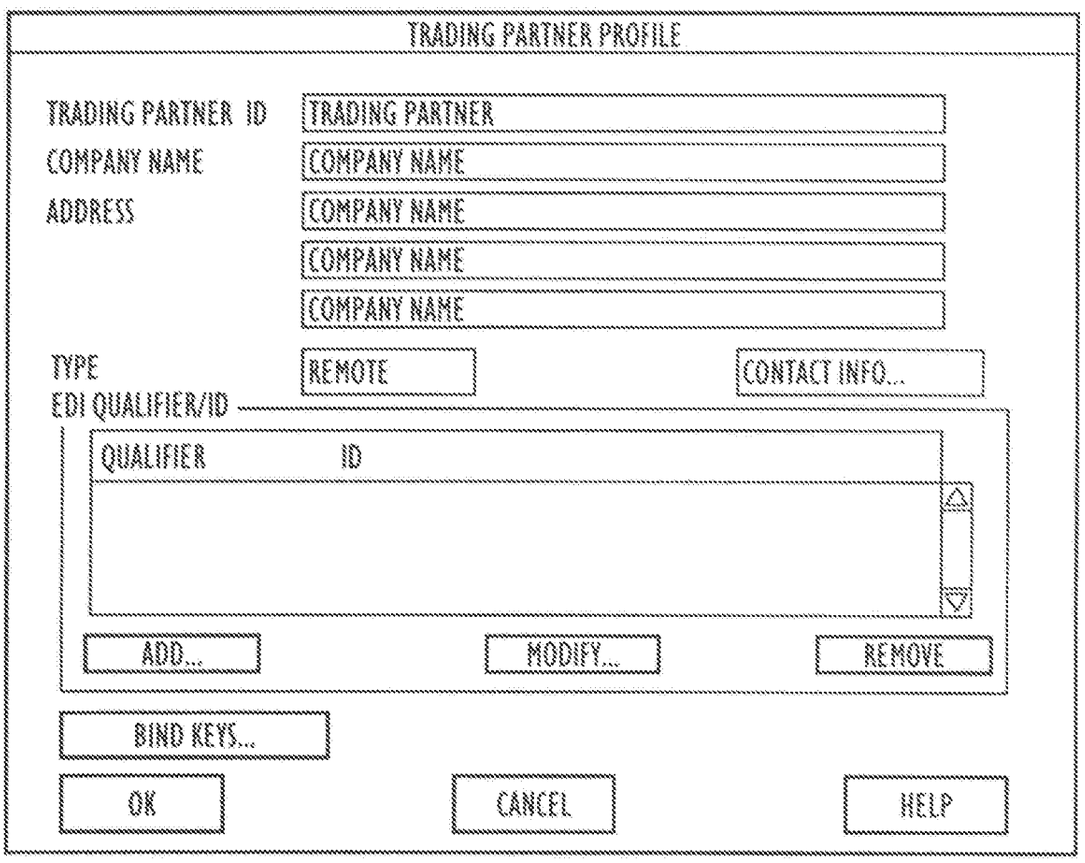


FIG. 16

BREV. MI-R
003072

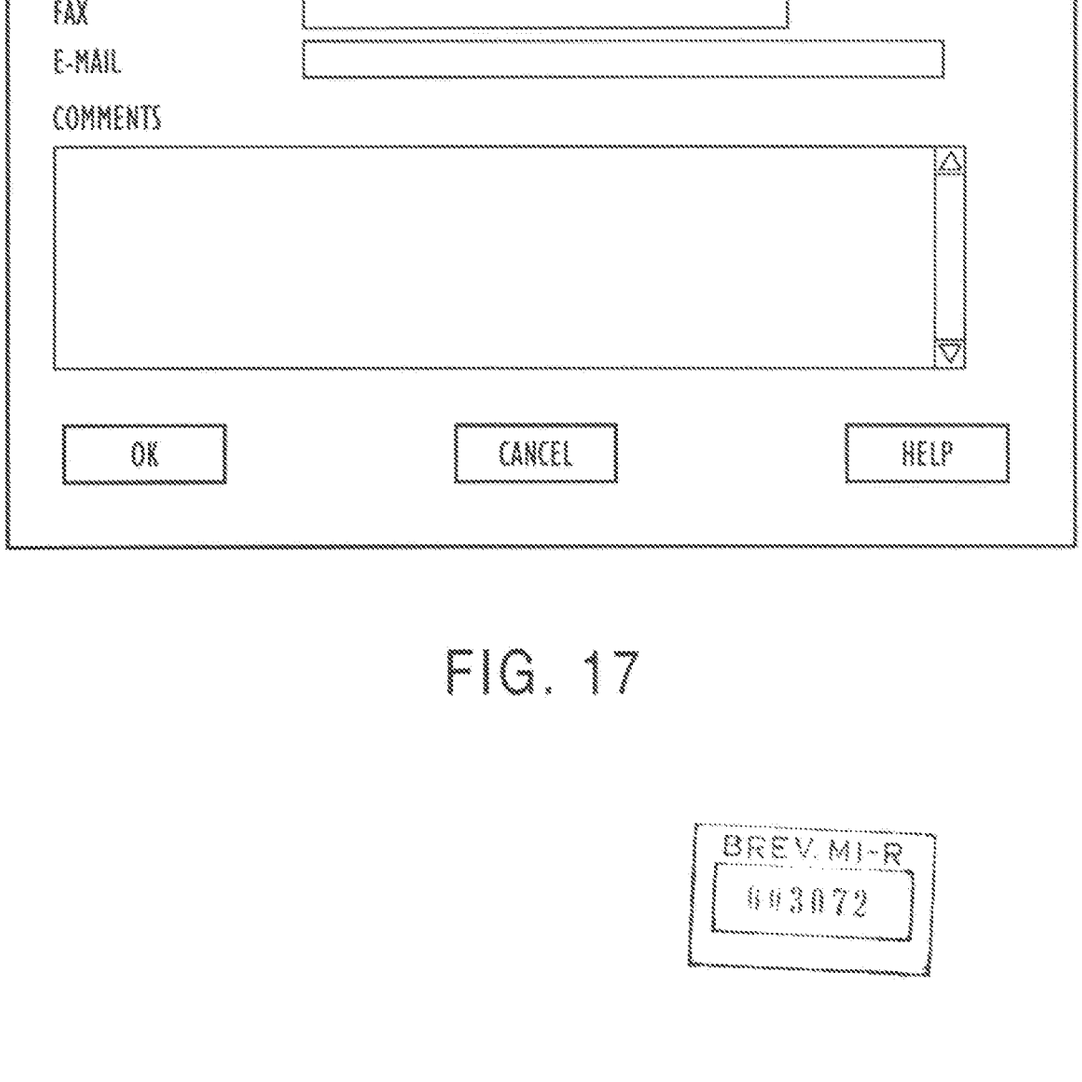


FIG. 17

BREV.MI-R
003072

MI 96 A 000519

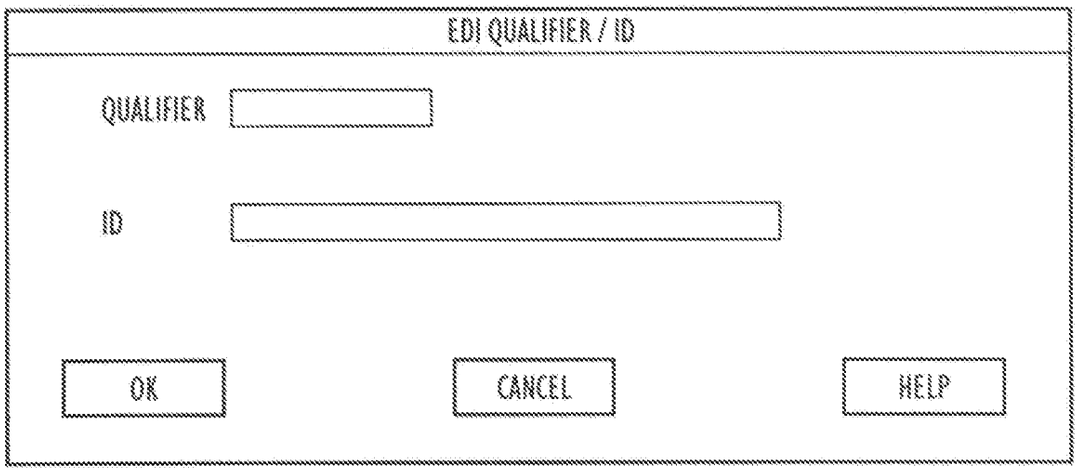


FIG. 18

BREV.MI-R
603072

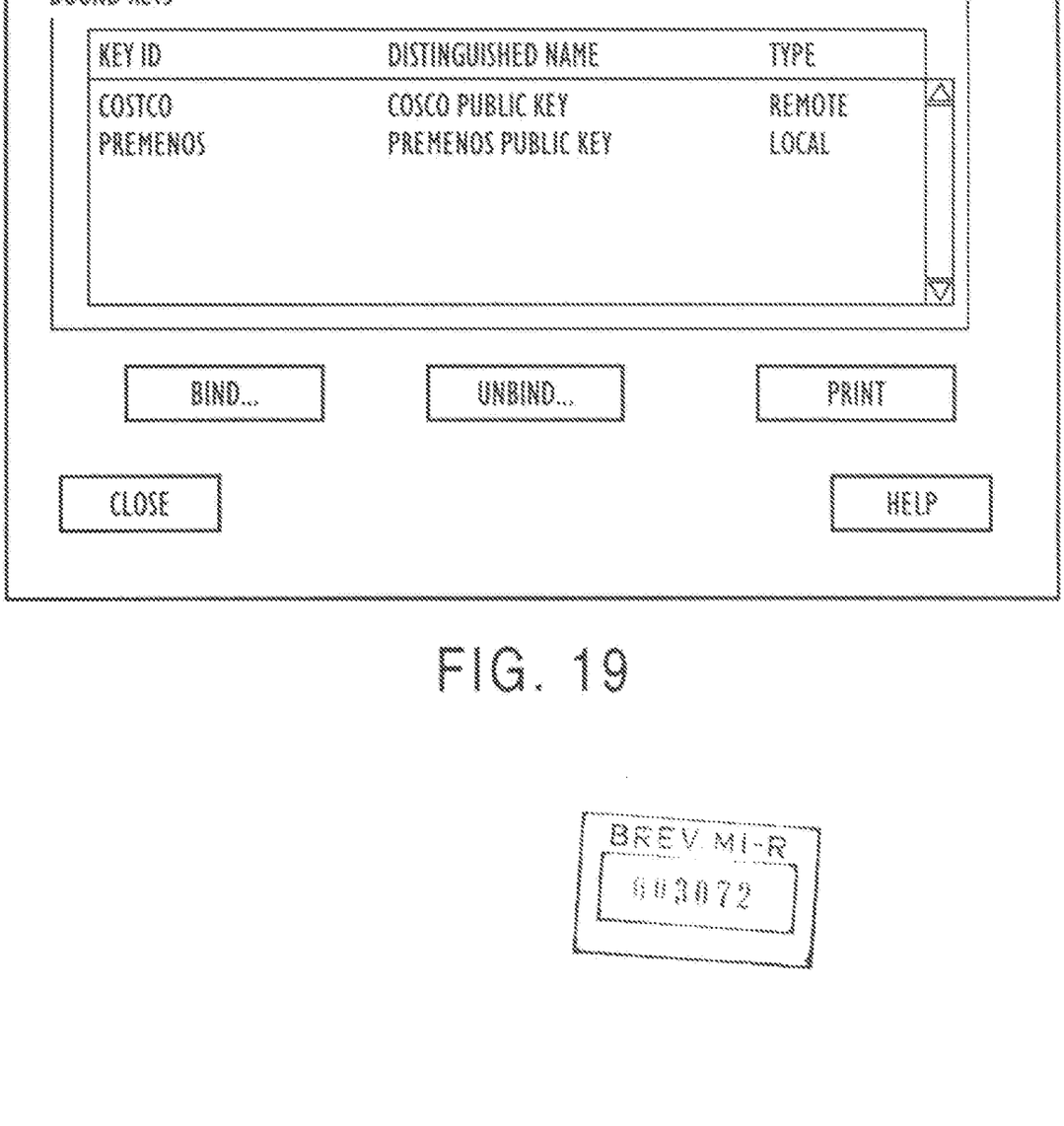


FIG. 19

BREVMI-R
003072

MI 36-A-00150

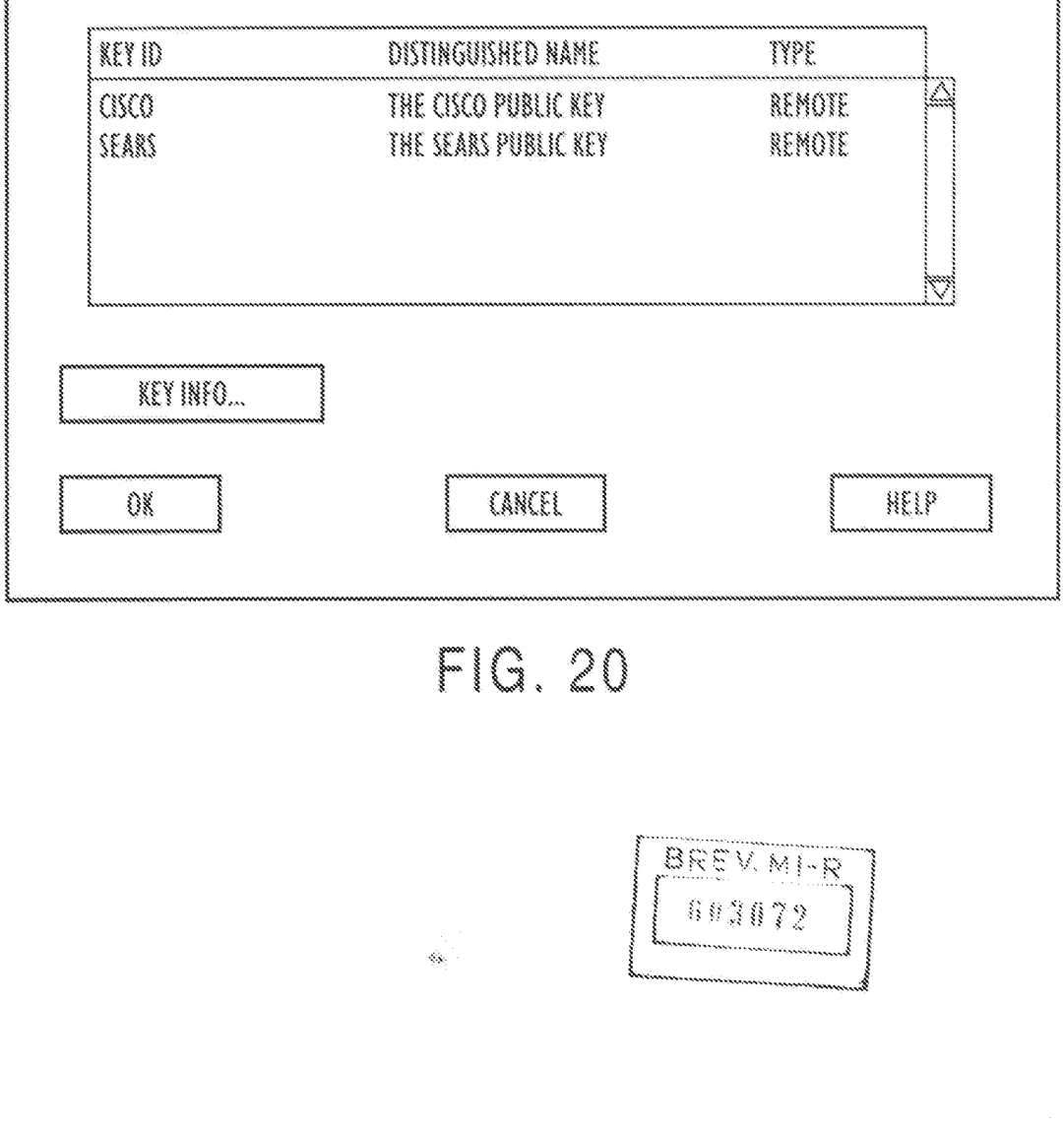


FIG. 20

BREVMI-R
603072

MI 36 A-001519

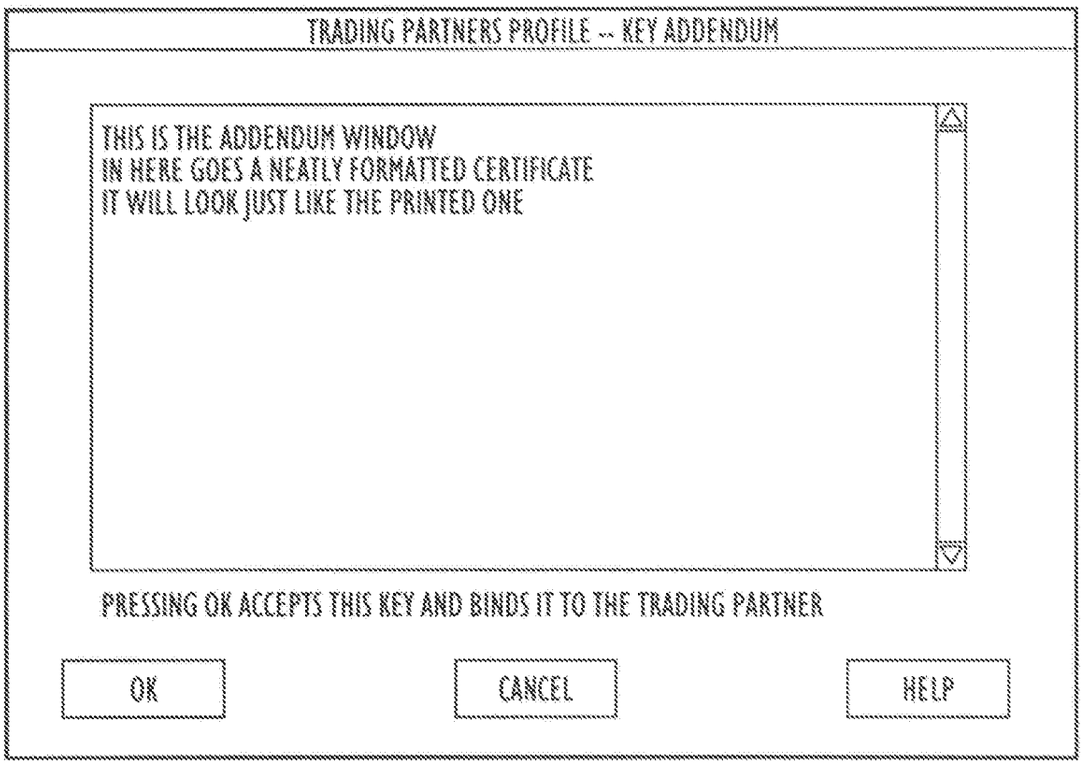


FIG. 21

BREV. MI-R
003072

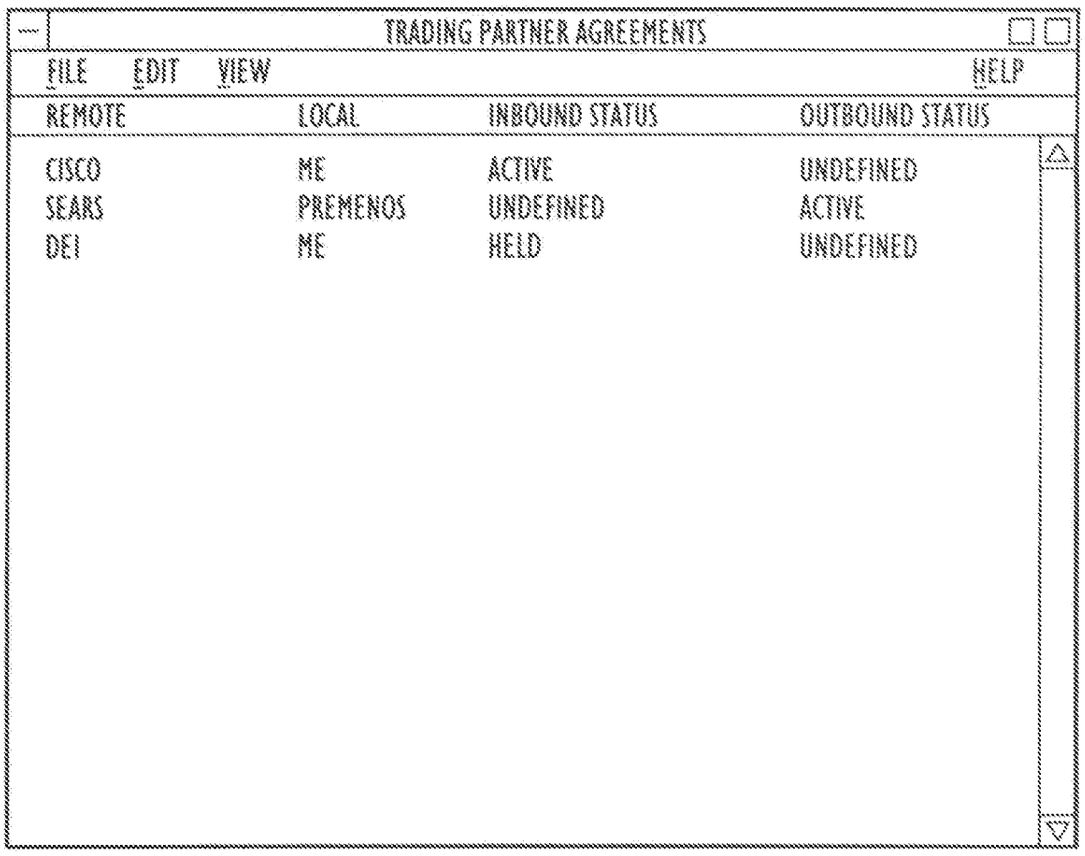


FIG. 22

BREV. MI-R
003072

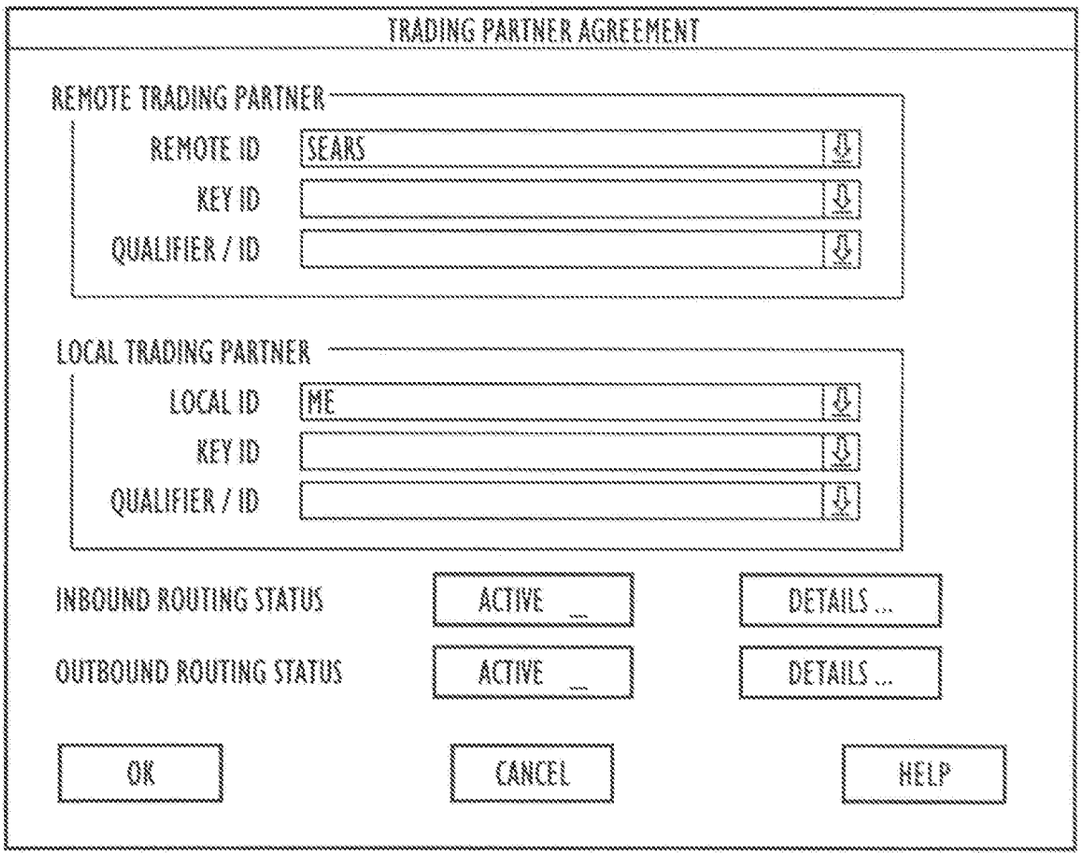


FIG. 23

BREV.MI-R
003072

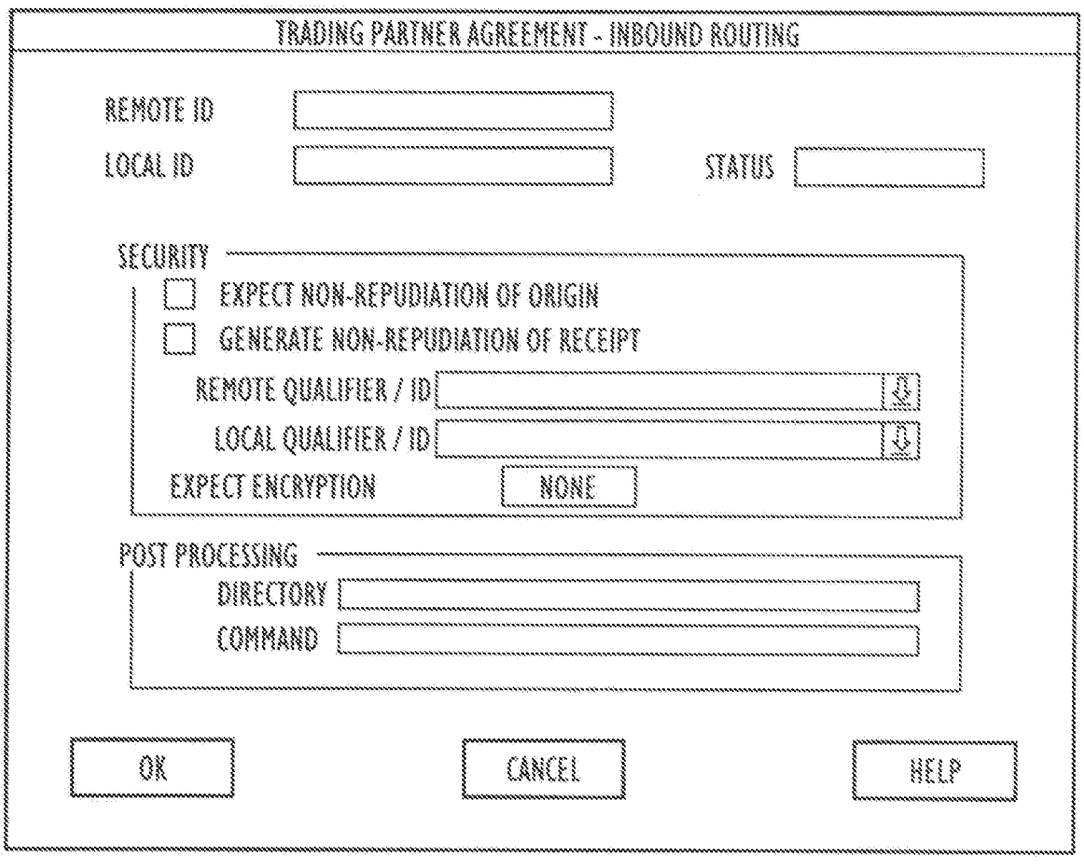


FIG. 24

BREV.MI-R
003072

MI 96 A 001510

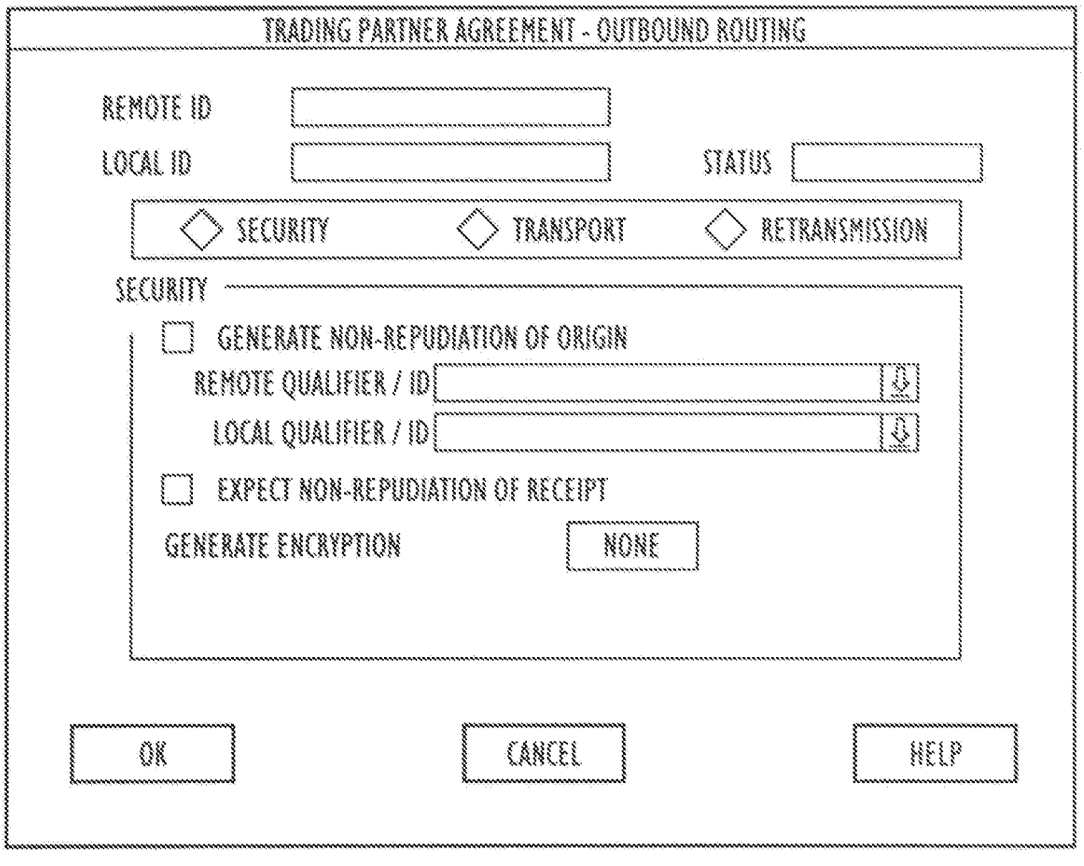


FIG. 25

BREV. MI-R
003072

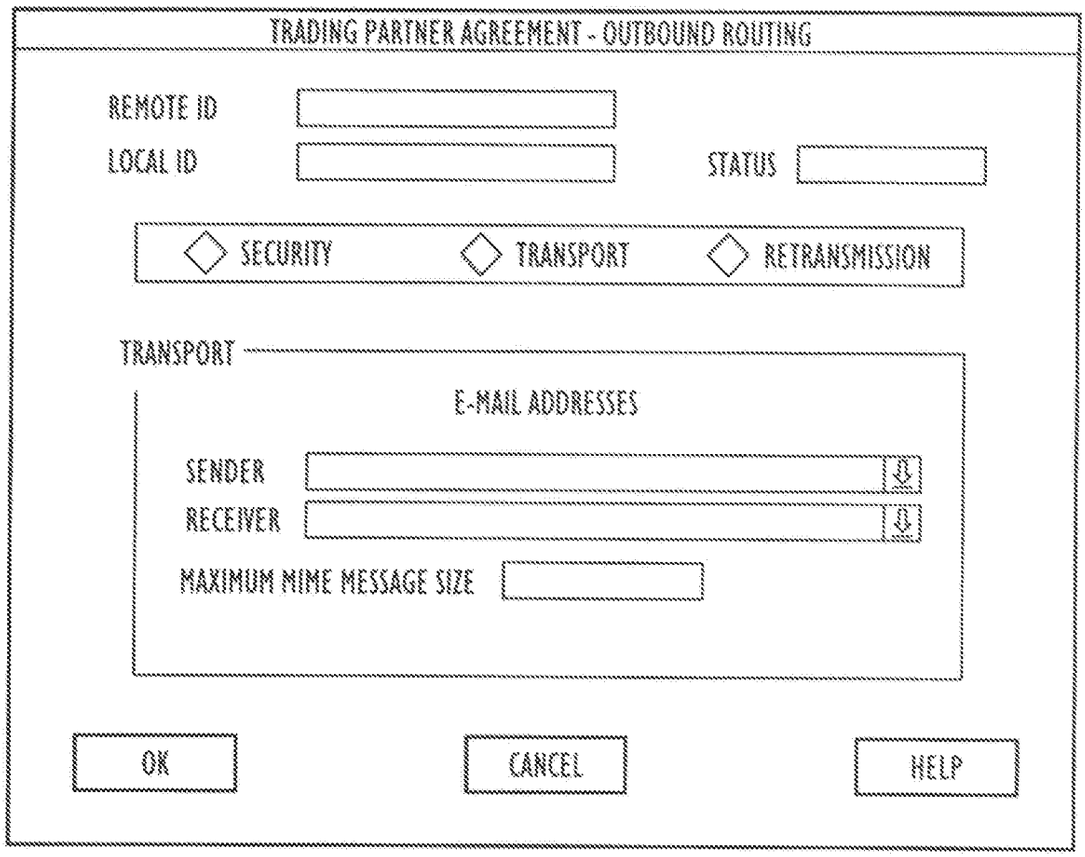


FIG. 26

BREV. MI-R
003072

MI 96 A 001503

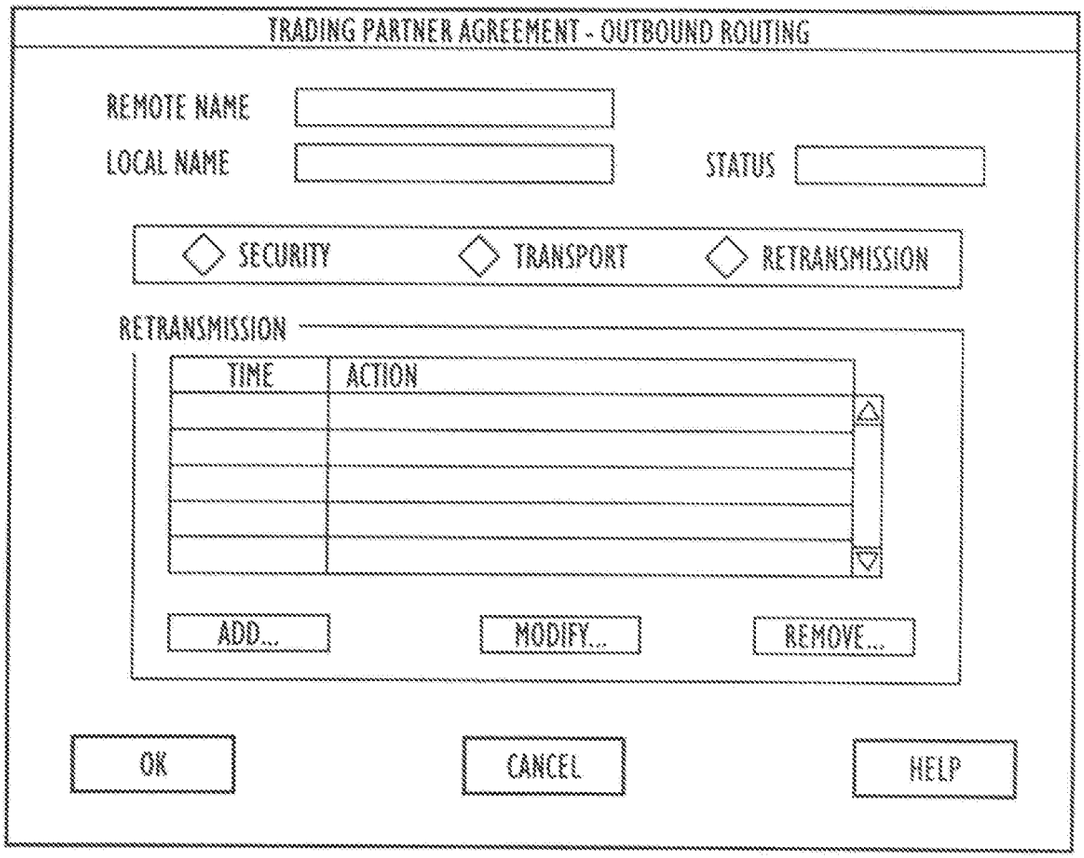


FIG. 27

BREVMI-R
003072

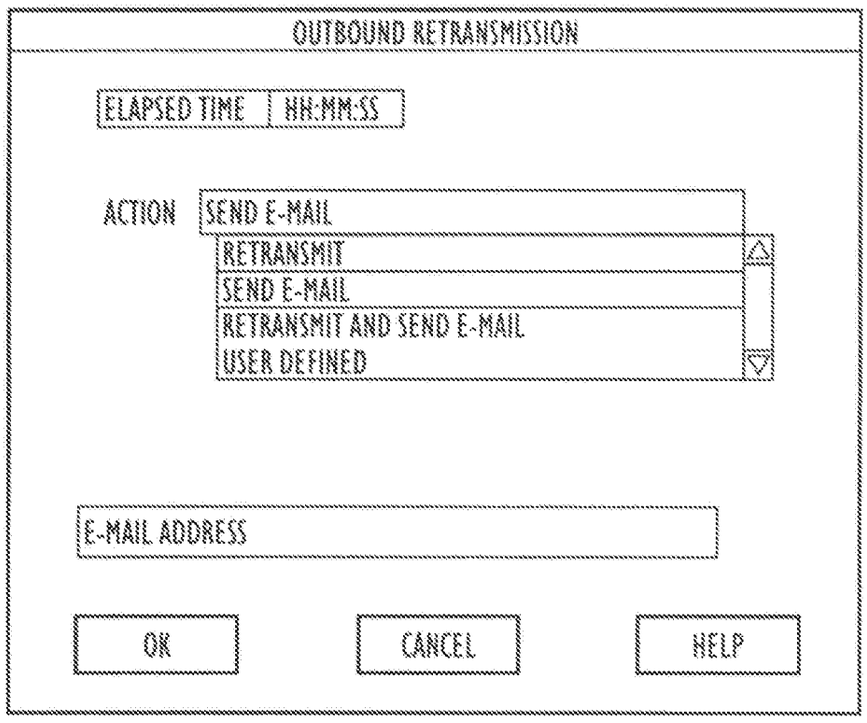


FIG. 28

BREV. MI-R
603072

MI 96 A-001619

TAV. XXIX

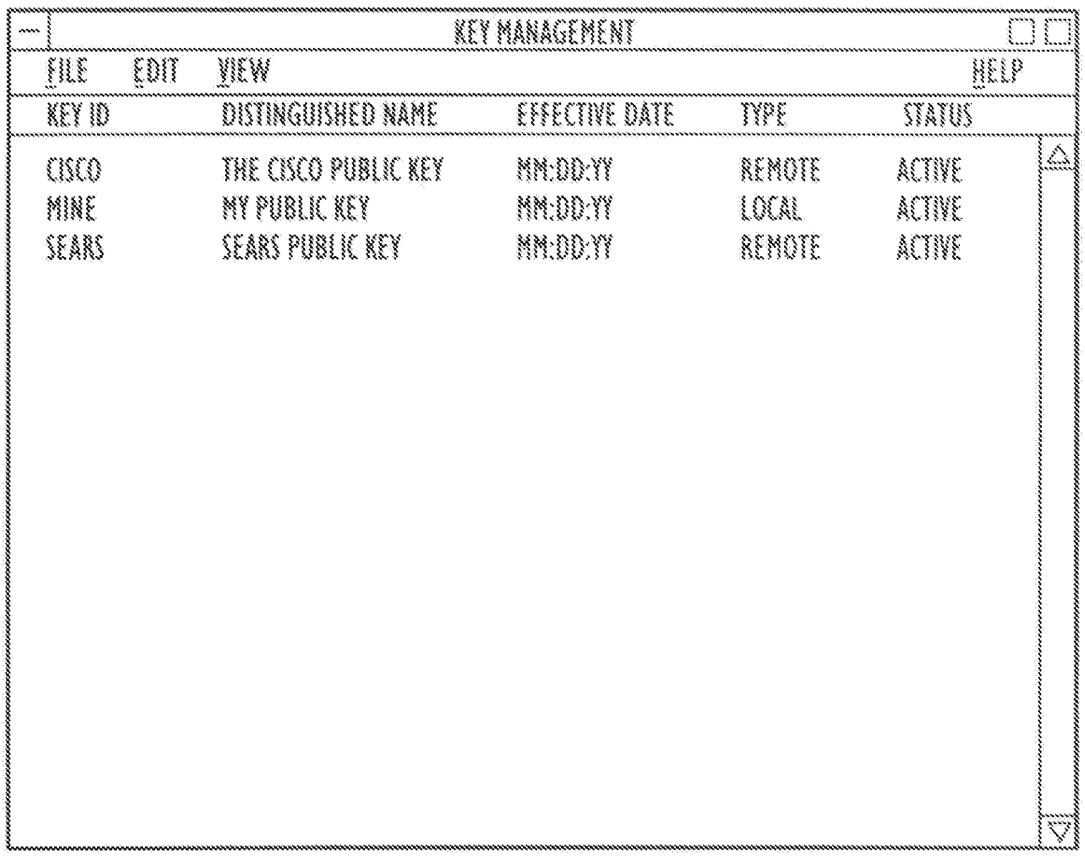


FIG. 29

BREV. MI-R
G#3072

MI 96 A-00513

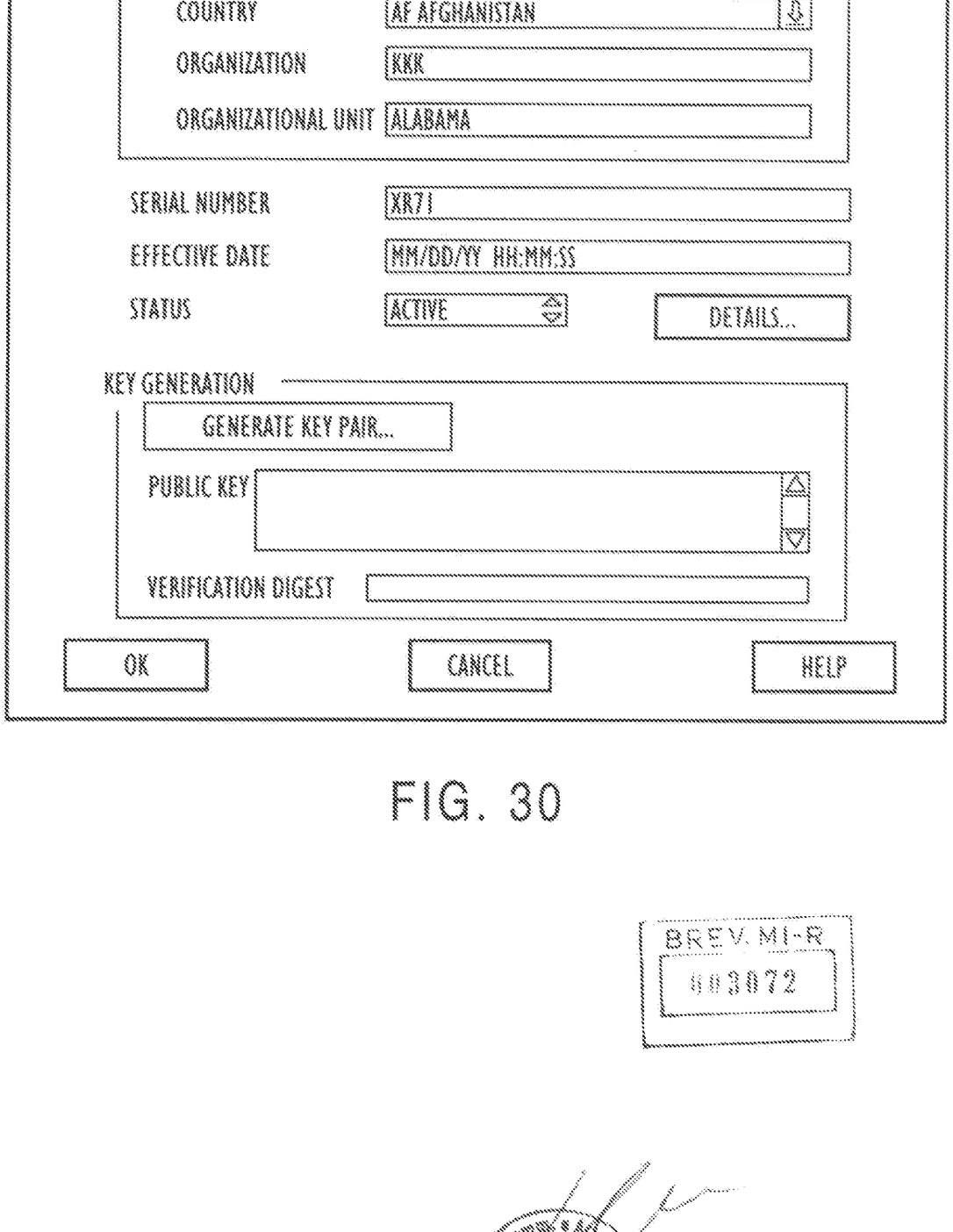


FIG. 30

BREV.MI-R
003072

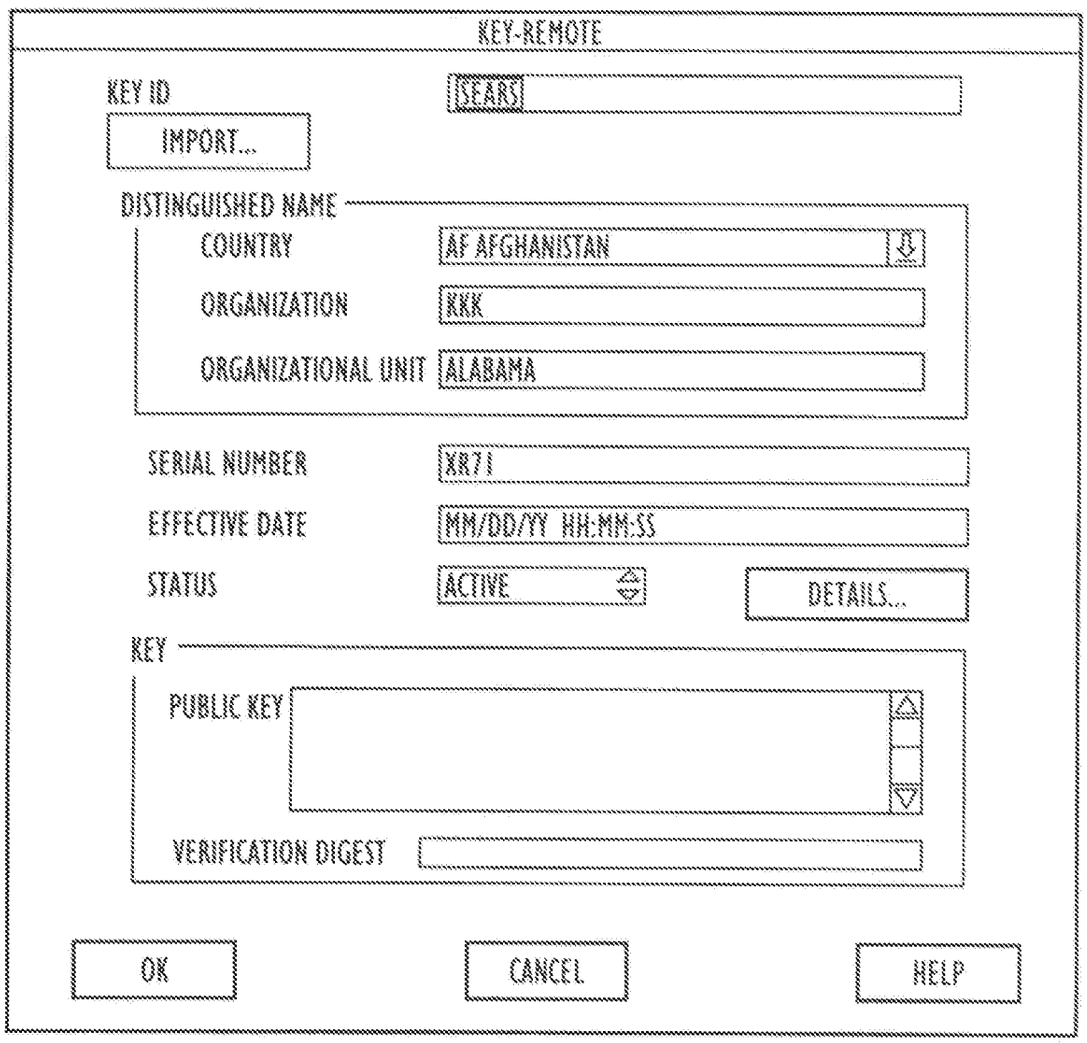


FIG. 31

BREVMI-R
003072

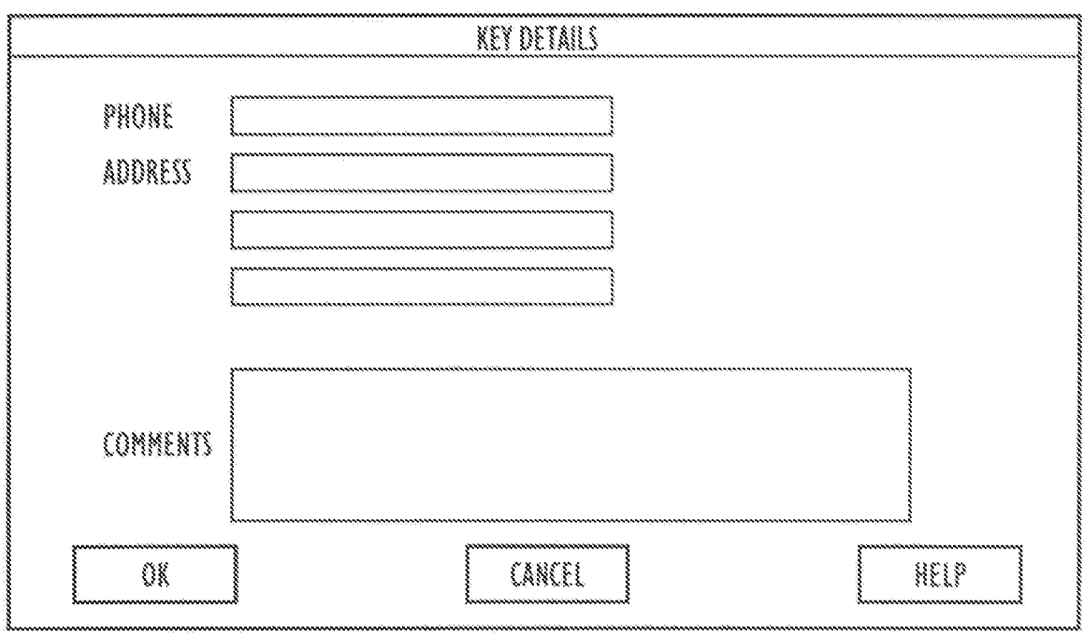


FIG. 32

BREV. MI-R
403072

MI 96 A-001519

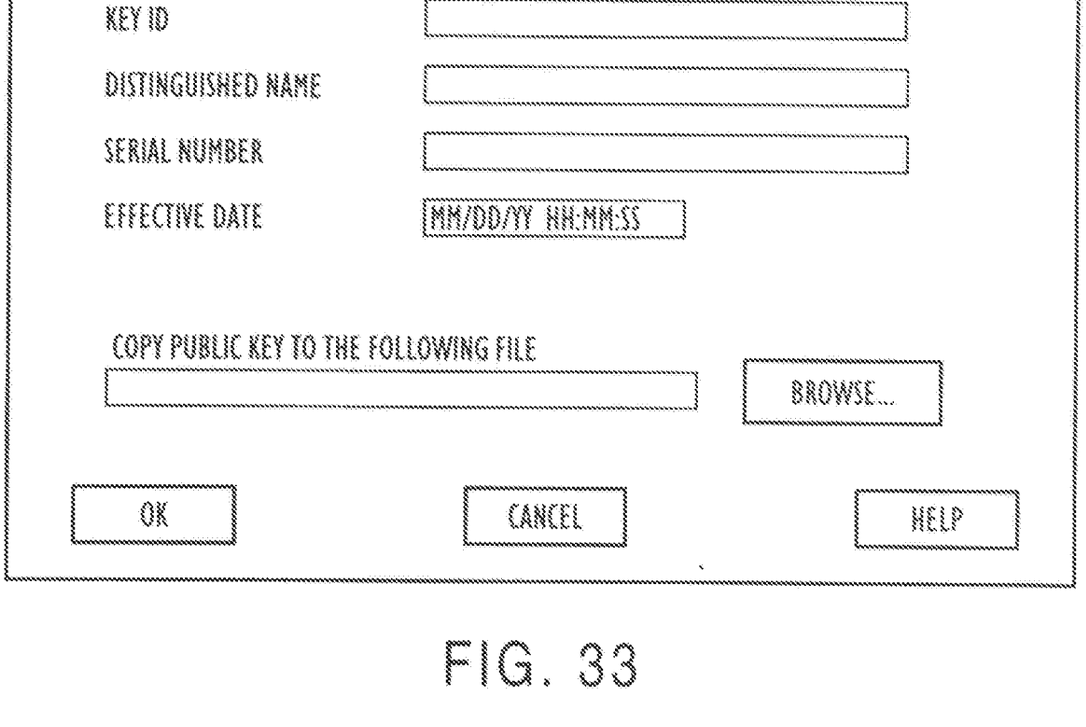


FIG. 33

BREV. MI-R
003072

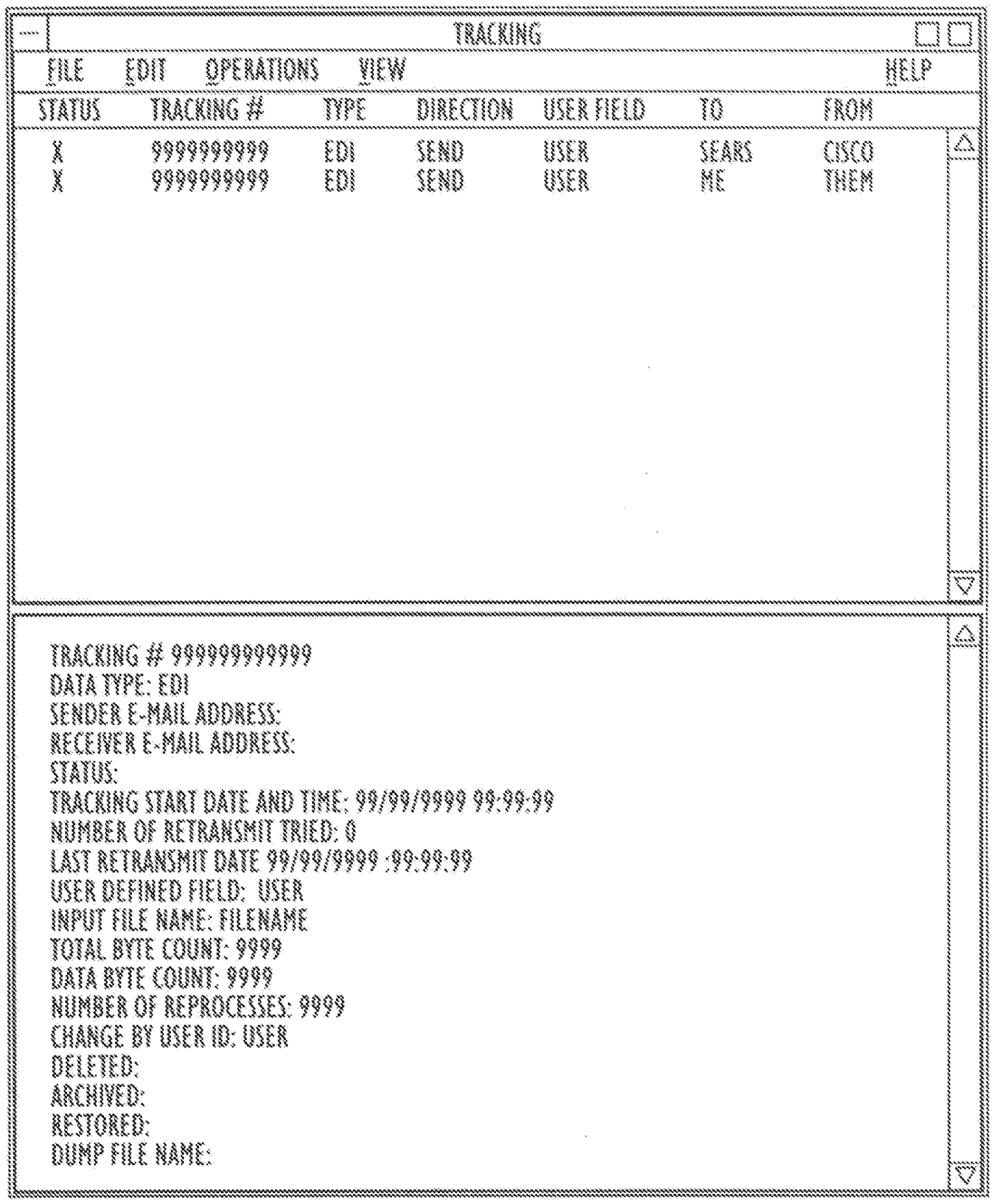


FIG. 34

BREVMI-R
003072

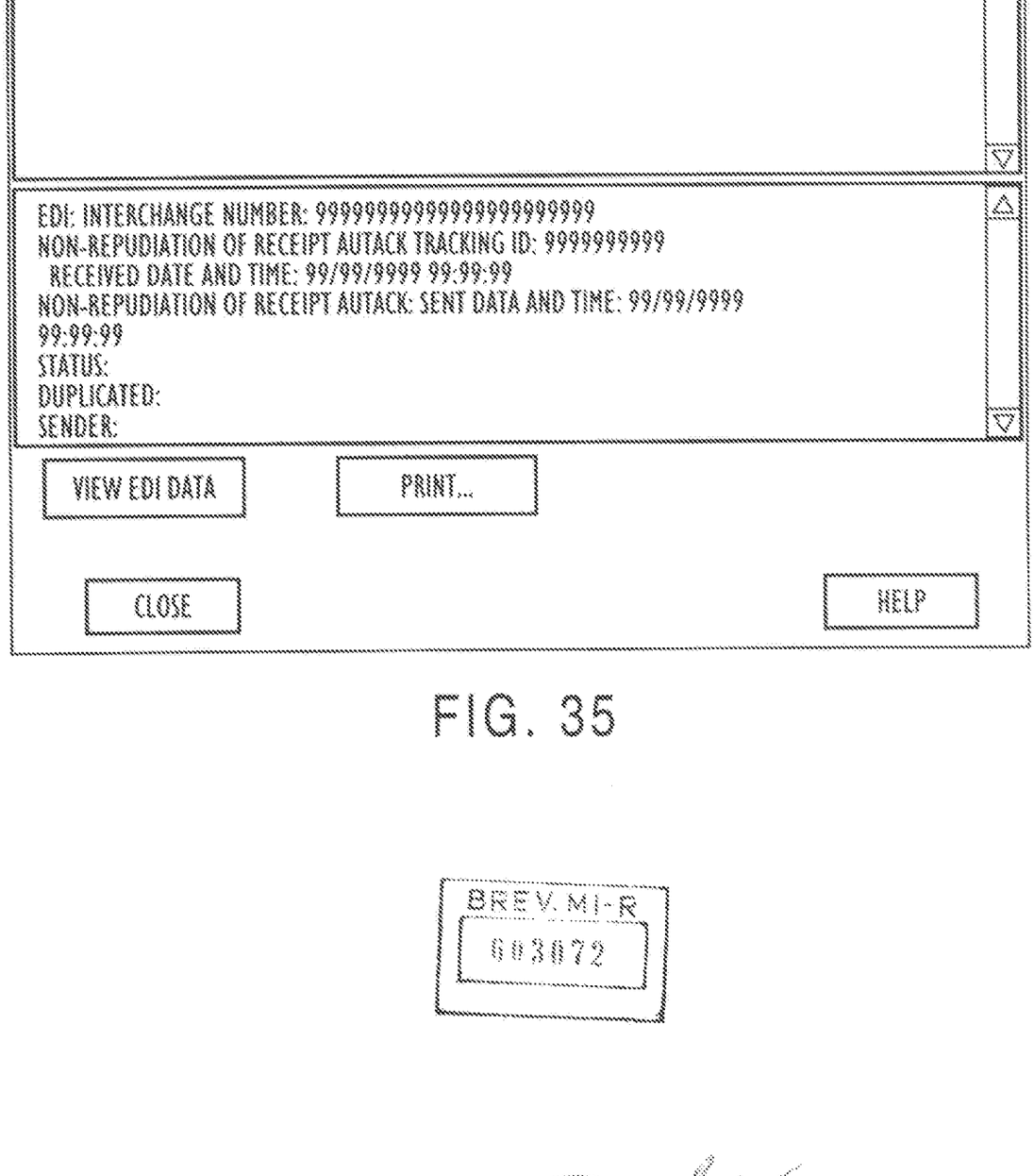


FIG. 35

BREVMI-R
003072

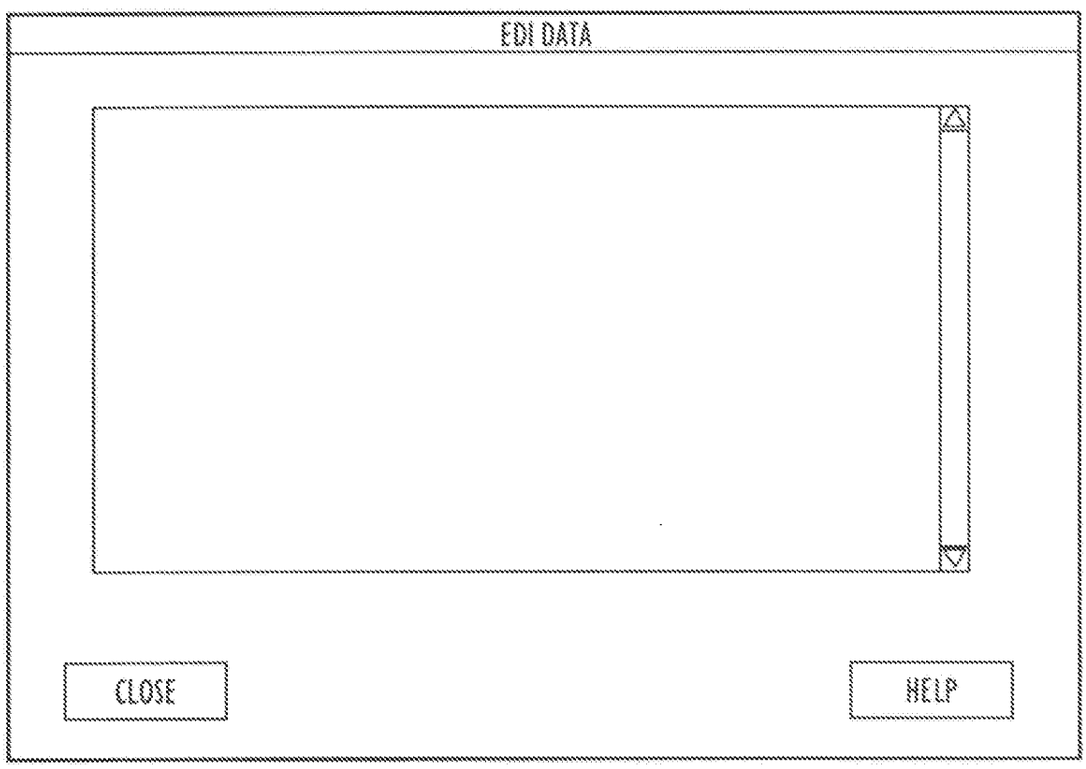


FIG. 36

BREV. MI-R
603072

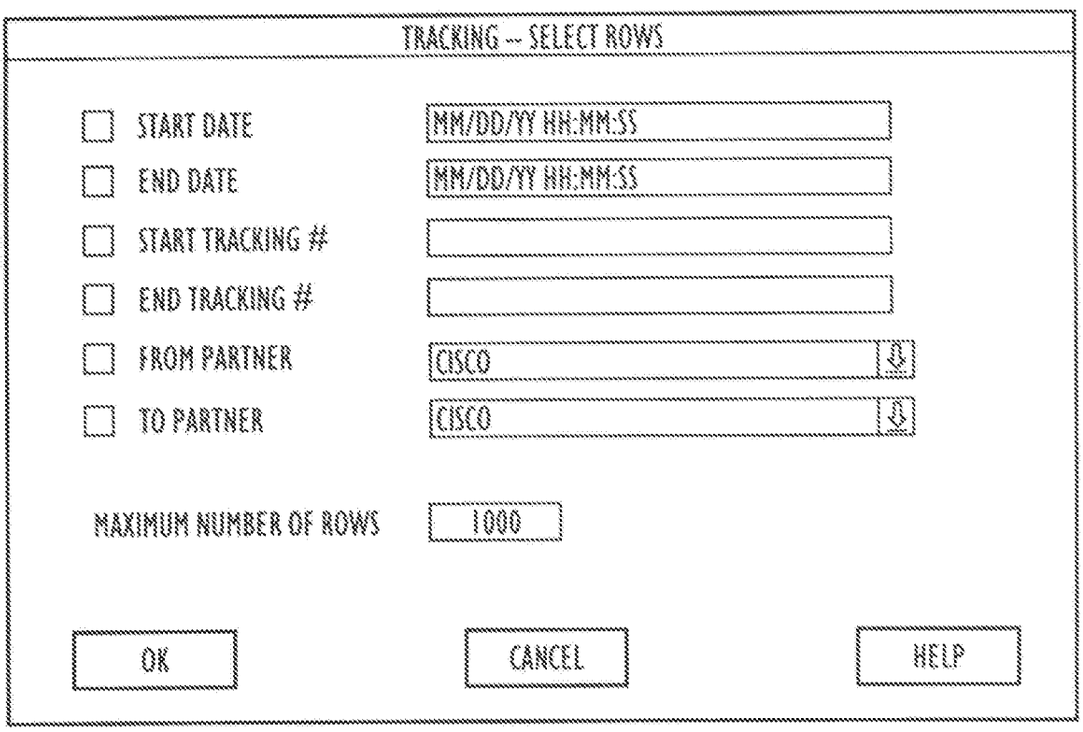


FIG. 37

BREV. MI-R
6#3072

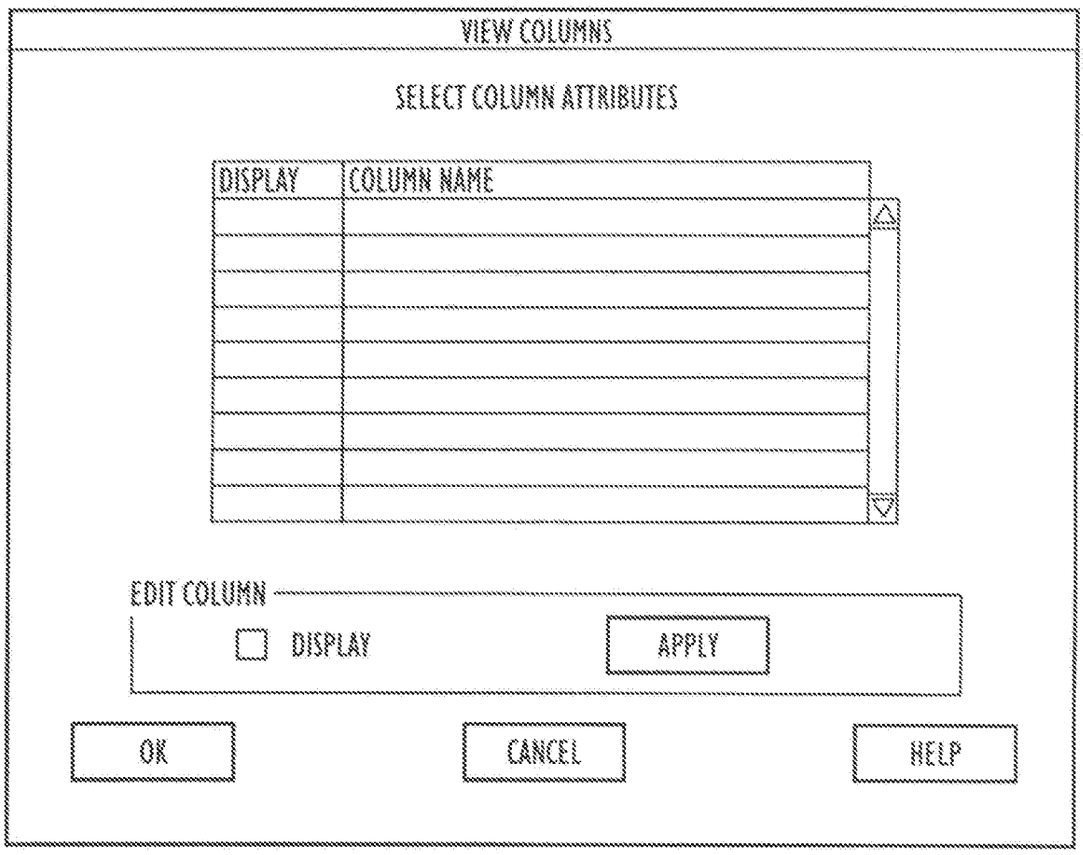


FIG. 38

BREV. MI-R
403072

HI 36 p-001513

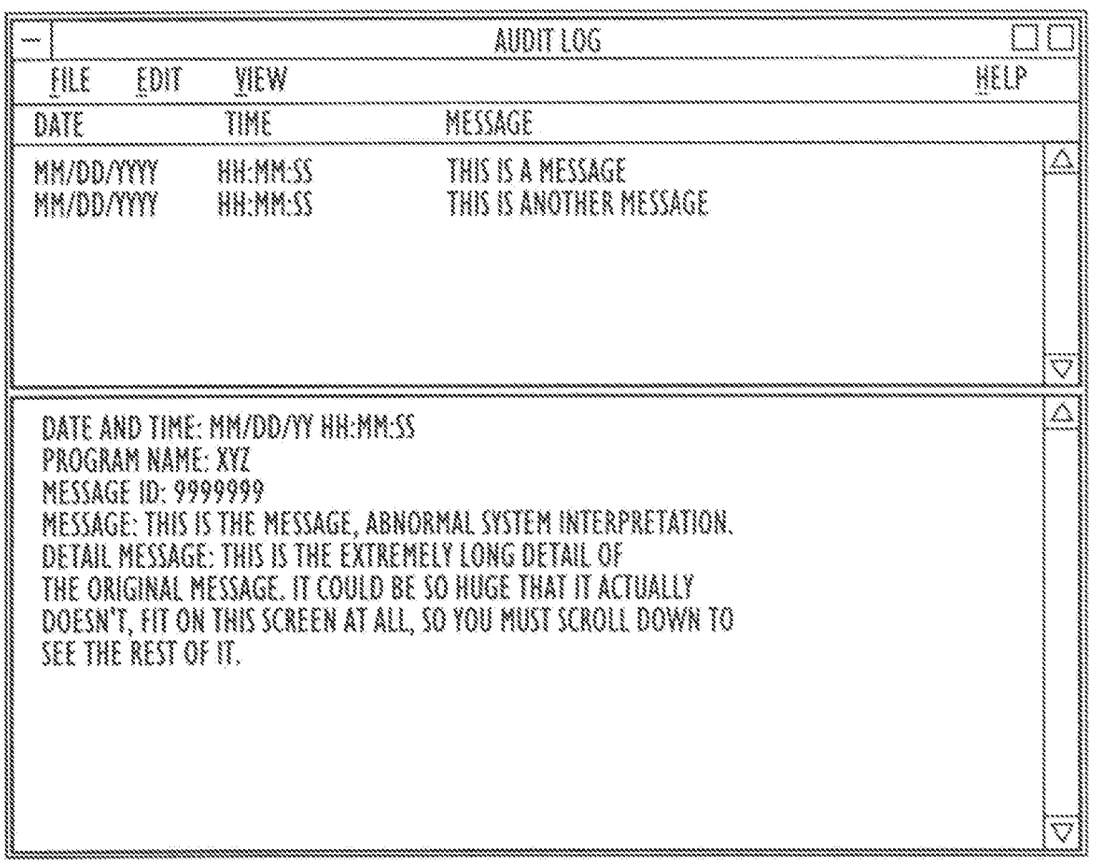


FIG. 39

BREV. MI-R
603072

MI96B.001519

TAV. XL

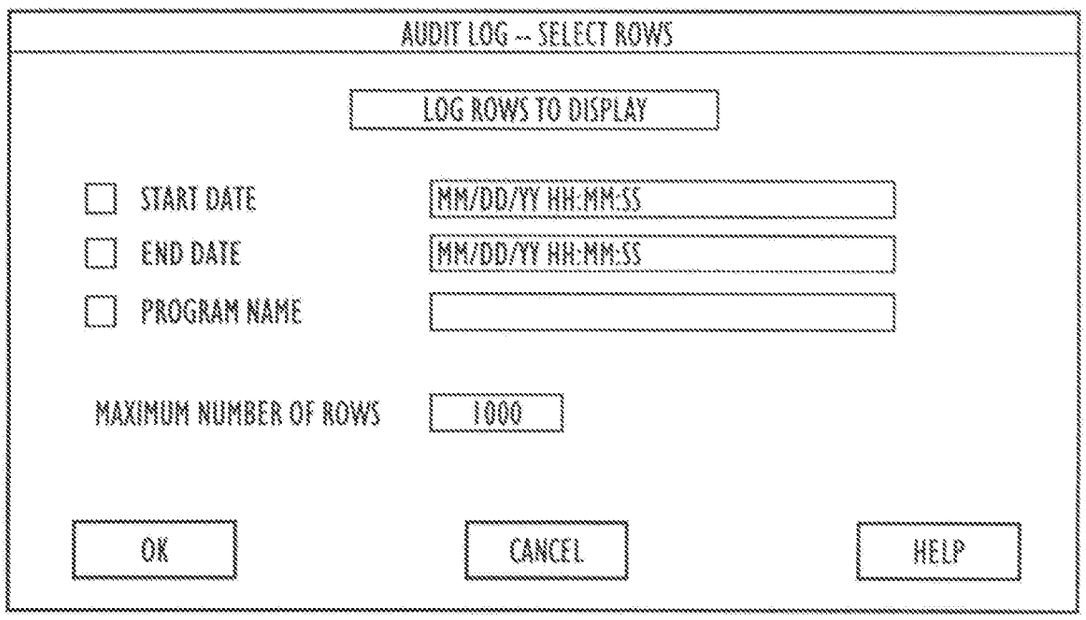


FIG. 40

BREV.MI-R
003072

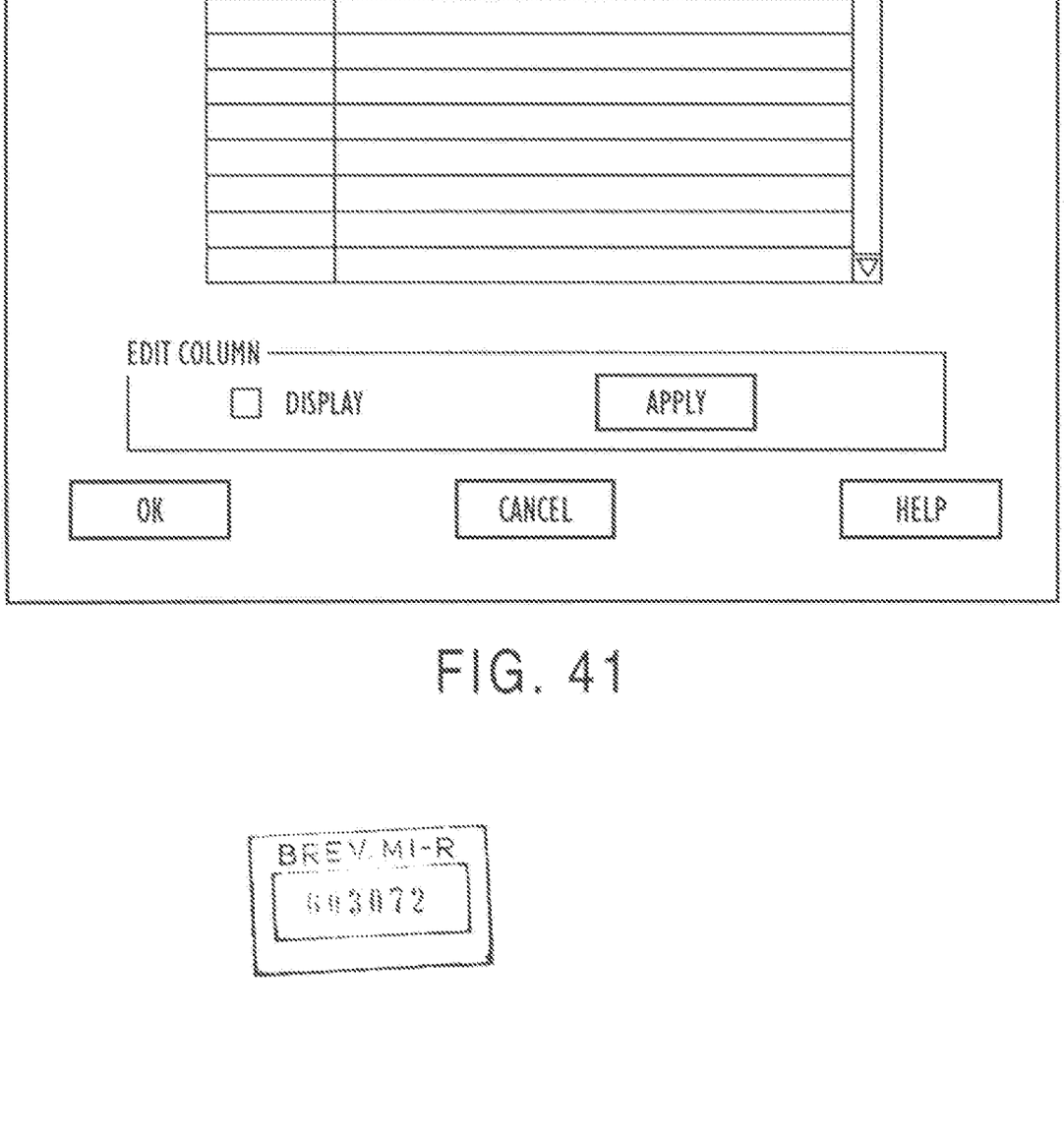


FIG. 41

BREVMI-R
603072