WHAT IS CLAIMED IS:

1. A method comprising:

receiving, at a hardware security module (HSM), a cryptographic operation request comprising a cryptographic key and at least one authorization token generated by the HSM;

verifying that the HSM generated and signed the at least one authorization token;

determining, by the HSM, whether an access control list (ACL) associated with the cryptographic key of the cryptographic operation request is authorized to govern access to the cryptographic key;

validating, by the HSM, the at least one authorization token; and

when the at least one authorization token is valid and the ACL is authorized to govern access to the cryptographic key of the cryptographic operation request, processing, by the HSM, the cryptographic operation request.

2. The method of claim 1, wherein the at least one authorization token is valid when at least one of:

the at least one authorization token is signed by an authorizer key;

the cryptographic operation request has been received by the HSM within an authorization time period defined by the at least one authorization token; or

the HSM has received the cryptographic operation request less times than a limit number defined by the at least one authorization token.

3. The method of claim 1 or 2, further comprising:

when the ACL is authorized to govern access to the cryptographic key of the cryptographic operation request, determining, by the HSM, whether a cryptographic operation requested by the cryptographic operation request is allowed by the ACL; and

when the cryptographic operation requested by the cryptographic operation request is allowed by the ACL, processing the cryptographic operation request.

4. The method of any one of claims 1–3, further comprising:

receiving, at the HSM, a challenge request from an owner of the cryptographic key; and

issuing, from the HSM, a corresponding authorization token to the owner of the cryptographic key.

5. The method of claim 4, wherein the corresponding authorization token comprises data identifying the HSM and a cryptographic signature of the HSM.

6. The method of claim 1, wherein the ACL associated with the cryptographic key is included as an intrinsic property of the cryptographic key received at the HSM.

7. The method of claim 1, wherein the ACL associated with the cryptographic key is encoded in the authorization token received at the HSM.

8. A hardware security module (HSM) comprising:

data processing hardware; and

memory hardware in communication with the data processing hardware, the memory hardware storing instructions that when executed on the data processing hardware cause the data processing hardware to perform operations comprising:

receiving a cryptographic operation request comprising a cryptographic key and at least one authorization token generated by the HSM;

verifying that the HSM generated and signed the at least one authorization token;

determining whether an access control list (ACL) associated with the cryptographic key of the cryptographic operation request is authorized to govern access to the cryptographic key;

validating the at least one authorization token; and

when the at least one authorization token is valid and the ACL is authorized to govern access to the cryptographic key of the cryptographic operation request, processing the cryptographic operation request.

9. The HSM of claim 8, wherein the at least one authorization token is valid when at least one of:

the at least one authorization token is signed by an authorizer key;

the cryptographic operation request has been received by the HSM within an authorization time period defined by the at least one authorization token; or

the HSM has received the cryptographic operation request less times than a limit number defined by the at least one authorization token.

10. The HSM of claim 8 or 9, wherein the operations further comprise:

when ACL is authorized to govern access to the cryptographic key of the cryptographic operation request, determining whether a cryptographic operation requested by the cryptographic operation request is allowed by the ACL; and

when the cryptographic operation requested by the cryptographic operation request is allowed by the ACL, processing the cryptographic operation request.

11. The HSM of any one of claims 8–10, wherein the operations further comprise:

receiving a challenge request from an owner of the cryptographic key; and

issuing a corresponding authorization token to the owner of the cryptographic key.

12. The HSM of claim 11, wherein the corresponding authorization token comprises data identifying the HSM and a cryptographic signature of the HSM.

13. The HSM of claim 8, wherein the ACL associated with the cryptographic key is included as an intrinsic property of the cryptographic key received at the HSM.

14. The HSM of claim 8, wherein the ACL associated with the cryptographic key is encoded in the authorization token received at the HSM.

15. A method comprising:

receiving, at a distributed system, a cryptographic operation request from a user, the cryptographic operation request comprising a cryptographic key and at least one authorization token;

sending, by the distributed system, the cryptographic operation request to a hardware security module (HSM) configured to perform operations comprising:

verifying that the HSM generated and signed the at least one authorization token;

determining whether an access control list (ACL) associated with the cryptographic key of the cryptographic operation request is authorized to govern access to the cryptographic key;

validating the at least one authorization token; and

when the at least one authorization token is valid and the ACL is authorized to govern access to the cryptographic key of the cryptographic operation request, processing the cryptographic operation request;

receiving, at the distributed system, a response from the HSM, and when the HSM processes the cryptographic operation request, the response comprises a result of the cryptographic operation; and

sending the response from the distributed system to the user.

16. The method of claim 15, wherein the at least one authorization token is valid when at least one of:

the at least one authorization token is signed by an authorizer key;

the cryptographic operation request has been received by the HSM within an authorization time period defined by the at least one authorization token; or

the HSM has received the cryptographic operation request less times than a limit number defined by the at least one authorization token.

17. The method of claim 15 or 16, wherein the operations of the HSM further comprise:

when the ACL is authorized to govern access to the cryptographic key of the cryptographic operation request, determining whether a cryptographic operation requested by the cryptographic operation request is allowed by the ACL; and

when the cryptographic operation requested by the cryptographic operation request is allowed by the ACL, processing the cryptographic operation request.

18. The method of any one of claims 15–17, further comprising:

receiving, at the distributed system, a challenge request from an owner of the cryptographic key; and

sending the challenge request to the HSM, the HSM configured to issue a corresponding authorization token to the owner of the cryptographic key.

19. The method of claim 18, wherein the corresponding authorization token comprises data identifying the HSM and a cryptographic signature of the HSM.

20. The method of claim 15, wherein the ACL associated with the cryptographic key is included as an intrinsic property of the cryptographic key received at the HSM.

21. The method of claim 15, wherein the ACL associated with the cryptographic key is encoded in the authorization token received at the HSM.

22. A method comprising:

receiving, at a distributed system, a cryptographic operation request from a user, the cryptographic operation request comprising a cryptographic key;

obtaining, by the distributed system, at least one authorization token;

sending, by the distributed system, the operation request and the least one authorization token to a hardware security module (HSM) configured to perform operations comprising:

verifying that the HSM generated and signed the at least one authorization token;

determining whether an access control list (ACL) associated with the cryptographic key of the cryptographic operation request is authorized to govern access to the cryptographic key;

validating the at least one authorization token; and

when the at least one authorization token is valid and the ACL is authorized to govern access to the cryptographic key of the cryptographic operation request, processing the cryptographic operation request;

receiving, at the distributed system, a response from the HSM, and when the HSM processes the cryptographic operation request, the response comprises a result of the cryptographic operation; and

sending the response from the distributed system to the user.

23. The method of claim 22, wherein the at least one authorization token is valid when at least one of:

the at least one authorization token is signed by an authorizer key;

the cryptographic operation request has been received by the HSM within an authorization time period defined by the at least one authorization token; or

the HSM has received the cryptographic operation request less times than a limit number defined by the at least one authorization token.

24. The method of claim 22 or 23, wherein the operations of the HSM further comprise:

when the cryptographic key of the cryptographic operation request matches the corresponding cryptographic key of the ACL, determining whether a cryptographic operation requested by the cryptographic operation request is allowed by the ACL; and

when the cryptographic operation requested by the cryptographic operation request is allowed by the ACL, processing the cryptographic operation request.

25. The method of any one of claims 22–24, further comprising:

receiving, at the distributed system, a challenge request from an owner of the cryptographic key; and

sending the challenge request to the HSM, the HSM configured to issue a corresponding authorization token to the owner of the cryptographic key.

26. The method of claim 25, wherein the corresponding authorization token comprises data identifying the HSM and a cryptographic signature of the HSM.

27. The method of claim 22, wherein the ACL associated with the cryptographic key is included as an intrinsic property of the cryptographic key received at the HSM.

28. The method of claim 22, wherein the ACL associated with the cryptographic key is encoded in the authorization token received at the HSM.