

WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:
receiving a delegation request from a first entity, fulfilment of which involves granting a second entity an access privilege to a computing resource;
generating a session key based at least in part on a restriction and a secret credential shared with the first entity, the restriction indicating a limitation on access to be granted to the second entity;
providing the session key to the first entity;
receiving, from the second entity, an access request to access the computing resource, the access request including information that indicates access to the session key;
validating the access request based at least in part on the session key; and
granting, to the second entity, access to the computing resource.
2. The computer-implemented method of claim 1, wherein the restriction corresponds to an identity of a key zone of a plurality of key zones.
3. The computer-implemented method of claim 1, wherein:
the delegation request includes an identity of the entity for which the session key is to be generated; and
the restriction is based at least in part on the identity of the entity.
4. The computer-implemented method of claim 1, wherein the restriction corresponds to a restriction on a permitted action.
5. The computer-implemented method of claim 1, wherein:
the access request further includes the restriction provided by the first entity;
and

validating the access request includes validating that the session key was generated based at least in part on the restriction included in the access request.

6. The computer-implemented method of claim 1, wherein the restriction corresponds to a limit on an amount of time the session key is valid.

7. A system, comprising:
one or more processors; and
memory including instructions that, when executed by the one or more processors, cause the system to:
receive a delegation request from a first entity, fulfilment of which involving granting a second entity an access privilege to a computing resource;
in response to receipt of the delegation request:
generate a session key based at least in part on passing a secret credential, shared between the first entity and the one or more computer systems, and a session restriction through a cryptographic hash algorithm, the session restriction indicating a limitation on access to be granted to the second entity; and
provide the session key to the first entity;
receive an access request from the second entity to access the computing resource, the access request associated with the session key; and
in response to receipt of the access request:
validate the access request based at least in part on the session key; and
grant, to the second entity, access to the computing resource.

8. The system of claim 7, wherein the instructions that validate the access request include instructions that cause the system to validate whether the request complies with the session restriction.

9. The system of claim 7, wherein the access request is a first access request and the instructions include further instructions that cause the system to:

- receive a second access request from a third entity to access the computing resource, the second access request associated with the session key; and
- in response to receipt of the second access request:
 - validate the second access request based at least in part on the session key; and
 - grant, to the third entity, access to the computing resource.

10. The system of claim 7, further comprising the first entity, wherein the first entity comprises one or more computer systems configured with first instructions that, when executed by the one or more computer systems, causes the one or more computer systems to, as a result of receiving the session key, provide the session key to the second entity without providing the secret credential to the second entity.

11. The system of claim 10, wherein the first instructions that provide the session key to the second entity include instructions that cause the one or more computer systems to provide information, usable by the second entity to obtain the session key, to an electronic destination accessible to the second entity.

12. The system of claim 11, wherein the electronic destination is an e-mail address.

13. The system of claim 7, wherein the instructions that cause the system to validate the access request, include instructions that cause the system to apply the cryptographic hash algorithm both to a first set of inputs and a second set of inputs, wherein:

- the first set of inputs include the secret credential, the access request, and the session restriction; and
- the second set of inputs include the session key and the access request.

14. The system of claim 13, wherein the cryptographic hash algorithm is a hash-based message authentication code function.

15. The system of claim 7, wherein the access request is associated with the session key by providing a digital signature with the access request generated using the session key.

16. The system of claim 15, wherein the instructions that cause the system to validate the access request, include instructions that cause the system to:

apply the cryptographic hash algorithm to the secret credential, the access request, and the session restriction to obtain a hash result; and
compare the hash result to the digital signature.

17. A non-transitory computer-readable storage medium having stored thereon executable instructions that, when executed by one or more processors of a computer system, cause the computer system to at least:

receive a first request from a first entity, fulfilment of which involving granting a second entity an access privilege to a computing resource;

generate a session key based at least in part on a restriction and a secret credential shared between the first entity and the computer system, the restriction indicating a limitation on access to be granted to the second entity;

provide the session key, usable at least in part to prove possession of an access privilege to a computing resource, to the first entity;

receive a second request to access the computing resource, fulfilment of which involves providing a second entity access to a computing resource, the second request associated with the session key;

validate the second request based at least in part on the session key; and

fulfill the second request by providing access to the computing resource depending at least in part on validation of the session key.

18. The non-transitory computer-readable storage medium of claim 17, wherein the executable instructions that cause the computer system to fulfill the second request include executable instructions that cause the computer system to fulfill the second request without providing the second entity access to the secret credential.

19. The non-transitory computer-readable storage medium of claim 17, wherein the executable instructions further include executable instructions that cause the computer system to:

receive a third request to access the computing resource, fulfilment of which involves providing a third entity access to the computing resource, the third request associated with the session key;

validate the third request based at least in part on the session key; and

fulfill the third request by providing access to the computing resource depending at least in part on validation of the session key.

20. The non-transitory computer-readable storage medium of claim 17, wherein:

the second request includes a digital signature generated using the session key; and

validating the second request further includes validating authenticity of the digital signature.