

CLAIMS

1. An access management process orchestration method, comprising:
 - receiving a request for accessing a managed resource of an information system;
 - querying an authorization for accessing the resource from an access manager; and
 - in response to the querying of the authorization, requesting an access control policy update to grant the access to the managed resource;wherein receiving the request, querying the authorization, and requesting the access control policy update comprises:
 - generating a transaction record; and
 - adding the transaction record to a distributed ledger, wherein the distributed ledger simultaneously maintains the transaction record at multiple nodes throughout a network.
2. The method of claim 1, wherein the method further comprises exchanging the transaction record between the multiple nodes of the distributed ledger.
3. The method of any one of the preceding claims, wherein the multiple nodes are interconnected via cryptographically secured channels.
4. The method of any one of the preceding claims, wherein the transaction record comprises at least one administrative action selected from the group consisting of a request access action, an access approved action, an access denied action, an access granted action, a revoke access action, and an access revoked action.
5. The method of claim 4, wherein the administrative action associated with the access granted action changes an authorization policy to allow access of a user to the information system.
6. The method of any one of claims 4 to 5, wherein the administrative action associated with the revoke access action changes an authorization policy to deny access of a user to the information system.
7. The method of any one of claims 4 to 6, further comprising:
 - transmitting the transaction record to the information system; and

automatically executing the administrative action on the information system.

8. The method of any one of the preceding claims, wherein requesting the access control policy update comprises executing a smart contract that processes transactions in the distributed ledger.
9. The method of any one of the preceding claims, wherein:
 - the managed resource of the information system is one of a plurality of managed resources of a plurality of information systems;
 - each of the plurality of information systems includes a local access control system;
 - and
 - the method further comprises calling one of the local access control systems to request a change to a local authorization policy.
10. The method of any one of the preceding claims, further comprising:
 - transmitting the received request to an owner of the information system;
 - receiving an approval responsive to the request from the owner of the information system;
 - recording the approval in the distributed ledger;
 - transmitting the request to an administrator of the information system;
 - executing an action responsive to the request on the information system; and
 - recording the action in the distributed ledger.
11. An access management governance orchestrator, comprising:
 - a peer node associated with a blockchain network, the blockchain network comprising a plurality of nodes associated with at least one of an asset owner function, an administrator function, and an auditor function, the peer node adapted to:
 - record a request access record from a user of an information system in a distributed ledger;
 - record an owner approval record from the asset owner function, the owner approval record responsive to the request access record in the distributed ledger;
 - execute a smart contract responsive to the request access record and the owner approval record granting access on the information system, wherein the smart

contract changes an authorization policy to allow access of the user to the information system; and
record an execution record of the smart contract in the distributed ledger.

12. The access management governance orchestrator of claim 11, wherein the peer node is further adapted to:

storing one or more of the request access record, the owner approval record, and the execution record in a transaction block;
selecting one of the plurality nodes as a signature node to sign the transaction block according to a consensus protocol; and
signing, by the selected signature node, the transaction block.

13. The access management governance orchestrator of any one of claims 11 to 12, wherein the peer node is further adapted to:

receive a new peer request to add a new node to the blockchain network; and
transmitting the new peer request to the plurality of nodes in the blockchain network for approval according to a consensus protocol.

14. The access management governance orchestrator of any one of claims 11 to 13, wherein changing the authorization policy comprises calling a local access control system associated with the information system to request a change to a local authorization policy.

15. The access management governance orchestrator of any one of claims 11 to 14, wherein the peer node is further adapted to review the distributed ledger for execution records that are not associated with owner approval records.

16. A computer program product comprising a non-transitory computer readable storage medium having a plurality of instructions stored thereon, which, when executed by a processor, cause the processor to:

receive a request for accessing to a managed resource of an information system;
query an authorization for accessing the resource from an access manager; and
in response to the querying the authorization, request an access control policy update to grant the access to the managed resource;

wherein receiving the request, querying the authorization, and requesting the access control policy update comprises:

generating a transaction record; and
adding the transaction record to a distributed ledger.

17. The computer program product of claim 16, wherein the transaction record includes at least one administrative action chosen from the group consisting of a request access record, an access approved record, an access denied record, an access granted record, a revoke access record, and an access revoked record.

18. The computer program product of any one of claims 16 to 17, wherein:
the managed resource of the information system is one of a plurality of managed resources of a plurality of information systems;
each of the information systems includes a local access control system;
and
further comprising instructions which, when executed by a processor, cause the processor to call one of the local access control systems to request a change to a local authorization policy.

19. The computer program product of any one of claim 16 to 18, further comprising instructions which, when executed by a processor, cause the processor to:
transmit the received request to an owner of the information system;
receive an approval responsive to the request from the owner of the information system;
record the approval in the distributed ledger;
transmit the request to an administrator of the information system;
execute an action responsive to the request on the information system; and
recording the action in the distributed ledger.

20. The computer program product of any one of claims 16 to 19, wherein requesting the access control policy update comprises executing a smart contract that processes transactions in the distributed ledger.