CLAIMS

What is claimed is:

1. A system, comprising:

storage configured to store a master key and a stored counter value associated with a contactless card;

one or more servers comprising processing components and memory components, the memory components configured to store instructions executable by the processing components, the instructions, when executed, to cause the processing components to:

process authentication information to authenticate a user to perform a service;

determine second-factor authentication is required to perform the service for the user;

send an authentication request to a device associated with the user to perform the second-factor authentication;

receive from the device a cryptogram, wherein the cryptogram is generated by a contactless card, and the cryptogram comprises an encrypted shared secret;

generate a diversified key to decrypt the encrypted secret with the master key and the stored counter value;

decrypt the encrypted shared secret to generate a decrypted shared secret, the encrypted shared secret decrypted with the diversified key generated from the master key associated with the contactless card;

perform the second-factor authentication by comparing the decrypted shared secret with a stored shared secret and the counter value with the stored counter value; and

enable the service in response to the decrypted shared secret matching the stored shared secret.

2. The system of claim 1, the processing components configured to prevent performance of the service in response to the decrypted shared secret not matching the stored shared secret.

3. The system of claim 1, the processing components to:

receive the authentication information over a first communication channel; and perform the second-factor authentication over a second communication channel that is different than the first communication channel.

4. The system of claim 1, the processing components configured to: determine the service is a customer service call; and

determine, in response to the service being the customer service call, determine the second-factor authentication is required.

5. The system of claim 1, wherein the processing components to determine the second-authentication request is required based on the service comprising a customer service call switching from a first call agent to a second call agent.

6. The system of claim 1, wherein the processing components to determine the second authentication request is required based on a call agent detecting suspicious activity.

7. A computer-implemented method, comprising:

storing a master key and a stored counter value associated with a contactless card;

processing authentication information to authenticate a user to perform a service;

determining second-factor authentication is required to perform the service for the user; sending an authentication request to a device associated with the user to perform the second-factor authentication;

receiving from the device a cryptogram, wherein the cryptogram is generated by a contactless card, and the cryptogram comprises an encrypted shared secret and a counter value;

generating a diversified key to decrypt the encrypted shared secret with the master key and the stored counter value;

decrypting the encrypted shared secret to generate a decrypted shared secret, the encrypted shared secret decrypted with the diversified key generated from the master key assoc iated with the contactless card;

performing the second-factor authentication by comparing the decrypted shared secret with a stored shared secret and the counter value with the stored counter value; and

enabling the service in response to the decrypted shared secret matching the stored shared secret and the counter value matching the stored counter value.

8. The method of claim 7, comprising preventing performance of the service in response to the decrypted shared secret not matching the stored shared secret.

9. The method of claim 7, comprising:

receiving the authentication information over a first communication channel; and performing the second-factor authentication over a second communication channel that is

different than the first communication channel.

10. The method of claim 7, comprising:

determining the service is a customer service call; and

determining, in response to the service being the customer service call, determine the second-factor authentication is required.

11. The method of claim 7, wherein determining the second-authentication request is required based on the service comprising a customer service call switching from a first call agent to a second call agent.

12. The method of claim 7, wherein determining the second authentication request is required based on a call agent detecting suspicious activity.

13. A computer-readable medium comprising instructions, that when executed by processing circuitry, cause the processing circuitry to:

store a master key and a stored counter value associated with a contactless card;

authenticate a user with authentication information;

determine a second-factor authentication is required to perform a requested service for the user;

communicate an authentication request to a device associated with the user; receive from a contactless card via the device a cryptogram, wherein the cryptogram comprises an encrypted shared secret;

determine a diversified key from the master key associated with the contactless card;

decrypt, with the diversified key, the encrypted shared secret to generate a decrypted shared secret and a counter value;

perform the second-factor authentication by comparing the decrypted shared secret with a stored shared secret and the counter value with the stored counter value; and

enable the service in response to the decrypted shared secret matching the stored shared secret and the counter value matching the stored counter value.

14. The computer-readable medium of claim 13, wherein the instructions to cause the processing circuitry to prevent performance of the service in response to the decrypted shared secret not matching the stored shared secret.