SUMMARY OF THE DISCLOSURE

[0004a] An aspect of the present disclosure provides an identity verification system, comprising a server comprising a processor and a memory, wherein the server is configured to: receive, from a first application executing on a first client device after entry of a contactless card into a communication field generated by the first client device, a request to perform an identity verification process on identity data, perform the identity verification process, determine one or more outcomes based on the identity verification process, generate one or more notifications based on the one or more outcomes, and transmit, to a second application executing on a second client device, the one or more notifications, wherein: the one or more notifications including an option indicative of requested access to shareable information relating to a first user, and the option includes a choice to accept or decline access to the shareable information.

[0004b] Another aspect of the present disclosure provides a method of identity verification performed by a server comprising a processor and a memory, the method comprising: receiving, from a first application executing on a first client device after entry of a contactless card into a communication field generated by the first client device, a request to perform an identity verification process on identity data; performing the identity verification process; determining one or more outcomes based on the identity verification process; generating one or more notifications based on the one or more outcomes; and transmitting, to a second application executing on a second client device, the one or more notifications, wherein: the one or more notifications including an option indicative of requested access to shareable information relating to a first user, and the option including a choice to accept or decline access to the shareable information.

[0004c] Another aspect of the present disclosure provides a non-transitory computer readable medium comprising instructions that, when executed by server comprising a processor and a memory, cause the server to perform procedures comprising: receiving, from a first application executing on a first client device after entry of a contactless card into a communication field generated by the first client device, a request to perform an identity verification process on identity data; performing the identity verification process; determining one or more outcomes based on the identity verification process; generating one or more notifications based on the one or more outcomes; and transmitting, to a second application executing on a second client device, the one or more notifications, wherein: the one or more notifications including an option indicative of requested access to shareable information relating to a first user, and the option including a choice to accept or decline access to the shareable information.

[0005] Embodiments of the present disclosure provide an identity verification system, including a contactless card comprising a processor and a memory. The system may comprise one or more applications comprising instructions for execution on one or more devices. A first application may be configured to transmit, after entry of the contactless card into a communication field, identity data. The first application may comprise instructions for execution on a first client device. A second application may be configured to receive a notification based on an identity verification process. The second application may comprise instructions for execution on a second client device. The notification may include an option indicative of requested access to specified information about the first user. The option may further include a choice to accept or decline access to the specified information about the first user. The first application may be configured to receive the requested access to specified information about the first user based on selection of the option. The application may be

configured to determine a capability associated with the contactless card after a first entry into a communication field. The application may be configured to request additional information based on the determination. The one or more applets may be configured to transmit, to the application, a generated tokenized link after a second entry into the communication field based on the requested additional information. The application may be configured to transmit the link to obtain the requested additional information.

[0006] Embodiments of the present disclosure provide a method of identity verification. The method may include transmitting, after entry of a contactless card into a communication field, identity data by a first application comprising instructions for execution on a first client device. The method may include receiving, based on an identity verification process of the identity data,

CLAIMS

1. An identity verification system, comprising:

a server comprising a processor and a memory,

wherein the server is configured to:

receive, from a first application executing on a first client device after entry of a contactless card into a communication field generated by the first client device, a request to perform an identity verification process on identity data,

perform the identity verification process,

determine one or more outcomes based on the identity verification process,

generate one or more notifications based on the one or more outcomes, and

transmit, to a second application executing on a second client device, the one or more notifications, wherein:

the one or more notifications including an option indicative of requested access to shareable information relating to a first user, and

the option includes a choice to accept or decline access to the shareable information.

2. The identity verification system of claim 1, wherein the requested access is revocable based on one or more permissions.

3. The identity verification system of claim 2, wherein the one or more permissions comprise a geographic restriction.

4. The identity verification system of claim 3, wherein the geographic restriction comprises a requirement for proximity between the first application and the second application.

5. The identity verification system of claim 2, wherein:

the one or more permissions comprise a pre-authorization verification, and

the pre-authorization verification is performed prior to the transmission of the one or more notifications.

6. The identity verification system of claim 1, wherein the server is further configured to perform one or more iterations of the identity verification process.

7. The identity verification system of claim 1, wherein at least one outcome of the one or more outcomes comprises a successful or unsuccessful match between one or more subsets of the identity data and one or more subsets of reference data.

8. The identity verification system of claim 7, wherein at least one outcome of the one or more outcomes comprises an unsuccessful match between the identity data and reference data.

9. The identity verification system of claim 8, wherein the at least one outcome triggers a different comparison between the identity data and the reference data.

10. The identity verification system of claim 1, wherein the first client device and the contactless card are associated with the first user.

11. A method of identity verification performed by a server comprising a processor and a memory, the method comprising:

receiving, from a first application executing on a first client device after entry of a contactless card into a communication field generated by the first client device, a request to perform an identity verification process on identity data;

performing the identity verification process;

determining one or more outcomes based on the identity verification process;

generating one or more notifications based on the one or more outcomes; and

transmitting, to a second application executing on a second client device, the one or more notifications, wherein:

the one or more notifications including an option indicative of requested access to shareable information relating to a first user, and

the option including a choice to accept or decline access to the shareable information.

12. The method of claim 11, wherein the one or more notifications enable a response in which additional information is selected for sharing.

13. The method of claim 11, wherein selection of the option is associated with a predetermined time duration prior to a timeout of the requested access.

14. The method of claim 11, wherein the requested access is revocable based on exceeding a predetermined threshold over a predetermined time.

15. The method of claim 11, wherein the requested access is revocable if the shareable information comprises personally identifiable information relating to the first user.

16. The method of claim 11, wherein the requested access is revocable if the request is performed at a time different than a previous request history.

17. The method of claim 11, wherein the requested access is revocable if the request is performed outside of a predetermined time period.

18. A non-transitory computer readable medium comprising instructions that, when executed by server comprising a processor and a memory, cause the server to perform procedures comprising:

receiving, from a first application executing on a first client device after entry of a contactless card into a communication field generated by the first client device, a request to perform an identity verification process on identity data;

performing the identity verification process;

determining one or more outcomes based on the identity verification process;

generating one or more notifications based on the one or more outcomes; and

transmitting, to a second application executing on a second client device, the one or more notifications, wherein:

the one or more notifications including an option indicative of requested access to shareable information relating to a first user, and

the option including a choice to accept or decline access to the shareable information.

19. The non-transitory computer-readable medium of claim 18, wherein the identity verification process comprises a comparison between the identity data and reference data.

20. The non-transitory computer-readable medium of claim 19, wherein upon an unsuccessful comparison, the procedures further comprise performing a different comparison between the identity data and reference data.