Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2305249 A1 2001/10/14

(21) 2 305 249

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2000/04/14

(41) Mise à la disp. pub./Open to Public Insp.: 2001/10/14

(51) Cl.Int.^{7}/Int.Cl.^{7} H04L 12/16, G06F 17/60, H04L 9/32, H04L 12/22

(71) Demandeur/Applicant:
SARCANIN, BRANKO, CA

(72) Inventeur/Inventor:
SARCANIN, BRANKO, CA

(74) Agent: FASKEN MARTINEAU DUMOULIN LLP

(54) Titre : COFFRE-FORT VIRTUEL
(54) Title: VIRTUAL SAFE

FIELD OF THE INVENTION

The present invention relates to the complete payment and fulfillment process conducted over a communication network, and more specifically, it relates to a secure virtual entity which comprises of purchase transaction, payment transaction, and shipping and delivery components. In total, the invention represents a process which executes a complete financial transaction for goods or services which previously was transacted with credit card, cash or other payment of goods, and subsequently fulfilled separately.

BACKGROUND OF THE INVENTION

The present invention relates to payment and fulfillment processes involved in completing a financial exchange of goods and/or services for monetary payment. The electronic process for implementing money payments and delivery is an alternative medium of economic exchange to cash, checks, credit and debit cards, and electronic funds transfer over an open network. The Virtual Digital Safe is a hybrid of secure encrypted digital communication, existing payment methods (including currency, check, card payment systems, and electronic funds transfer systems), fulfillment and clearinghouse processes for delivery of goods and/or services. The solution possesses many of the benefits of these systems with few of their limitations. The system utilizes electronic representations of money and shopping entities, which are designed to be securely housed in an independent digital environment from the remote shopper's computer terminal.

Today, approximately $US350 billion per year in online purchase transactions occur between individuals and institutions every year. The extensive use of the Internet for financial transactions has been limited by the risks due to fraud, misrepresentation, or incomplete fulfillment. Individual Internet transactions are burdened by the need to have the transaction occur securely, quickly, and in way that insures that all parties are in receipt of goods/services and payment. Furthermore, the handling and managing of credit/debit accounts is inconvenient for merchants, and delivery/fulfillment is costly and time consuming for both merchants and financial institutions.

Although online transactions may be carried out under specific secure circumstances, such as the use of Secure Sockets Layer (SSL), this method is very limited in its lack of authentication of purchaser and control of fulfillment process. The existing Internet transaction methods decouple payment

and fulfillment and hence rely on multi-system solutions, which are not necessarily secure.

System, method and article of manufacture for network electronic payment, credit collection utilizing a payment, and remote secure storage of fulfillment processes.

An electronic inter-networking payment system provides for transactions utilizing an electronic payment system that emulates a wallet or a purse that is customarily used for keeping money, credit cards and other forms of payment organized.

Access to the instruments in the wallet or purse is restricted by a sophisticated encryption and authentication method to avoid unauthorized payments. A successful cryptographic authentication is required in order to obtain an access to the wallet or purse.

The authentication protocol obtains the information necessary for creating a network session granting authority to utilize an instrument, a payment holder and a complete electronic wallet. Electronic approval results in the generation of an electronic transaction to complete the order.

Upon selection of a particular payment transaction by the user, a particular transaction notification will be generated based on the order. The transaction notification is processed by means of a secure connection to a transaction server. The transaction server consists of the required elements for order fulfillment, including connectivity to: credit card issuer, acquiring bank or funds-holding institution, product or service merchant, delivery provider, and the user or customer account.

An electronic payment transaction is generated in a computer-based method for effecting a transfer of funds from an account of a payer in a funds-holding institution to a payee. The electronic instrument includes an cryptographic digital signature of the payer, digital representations of payment instructions, the cryptographic authenticated identity of the payer, the identity of the payee, and the identity of the funds-holding institution.

The invention is more clearly explained as follows:

1. Executive Summary

There currently exists a large unmet need in the area of e-commerce. An enterprise with the ability to resolve all of the security, privacy, convenience and cost impediments that exist with online commerce will have the power to profoundly change the status quo.

VirtualSafe is in the business of making it exceptionally easy and virtually risk-free for businesses of all sizes to engage in e-commerce. It accomplishes this by providing technology and relationships to online buyers and sellers, which creates a frictionless transaction environment.

To potential online sellers of goods and services, VirtualSafe makes it exceedingly easy to build a website. However, the Company also "fronts" the merchant relationship with appropriate credit card companies. Further, VirtualSafe will provide pre-arranged logistics services through companies such as FedEx, UPS, Purolator, etc. The setting up of such arrangements can be time-consuming and costly for a typical small business, and thus it remains a significant barrier to entry to e-commerce.

Beyond the above services however, VirtualSafe also provides blanket fraud insurance to the merchant which mitigates a risk which has become a very major concern to merchants, credit card companies and consumers alike.

VirtualSafe has successfully combined a number of technologies which in turn are based on the public key infrastructure (PKI). This combination of technologies is at the heart of what enables VirtualSafe to stand out from all of the other Internet Privacy endeavours that have arisen. The technology enables VirtualSafe to register consumers' personal data (ie: credit card information) once and then issue a digital ID to that individual. Henceforth the consumer never has to enter their data online again, an obvious attraction to consumers. The data is then held in a database file in a highly secure server site.

All parts of a transaction are then in essence routed through the Safe, with private data being protected. A purchase can then be made with all interested parties, (merchant, credit card issuer,

bank, couriers) seeing only information that is absolutely pertinent to their role. At the same time, the programming ensures that it is exceedingly unlikely that anyone other than the credit card holder could execute the transaction. In fact VirtualSafe estimates that, using their technology, online fraud would be reduced by at least 90%.

Combining all three of these features (security, privacy, and ease) makes VirtualSafe unique in the realm of e-commerce enablement. VirtualSafe believes it has a sufficient technology lead to enable it to embark on a branding plan, which will give it a commanding presence in this market. As this is accomplished, the company believes it can further enhance revenues by increasing market share as well as by adding related services.

Digital Certificates

Definition & Benefits

Public Key Infrastructure (PKI)

Definition - PKI is the infrastructure that makes certificates work…

Certificate Advantages

- Cost
- Portability - option of file or smart card (how realistic is smart card)
- Liability - Lloyds of London Insurance

SET

Safe has to be SET compatible

Remote SET functions with PC smart card interface (pointer)

The overall platform and architecture objectives of the Virtual Safe solution are:

- **Maximum Security** to ensure that access to the system meets "world-class" security requirements, to meet or exceed requirements of financial, government and other security concentric organizations.

- The solution should allow implementation on platforms that require fault-tolerance, scalability and high-availability. All Denial Of Service vulnerabilities should be investigated and minimized.

- To create a solution where platform does not become an issue/consideration. This will eliminate a 'stove-pipe' deployment of applications, which require their own serving environment.

- Safe internal revision storage with optional external supervision

- **Maximum speed** and efficiency to ensure that the authentication system ensures only a minimum amount of time is required to complete the authentication of an application or individual.

- **Maximum scalability and flexibility** to allow the virtual Safe to support the addition or deletion of data as required. This will allow the ability to store and retrieve data such as credit card processing information, authorization level access control, Air Miles information, Medical Information, remote signing of documents, file encryption etc.

Security Architecture

The "Virtual Safe" security architecture involves multiple layers of protection comprised of four different areas.

1. **Server Protection:** includes operating system level protection, application tampering monitor tools, assurance and verification, and server level intrusion monitoring tools.

2. **Physical Site Protection:** involves using a world-class security facility and data center to host the hardware. E-Certify's security and data center is an example of such a premise, will require additional security requirements.

3. **Firewall Defense:** can include access routers, multiple firewalls, LAN switches, and intrusion monitoring tools at the network level.

4. **Application Security:** provides a role-based mechanism to control data access in the Virtual Safe system.

Application Security

Application Architecture Overview

The "Virtual Safe" software application system uses web servers that process HTTPS transactions from clients communicating over the Internet and Extranets.

Any sensitive data entered by clients will be conducted over a secure channel using 128-bit SSL encryption via web server certificates.

The web server will authenticate to connecting clients using a Server Certificate issued by a certified and trusted CA such as E-Certify. This guarantees users that they are indeed connecting to the Virtual Safe web pages. This authentication is performed within the SSL protocol implemented in the Web Server.

* Safe will use Elliptic Curve Encryption inside of Virtual Safe

Application Logging

All functions performed by administrators of the Virtual Safe system will be written to log files, and placed in a secure database. All relevant transactions and events performed by officers will be placed in digitally signed log files, produced daily. All database fields that contain sensitive information are stored in encrypted form, and are decrypted only when made available to authorized administrators. Log revisions (before and after) will be automatically copy to revision server. Additionally to this will be in existence supervision access read only.

The logs will contain timestamp, administrator name, role, app name, and event type name and description information. The "Security Log Application", a secure application will allow for the viewing of log files. It will support the ability to verify the Digital Signature on the log file to ensure log files have not been tampered or modified.

Real-time Security Alert System

The "Real-time security alert system", will provide the ability for authorized administrators to review and monitor any security breaches or attacks on the system. All failed logon attempts will be logged within the system, and viewable only by authorized administrators using again revision server capability.

The security system will support different levels of notification including e-mails and possibly audible alarms.

Data Transmission Security

The "Virtual Safe" communication and transmission security will ensure encryption of all information whenever that information is transmitted within or outside the secure production network.

When transmitting data, to a browser for display, "Virtual Safe" currently allows either SSL 40-bit or 128-bit encryption, configurable on an application basis. The stronger SSL 128-bit encryption is required for all administrative access to services.

Link to Hot sites will be additionally secure use Elliptic Curve Encryption's and additional use of possible biometrics.

Digital Certificates

The Virtual Safe secure solution uses digital certificates for both server and client authentication. The SSL protocol implemented in the web server and browser software makes use of certificates for HTTP session encryption;

The Virtual Safe supports certificates in X.509 format, with the RSA asymmetric encryption algorithms. Second phase will implement Elliptic Curve Algorithm.

Scope

This section shall explain what the Virtual Safe will and, if necessary, will not do; and describe the application of the software being specified to include a description of all relevant benefits and objectives.

Payment Profile

The virtual Safe can act as a simple yet secure payment solution. It will allow individuals the ability to store their credit card information in a secure location, available for use when performing online purchases.

Users will be able to identify all information required for online shopping sites once to prevent having to enter the same information repeatedly. This reduces the time required to make online purchases, and makes the purchase experience much more user friendly. This will reduce or eliminate purchases failing due to typographical errors when users enter their payment and shipping information.

The information that can be entered to ensure payment and delivery of online purchases is as follows:

Description	Shipping Information	Billing Information	Receipt Information
Title			
First Name			
Middle Name			
Last Name			
Street Name			
City			
State or Province			
Zip or Postal Code			
Country			
Phone			
E-mail			
Drivers License #			
SIN			

Credit/ Debit Card Information
Name on Card
Card Type
Card Number
Card Holder Verification Value
Card Expiration Month/Year
Card
State or Province
Zip or Postal Code
Country
Phone
E-mail

- MULTIPLE credit CARD OPTION
- Multiple Identification options

Corporate Profile

The corporate profile, allows organizations and company's to store in a single location, authentication, authorization, and access control information in a single location. For example once a user is authenticated, the applications or access they have to services or

applications can be located in their corporate profile. This has the benefits of storing access information in one location. When users leave organizations or their access changes, it can be performed in one location.

Authentication and Identification Requirements

The first requirement is for individual user identification. Second, there is a need for authentication. Without authentication, user identification has no credibility. Without a credible identity (no) security policies can be properly invoked because there is no assurance that proper authorizations can be made.

Allow "Virtual Safe" holders the ability to access the safe via *two-factor authentication,* something they physically have and something they know. A Digital Certificate is the physical item a user will have to present. The item they will have to know will be an item they have identified in their "Virtual Safe".

Some high-security institutions like financial companies and hospitals assign passwords instead of letting users choose, or force users to change their passwords every 30 or 60 days, which results in periodic spikes in reset calls to technical support staffs.

Smart cards, which carry digital signatures and are used for phone calls and purchases, are growing at a rate of 30 percent a year, predominantly in Europe.

* External Digital ID is only access ID. to access Virtual Safe. Real certificate will seat at safe location and can be higher strength, with all Smart Card options. PIN code will activate remote digital certificate.

Virtual Safe has to recognize valid and trusted certificate issue by Virtual Safe or third party CA.

If user access from other computer and do not have digital certificate on present PC logging to Virtual Safe require user name. Virtual Safe will send and install
Temporary access certificate with remote option window to secure communication and PIN will open remote certificate inside of Virtual Safe to proceed with required application. Unknown E-mail address or proxy access will required additional password protection.

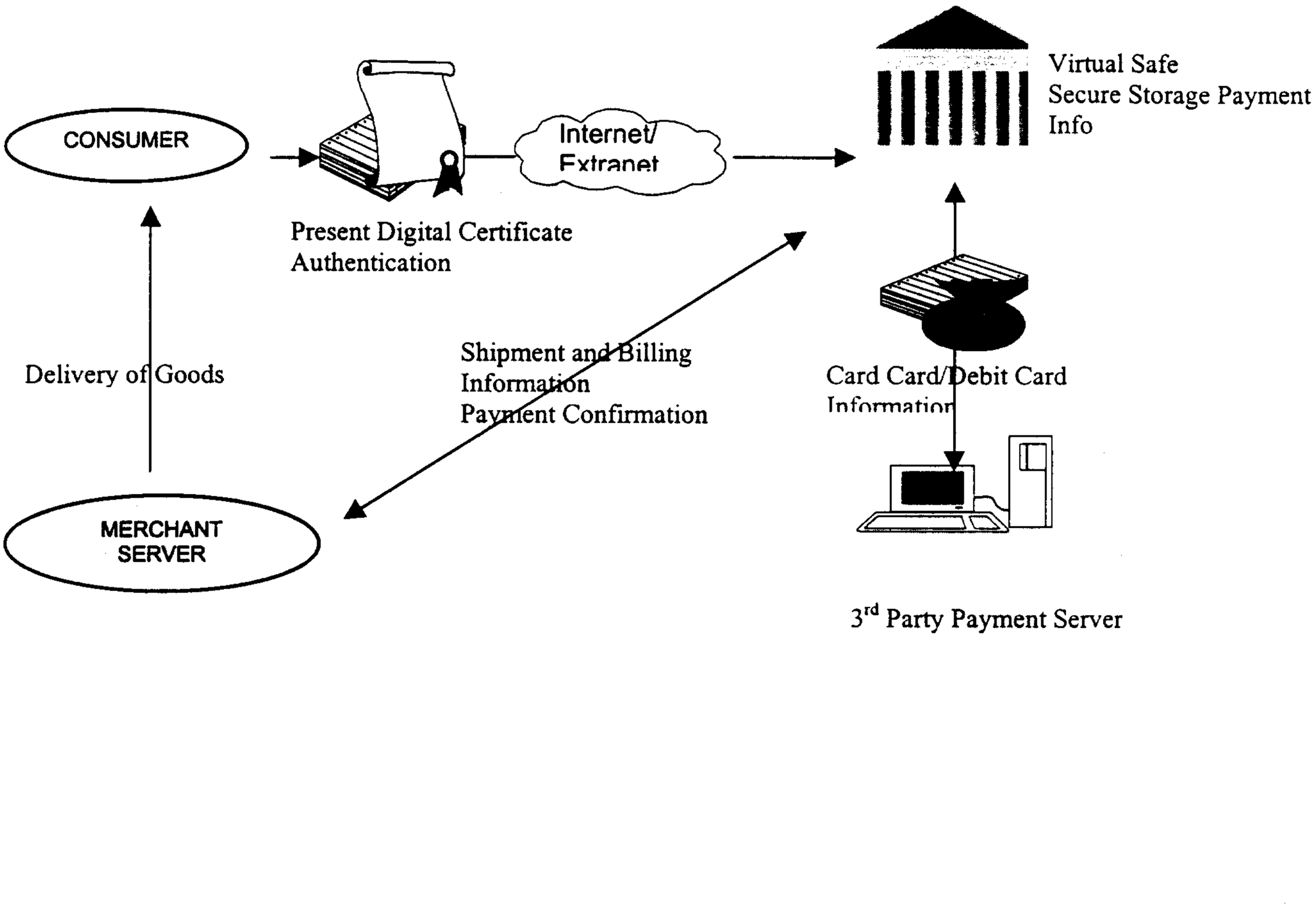
Courier monitoring required holds delivery of goods.

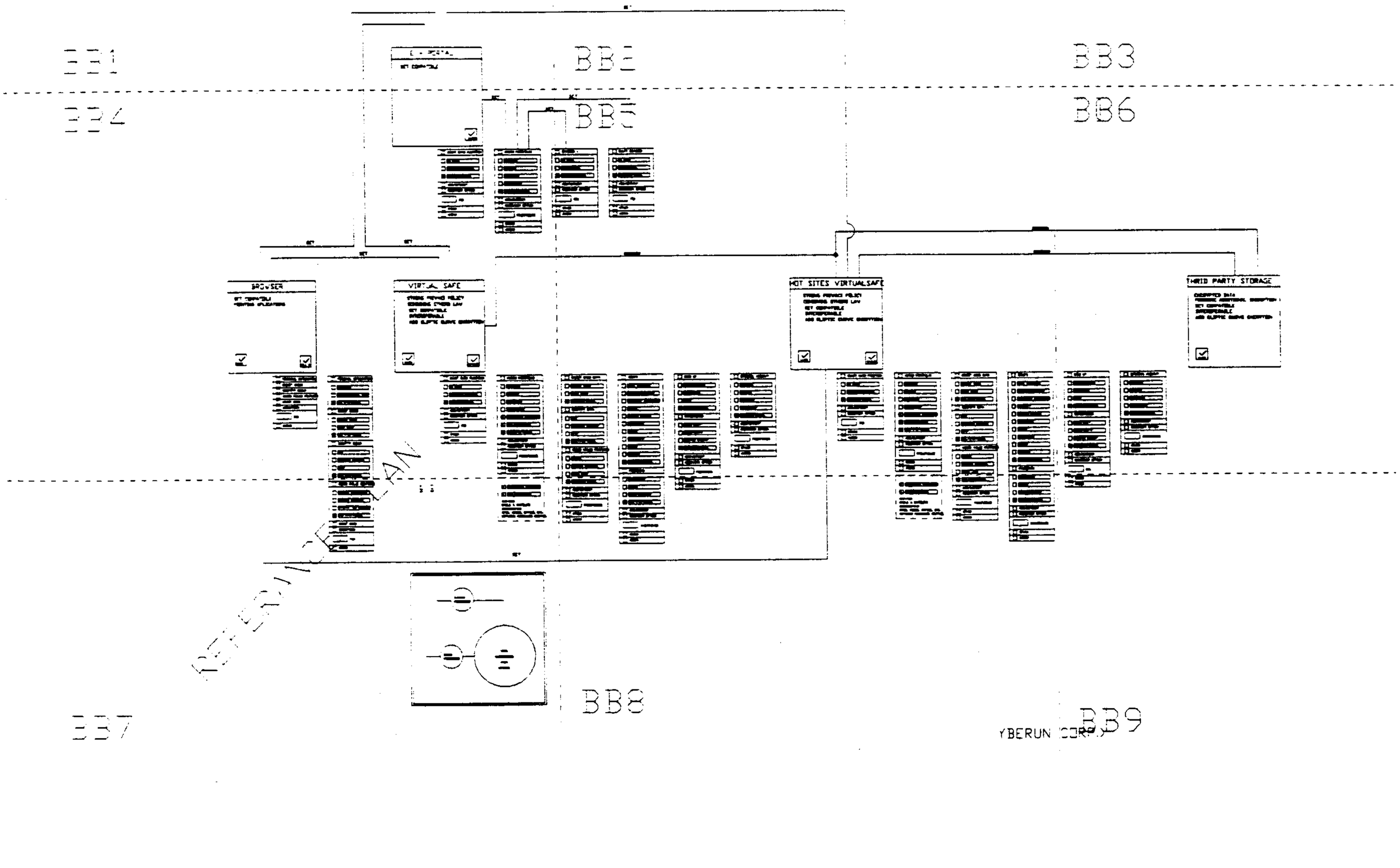
APPENDIX A

A.1 Definitions, Acronyms, and Abbreviations

Password A character string used to authenticate an identity.
Knowledge of the password that is associated with a user ID is considered proof of authorization to use the capabilities associated with that user ID.

User ID A unique symbol or character string that is used by the system to uniquely identify a user. The security provided by a password system should not rely on secrecy of the user's ID.


CONSUMER
Internet/
Extranet
Virtual Safe
Secure Storage Payment
Info
Present Digital Certificate
Authentication
Delivery of Goods
Shipment and Billing
Information
Payment Confirmation
Card Card/Debit Card
Information
MERCHANT
SERVER
3rd Party Payment Server



B2B

3B1

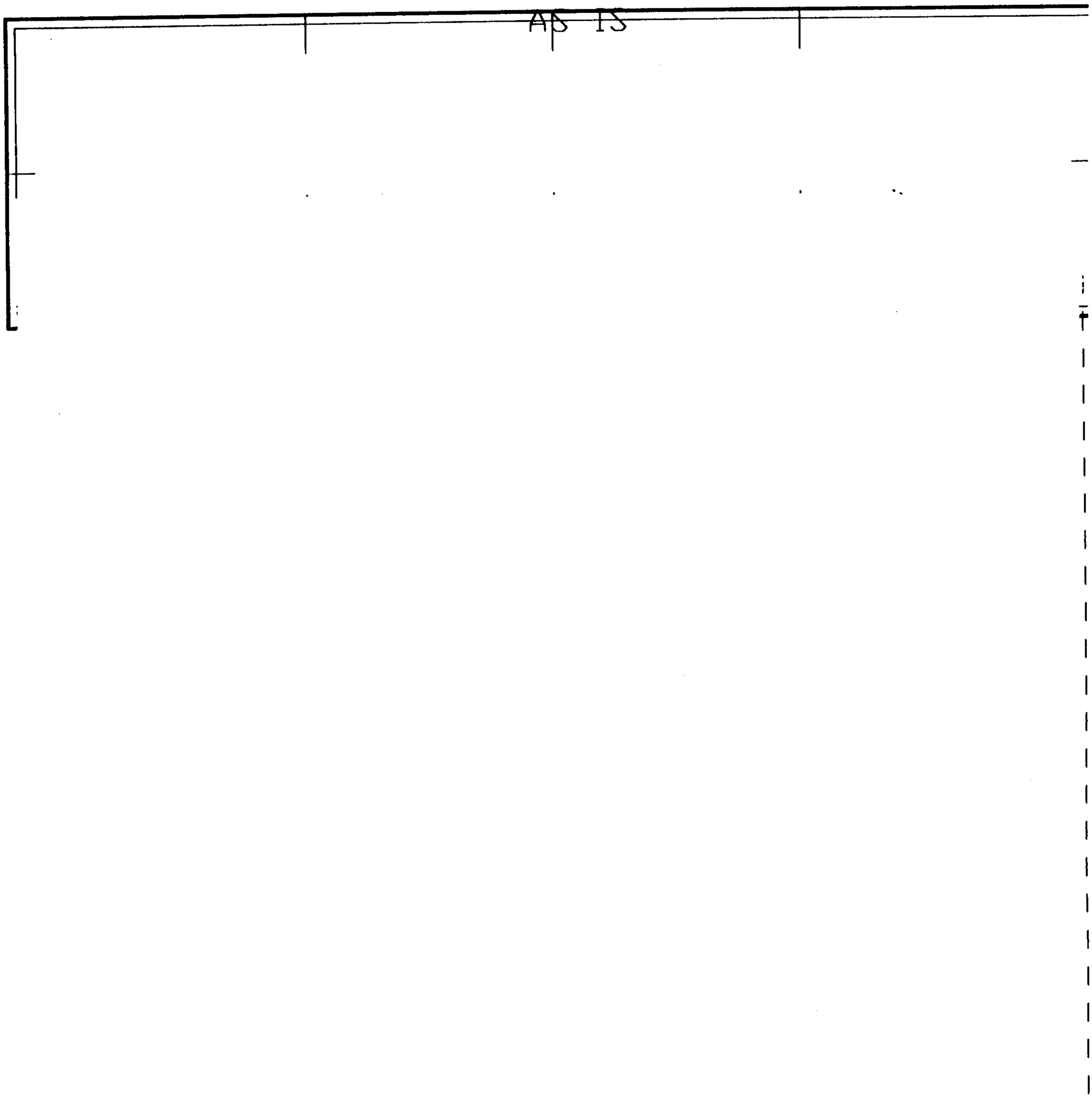
E - PORTAL

SET COMPATIBLE

CA 023052 49 2000-04-14

SET

BB2


AS IS

BB4

SET

SET

SET

SET

W/DI

SMART CARD FUNCTION
DI DATA
AUTH/MULTILEVEL
MULTI-OPTIONAL
ADD/AUTHENT
RECOVERY OPTION
PIN
OTHER
AMEND

ACCES PORTFOLIO
PRIVATE
SHARED
BUSINESS
GOVERMENT
MULTI-OPTIONAL
ADD/AUTHENT
RECOVERY OPTION
PARAPHRASE
OTHER
AMEND

BROWSER

SET COMPATIBLE
POINTING APLICATIONS

CERT

FILL IN

PERSONAL INFORMATION
CREDIT CARDS
IDENTITY DOCUS
ADDED VALUE FEATURES
SMART CARD
BIOMETRICS
PIN
AMEND

PERSONAL INFORMATION
REQUIRED
OTHER/MEDICAL ETC.
MULTI-OPTIONAL
CREDIT CARDS
CREDIT CARD
BANK CARD
MULTI-OPTIONAL
IDENTITY DOCUS
SIN
DRIVERS LICENCE
OHIP

VIRTUAL SAFE

STRONG PRIVACI POLICY
COMBINING OTHERS LAW
SET COMPATIBLE
INTEROPERABLE
ADD ELIPTIC CURVE ENCRYTION

W/DI

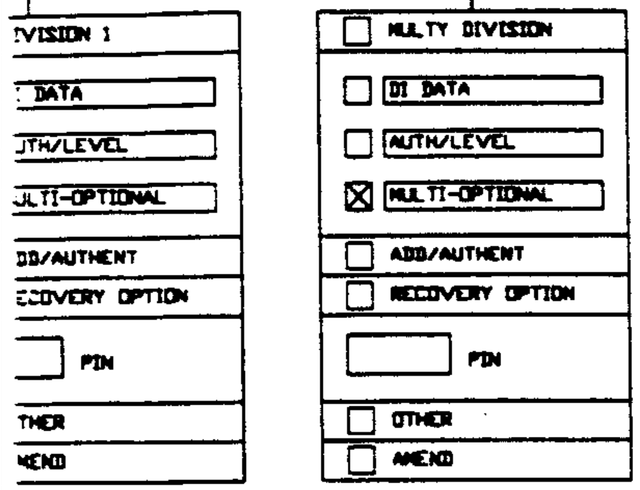
W-O/DI

SMART CARD FUNCTION
DI DATA
AUTH/MULTYLEVEL
MULTI-OPTIONAL
ADD/AUTHENT
RECOVERY OPTION
PIN
OTHER
AMEND

ACCES PORTFOLIO
PRIVATE
SHARED
BUSINESS
GOVERMENT
R SOFTVARE LICENCING
R APL/LICENCING
MULTI-OPTIONAL
ADD/AUTHENT
RECOVERY OPTION
PARAPHRASE
OTHER
AMEND

CA 02305249 2000-04-14

BBS



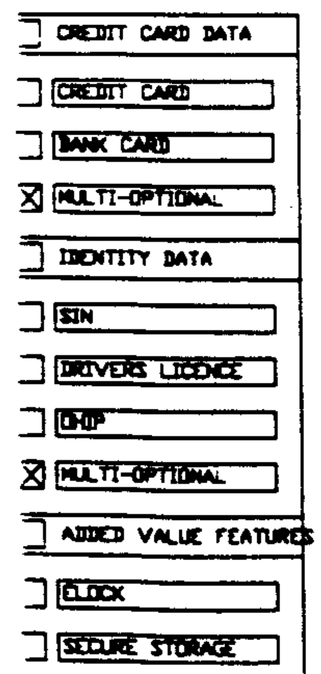
BIOMETRICS

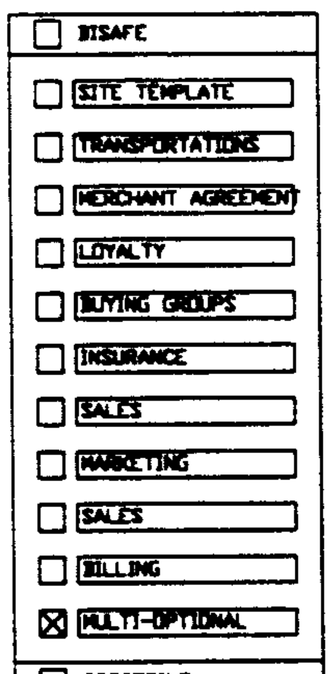
BIOMETRICS

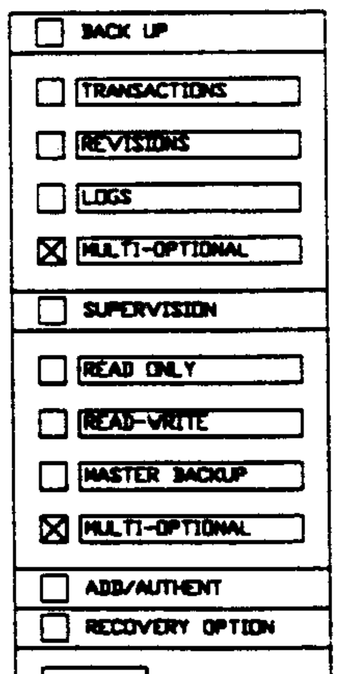
BIOMETRICS

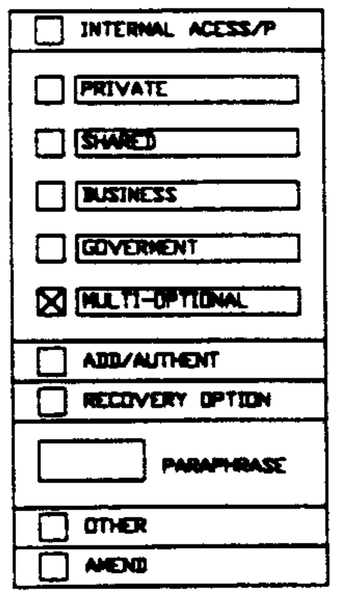
HOT SITES VIRTUALSAFE

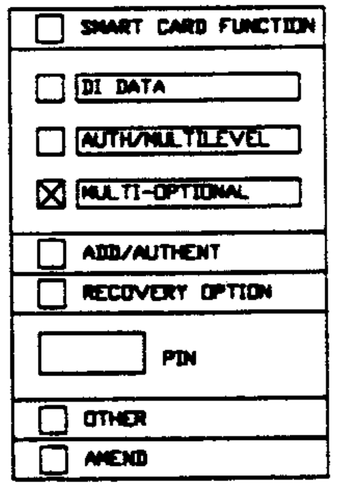
STRONG PRIVACI POLICY
COMBINING OTHERS LAW
SET COMPATIBLE
INTEROPERABLE
ADD ELIPTIC CURVE ENCRYTION

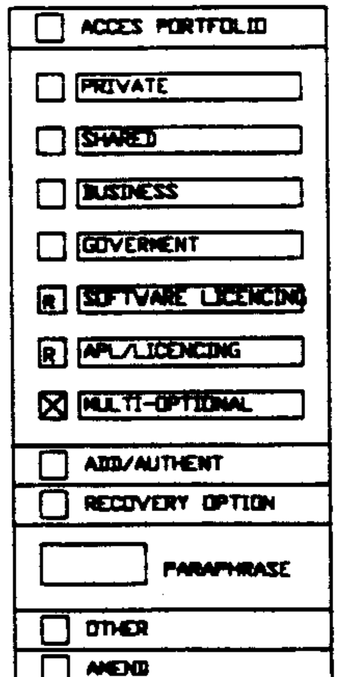


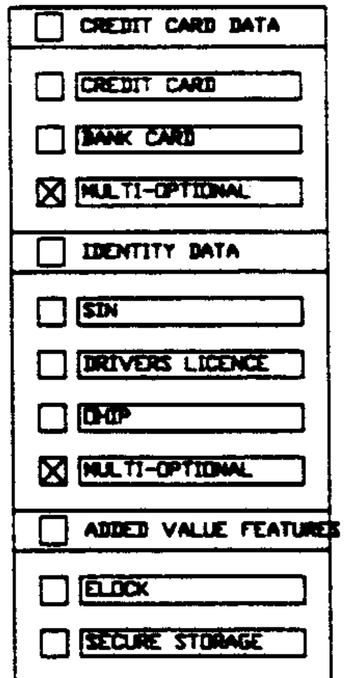


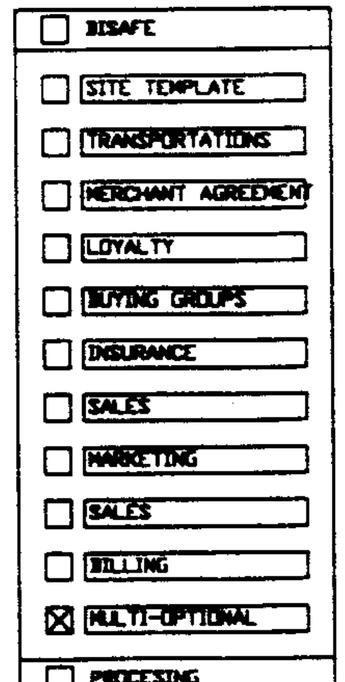




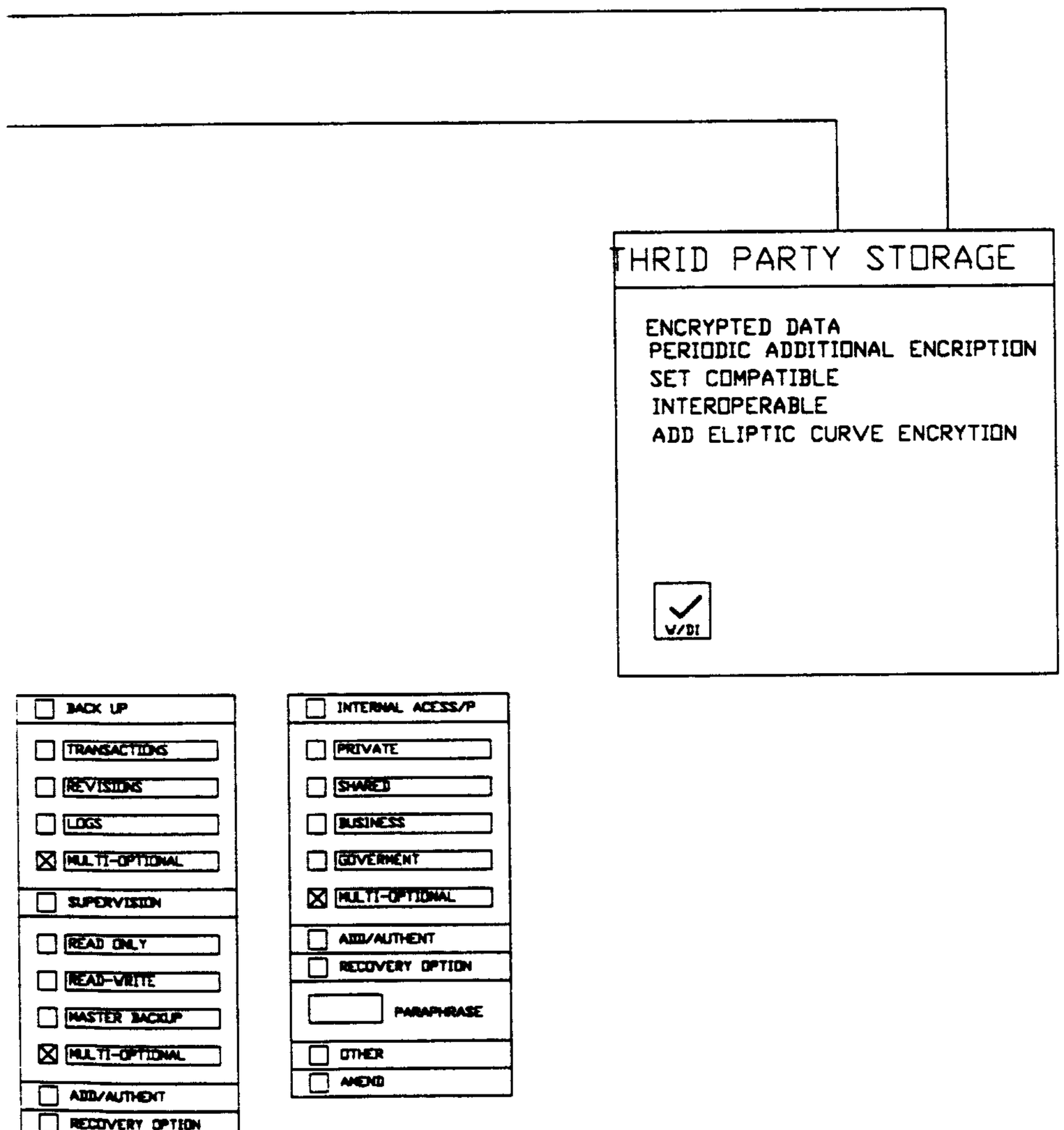


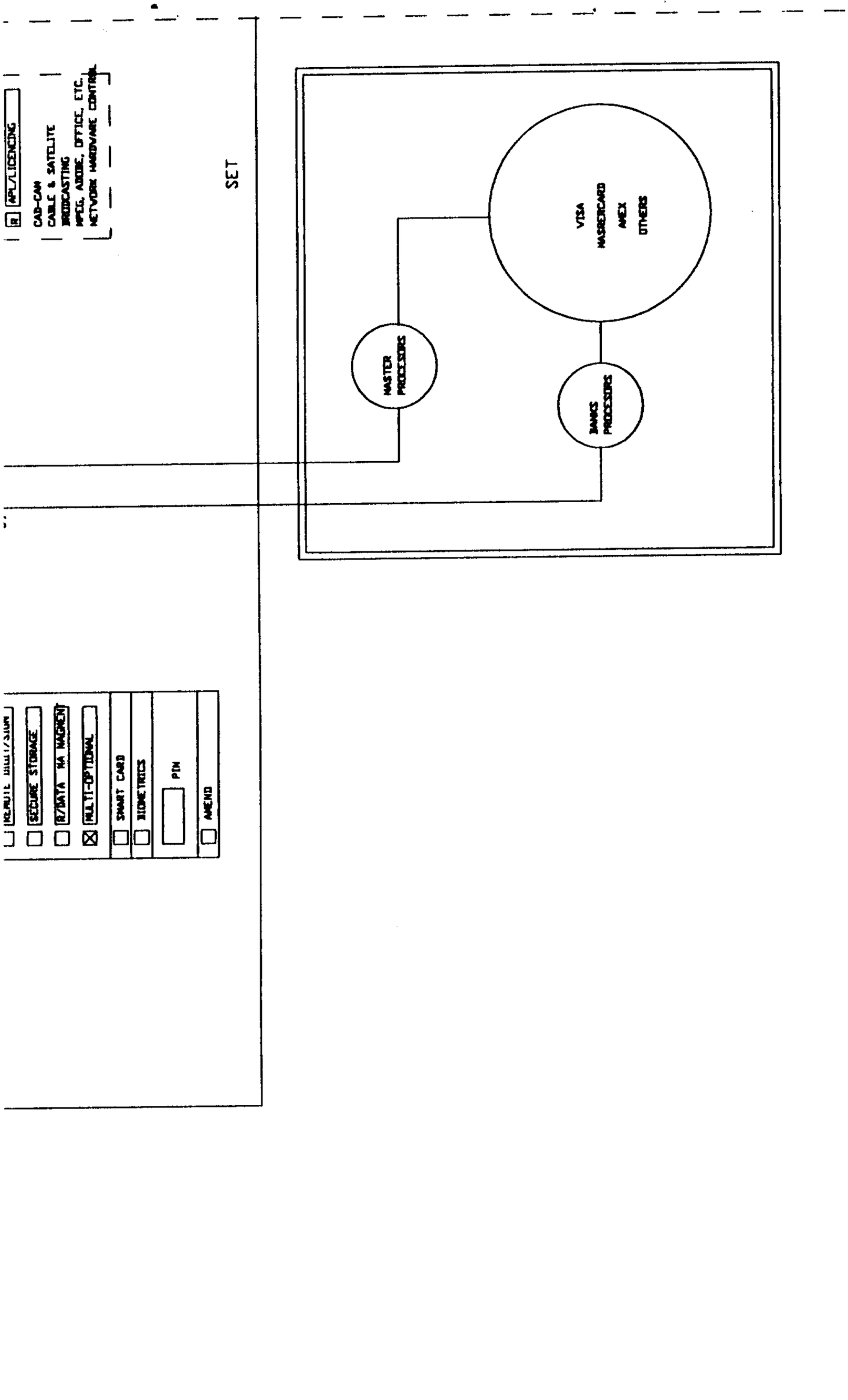


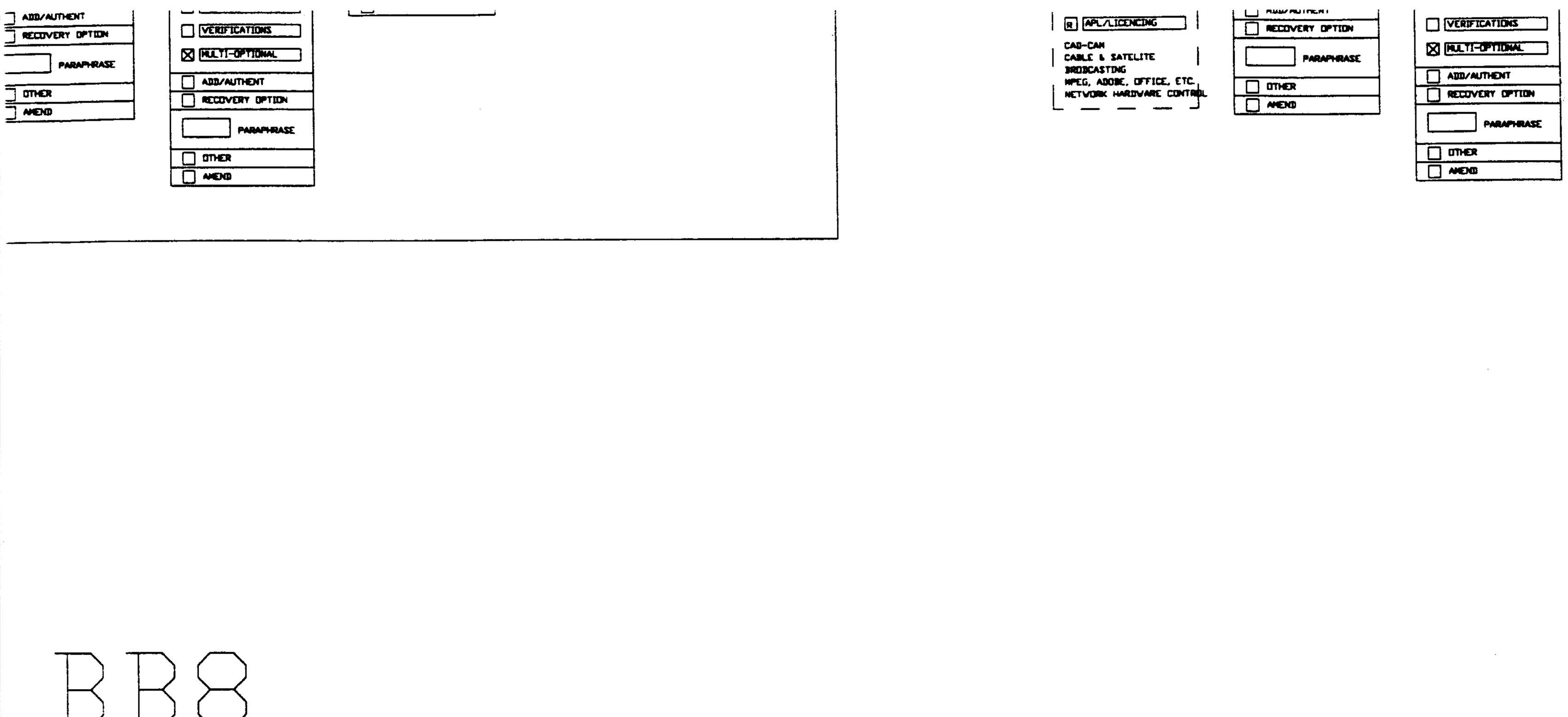




B66




APL/LICENCING
CAD-CAM
CABLE & SATELLITE
BROADCASTING
MPEG, ADOBE, OFFICE, ETC.
NETWORK HARDWARE CONTROL
SET
VISA
MASTERCARD
AMEX
OTHERS
MASTER PROCESSORS
BANKS PROCESSORS
SECURE STORAGE
R/DATA NA MAGMENT
MULTI-OPTIONAL
SMART CARD
BIOMETRICS
PIN
AMEND



BB8