

CLAIMS

1. A system, comprising:
a plurality of instance hosts of a virtual computing service of a provider network,
including at least a first instance host comprising one or more compute instances;
wherein a particular compute instance of the one or more compute instances is configured to:
 - in response to a first identity query from a first authenticator associated with a first application, provide an indication of a first cryptographically verifiable identity (CVI) assigned to the particular compute instance within a first instance identity namespace (IIN), wherein the first CVI is associated with a cryptographic key pair designated for the first compute instance, wherein a private key of the cryptographic key pair is managed by a secure key store configured to prevent copying of the private key to locations external to the secure key store, and wherein the virtual computing service enables the particular compute instance to use the private key to provide the indication of the first CVI;
 - in response to a determination that the first CVI has been accepted by the first authenticator, perform one or more operations of the first application;
 - in response to a second identity query from a second authenticator associated with a second application, provide an indication of a different CVI assigned to the first compute instance within a different IIN; and
 - in response to a determination that the second CVI has been accepted by the second authenticator, perform one or more operations of the second application.
2. The system as recited in claim 1, wherein the indication of the first CVI includes a first certificate formatted in accordance with a public key infrastructure (PKI) standard.
3. The system as recited in claim 1, wherein the particular compute instance is further configured to:

invoke a programmatic interface implemented by a virtualization management component of the first instance host to obtain at least one artifact included in the indication of the first CVI.

4. The system as recited in claim 1, wherein the secure key store comprises one of: (a) a hardware security module of a security service of a provider network, or (b) a peripheral device attached to a communication bus of the first instance host.

5. The system as recited in claim 1, wherein the first CVI comprises one or more of: (a) a DNS (Domain Name System) name of the particular compute instance based at least in part on a virtual IP (Internet Protocol) address assigned to the particular compute instance, (b) a public IP address assigned to the particular compute instance, (c) a private IP address assigned to the particular compute instance, (d) a unique name assigned to the particular compute instance by the virtual computing service (VCS) of the provider network from a VCS-defined namespace, (e) a unique name selected from a customer-defined namespace by a customer of the provider network, (f) a name selected from a VCS-defined namespace by a customer of the provider network, (g) a DNS name selected by a customer of the provider network, or (h) a name assigned to the particular compute instance within a namespace defined by a third party.

6. A method, comprising:

launching, at an instance host of a virtual computing service at a provider network, one or more compute instances;

receiving, at a first compute instance of the one or more compute instances, a first identity query;

providing, from the first compute instance in response to the first identity query, an indication of a first cryptographically verifiable identify (CVI) assigned to the first compute instance within a first instance identity namespace (IIN), wherein the first CVI is associated with a cryptographic key pair, wherein a private key of the cryptographic key pair is managed by a secure key store configured to prevent copying of the private key, and wherein the virtual computing service enables the

first compute instance to use the private key to provide the indication of the first CVI;
receiving, at the first compute instance, a second identity query; and
providing, from the first compute instance in response to the second identity query, an indication of a different CVI assigned to the first compute instance within a different IIN.

7. The method as recited in claim 6, wherein the indication of the first CVI includes a first certificate formatted in accordance with a public key infrastructure (PKI) standard.

8. The method as recited in claim 6, further comprising:
invoking, by the first compute instance, a programmatic interface implemented by a virtualization management component of the instance host to obtain at least a portion of an artifact included in the indication of the first CVI.

9. The method as recited in claim 6, wherein the second CVI is associated with a different cryptographic key pair.

10. The method as recited in claim 6, wherein the secure key store comprises one of: (a) a hardware security module of a security service of a provider network, or (b) a peripheral device attached to a communication bus of the instance host.

11. The method as recited in claim 6, wherein the first CVI comprises one or more of: (a) a DNS (Domain Name System) name of the first compute instance based at least in part on a virtual IP (Internet Protocol) address assigned to the first compute instance, (b) a public IP address assigned to the first compute instance, (c) a private IP address assigned to the first compute instance, (d) a unique name assigned to the first compute instance by a virtual computing service (VCS) of the provider network from a VCS-defined namespace, (e) a unique name selected from a customer-defined namespace by a customer of the provider network, (f) a name selected from a VCS-defined namespace by a customer of the provider network, (g) a DNS

name selected by a customer of the provider network, or (h) a name assigned to the particular compute instance within a namespace defined by a third party.

12. The method as recited in claim 6, wherein the indication of the first CVI includes an identity validator comprising one or more of: (a) a public certificate authority (CA), (b) a validation authority implemented within the provider network, (c) a validation authority implemented within a customer network owned by a customer of the provider network to whom the first compute instance is assigned, or (d) a third party validation authority.

13. The method as recited in claim 6, further comprising:
providing, from the first compute instance in response to the first identity query, an indication of a first validity period of the first CVI; and
providing, from the first compute instance in response to the second identity query, an indication of a second validity period of the second CVI, wherein the second validity period differs from the first validity period.

14. The method as recited in claim 6, further comprising:
receiving, at a control-plane component of the provider network, an instance configuration request indicating that the first compute instance is to be assigned an identity within the first IIN; and
initiating, by the control-plane component in response to the instance configuration request, an assignment of an identity to the first compute instance within the first IIN.

15. The method as recited in claim 6, wherein the first identity query is received at the first compute instance from a license manager associated with a first application, and wherein the first CVI is used by the license manager to verify that the first compute instance is licensed to utilize the first application.

16. The method as recited in claim 6, further comprising:

establishing, by a service manager of a particular service implemented at the provider network, an instance failover group comprising a second compute instance and a third compute instance, wherein in the event of a failure at the second compute instance, an application which was executing at the second compute instance is to be failed over to the third compute instance; and

initiating, by the service manager, (a) an assignment of a shared CVI to the second compute instance and (b) an assignment of the shared CVI to the third compute instance, wherein the shared CVI is to be used to verify that the application can be executed at the second compute instance and at the third compute instance.

17. A non-transitory computer-accessible storage medium storing program instructions that when executed on one or more processors:

receive, at a first compute instance of a virtual computing service, a first identity query;

provide, from the first compute instance in response to the first identity query, an indication of a first cryptographically verifiable identify (CVI) assigned to the first compute instance within a first instance identity namespace (IIN), wherein the first CVI is associated with a cryptographic key pair, wherein a private key of the cryptographic key pair is managed by a secure key store configured to prevent copying of the private key, and wherein the virtual computing service enables the first compute instance to use the private key to provide the indication of the first CVI;

receive, at the first compute instance, a second identity query; and

provide, from the first compute instance in response to the second identity query, an indication of a different CVI assigned to the first compute instance within a different IIN.

18. The non-transitory computer-accessible storage medium as recited in claim 17, wherein the indication of the first CVI includes a first certificate formatted in accordance with a public key infrastructure (PKI) standard.

19. The non-transitory computer-accessible storage medium as recited in claim 17, wherein the instructions when executed on the one or more processors:

invoke, from the first compute instance, a programmatic interface implemented by a virtualization management component of an instance host to obtain at least a portion of data included in the indication of the first CVI.

20. The non-transitory computer-accessible storage medium as recited in claim 17, wherein the first CVI comprises one or more of: (a) a DNS (Domain Name System) name of the first compute instance based at least in part on a virtual IP (Internet Protocol) address assigned to the instance, (b) a public IP address assigned to the first compute instance, (c) a private IP address assigned to the first compute instance, (d) a unique name assigned to the first compute instance by a virtual computing service (VCS) of a provider network from a VCS-defined namespace, (e) a unique name selected from a customer-defined namespace by a customer of a provider network, (f) a name selected from a VCS-defined namespace by a customer of a provider network, (g) a DNS name selected by a customer of a provider network, or (h) a name assigned to the first compute instance within a namespace defined by a third party.