SYSTEMS AND METHODS FOR AUTHENTICATED PEER-TO-PEER DATA TRANSFER USING RESOURCE LOCATORS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to U.S. Patent Application No. 17/162,783 filed January 29, 2021, the disclosure of which is incorporated herein by reference in its entirety.

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates to systems and methods for peer-to-peer data transfers, and in particular, authenticated peer-to-peer data transfer using resource locators.

BACKGROUND

[0003] When two peer devices are not already connected through an existing network, peer-to-peer data transfers may be cumbersome. This is because both peer devices must be registered with and configured for communication on the same network in order to accomplish the transfer. In addition, configuring and scheduling the transfer of data may be detrimental to the user experience. Security risks are also present, and may include risks associated with data integrity and vulnerability when crossing between platforms, and the misidentification of an account by the use of an email address or other account identifier. These risks and shortcomings may reduce user demand for cross-application communication and inhibit the functionality and efficiency of cross-application communications.

[0004] These and other deficiencies exist. Accordingly, there is a need for systems and methods for peer-to-peer data transfer that provide enhanced security and an improved user experience.

SUMMARY OF THE DISCLOSURE

[0004a] According to an aspect of the present disclosure, there is provided a secure peer-to-peer data transfer system, comprising: a contactless card associated with a cardholder, comprising a processor and a memory, wherein the processor is configured to: generate a link

after the contactless card enters a communication field associated with a communication device of a recipient user distinct from the cardholder, the link being operative to initiate a secure peer-to-peer data transfer involving the recipient user and the cardholder, wherein the link comprises: a first set of information comprising one or more abstracted identification information uniquely identifying the contactless card and a specific peer-to peer data transfer session, a second set of information including information associated with the cardholder loaded on to the contactless card at the time of personalization of the card, and one or more data fields for specifying one or more transfer parameters.

[0004b] According to another aspect of the present disclosure, there is provided a method of implementing a secure peer-to-peer data transfer, comprising: generating, after entry of the processors of the contactless card into a communication field of a first device associated with a recipient, a link, the link including abstracted identifier information and one or more account and identity information associated with the cardholder; and transmitting, the link to a first application running on the first device, the link being operative to initiate a secure peer-to-peer data transfer in accordance to one or more transfer parameters.

[0004c] According to another aspect of the present disclosure, there is provided a computer readable non-transitory medium comprising computer-executable instructions that, when executed by a processor, perform procedures comprising the steps of: generating, after entry of the processors of the contactless card into a communication field of a first device associated with a recipient, a link, the link including abstracted identifier information and one or more account and identity information associated with the cardholder; and transmitting, the link to a first application running on the first device, the link being operative to initiate the secure peer-to-peer data transfer in accordance to one or more transfer parameters.

[0005] Embodiments of the present disclosure provide an authenticated data transfer system, including a contactless card comprising a processor and a memory. After entering a