

### Claims

1. A computer-implemented system for improved security of data, comprising:

at least one processor, including hardware and software, the at least one processor configured to:  
receive a computer-based intelligent cipher transfer object comprising:

owner data secured by one or more inner cloaking patterns, and a portable dynamic rule set, said portable dynamic rule set comprising a machine-executable code secured by one or more outer cloaking patterns, receive, from an external agent, a request to access some or all of the owner data; reverse the outer cloaking patterns to retrieve the machine-executable code; and activate the portable dynamic rule set by executing the machine-executable code, thereby causing the at least one processor to:

verify, using portable dynamic rule set, that the external agent is authorized to access some or all of the owner data as requested, and upon verifying that the external agent is authorized, provide access to some or all of the owner data for which the external agent has been verified for access by reversing at least a portion of the one or more inner cloaking patterns.

2. The system of claim 1, wherein the portable dynamic rule set is located at variable locations within the intelligent cipher transfer object.

3. The system of claim 1, wherein the machine-executable code is located at variable locations within the intelligent cipher transfer object.

4. The system of claim 1, wherein the portable dynamic rule set includes at least one rule that identifies which external agents may access some or all of the owner data, and a context in which a particular external agent may access some or all of the owner data.

5. The system of claim 1, wherein a context in which a particular external agent may access some or all of the owner data comprises one or more of the following: a time period, a location, or an identity of a computing device.

6. The system of claim 1, wherein the computer-based intelligent cipher transfer object further comprises mixture metadata.

7. The system of claim 6, wherein the mixture metadata includes information identifying the one or more inner or outer cloaking patterns securing the owner data and the portable dynamic rule set.

8. The system of claim 1, wherein the one or more inner cloaking patterns are used to secure at least a portion of the portable dynamic rule set.

9. The system of claim 1, wherein the executing the machine-executable code further causes the at least

one processor to: upon failing to verify that the external agent is authorized, execute at least one rule in the portable dynamic rule set, thereby causing at least one of the following events to occur: the intelligent cipher transfer object self-destructs, the intelligent cipher transfer object denies access to at least a portion of the owner data, a message or alert is sent to an owner associated with the owner data, and a record of the request is stored in the intelligent cipher transfer object.

10. The system of claim 1, wherein the executing the machine-executable code further causes the at least one processor to:

upon providing access to some or all of the set of participants for which the external agent has been verified for access, execute at least one rule in the portable dynamic rule set, thereby causing at least one of the following events to occur:

a message or alert is sent to an owner associated with the owner data, a record of the request is stored in the intelligent cipher transfer objects, the intelligent cipher transfer object provides limited access to at least a portion of the owner data, the limited access comprising at least one of read privileges and write privileges; a signature of the external agent is associated with the owner data, and at least one rule in the portable dynamic rule set is added, modified, or deleted.

11. The system of claim 1, wherein the intelligent cipher transfer object is nested within a second intelligent cipher transfer object.

12. The system of claim 11, wherein the second intelligent cipher transfer object is nested within one or more additional intelligent cipher transfer objects.

13. The system of claim 1, wherein the computer-based intelligent cipher transfer object further comprises a first set of identifying information for one or more authorized agents, and the executing the machine-executable code causes the at least one processor to verify that the external agent is authorized by:

prompting the external agent provide a second set of identifying information; receiving the second set of identifying information; and verifying the external agent is authorized by comparing the first set of identifying information and the second set of identifying information.

14. The system of claim 1, wherein the computer-based intelligent cipher transfer object further comprises one or more decryption keys, and the executing the machine-executable code causes the at least one processor to reverse the at least the portion of the one or more inner cloaking patterns by using the one or more decryption keys.

15. The system of claim 1, wherein the at least one processor comprises a local processor, wherein activating the portable dynamic rule set comprises activating the portable dynamic rule set on the local processor.

16. A computer implemented system for improved security using digital signatures or verifications, comprising:

at least one processor, including hardware and software, the at least one processor configured to:

receive a computer-based intelligent cipher transfer object comprising a portable dynamic rule set, said portable dynamic rule set comprising machine-executable code secured by one or more outer cloaking patterns, reverse the outer cloaking patterns to retrieve the machine-executable code, and activate the portable dynamic rule set by executing the machine-executable code, thereby causing the at least one processor to:

verify, using portable dynamic rule set, an identity of an external agent, upon verifying the identity of the external agent, storing data indicative of the identity of the external agent in the computer-based intelligent cipher transfer object, and securing the data indicative of the identity of the external agent using one or more inner cloaking patterns.

17. The system of claim 16, wherein the portable dynamic rule set is located at variable locations within the intelligent cipher transfer object.

18. The system of claim 16, wherein the data indicative of the identity of the external agent is located at variable locations within the intelligent cipher transfer object.

19. The system of claim 16, wherein the inner cloaking patterns are used to cloak at least a portion of the portable dynamic rule set.

20. The system of claim 16, wherein the at least one processor comprises a local processor, wherein activating the portable dynamic rule set comprises activating the portable dynamic rule set on the local processor.