

CLAIMS

1. A computer-implemented method, comprising:
 - receiving, by a service provider system, a request to access a website from a first computing device, the request comprising identifying information to identify a user of the website;
 - sending, by the service provider system, an authentication request to a second computing device associated with the user;
 - receiving, by the service provider system, encrypted authentication information from the second computing device, wherein the encrypted authentication information is retrieved by the second computing device from a contactless card, wherein the encrypted authentication information is encrypted by the contactless card applying an encryption algorithm utilizing at least a counter value, and the counter value is a number of times data is retrieved from the contactless card;
 - authenticating, by the service provider system, the encrypted authentication information based on authenticated information for the user and successfully decrypting the encrypted authentication information; and
 - responsive to authenticating the encrypted authentication information, permitting, by the service provider system, the first computing device to access the website.
2. The computer-implemented method of claim 1, wherein the encrypted authentication information is comprised in a cryptogram generated by the contactless card.
3. The computer-implemented method of claim 1, wherein the encrypted authentication information is generated by the contactless card with a key and a cryptographic algorithm stored on the contactless card.
4. The computer-implemented method of claim 1, wherein the encrypted authentication information is based on a user identifier and the counter value.

5. The computer-implemented method of claim 4, wherein the user identifier is a username for the website and the counter value is related to a dynamic password to access the website.
6. The computer-implemented method of claim 1, wherein the second computing device, the contactless card, or both are registered to an account associated with the user.
7. The computer-implemented method of claim 1, comprising identifying the second computing device based on an associated between the identifying information and the second computing device.
8. The computing-implemented method of claim 1, wherein the identifying information comprises a username for the website, an Internet Protocol (IP) address, an identifier associated with the first computing device, a medium access control (MAC) address, or another identifier associated with the user.
9. A service provider system, comprising:
 - one or more servers comprising:
 - memory comprising instructions; and
 - one or more processors coupled with the memory, the one or more processors,
 - when processing the instructions, to:
 - process a request to access a website received from a first computing device, the request comprising identifying information to identify a user of the website;
 - cause communication of an authentication request to a second computing device associated with the user;
 - process encrypted authentication information received from the second computing device, wherein the encrypted authentication information is retrieved by the second computing device from a contactless card, wherein the encrypted authentication information is encrypted by the contactless card applying an encryption algorithm utilizing at least a counter value, and the counter value is a number of times data is retrieved from the contactless card;

authenticate the encrypted authentication information based on authenticated information for the user and successfully decrypting the encrypted authentication information; and

responsive to authenticating the encrypted authentication information, permit the first computing device to access the website.

10. The service provider system of claim 9, wherein the encrypted authentication information is comprised in a cryptogram generated by the contactless card.

11. The service provider system of claim 9, wherein the encrypted authentication information is generated by the contactless card with a key and a cryptographic algorithm stored on the contactless card.

12. The service provider system of claim 9, wherein the encrypted authentication information is based on a user identifier and the counter value.

13. The service provider system of claim 12, wherein the user identifier is a username for the website and the counter value is related to a dynamic password to access the website.

14. The service provider system of claim 9, wherein the second computing device, the contactless card, or both are registered to an account associated with the user.

15. The service provider system of claim 9, wherein the instructions are further configured to cause the one or more processors to identify the second computing device based on an associated between the identifying information and the second computing device.

16. The service provider system of claim 9, wherein the identifying information comprises a username for the website, an Internet Protocol (IP) address, an identifier associated with the first computing device, a medium access control (MAC) address, or another identifier associated with the user.

17. A computer-implemented method, comprising:
 - receiving, by a system, a request to access an account from a computing device, the request comprising identifying information to identify a user associated with the account;
 - sending, by the system, an authentication request to the computing device;
 - receiving, by the system, encrypted authentication information from a contactless card via the computing device, wherein the encrypted authentication information is received by the computing device from the contactless card and communicated to the system, wherein the encrypted authentication information is encrypted by the contactless card applying an encryption algorithm utilizing at least a counter value, and the counter value is a number of times data is retrieved from the contactless card;
 - authenticating, by the system, the encrypted authentication information based on authenticated information for the user and successfully decrypting the encrypted authentication information; and
 - responsive to authenticating the encrypted authentication information, permitting, by the system, the computing device to access the account.
18. The computer-implemented method of claim 17, wherein the encrypted authentication information is comprised in a cryptogram generated by the contactless card.
19. The computer-implemented method of claim 17, wherein the encrypted authentication information is generated by the contactless card with a key and a cryptographic algorithm stored on the contactless card.
20. The computer-implemented method of claim 17, wherein the encrypted authentication information is based on a user identifier and the counter value.