

CLAIMS

~~What is claimed is:~~

- ~~1. A contactless delivery system, comprising:

a contactless card comprising a processor and a memory, the memory storing a cryptogram that contains an 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 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.~~
- ~~2. The contactless delivery system of claim 1, wherein the one or more intermediary devices comprise a communication interface configured to generate the communication field.~~
- ~~3. The contactless delivery system of claim 1, wherein:

the memory further contains a counter value and a plurality of keys, and

——— the processor of the contactless card is configured to generate the cryptogram using the counter value, the plurality of keys, and the unique identifier.~~

~~4. The contactless delivery system of claim 3, wherein~~

~~the processor of the contactless card is configured to update the counter value.~~

~~5. The contactless delivery system of claim 1, wherein:~~

~~—the verification notification is transmitted to a user device storing information on a delivery package, and~~

~~——the server is further configured to receive the information on the delivery package as an authentication factor to verify the identity of the user account.~~

~~6. The contactless delivery system of claim 1, wherein the database contains one or more documents associated with the user account, the one or more documents comprising a copy of a driver license.~~

~~7. The contactless delivery system of claim 6, wherein the server is configured to receive, from the database, the one or more documents to verify the identity of the user account.~~

~~8. The contactless delivery system of claim 1, wherein:~~

~~the server is configured to transmit the verification notification to a user device, and~~

~~the digital signature is displayed on a display of the user device, the digital signature being used to sign a package receipt document displayed on the display of the user device.~~

~~9. The contactless delivery system of claim 1, wherein the contactless card includes a host card emulation device emulating the contactless card.~~

~~10. The contactless delivery system of claim 1, wherein the server is configured to:
retrieve a profile picture of the user account from the database, and
transmit the profile picture to verify the identity of the user account.~~

~~11. The contactless delivery system of claim 1, wherein the server is further configured to:

retrieve a document of the user account from the database, and
transmit the document to verify the identity of the user account.~~

~~12. A contactless delivery system, comprising:

a server comprising a processor and a memory, wherein 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,

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.~~

~~13. The contactless delivery system of claim 12, wherein:~~

~~the cryptogram is stored on a contactless card; and~~

~~the server is configured to receive the cryptogram via an intermediary device~~

~~configured to generate a communication field for data communication with the contactless card.~~

~~14. The contactless delivery system of claim 13, wherein the server is configured to receive a geo-signature of the intermediary device.~~

~~15. The contactless delivery system of claim 14, wherein the server is further configured to:~~

~~receive a geo-signature of a user device,~~

~~compare the geo-signature of the intermediary device with the geo-signature of the user device, and~~

~~generate the digital signature based on the comparison.~~

~~16. The contactless delivery system of claim 12, wherein the server is configured to:~~

~~receive one or more authentication factors, the one or more authentication factors comprising at least one selected from a group of a password, a personal identification (PIN), and a biometric feature, and~~

~~verify the identity of the user account based on the one or more authentication factors.~~

~~17. The contactless delivery system of claim 12, wherein the server is configured to:~~

~~receive a card tap notification;~~

~~prompt to read a contactless card based on the card tap notification;~~
~~receive a tap completed notification; and~~
~~generate the digital signature of the identity of the user account using the tap-~~
~~completed notification.~~

~~18. The contactless delivery system of claim 12, wherein the server is configured to:~~

~~receive a universal resource locator (URL) link;~~
~~open the URL link to display a web page;~~
~~read a contactless card through the web page; and~~
~~generate the digital signature of the identity of the user account using the web page.~~

~~19. A contactless delivery method, comprising:~~

~~receiving a cryptogram, the cryptogram containing an unique identifier associated~~
~~with a user account;~~

~~validating the cryptogram;~~

~~decrypting the cryptogram and extracting the unique identifier;~~

~~querying, using the unique identifier, a database for an identity of the user account;~~

~~generating a digital signature based on the identity of the user account; and~~

~~transmitting a verification notification including the identity of the user account and~~
~~the digital signature.~~

~~20. The contactless delivery method of claim 19, comprising receiving an additional~~
~~cryptogram.~~

1. 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.
2. The contactless delivery system of claim 1, wherein the one or more intermediary
devices comprises a communication interface configured to generate the communication
field.
3. The contactless delivery system of claim 1, wherein the server is configured to
transmit a verification notification including the identity of the user account and the digital
signature.
4. The contactless delivery system of claim 3, wherein:

the verification notification is transmitted to a user device storing information on a delivery package, and

the server is configured to receive the information on the delivery package as an authentication factor to verify the identity of the user account.

5. The contactless delivery system of claim 4, wherein:

the server is configured to transmit the verification notification to a delivery device, and

the digital signature is displayed on a display of the delivery device, the digital signature being used to sign a package receipt document displayed on the display of the delivery device.

6. The contactless delivery system of claim 1, wherein:

the memory contains a counter value and a plurality of keys, and
the processor of the contactless card is configured to generate the cryptogram using the counter value, the plurality of keys, and the unique identifier.

7. The contactless delivery system of claim 6, wherein the processor of the contactless card is configured to update the counter value.

8. The contactless delivery system of claim 1, wherein the database contains one or more documents associated with the user account, the one or more documents comprising a copy of a driver license.

9. The contactless delivery system of claim 8, wherein the server is configured to receive, from the database, the one or more documents to verify the identity of the user account.
10. The contactless delivery system of claim 1, wherein the contactless card includes a host card emulation device emulating the contactless card.
11. The contactless delivery system of claim 1, wherein the server is configured to:
retrieve a profile picture of the user account from the database, and
transmit the profile picture to verify the identity of the user account.
12. The contactless delivery system of claim 1, wherein the server is configured to:
retrieve a document of the user account from the database, and
transmit the document to verify the identity of the user account.
13. 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.

14. The contactless delivery system of claim 12, wherein:

the cryptogram is stored on a contactless card, and

the server is configured to receive the cryptogram via an intermediary device configured to generate a communication field for data communication with the contactless card.

15. The contactless delivery system of claim 14, wherein the server is configured to receive a geo-signature of the intermediary device.

16. The contactless delivery system of claim 15, wherein the server is configured to:

receive a geo-signature of a user device,

compare the geo-signature of the intermediary device with the geo-signature of the user device, and

generate the digital signature based on the comparison.

17. The contactless delivery system of claim 13, wherein the server is configured to transmit a verification notification including the identity of the user account and the digital signature.

18. The contactless delivery system of claim 12, wherein the server is configured to:
receive one or more authentication factors, the one or more authentication factors
comprising at least one selected from a group of a password, a personal identification (PIN),
and a biometric feature, and
verify the identity of the user account based on the one or more authentication factors.

19. The contactless delivery system of claim 12, wherein the server is configured to:
receive a card tap notification;
prompt to read a contactless card based on the card tap notification;
receive a tap-completed notification; and
generate the digital signature of the identity of the user account using the tap-
completed notification.

20. 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.