

CLAIMS

1. A method (20) for authenticating to a device (12), comprising:
 - receiving (214), by the device, from a chip (14), data;
 - retrieving (216), by the device, based on the received data, a predetermined encrypted credential;
 - sending (218), by the device, to the chip, a decryption request for decrypting the encrypted credential including or being accompanied with the encrypted credential to be decrypted;
 - retrieving (220), by the chip, a secret key;
 - decrypting (222), by the chip, the encrypted credential by using the secret key;
 - sending (224), by the chip, to the device, as a decryption request response, the credential;
 - verifying (226), by the device, whether the credential is or is not valid; and
 - authenticating (228), by the device, only if the credential is valid, the chip.
2. Method according to claim 1, wherein, to ascertain that the credential is valid, the device decrypts successfully a predetermined encrypted key by using the credential, the key, as a decrypted encrypted key, being used for encrypting at least one resource that belongs to either a chip user who is authorized to access the at least one resource or a role which a chip user has and authorizes to access the at least one resource, the device decrypts at least one encrypted resource by using the key, in order to access the at least one resource.
3. Method according to claim 1, wherein, prior to decrypting the encrypted credential, the chip has successfully authenticated the user.
4. Method according to claim 3, wherein, to authenticate successfully the user, the chip requests the user to provide user authentication credentials, the chip compares the provided user authentication credentials to predetermined reference user authentication credentials and the chip ascertains that the provided user authentication credentials matches the reference user authentication credentials.
5. Method according to claim 1, wherein, once the device has verified the credential, the method further comprises deleting, by the device, the credential.
6. Method according to claim 1, wherein, once the chip has sent the credential, the method further comprises deleting, by the chip, the credential.

7. An authentication device (12), wherein the authentication device is configured to:
- receive (214), from a chip, data;
 - retrieve (216), based on the received data, a predetermined encrypted credential;
 - 5 - send (218), to the chip, a decryption request for decrypting the encrypted credential including or being accompanied with the encrypted credential to be decrypted;
 - receive (224), from the chip, as a decryption request response, the credential;
 - verify (226), whether the credential is or is not valid; and
 - authenticate (228), only if the credential is valid, the chip.
- 10 8. Authentication device according to claim 7, wherein the authentication device is at least one element comprised in a group including:
- a hardware security module type device;
 - a mobile device;
 - a mobile phone;
 - 15 - a user terminal;
 - a Personal Computer;
 - a tablet;
 - a computing device.
9. A chip (14) for authenticating to a device (12), wherein the chip is configured to:
- 20 - send (214), to the device, data;
- receive (218), from the device, a decryption request for decrypting an encrypted credential including or being accompanied with the encrypted credential to be decrypted;
 - retrieve (220) a secret key;
 - 25 - decrypt (222) the encrypted credential by using the secret key; and
 - send (224), to the device, as a decryption request response, the credential.
10. An authentication system (10), wherein, the system including at least one device (12) and at least one chip (14), the at least one device includes the authentication device according to claim 7 and the at least one chip is configured to:
- 30 - send (214), to the device, data;
- receive (218), from the device, a decryption request for decrypting an encrypted credential including or being accompanied with the encrypted credential to be decrypted;

- retrieve (220) a secret key;
- decrypt (222) the encrypted credential by using the secret key; and
- send (224), to the device, as a decryption request response, the credential.