

CLAIMS

What is claimed is:

1. ~~A system, comprising:~~
 ~~a processor; and~~
 ~~a memory storing instructions which when executed by the processor~~
 ~~cause the processor to:~~
 ~~receive, by an application executing on the processor, a~~
 ~~request to perform an operation associated with an account;~~
 ~~receive, by the application, encrypted data from a contactless~~
 ~~card~~
 ~~associated with the account, the encrypted data based on a~~
 ~~cryptographic algorithm, a customer identifier, and a private key for~~
 ~~the contactless card;~~
 ~~receive, by the application from an authentication server, an~~
 ~~indication specifying that the authentication server verified the encrypted~~
 ~~data based on the private key for the contactless card;~~
 ~~receive, by the application, encrypted passport data from the~~
 ~~contactless card, the encrypted passport data for a passport~~
 ~~associated with the account, the encrypted passport data encrypted~~
 ~~based on at least one attribute of the passport;~~
 ~~determine, by the application, the at least one attribute of the~~
 ~~passport based at least in part on image data or text input;~~
 ~~decrypt, by the application, the encrypted passport data based on~~
 ~~the at least one attribute of the passport; and~~
 ~~initiate performance of the operation based on the received~~
 ~~indication specifying that the authentication server verified the~~
 ~~encrypted data and the decryption of the encrypted passport data.~~
2. ~~The system of claim 1, the memory storing instructions which when~~
 ~~executed by the processor cause the processor to:~~
 ~~receive, by the application, a first image depicting at least one page~~
 ~~of the passport;~~

~~extract, by the application, a text of the at least one page of the passport depicted the first image; and~~

~~determine the at least one attribute of the passport from the extracted text of the at least one page of the passport, wherein the at least one attribute of the passport comprises a passport number, a passport issue date, and a passport expiration date.~~

~~3. The system of claim 2, the memory storing instructions which when executed~~

~~by the processor cause the processor to:~~

~~output, by the application, an indication specifying to capture the first image to~~

~~authorize the operation; and~~

~~capture the first image by an image capture device of the system.~~

~~4. The system of claim 3, the memory storing instructions which when executed by the processor cause the processor to:~~

~~receive, by the application, authentication credentials associated with the account, the authentication credentials comprising one or more of a login, a password, or biometric credentials; and~~

~~determine, by the application, that a digital signature of the encrypted passport data received from the contactless card is a valid digital signature based on a public key associated with an entity providing the digital signature.~~

~~5. The system of claim 1, the memory storing instructions which when executed by the processor cause the processor to prior to initiate performance of the operation: determine, by the application, that a current permissions level~~

~~for the account does not meet a required permissions level to perform the operation;~~

~~transmit, by the application to the authentication server, an indication of the current permissions level for the account and an indication specifying that the encrypted passport data was decrypted; and~~

~~receive, by the application from the authentication server, an updated permissions level assigned by the authentication server to the account~~

based on the received indication specifying that the encrypted passport data was decrypted, the updated permissions level having greater permissions relative to the current permissions level.

6. — The system of claim 5, the memory storing instructions which when executed by the processor cause the processor to:

determine, by the application, that the updated permissions level meets the required permissions level to perform the operation; and

authorize performance of the operation by the application based on the determination that the updated permissions level meets the required permissions level to perform the operation.

7. — The system of claim 1, wherein the type of the operation comprises one or more of: (i) viewing attributes of the account, (ii) modifying the attributes of the account, (iii) accessing a page of the application, or (iv) processing a transaction using the contactless card, the memory storing instructions which when executed by the processor cause the processor to:

receive, by the application, an updated version of the encrypted passport data; and

transmit, by the application to the contactless card, the updated version of the encrypted passport data for storage in the contactless card.

8. — A non-transitory computer-readable storage medium having computer-readable program code embodied therewith, the computer-readable program code executable by a processor to cause the processor to:

receive, by an application executing on the processor, a request to perform an operation associated with an account;

receive, by the application, encrypted data from a contactless card

associated with the account, the encrypted data based on a cryptographic algorithm, a customer identifier, and a private key for the contactless card;

receive, by the application from an authentication server, an indication specifying that the authentication server verified the encrypted data based on the private key for the contactless card;

~~receive, by the application, encrypted passport data from the contactless card, the encrypted passport data for a passport associated with the account, the encrypted passport data encrypted based on at least one attribute of the passport;~~

~~determine, by the application, the at least one attribute of the passport based at least in part on image data or text input;~~

~~decrypt, by the application, the encrypted passport data based on the at least one attribute of the passport; and~~

~~initiate performance of the operation based on the received indication specifying that the authentication server verified the encrypted data and the decryption of the encrypted passport data.~~

9. — ~~The non-transitory computer-readable storage medium of claim 8, further comprising computer-readable program code executable by the processor to cause the processor to:~~

~~receive, by the application, a first image depicting at least one page of the passport;~~

~~extract, by the application, a text of the at least one page of the passport depicted the first image; and~~

~~determine the at least one attribute of the passport from the extracted text of the at least one page of the passport, wherein the at least one attribute of the passport comprises a passport number, a passport issue date, and a passport expiration date.~~

10. — ~~The non-transitory computer-readable storage medium of claim 9, further comprising computer-readable program code executable by the processor to cause the processor to:~~

~~output, by the application, an indication specifying to capture the first image to authorize the operation; and~~

~~capture the first image by an image capture device of a device comprising the processor.~~

11. — ~~The non-transitory computer-readable storage medium of claim 10, further comprising computer-readable program code executable by the processor to cause the processor to:~~

~~receive, by the application, authentication credentials associated with the account, the authentication credentials comprising one or more of a login, a password, or biometric credentials; and~~

~~determine, by the application, that a digital signature of the encrypted passport data received from the contactless card is a valid digital signature based on a public key associated with an entity providing the digital signature.~~

~~12. — The non-transitory computer-readable storage medium of claim 8, further comprising computer-readable program code executable by the processor to cause the processor to prior to initiating performance of the operation:~~

~~determine, by the application, that a current permissions level for the account does not meet a required permissions level to perform the operation;~~

~~transmit, by the application to the authentication server, an indication of the current permissions level for the account and an indication specifying that the encrypted passport data was decrypted; and~~

~~receive, by the application from the authentication server, an updated permissions level assigned by the authentication server to the account based on the received indication specifying that the encrypted passport data was decrypted, the updated permissions level having greater permissions relative to the current permissions level.~~

~~13. — The non-transitory computer-readable storage medium of claim 12, further comprising computer-readable program code executable by the processor to cause the processor to:~~

~~determine, by the application, that the updated permissions level meets the required permissions level to perform the operation; and~~

~~authorize performance of the operation by the application based on the determination that the updated permissions level meets the required permissions level to perform the operation.~~

~~14. — The non-transitory computer-readable storage medium of claim 8, wherein the type of the operation comprises one or more of: (i) viewing attributes of the account, (ii) modifying the attributes of the account, (iii) accessing a page of the application, or (iv) processing a transaction using the~~

~~contactless card, further comprising computer-readable program code executable by the processor to cause the processor to:~~

~~receive, by the application, an updated version of the encrypted passport data; and~~

~~transmit, by the application to the contactless card, the updated version of the encrypted passport data for storage in a memory of the contactless card.~~

15.—A method, comprising:

~~receiving, by an application executing on a processor, a request to perform an operation associated with an account;~~

~~receiving, by the application, encrypted data from a contactless card associated with the account, the encrypted data based on a cryptographic algorithm, a customer identifier, and a private key for the contactless card;~~

~~receiving, by the application from an authentication server, an indication specifying that the authentication server verified the encrypted data based on the private key for the contactless card;~~

~~receiving, by the application, encrypted passport data from the contactless card, the encrypted passport data for a passport associated with the account, the encrypted passport data encrypted based on at least one attribute of the passport;~~

~~determining, by the application, the at least one attribute of the passport based at least in part on image data or text input;~~

~~decrypting, by the application, the encrypted passport data based on the at least one attribute of the passport; and~~

~~initiating performance of the operation based on the received indication specifying that the authentication server verified the encrypted data and the decryption of the encrypted passport data.~~

16.—The method of claim 15, further comprising:

~~receiving, by the application, a first image depicting at least one page of the passport;~~

~~extracting, by the application, a text of the at least one page of the passport depicted the first image; and~~

determining the at least one attribute of the passport from the extracted text of the at least one page of the passport, wherein the at least one attribute of the passport comprises a passport number, a passport issue date, and a passport expiration date.

17. The method of claim 16, further comprising:

outputting, by the application, an indication specifying to capture the first image to authorize the operation; and

capturing the first image by an image capture device of a device comprising

the processor.

18. The method of claim 17, further comprising:

receiving, by the application, authentication credentials associated with the account, the authentication credentials comprising one or more of a login, a password, or biometric credentials; and

determining, by the application, that a digital signature of the encrypted passport data received from the contactless card is a valid digital signature based on a public key associated with an entity providing the digital signature.

19. The method of claim 15, further comprising prior to initiating performance of the operation:

determining, by the application, that a current permissions level for the account does not meet a required permissions level to perform the operation;

transmitting, by the application to the authentication server, an indication of the current permissions level for the account and an indication specifying that the encrypted passport data was decrypted; and

receiving, by the application from the authentication server, an updated permissions level assigned by the authentication server to the account based on the received indication specifying that the encrypted passport data was decrypted, the updated permissions level having greater permissions relative to the current permissions level.

20. — ~~The method of claim 19, wherein the type of the operation comprises one or more of: (i) viewing attributes of the account, (ii) modifying the attributes of the account, (iii) accessing a page of the application, or (iv) processing a transaction using the contactless card, the method further comprising:~~

~~determining, by the application, that the updated permissions level meets the required permissions level to perform the operation; and
authorizing performance of the operation by the application based on the determination that the updated permissions level meets the required permissions level to perform the operation.~~

1. A method, comprising:

receiving, by an application executing on a processor of a device, a request to perform an operation associated with an account using a first function of a plurality of functions of the application;

receiving, by the application, encrypted data from a contactless card associated with the account;

receiving, by the application from an authentication server, a first permissions level for the account and an indication specifying that the authentication server verified the encrypted data;

determining, by the application, that the first permissions level for the account does not meet a required permissions level to perform the operation using the first function of the application;

determining, by the application based on the first permissions level not meeting the required permissions level and a first rule of a plurality of rules, that authentication using encrypted passport data is required to initiate performance of the requested operation using the first function of the application;

receiving, by the application, encrypted passport data and a digital signature for the encrypted passport data from the contactless card, the encrypted passport data for a passport associated with the account;

decrypting, by the application, the encrypted passport data;

validating, by the application, the digital signature of the encrypted passport data based on a public key;

transmitting, by the application to the authentication server based on the decryption of the encrypted passport data and the validation of the digital

signature, an indication of the first permissions level for the account, an indication reflecting the validation of the digital signature, and an indication specifying that the encrypted passport data was decrypted;

receiving, by the application from the authentication server, a second permissions level assigned to the account based on the decryption of the encrypted passport data, the second permissions level having greater permissions than the first permissions level; and

initiating, by the first function of the application, performance of the operation based on the received indication specifying that the authentication server verified the encrypted data, the decryption of the encrypted passport data, the second permissions level of the account, and the determination that the digital signature is valid.

2. The method of claim 1, wherein the encrypted data is based on a diversified key and a customer identifier associated with the contactless card, wherein the diversified key is based on a counter value and a master key associated with the contactless card, wherein the server verifies the encrypted data based on the diversified key, the counter value, and the master key.

3. The method of claim 1, further comprising:

receiving, by the application, an updated version of the encrypted passport data; and

transmitting, by the application to the contactless card, the updated version of the encrypted passport data for storage in the contactless card.

4. The method of claim 1, further comprising:

extracting, by the application, at least one attribute of the passport from a first image of the passport, wherein the first image depicts the at least one attribute of the passport, wherein the application decrypts the encrypted data based on the extracted at least one attribute.

5. The method of claim 1, wherein the operation comprises one or more of: (i) viewing attributes of the account using the first function provided by a first page of a plurality of pages of the application, (ii) modifying the attributes of the account using a second function of the plurality of functions provided by a second page of the plurality of pages of the application, (iii) accessing a third

function of the plurality of functions provided by a third page of the plurality of pages of the application, or (iv) processing a transaction using the contactless card using a fourth function of the plurality of functions provided by a fourth page of the plurality of pages of the application.

6. The method of claim 1, wherein the required permissions level is specified by a second rule of the plurality of rules.

7. The method of claim 1, wherein validating the digital signature comprises decrypting the digital signature based on the public key.

8. A non-transitory computer-readable storage medium, the computer-readable storage medium including instructions that when executed by a processor, cause the processor to:

receive, by an application executing on a processor of a device, a request to perform an operation associated with an account using a first function of a plurality of functions of the application;

receive, by the application, encrypted data from a contactless card associated with the account;

receive, by the application from an authentication server, a first permissions level for the account and an indication specifying that the authentication server verified the encrypted data;

determine, by the application, that the first permissions level for the account does not meet a required permissions level to perform the operation using the first function of the application;

determine, by the application based on the first permissions level not meeting the required permissions level and a first rule of a plurality of rules, that authentication using encrypted passport data is required to initiate performance of the requested operation using the first function of the application;

receive, by the application, encrypted passport data and a digital signature for the encrypted passport data from the contactless card, the encrypted passport data for a passport associated with the account;

decrypting, by the application, the encrypted passport data;

validate, by the application, the digital signature of the encrypted passport data based on a public key;

transmit, by the application to the authentication server based on the decryption of the encrypted passport data and the validation of the digital signature, an indication of the first permissions level for the account, an indication reflecting the validation of the digital signature, and an indication specifying that the encrypted passport data was decrypted;

receive, by the application from the authentication server, a second permissions level assigned to the account based on the decryption of the encrypted passport data, the second permissions level having greater permissions than the first permissions level; and

initiate, by the first function of the application, performance of the operation based on the received indication specifying that the authentication server verified the encrypted data, the decryption of the encrypted passport data, the second permissions level of the account, and the determination that the digital signature is valid.

9. The computer-readable storage medium of claim 8, wherein the encrypted data is based on a diversified key and a customer identifier associated with the contactless card, wherein the diversified key is based on a counter value and a master key associated with the contactless card, wherein the server verifies the encrypted data based on the diversified key, the counter value, and the master key.

10. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

receive, by the application, an updated version of the encrypted passport data; and

transmit, by the application to the contactless card, the updated version of the encrypted passport data for storage in the contactless card.

11. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to:

extract, by the application, at least one attribute of the passport from a first image of the passport, wherein the first image depicts the at least one attribute of the passport, wherein the application decrypts the encrypted data based on the extracted at least one attribute.

12. The computer-readable storage medium of claim 8, wherein the operation comprises one or more of: (i) view attributes of the account using the first function provided by a first page of a plurality of pages of the application, (ii) modifying the attributes of the account using a second function of the plurality of functions provided by a second page of the plurality of pages of the application, (iii) accessing a third function of the plurality of functions provided by a third page of the plurality of pages of the application, or (iv) processing a transaction using the contactless card using a fourth function of the plurality of functions provided by a fourth page of the plurality of pages of the application.

13. The computer-readable storage medium of claim 8, wherein the required permissions level is specified by a second rule of the plurality of rules.

14. The computer-readable storage medium of claim 8, wherein validating the digital signature comprises decrypting the digital signature based on the public key.

15. A computing apparatus comprising:

a processor; and

a memory storing instructions that, when executed by the processor, cause the processor to:

receive, by an application executing on a processor of a device, a request to perform an operation associated with an account using a first function of a plurality of functions of the application;

receive, by the application, encrypted data from a contactless card associated with the account;

receive, by the application from an authentication server, a first permissions level for the account and an indication specifying that the authentication server verified the encrypted data;

determine, by the application, that the first permissions level for the account does not meet a required permissions level to perform the operation using the first function of the application;

determine, by the application based on the first permissions level not meeting the required permissions level and a first rule of a plurality of rules, that authentication using encrypted passport data is required to initiate

performance of the requested operation using the first function of the application;

receive, by the application, encrypted passport data and a digital signature for the encrypted passport data from the contactless card, the encrypted passport data for a passport associated with the account;

decrypting, by the application, the encrypted passport data;

validate, by the application, the digital signature of the encrypted passport data based on a public key;

transmit, by the application to the authentication server based on the decryption of the encrypted passport data and the validation of the digital signature, an indication of the first permissions level for the account, an indication reflecting the validation of the digital signature, and an indication specifying that the encrypted passport data was decrypted;

receive, by the application from the authentication server, a second permissions level assigned to the account based on the decryption of the encrypted passport data, the second permissions level having greater permissions than the first permissions level; and

initiate, by the first function of the application, performance of the operation based on the received indication specifying that the authentication server verified the encrypted data, the decryption of the encrypted passport data, the second permissions level of the account, and the determination that the digital signature is valid.

16. The computing apparatus of claim 15, wherein the encrypted data is based on a diversified key and a customer identifier associated with the contactless card, wherein the diversified key is based on a counter value and a master key associated with the contactless card, wherein the server verifies the encrypted data based on the diversified key, the counter value, and the master key.

17. The computing apparatus of claim 15, wherein the instructions further cause the processor to:

receive, by the application, an updated version of the encrypted passport data; and

transmit, by the application to the contactless card, the updated version of the encrypted passport data for storage in the contactless card.

18. The computing apparatus of claim 15, wherein the instructions further cause the processor to:

extract, by the application, at least one attribute of the passport from a first image of the passport, wherein the first image depicts the at least one attribute of the passport, wherein the application decrypts the encrypted data based on the extracted at least one attribute.

19. The computing apparatus of claim 15, wherein the operation comprises one or more of: (i) view attributes of the account using the first function provided by a first page of a plurality of pages of the application, (ii) modifying the attributes of the account using a second function of the plurality of functions provided by a second page of the plurality of pages of the application, (iii) accessing a third function of the plurality of functions provided by a third page of the plurality of pages of the application, or (iv) processing a transaction using the contactless card using a fourth function of the plurality of functions provided by a fourth page of the plurality of pages of the application.

20. The computing apparatus of claim 15, wherein the required permissions level is specified by a second rule of the plurality of rules, wherein validating the digital signature comprises decrypting the digital based on the public key.