

**1506.** The RAD support server **1506** compares the identifier code with the particular RAD software package **1504** and accepts, or validates, the identifier code if appropriate. If valid, RAD support server **1506** determines the matching mask code for that identifier code from database **1502**. The RAD support server **1506** uses the mask code to encrypt the limited use card number as described above, and transmits this encrypted code to the user. The RAD software **1504** decrypts the encrypted code using the known mask code and reconstructs the initial digits, the BIN number and the checksum digit. The RAD software **1504** then arranges this information and reconstructs the limited use card number.

[**0241**] The RAD support server **1506** is an Internet based server that interfaces the RAD **1504** and the central processing station **1508**. The RAD support server **1506** receives requests for limited use numbers from users, validates each user, if appropriate, and supplies and validates limited use card numbers with specific limitations, as requested by each user, if appropriate. Such requests may be processed in any desired order, e.g., first come first served basis. The RAD support server **1506** may also be configured to provide for location identification verification, secure delivery of limited use numbers, automated completion of payment fields in a merchant's web page order form, review of previous transactions, access to additional issuer services and advertising. The RAD location identification verification is verifying the physical source of the request for a limited use number, e.g., home, office, ATM machine. This additional identification is evidence to limit a user's ability to deny a transaction. The RAD support server **1508** can be configured to require additional identification of the user if the RAD is being used from a physical source which is unknown to the RAD support server or which has not been previously associated with the RAD by the user.

[**0242**] To accomplish the above tasks, the RAD support server **1506** should have a high bandwidth Internet connection and highly secure firewalls to insulate critical information from undesired access. Communications between the RAD support server **1506** and the RAD **1504** is may be Internet based. Communication between the RAD support server **1506** and the central processing station **1508** and the database **1502** may be secured via private networks for additional security. In addition, to provide for additional security, the RAD support server **1506**, the central processing station **1508** and database **1502** may be located at the same physical location, for example, the issuer's processing facility or some other facility which meets the standards set for banking processing facilities.

[**0243**] Communication between the RAD **1504** and the RAD support server **1506** can use industry standard security protocols appropriate to the platform. For example, secure socket layer (SSL) encryption may be used in the case of communication by a personal computer of the Internet. Alternatively, one of the encryption schemes described herein may be implemented alone or in combination with password protection and/or smart card user authentication. Such communication security can be selectable by the issuer. For example, issuers can select what type of communication security they desire from a range of options.

[**0244**] 3. Controlled Payment Number (CPN) Applications

[**0245**] As can be seen from the above, the described limited-use credit card numbers can be provided with user

defined controls on how the numbers can be used. Hence, the phrase "controlled payment numbers" describes products which embody the invention described herein.

[**0246**] To appreciate how a software and hardware platform embodying the invention can be used to generate a range of payment products that span the virtual, wireless and real worlds it is necessary to consider the components of the complete platform and how these can be used in various combinations. To a large extent, remarkably distinct payment products can be derived using the existing platforms such as the RAD system **1500** of FIG. 15 in a range of configurations. Addition of standard additional components and interfaces further broadens the potential scope. The RAD system platform **1500** has been designed from the outset to support such applications. This provides a rapid development path for new payment products since development requirements are limited primarily to designing new client side components for configuring and controlling CPN payments.

[**0247**] At the heart of the CPN platform are a number of core components:

[**0248**] A card number generating and allocation system (e.g., support server **1508**) that allows for additional controls to be allocated to the cards in a dynamic manner.

[**0249**] A card issuing process for distribution of CPN's to users that supports industry standard protocols, such as shown in FIGS. 5 and 6.

[**0250**] A card authorization and settlement process (e.g., FIGS. 7 and 8) that provides additional verification and validation of cards against the current set of controls that have been set up for that card.

[**0251**] A mechanism for relating a specific CPN to an existing credit card, debit card or general financial account (e.g., FIGS. 11, 12 and 13).

[**0252**] The platform may be implemented with part as a personal computer connected to the Internet to provide communication with the card issuer. The customer can set a range of limitations as determined by the issuer and the card number is issued in virtual form to the users computer (usually) for immediate use.

[**0253**] This arrangement is ideal for e-commerce applications but, by altering how the core component functions are implemented and integrated, a range of additional applications can be produced. These applications can be broadly divided into:

[**0254**] 1. Card present Transactions;

[**0255**] 2. MOTO (Mail Order and Telephone Order);  
and

[**0256**] 3. Wireless applications.

[**0257**] Specifically these applications can be implemented by varying: (1) the patterns of how the controls on specific numbers are combined, (2) the controls available to user(s), (3) who sets the controls and when, (4) how the controls are communicated to the processing system, (5) the communication device(s) or channels used to deliver an issued CPN to the user, (6) the form in which the CPN is issued (virtual via software, voice generated, text message, paper receipt,