

CLAIMS

1. A method for managing electronic identity cards, comprising:
receiving personal information about a user of an electronic signature service;
receiving activity information about actions of the user on the electronic signature service;
generating an electronic identity card that includes the received personal information and the received activity information; and
providing information about the generated electronic identity card in association with a document signed by the user via the electronic signature service.
2. The method of claim 1, further comprising:
receiving social networking information about the user; and
incorporating the received social networking information into the generated electronic identity card.
3. The method of claim 2, wherein receiving the social networking information includes receiving credentials used by the user to access a social networking service.
4. The method of claim 1, wherein receiving the personal information includes receiving an indication of at least one of: a name, an address, an occupation, a telephone number, and an image of the user.
5. The method of claim 1, wherein providing the information about the generated electronic identity card includes incorporating information from the electronic identity card into a representation of the signed document, and transmitting the signed document.
6. The method of claim 1, wherein providing the information about the generated electronic identity card includes incorporating a reference to the electronic identity card into a representation of the signed document.

7. The method of claim 6 wherein the reference is a uniform resource locator that identifies a computing system configured to provide information about the electronic identity card.

8. The method of claim 1, further comprising:

tracking the activity information in response to document signature events occurring on the electronic signature service; and
incorporating statistics about the tracked activity information into the generated electronic identity card.

9. The method of claim 8 wherein tracking the activity information includes tracking at least one of: a number of documents signed by the user, a number of documents reviewed by the user, a number of documents uploaded for signature by the user, and a number of authentication challenges passed by the user.

10. The method of claim 8, further comprising:

tracking authentication challenges presented to and passed by the user;
incorporation information about the tracked authentication challenges into the generated electronic identity card; and
presenting the information about the tracked authentication challenges as part of a display of the generated electronic identity card.

11. The method of claim 10, wherein presenting the information about the tracked authentication challenges includes presenting a trust score that indicates a level of trust determined based on the information about the tracked authentication challenges.

12. A computer-readable storage medium having contents that, when executed by a computing system, facilitate management of electronic identity cards, by performing the method comprising:

receiving personal information about a user of an electronic signature service;

receiving activity information about actions of the user on the electronic signature service;
generating an electronic identity card that includes the received personal information and the received activity information; and
providing information about the generated electronic identity card in association with a document signed by the user via the electronic signature service.

13. The computer-readable storage medium of claim 12, wherein the computer-readable storage medium is a memory in the computing system, and wherein the contents are instructions in the memory that, when executed, cause the electronic signature service to perform the method.

14. The computer-readable storage medium of claim 12, wherein providing information about the generated electronic identity card includes displaying a green profile badge that indicates a level of ecological commitment based on how many times the user has used the electronic signature service to sign documents.

15. The computer-readable storage medium of claim 12, wherein providing information about the generated electronic identity card includes displaying an authentication level based on how many distinct authentication mechanisms have been used by the user to verify the user's identity, and further based on the types of the distinct authentication mechanisms.

16. A computing system configured to facilitate management of electronic identity cards, comprising:

a processor;

a memory; and

a module that is stored on the memory and that is configured, when executed by the processor, to perform a method comprising:

receiving personal information about a user of an electronic signature service;

receiving activity information about actions of the user on the electronic signature service;

receiving social networking information about the user;

generating an electronic identity card that includes the received personal information, the received activity information, and the received social networking information; and

providing information about the generated electronic identity card in association with a document signed by the user via the electronic signature service.

17. The computing system of claim 16 wherein the module includes software instructions for execution in the memory of the computing system.

18. The computing system of claim 16 wherein the module is an electronic signature service module.

19. The computing system of claim 16 wherein the activity information location information about the user, the location information including indications of locations at which the user reviewed and/or signed an electronic signature document.

20. The computing system of claim 19, wherein the method further comprises:
receiving the indications of locations from a mobile device operated by the user to interact with the electronic signature service.

CLAIMS

1. A method for managing electronic identity cards, comprising:
receiving personal information about a user of an electronic signature service;
receiving activity information about actions of the user on the electronic signature service;
receiving social networking information about the user;
generating an electronic identity card that includes the received personal information, the received activity information, and the received social networking information; and
providing information about the generated electronic identity card in association with a document signed by the user via the electronic signature service.
2. The method of claim 1, wherein receiving the social networking information includes receiving credentials used by the user to access a social networking service.
3. The method of claim 1, wherein receiving the personal information includes receiving an indication of at least one of: a name, an address, an occupation, a telephone number, and an image of the user.
4. The method of claim 1, wherein providing the information about the generated electronic identity card includes incorporating information from the electronic identity card into a representation of the signed document, and transmitting the signed document.
5. The method of claim 1, wherein providing the information about the generated electronic identity card includes incorporating a reference to the electronic identity card into a representation of the signed document.
6. The method of claim 5 wherein the reference is a uniform resource locator that identifies a computing system configured to provide information about the electronic identity card.

7. The method of claim 1, further comprising:
 - tracking the activity information in response to document signature events occurring on the electronic signature service; and
 - incorporating statistics about the tracked activity information into the generated electronic identity card.
8. The method of claim 7 wherein tracking the activity information includes tracking at least one of: a number of documents signed by the user, a number of documents reviewed by the user, a number of documents uploaded for signature by the user, and a number of authentication challenges passed by the user.
9. The method of claim 7, further comprising:
 - tracking authentication challenges presented to and passed by the user;
 - incorporation information about the tracked authentication challenges into the generated electronic identity card; and
 - presenting the information about the tracked authentication challenges as part of a display of the generated electronic identity card.
10. The method of claim 9, wherein presenting the information about the tracked authentication challenges includes presenting a trust score that indicates a level of trust determined based on the information about the tracked authentication challenges.
11. A computer-readable storage medium having contents that, when executed by a computing system, facilitate management of electronic identity cards, by performing the method comprising:
 - receiving personal information about a user of an electronic signature service;
 - receiving activity information about actions of the user on the electronic signature service;
 - receiving social networking information about the user;

generating an electronic identity card that includes the received personal information, the received activity information, and the received social networking information; and

providing information about the generated electronic identity card in association with a document signed by the user via the electronic signature service.

12. The computer-readable storage medium of claim 11, wherein the computer-readable storage medium is a memory in the computing system, and wherein the contents are instructions in the memory that, when executed, cause the electronic signature service to perform the method.

13. The computer-readable storage medium of claim 11, wherein providing information about the generated electronic identity card includes displaying a green profile badge that indicates a level of ecological commitment based on how many times the user has used the electronic signature service to sign documents.

14. The computer-readable storage medium of claim 11, wherein providing information about the generated electronic identity card includes displaying an authentication level based on how many distinct authentication mechanisms have been used by the user to verify the user's identity, and further based on the types of the distinct authentication mechanisms.

15. A computing system configured to facilitate management of electronic identity cards, comprising:

a processor;

a memory; and

a module that is stored on the memory and that is configured, when executed by the processor, to perform a method comprising:

receiving personal information about a user of an electronic signature service;

receiving activity information about actions of the user on the electronic signature service;

receiving social networking information about the user;

generating an electronic identity card that includes the received personal information, the received activity information, and the received social networking information; and

providing information about the generated electronic identity card in association with a document signed by the user via the electronic signature service.

16. The computing system of claim 15 wherein the module includes software instructions for execution in the memory of the computing system.

17. The computing system of claim 15 wherein the module is an electronic signature service module.

18. The computing system of claim 15 wherein the activity information location information about the user, the location information including indications of locations at which the user reviewed and/or signed an electronic signature document.

19. The computing system of claim 18, wherein the method further comprises:
receiving the indications of locations from a mobile device operated by the user to interact with the electronic signature service.