

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving, by a server computer from a relying entity computer associated
3 with a relying entity, a request for identity attributes associated with a target entity,
4 wherein the request for identity attributes includes a session identifier associated with
5 the target entity and an identifier of the relying entity and was generated by the relying
6 entity in association with a communication session with the target entity and the
7 identifier of the relying entity, wherein the session identifier is derived from an identifier
8 of the target entity and the identifier of the relying entity;
9 validating, by the server computer, the request ~~based on~~ by comparing the
10 session identifier to the identifier of the target entity to confirm that the session identifier
11 is derived from the identifier of the target entity and the identifier of the relying entity,
12 wherein, if the server computer cannot validate the session identifier, the server
13 computer refrains from proceeding to retrieve identity attributes;
14 identifying, by the server computer, based on the identifier of the relying
15 entity, a package defining types of identity attributes for the relying entity and a data
16 access token associated with the package;
17 based on validating the request, transmitting, by the server computer to a
18 digital identity provider computer, a request for a set of identity attributes corresponding
19 to the package, the request comprising the data access token; ~~and~~
20 receiving, by the server computer from the digital identity provider
21 computer, the set of identity attributes; and
22 transmitting, by the server computer to the relying entity computer, the set
23 of identity attributes so that the relying entity can use the session identifier and the set
24 of identity attributes to complete a task.

1 2. ~~—The method of claim 1, further comprising transmitting, by the~~
2 ~~server computer to the relying entity computer, the set of identity attributes.~~

1 ~~3.2.~~ The method of claim-2 1, further comprising generating an event in
2 an event log, the event being associated with the transmitting of the set of identity
3 attributes.

1 ~~4.3.~~ The method of claim-2 1, wherein:
2 the received request for the identity attributes further includes a Uniform
3 Resource Identifier (URI) which identifies a location to transmit the identity attributes;
4 and
5 transmitting the identity attributes to the relying entity computer includes
6 transmitting the set of identity attributes to the URI.

1 ~~5.4.~~ The method of claim 1, further comprising:
2 computing, by the server computer via a hash function and the set of
3 identity attributes, a message digest; and

transmitting, by the server computer to the relying entity computer, the set of identity attributes and the message digest.

~~6.5.~~ The method of claim ~~5~~ 4, further comprising generating a plurality of hash values by at least:

hashing a first identity attribute, of the set of identity attributes, to generate a first hash value;

hashing a second identity attribute, of the set of identity attributes, to generate a second hash value; and

generating a third hash value by hashing the first hash value and the second hash value.

~~7.6.~~ The method of claim ~~6~~ 5, further comprising storing, by the server computer, the plurality of hash values to an event log.

~~8.7.~~ The method of claim 1, wherein:
the identified package comprises a package of assertions associated with the target entity; and
the package of assertions comprises a set of assertions about the target entity, wherein the set of identity attributes are basis for the set of assertions.

~~9.8.~~ The method of claim ~~8~~ 7, wherein the package of assertions specifies a set of assertion types corresponding to the set of assertions, and the method further comprises, prior to receiving the request from the relying entity:

for each assertion type, of the set of assertion types, generating the set of assertions by:

determining a type of identity attribute corresponding to the assertion type;

obtaining an identity attribute, of the set of identity attributes, corresponding to the determined type of identity attribute;

calculating an assertion value corresponding to the assertion type based on the obtained identity attribute; and

storing the assertion value.

1 ~~10.9.~~ The method of claim ~~9.8~~, wherein a plurality of assertion values are
2 stored as the package of assertions in association with the data access token for
3 retrieving the corresponding identity attributes.

1 ~~11.10.~~ The method of claim ~~9.8~~, wherein the server computer refrains from
2 storing the corresponding identity attributes.

1 ~~12.11.~~ The method of claim 1, further comprising requesting, from the
2 target entity, permission to access the identity attributes.

1 ~~13.12.~~ The method of claim ~~12.11~~, further comprising, prior to receiving the
2 request for identity attributes associated with a target entity:
3 receiving, by the server computer from the relying entity computer, a
4 request for assertions associated with the target entity, wherein the request for
5 assertions includes the identifier of the relying entity and an identifier of the target entity;
6 identifying, by the server computer based on the identifier of the relying
7 entity, the package defining types of identity attributes for the relying entity, the package
8 further defining types of assertions for the relying entity;
9 determining a set of assertion values associated with the target entity,
10 based on the types of assertions defined by the package;
11 generating a package of assertions associated with the target entity,
12 based on the set of assertion values for the target entity; and
13 transmitting, to the relying entity computer, the package of assertions
14 associated with the target entity.

1 ~~14.13.~~ A system comprising a server computer comprising:
2 a processor; and
3 a non-transitory computer-readable medium comprising code, executable
4 by the processor, to implement a method as recited in any of claims 1 –~~13.12~~.

1 ~~15.14.~~ A method comprising:
2 generating, by a client computer of a relying entity, a request for a
3 plurality of identity attributes associated with a target entity, wherein the request for

identity attributes includes a session identifier associated with the target entity and an identifier of the relying entity and was generated by the relying entity in association with a communication session with the target entity, and the identifier of the relying entity, wherein the session identifier is derived from an identifier of the target entity and the identifier of the relying entity;

transmitting, by the client computer, the request to a server computer;

thereby causing the server computer to:

validate the request ~~based on~~ by comparing the session identifier to the identifier of the target entity to confirm that the session involves the target entity, wherein, if the server computer cannot validate the session identifier, the server computer refrains from proceeding to retrieve identity attributes;

identify, based on the identifier of the relying entity, a package defining types of identity attributes for the relying entity and a data access token associated with the package,

transmit, to a digital identity provider, a request for a set of identity attributes corresponding to the package, the request comprising the data access token,

receive, from the digital identity provider, the set of identity attributes, and

transmit, to the client computer of the relying entity, the set of identity attributes; ~~and~~

receiving, by the client computer of the relying entity, the set of identity attributes, and

using the session identifier and the set of identity attributes to complete a task.

~~16.15.~~ The method of claim ~~15~~ 14, wherein:

the request for the identity attributes further includes a Uniform Resource Identifier (URI) which identifies a location to transmit the set of identity attributes; and

the client computer of the relying entity receives the identity attributes via the URI.

~~17.16.~~ The method of claim ~~15~~ 14, further comprising:

2 establishing, by the client computer, a communication session with the
3 target entity;
4 generating, by the client computer, the session identifier for the
5 communication session;
6 transmitting, by the client computer to the target entity during the
7 communication session, a request for permission to retrieve the identity attributes; and

8 receiving, by the client computer from the target entity during the
9 communication session, permission to retrieve the identity attributes.

1 ~~18.~~17. The method of claim ~~15~~ 14, further comprising:
2 receiving, by the client computer, a message digest with the set of identity
3 attributes,
4 wherein the message digest was computed by the server computer via a
5 hash function and the set of identity attributes.

1 ~~19.~~ ~~The method of claim 15, further comprising using the session~~
2 ~~identifier and the set of identity attributes to complete a task.~~

1 ~~20.~~18. The method of claim ~~15~~ 14, wherein the server computer
2 determines an assertions model based on the identifier of the relying entity, and
3 determines the set of identity attributes associated with the relying entity based on the
4 assertions model.

1 ~~21.~~19. A system comprising a client computer comprising:
2 a processor; and
3 a non-transitory computer-readable medium comprising code,
4 executable by the processor, to implement a method as recited in any of claims ~~15—20~~
5 14 – 18.