

require the customer to verify himself or herself to the delivery person, such that the package can be delivered to the correct recipient and in a secure manner. In many such interactions, social distancing is not possible and the identification and verification process is not efficient.

[0005] These and other deficiencies exist. Accordingly, there is a need to provide systems and methods that overcome these deficiencies to verify customers in a secure and efficient manner while minimizing physical contact or close interactions between people.

SUMMARY

[0006] Aspects of the disclosed technology include systems and methods for contactless package delivery.

[0006a] According to an aspect, there is provided a contactless delivery system, comprising a contactless card comprising a processor and a memory, the memory storing a cryptogram that contains a unique identifier associated with a user account, wherein, after entry into a communication field, the contactless card is configured to transmit the cryptogram to a server via one or more intermediary devices, and wherein, upon receipt of the cryptogram, the server is configured to: validate the cryptogram, decrypt the cryptogram, extract the unique identifier from the cryptogram, query, using the unique identifier, a database for an identity of the user account, and generate a digital signature based on the identity of the user account.

[0006b] According to another aspect, there is provided a contactless delivery system, comprising a server comprising a processor and a memory, wherein the server is configured to: receive a cryptogram containing a unique identifier associated with a user account, validate the cryptogram, decrypt the cryptogram, extract the unique identifier from the cryptogram, query, using the unique identifier, a database for an identity of the user account, and generate a digital signature based on the identity of the user account.

[0006c] According to another aspect, there is provided a contactless delivery method performed by a server, the method comprising receiving a cryptogram containing a unique identifier associated with a user account; validating the cryptogram; decrypting the cryptogram; extracting the unique identifier from the cryptogram; querying, using the unique identifier, a database for an identity of the user account, and generating a digital signature based on the identity of the user account.

[0007] Embodiments of the present disclosure provide a contactless delivery system. The contactless delivery system includes a contactless card. The contactless card includes a processor and a memory. The memory stores a cryptogram that contains a unique identifier associated with a user account. After entry into a communication field, the contactless card is configured to transmit the cryptogram to a server via one or more intermediary devices. Upon receipt of the cryptogram, the server is configured to: validate the cryptogram; decrypt the cryptogram and extract the unique identifier; query, using the unique identifier, a database for an identity of the user account; generate a digital signature based on the identity of the user account; and transmit a verification notification including the identity of the user account and the digital signature.

[0008] Embodiments of the present disclosure provide a contactless delivery system. The contactless system includes a server comprising a processor and a memory. The server is configured to: receive a cryptogram containing an unique identifier associated with a user account; validate the cryptogram; decrypt the cryptogram and extract the unique identifier;