

WHAT IS CLAIMED IS:

1. A computer-implemented method, comprising:
 - generating a signing key by performing at least:
 - obtaining a key that is a shared secret between a client device and a computer system of a service;
 - deriving, based at least in part on the shared secret and information indicating a date on which use of the signing key is to be restricted, a date key whose use is limited to the date;
 - deriving, based at least in part on the date key and information indicating a region in which use of the signing key is to be restricted, a region key whose use is restricted to both the date and the region; and
 - deriving, based at least in part on the region key and information indicating a service to which use of the signing key is to be restricted, a service key whose use is restricted to the date, the region, and the service;
 - obtaining, at the computer system of the service, a canonicalized message from the client device and a first digital signature;
 - deriving, at the computer system of the service, a second digital signature based at least in part on the canonicalized message and the signing key; and
 - determining, at the computer system of the service, that the canonicalized message is authentic as a result of the first digital signature matching the second digital signature.
2. The computer-implemented method of claim 1, wherein the service key is the signing key.
3. The computer-implemented method of claim 1, wherein deriving the date key, deriving the region key, and deriving the service key are performed using a hash-based message authentication code function.
4. The computer-implemented method of claim 3, wherein the hash-based message authentication code function utilizes a secure hash algorithm (SHA)-256 cryptographic hash function.

5. The computer-implemented method of claim 1, wherein the service is from a plurality of services with respective identifiers that indicate key restrictions to those services.

6. The computer-implemented method of claim 1, wherein the canonicalized message is an application programming interface request and the method further comprises fulfilling the application programming interface request conditioned on the canonicalized message being authentic.

7. A non-transitory computer-readable storage medium storing thereon instructions executable by one or more processors of a first computer system to cause the first computer system to:

- generate a signing key by performing at least:

- obtaining a key that is a shared secret between the first computer system and a second computer system;

- deriving, based at least in part on the shared secret and information indicating a date on which use of the signing key is to be restricted, a date key whose use is limited to the date;

- deriving, based at least in part on the date key and information indicating a region in which use of the signing key is to be restricted, a region key whose use is restricted to both the date and the region; and

- deriving, based at least in part on the region key and information indicating a service to which use of the signing key is to be restricted, a service key whose use is restricted to the date, the region, and the service;

- canonicalize a message to result in a canonicalized message;

- derive a digital signature of the canonicalized message based at least in part on the canonicalized message and the signing key; and

- transmit the canonicalized message and the digital signature to the second computer system.

8. The non-transitory computer-readable storage medium of claim 7, wherein the first computer system is a client computer system and the second computer system is a server of the service.
9. The non-transitory computer-readable storage medium of claim 7, wherein the message is an application programming interface request.
10. The non-transitory computer-readable storage medium of claim 7, wherein deriving the date key, deriving the region key, and deriving the service key utilizes a cryptographic hash function.
11. The non-transitory computer-readable storage medium of claim 7, wherein the information indicating the date, the information indicating the region, and the information indicating the service are encoded as strings.
12. A system, comprising:
 one or more processors; and
 memory storing instructions executable by the one or more processors to cause the system to:
 obtain a signing key by at least:
 obtaining a key that is a shared secret between the system and another system;
 utilize a cryptographic hash function, the key, information indicating a date to which use of the signing key is to be restricted, information indicating a region in which use of the signing key is to be restricted, and information indicating a service to which use of the signing key is to be restricted to derive the signing key;
 obtain a canonicalized message;
 use the signing key to generate a digital signature of the canonicalized message.
13. The system of claim 12, wherein the canonicalized message is an application programming interface request.

14. The system of claim 12, wherein the cryptographic hash function is used in a hash-based message authentication code function.

15. The system of claim 12, wherein the instructions that cause the system to derive the signing key are executable to cause the system to:

- derive a date key based at least in part on the information indicating the date and the key;

- derive a region key based at least in part on the date key and the information indicating the region; and

- derive the signing key based at least in part on the region key and the information indicating the service