WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a digital identity computer, a request for personal data associated with a user comprising a first public key associated with a relying party;

retrieving, by the digital identity computer, encrypted personal data associated with the user, wherein the personal data is encrypted with a second public key associated with the user;

encrypting, by the digital identity computer, the encrypted personal data with the first public key associated with the relying party to form subsequently encrypted personal data; and

transmitting, by the digital identity computer, the subsequently encrypted personal data and a consent request that the user consents to sharing the personal data with the relying party to a user device operated by the user and wherein the user device is programmed to display the consent request to the user, receive the user's consent from the user in response to the consent request, use a second secret key associated with the second public key to remove a layer of encryption from the subsequently encrypted personal data to form a derivative of the subsequently encrypted personal data and then transmit the derivative of the subsequently encrypted personal data and a consent response to the digital identity computer;

receiving, by the digital identity computer, the derivative of the subsequently encrypted personal data and the consent response;

generating, by the digital identity computer, an access token based on the consent response; and

transmitting, the derivative of the subsequently encrypted personal data and the access token to a relying party computer, which is programmed to obtain the personal data from the derivative of the subsequently encrypted personal data in accordance with the access token using a first private key associated with the first public key, and perform an interaction with the user based on the personal data.

2. The method of claim 1, wherein the request for the personal data associated with the user is received from the relying party computer, and

wherein the digital identity computer accesses a database to retrieve the encrypted personal data.

3. The method of claim 1, wherein the request for the personal data associated with the user is received from the user device,

wherein the digital identity computer accesses a database to retrieve the encrypted personal data.

4. The method of claim 1, wherein the digital identity computer accesses a database to retrieve the personal data encrypted with the second public key associated with the user.

5. The method of claim 1, wherein retrieving the encrypted personal data associated with the user comprises:

transmitting, by the digital identity computer to an identity provider computer, a request for the personal data encrypted with the second public key associated with the user,

receiving, by the digital identity computer from the identity provider computer, the encrypted personal data, wherein the personal data is encrypted with the second public key associated with the user.

6. The method of claim 1, wherein the user device is a mobile device.

7. The method of claim 1, wherein the encrypted personal data associated with the user comprises an assertion of the personal data requested.

8. The method of claim 1, wherein the consent response comprises a length of consent for the personal data to be shared for and a level of access of the personal data.

9. The method of claim 1, wherein the second public key associated with the user is a public key unique to and stored by a digital identity application on the user device.

10. The method of claim 1, wherein the first public key associated with the relying party and the second public key associated with the user are generated using a public-secret key commutative encryption scheme.

11. The method of claim 1, wherein the personal data associated with the user comprises identity data.

12. A digital identity computer comprising:

a processor; and

a non-transitory computer readable medium comprising instructions executable by the processor to perform operations including:

receiving a request for personal data associated with a user comprising a first public key associated with a relying party;

retrieving encrypted personal data associated with the user, wherein the personal data is encrypted with a second public key associated with the user;

encrypting the encrypted personal data with the first public key associated with the relying party to form subsequently encrypted personal data;

transmitting the subsequently encrypted personal data and a consent request that the user consents to sharing the personal data with the relying party to a user device operated by the user and wherein the user device is programmed to display the consent request to the user, receive the user's consent from the user in response to the consent request, use a second secret key associated with the second public key to remove a layer of encryption from the subsequently encrypted personal data to form a derivative of the subsequently encrypted personal data and then transmit the derivative of the subsequently encrypted personal data and a consent response to the digital identity computer;

receiving, by the digital identity computer, the derivative of the subsequently encrypted personal data and the consent response;

generating, by the digital identity computer, an access token based on the consent response; and

transmitting, the derivative of the subsequently encrypted personal data and the access token to a relying party computer, which is programmed to obtain the personal data from

the derivative of the subsequently encrypted personal data in accordance with the access token using a first private key associated with the first public key, and perform an interaction with the user based on the personal data.

13. The digital identity computer of claim 12, further comprising a database comprising encrypted personal data for a plurality of users, wherein the personal data of one of the plurality of users is encrypted using a public key unique to the user.

14. A method comprising:

initiating, by a user device operated by a user, a request for personal data associated with the user operating the user device, wherein a relying party computer operated by a relying party communicating with the user device transmits the request for the personal data to a digital identity computer;

receiving, by the user device from the digital identity computer, subsequently encrypted personal data and a consent request;

displaying, by the user device, the consent request to the user;

using a second secret key associated with a second public key to remove a layer of encryption from the subsequently encrypted personal data to form a derivative of the subsequently encrypted personal data; and

transmitting, by the user device to the digital identity computer, a consent response for the personal data to be shared with the relying party and the derivative of the subsequently encrypted personal data, wherein the digital identity computer is programmed to:

encrypt encrypted personal data with a first public key associated with the relying party to form the subsequently encrypted personal data,

generate an access token based on the consent response,

transmit the subsequently encrypted personal data to the user device, and

transmit the derivative of the subsequently encrypted personal data and the access token to the relying party computer, wherein the relying party computer is programmed to obtain the personal data from the derivative of the subsequently encrypted personal data using a first private key associated with the first public key, access the personal data according to details in the access token, and perform an interaction with the user based on the accessed personal data.

15. The method of claim 14, wherein the user device is a mobile device.

16. The method of claim 14, wherein the consent response comprises a length of time in which the relying party computer can have access to the personal data, and a level of access, where the level of access determines if the personal data is sent or an assertion of the personal data is sent.

17. The method of claim 14, wherein the personal data comprises a date of birth of the user or contact information of the user.

18. The method of claim 14, wherein the user device comprises a digital identity application comprising the personal data and payment account data, the relying party computer also being programmed to use the payment account data to perform the interaction.

19. The method of claim 14, wherein the personal data comprises information about the user.