

tion, ACS 114 provides digitally signed receipts to an authentication requestor, controls access to the account authentication system, and validates account holder participation in the service. A card issuer or a service organization such as Visa can operate ACS 114 for the trusted party. While the account authentication service does not require any additional account holder software to be used, optional account holder software and hardware may be deployed. Additional account holder software can support additional authentication techniques such as digital certificates, integrated circuit cards (chip cards) and chip card readers. Note that in the present invention, the only system participant requiring a certificate is the issuing financial institution.

[0039] Account holder file 118 is a trusted party managed database for storing information relating to the account holders who are successfully enrolled with the account authentication system. Issuer account holder system 110 (or Trusted Party Account Holder System) is controlled by the trusted party and contains information about account holders. Such information relates to account information, services utilized by the account holder, etc. Some of the information within the issuer account holder system 110 can be used in enrolling account holders into the account authentication service.

[0040] Requestor 180 of requester domain 105 typically desires the authentication of an account holder. Party 180 manages requesting plug-in software 182 that facilitates the authentication protocol. Requesting plug-in software module 182 is a software module that integrates into a third or requestor's web site. Plug-in software module 182 provides the interface between the account authentication system and the requestor's processing software, for example, the payment processing software of a merchant.

[0041] Interoperability domain 104 contains the directory server 128, is supported by the Internet, and includes components used by both the trusted party and the requestor. Directory server 128 routes authentication requests from requestors to specific ACS's, such as ACS 114. Directory server 128 is operated by a card scheme manager or a service organization, such as Visa. Interoperability domain 104 can also be supported by a network other than the Internet.

Account Authentication System for Payment Transactions

[0042] A description of the system architecture for authenticating an account holder in the realm of payment transactions will now be provided. Note that many of the general concepts described in this section are applicable to various fields of use since the authentication process for payment applications is analogous to non-payment applications.

[0043] An exemplary use of the authentication system and protocol in payment transactions is described as follows. The authentication system is useful in a scenario when an account holder shops online, adds items to a "shopping cart," proceeds to the online merchant's checkout page, and completes the online merchant's checkout forms. The authentication processes can take place after the consumer decides to buy his or her desired products or services, for example, after the consumer clicks a "buy" button. The authentication process can also begin at various other times in the consumer's payment transaction. The authentication process is conducted mostly in a transparent mode to the

consumer by utilizing software that has been incorporated in several points of a payment network. The system validates participation by the account holder and the account holder's financial institution with the authentication service. Then a window is created in which the consumer can confirm his or her identity by requesting a previously registered password from the account holder. If the identity of the consumer is confirmed, the payment information and notice of the consumer's authentication is sent back to the merchant. Then, as conventionally performed, the payment transaction is processed by the merchant. For example, the merchant may send an order confirmation message to the account holder's browser.

[0044] FIG. 2 schematically illustrates one embodiment of a system architecture 200 that supports the authentication service in payment transactions. As with the general system architecture 100 of FIG. 1, architecture 200 is divided into three domains: issuer domain 102, interoperability domain 104, and acquirer domain 106. Issuer domain 102 and acquirer domain 106 of FIG. 2 are analogous to trusted party domain 103 and requestor domain 105 of FIG. 1, respectively.

[0045] Issuer domain 102 includes an enrollment site 108, an issuer account holder system 110, an account holder client device 122, an enrollment server 112, an access control server (ACS) 114, an issuer or requestor identity authentication component 116, and an account holder file 118. Optionally, the issuer domain 102 can include an issuer file of approved account holders 120. An account holder is another term that refers to a presenter since the account holder will hold itself out as having a specific identity. Enrollment server 112 is a computer that manages account holder enrollment into the account authentication system through presenting a series of questions via a web interface to be answered by the account holder and verified by the issuer. Enrollment server 112 is connected via the Internet to the Internet Payment Gateway Service 124, which is in turn, connected to a telecommunications network 126, for example, VisaNet. The Internet Payment Gateway Service 124 allows enrollment server 112 to communicate with telecommunications network 126. The connection via Payment Gateway Service 124 allows enrollment server 112 to query the issuer's authorization system 127 to determine if an account holder being enrolled has an active card account. Enrollment site 108 is an Internet web site where the account holder can register to participate in the account authentication service provided by the account authentication system.

[0046] Account holder client device 122 is used by the account holder to participate in the account authentication system. Specifically, account holder client device 122 can be any device capable of accessing the Internet, such as a personal computer, mobile telephone, a personal data assistant, or an interactive cable television. In some embodiments, account holder client device 122 cannot connect to the Internet, however such devices can still be used by an account holder because input and output messages from client device 122 are routed through special nodes that can handle non-Internet based messages. For example, mobile telephones that transmit and receive messages based upon voice and/or text messages do not connect to the Internet, however they can still be used with the account authentication system by routing messages in a different manner. The Short Message Service (SMS) is a commonly used example