CLAIMS

1. A computer-implemented method for sharing access to an electronic lock comprising:

   generating, by the access management system, an access unique resource locator (URL) associated with an instant application for provisioning access to the electronic lock to a grantee, wherein the access URL includes an access token;

   sending the access URL to a mobile device of the grantee

   receiving, by the access management system, an access request from the mobile device to activate the access URL, wherein the access request includes a first access token,

   verifying the access request by matching the first access token with the access token generated for the access URL;

   transmitting an access credential to the mobile device to cause the instant application to be rendered on the mobile device upon a positive verification of the access request, wherein the instant application includes one or more configurable elements configured based on the access token associated with the access rights provided to the grantee;

   and

   transmitting the access credential to the electronic lock so as to cause the electronic lock to be unlocked in response to receipt of an unlock request on the instant application.

2. The computer-implemented method according to claim 1, wherein the access URL includes a shortened uniform resource locator hyperlink.

3. The computer-implemented method according to claim 1, wherein the access URL includes a matrix barcode.

4. The computer-implemented method according to claim 1, wherein the access token is associated with an access identity of the grantee.

5. The computer-implemented method according to claim 4, wherein the access identity includes one or more user identifiers associated with the grantee.

6. The computer-implemented method according to claim 1 or claim 4, wherein the access token is associated with an access right granted to the grantee.

7. The computer-implemented method according to claim 1, wherein the access credential is transmitted to a bridge before the access credential is transmitted to the electronic lock.

8. The computer-implemented method according to claim 1, further including the steps of;

in response to the positive verification of the access request, generating, by the access management system, a first factor authentication request to be transmitted to the mobile device;

receiving, by the access management system, an input first factor authentication data from the mobile device;

determining, if the input first factor authentication data corresponds with the first factor authentication data associated with the grantee.

9. The computer-implemented method according to claim 8, further including the steps of;

generating, by the access management system, a second factor authentication request for transmission to the mobile device in response to the input first factor authentication data matching the first factor authentication data associated with the grantee;

receiving, by the access management system, an input second factor authentication data from the mobile device; and

determining if the input second factor authentication data corresponds with the second factor authentication data associated with the grantee.

10. A system for sharing access to an electronic lock, the system comprising:

at least one processor; and

at least one memory including computer program code;

the at least one memory and the computer program code configured to, with the at least one processor, cause the system at least to:

generate, by the access management system, an access unique resource locator (URL) associated with an instant application for provisioning access to the electronic lock to a grantee, wherein the access URL includes an access token;

send the access URL to a mobile device of the grantee;

receive, by the access management system, an access request from the mobile device to activate the access URL, wherein the access request includes a first access token;

verify the access request by matching the first access token with the access token generated for the access URL;

transmit an access credential to the mobile device to cause the instant application to be rendered on the mobile device upon a positive verification of the access request wherein the instant application includes one or more configurable elements configured based on the access token associated with the access rights provided to the grantee; and

transmit the access credential to the electronic lock so as to cause the electronic lock to be unlocked in response to receipt of an unlock request on the instant application.

11. The system according to claim 10, wherein the access URL includes a shortened uniform resource locator hyperlink.

12. The system according to claim 10, wherein the access URL includes a matrix barcode.

13. The system according to claim 10, wherein the access token is associated with an access identity of the grantee.

14. The system according to claim 10, wherein the access identity includes one or more user identifiers associated with the grantee.

15. The system according to claim 10 or claim 13, wherein the access token is associated with an access right granted to the grantee.

16. The system according to claim 10, wherein the access credential is transmitted to a bridge before the access credential is transmitted to the electronic lock.

17. The system according to claim 10, further including the steps of;

in response to the positive verification of the access request, generate, by the access management system, a first factor authentication request to be transmitted to the mobile device;

receive, by the access management system, an input first factor authentication data from the mobile device;

determine, if the input first factor authentication data corresponds with the first factor authentication data associated with the grantee.

18. The system according to claim 17, further including the steps of;

generate, by the access management system, a second factor authentication request for transmission to the mobile device in response to the input first factor authentication data matching the first factor authentication data associated with the grantee;

receive, by the access management system, an input second factor authentication data from the mobile device; and

determine if the input second factor authentication data corresponds with the second factor authentication data associated with the grantee.

19. A computer program comprising instructions which, when the program is executed by a computer, cause the computer to carry out the method of any one of claims 1-9.

20. A computer-readable medium comprising instructions which, when executed by a computer, cause the computer to carry out the method of any one of claims 1-9.