

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.