

CLAIMS

1. A method performed by data processing apparatus, the method comprising:
 - launching a root enclave;
 - accessing an enclave manifest by the root enclave, wherein the enclave manifest specifies, for each of a plurality of component enclaves, a unique role for the respective component enclave, wherein each enclave is a trusted execution environment and each role is a task to be performed by the respective component enclave; and
 - instantiating each of the component enclaves, each component enclave configured to perform its respective role;
 - wherein the root enclave and component enclaves form an enclave pod, wherein:
 - each component enclave of the enclave pod has a respective first key to securely communicate with other component enclaves of the enclave pod, wherein the first key of each component enclave is certified by the root enclave by use of a second key; and
 - each component enclave of the enclave pod ensures that the first key of another component enclave of the enclave pod is also certified by the same second key to share information.
2. The method of claim 1, further comprising:
 - generating logs based on all transactions or actions performed in at least the component enclaves; and
 - cryptographically signing the logs with keys of the enclave pod.
3. The method of claim 1 or claim 2, further comprising:
 - providing, from the root enclave, to a verifier, the identities of the root enclave and the manifest; and
 - in response to a verification of the identities of the root enclave and the manifest, receiving, from the verifier, one or more of data and code for the component enclaves.

4. The method of any preceding claim, wherein the enclave pod is an isolated and secure execution environment.

5. A system, comprising:
 - a plurality of computers each in data communication with each other; and
 - a non-transitory computer readable medium storing instructions executable by the computers so as to cause the computers to perform operations comprising:
 - launching a root enclave;
 - accessing an enclave manifest by the root enclave, wherein the enclave manifest specifies, for each of a plurality of component enclaves, a unique role for the respective component enclave, wherein each enclave is a trusted execution environment and each role is a task to be performed by the respective component enclave; and
 - instantiating each of the component enclaves, each component enclave configured to perform its respective role;
 - wherein the root enclave and component enclaves form an enclave pod, wherein the enclave pod is an isolated and secure execution environment, wherein:
 - each component enclave of the enclave pod has a respective first key to securely communicate with other component enclaves of the enclave pod, wherein the first key of each component enclave is certified by the root enclave by use of a second key; and
 - each component enclave of the enclave pod ensures that the first key of another component enclave of the enclave pod is also certified by the same second key to share information.
6. The system of claim 5, the operations further comprising:
 - generating logs based on all transactions or actions performed in at least the component enclaves; and
 - cryptographically signing the logs with keys of the enclave pod.
7. The system of claim 5 or claim 6, the operations further comprising:
 - providing, from the root enclave, to a verifier, the identities of the root enclave and the manifest; and
 - in response to a verification of the identities of the root enclave and the manifest, receiving, from the verifier, one or more of data and code for the component enclaves.

8. The system of any of claims 5 to 7, wherein the enclave pod is an isolated and secure execution environment.