

[0030] Then in FIG. 8, the description describes an embodiment of the account authentication process that includes a value-adding component. Value is added by first sharing information about a customer with a value-adding party. The customer information is rich in detail about the customer since it is collected by each of the parties in the account authentication process. The value-adding party can then use this information in various manners. For instance, the value-adding party can then provide focused information to the customer or ship a good to the customer. All of the parties involved can benefit from sharing the customer information and each party can agree as to how they can help each other gain the benefits. By using a transaction identifier, which identifies a specific transaction between a customer and a merchant and the customer information, each of the parties can also audit the transactions and any agreements related to the customer information. This application describes how the sharing of such information can be advantageously used in a wide range of applications to the benefit of a wide range of parties.

Account Authentication System

[0031] The account authentication system is designed to authenticate account ownership of an account holder during transactions in which one party cannot physically verify the identity of another party who purports to be the owner of a specific account. For example, the account authentication system can be used in various transactions when a trusted party authenticates the identity of a presenter for the benefit of a requestor. A presenter is any individual or entity that presents itself as having a specific identity. A requestor is any individual or entity that requests a trusted party to authenticate the identity of the presenter. A trusted party is an entity capable of authenticating the identity of the presenter and whom the presenter and requestor trust to perform the authentication process. The trusted party can agree to protect the interests of the requestor in case of mistakes or fraud with respect to the identity of the presenter. An important application of the account authentication system is in the field of payment transactions that take place either online or over portable electronic devices.

[0032] However, the system can be useful in many applications aside from payment transactions. The system of the present invention can be used in various non-payment situations where the identity of a customer requires authentication. For example, non-payment transactions include transactions such as authenticating a customer who accesses an Internet web site to complete an online form, e.g., for a registration process. Non-payment transactions also include many aspects of retail banking, wholesale banking, medical businesses, insurance businesses, and brokerage businesses, just to mention a few. Retail banking involves account numbers used with cards such as debit cards, purchase cards, and stored value cards. Non-payment transactions also include filling out online forms for things such as identification cards and licenses. For example, the American Automobile Association (AAA) can use the system to authenticate the identity of one of its customers or a telephone card company can use the system to authenticate the identity of the user of a specific card.

[0033] FIG. 1 illustrates one embodiment of system architecture 100 for implementing the account authentication system for various types of account authentication applica-

tions. System architecture 100 includes three domains: a trusted party domain 103, an interoperability domain 104, and a requester domain 105. The trusted party and requestor domains define functional realms within which are components that are totally or at least partially controlled by the trusted party or requestor, respectively. The interoperability domain defines a functional realm within which are components that may be utilized by the trusted party, the requestor, as well as other parties, such as a service organization.

[0034] The trusted party domain 103 includes components that are primarily controlled by a trusted party. An example of a trusted party is a financial institution that issues payment cards to consumers, known as an issuing bank. Specifically, an issuer, or a card issuer, personalizes new cards received from a card supplier and then issues these cards to its customers. Personalization may also be performed by the card supplier or by a personalization bureau. In addition to being a financial institution, an issuer may be any suitable issuing entity such as telecommunications network operator, a service association, a merchant or other organization, or even an agent acting for an issuer. Requestor domain 105 includes components that are primarily controlled by a requestor. A requestor can be any party who makes a request for the identity of an account holder to be authenticated. For example, a requestor can be a merchant who desires to authenticate the identity of a person alleging to be the owner of a credit card account. An acquirer can be a financial institution that enrolls requestors in the payment scheme and manages the accounts of requestors. An acquirer also routes information from an online merchant to the telecommunications network. In other embodiments, a merchant can directly route information to the telecommunications network.

[0035] Interoperability domain 104 can be supported by the Internet and includes components used by both the trusted party and the requestor.

[0036] Trusted party domain 103 includes an issuer account holder system 110, an enrollment server 112, an access control server (ACS) 114, and an account holder file 118. Additional components are included within trusted party domain 103 depending upon the specific field of use in which the system will be used. For example in the payment transactions below, additional components in each of the domains are present for the purpose of authenticating account holder identities with respect to payment transactions.

[0037] Enrollment server 112 is a computer that manages an account holder's enrollment into the account authentication system by presenting a series of questions via a web interface to be answered by the account holder and verified by the trusted party. As shown in FIG. 1, the trusted party operates enrollment server 112. However, a service organization such as Visa can operate enrollment server 112 on behalf of the trusted party. The trusted party can use a web-enabled, interactive "identity authentication service" provided by an outside entity during the enrollment process to help validate an account holder's identity.

[0038] ACS 114 is a computer that has a database of account holders registered for the account authentication service provided by the account authentication system. ACS 114 contains account and password information for each account holder. During an account authentication transac-