

WHAT IS CLAIMED IS:

1. A method for orchestrating a security object, the method comprising:

defining and storing a plurality of policies in a database coupled to a policy engine;

receiving, by the policy engine, the security object for distributing at least one communication device and at least one object attribute associated with the security object;

determining, with the policy engine, acceptability of the security object based, at least in part, on the at least one object attribute and at least one of the plurality of policies corresponding to the at least one object attribute;

transmitting a rejection indicator to a key source in response to determining that the security object is unacceptable, wherein the security object is received from the key source; and

transmitting a hint to the key source informing inadequacies of the security object.

2. The method of claim 1, wherein the security object is an encryption key.

3. The method of claim 1, wherein the at least one object attribute comprises at least one of a security object size, time when the security object is generated, geo-location where the security object is generated, classification of the security object, role associated with the key source, role associated with a source device, and role associated with a target device.

4. The method of claim 3, wherein the plurality of policies comprises accepting the security object when the security object size is within a predetermined size range.

5. The method of claim 3, wherein the plurality of policies comprises accepting the security object when the security object is generated within a predetermined time interval.

6. The method of claim 3, wherein the plurality of policies comprises accepting the security object when the geo-location where the security object is generated is within a predetermined area.

7. The method of claim 3, wherein the plurality of policies comprises accepting the security object when the classification of the security object is associated with a predetermined security object classification group.
8. The method of claim 3, wherein the plurality of policies comprises accepting the security object when the role associated with the key source, the source device, or the target device is associated with a predetermined group of roles.
9. The method of claim 1, wherein the key source generates a different security object based on the hint.
10. The method of claim 1, wherein the hint indicates one of the at least one object attribute caused the security object being rejected.
11. The method of claim 1, wherein the received encryption object and one or both of the rejection indicator or the hint are returned to the key source.
12. A non-transitory computer-readable medium comprising computer-readable instructions that, when executed, cause a processor to:
- define a plurality of policies in a database;
 - receive the security object for distributing to at least one communication device and at least one object attribute associated with the security object;
 - determine acceptability of the security object based, at least in part, on the at least one object attribute and at least one of the plurality of policies corresponding to the at least one object attribute;
 - transmit a rejection indicator to a key source in response to determining that the security object is unacceptable, wherein the security object is received from the key source; and
 - transmit a hint to the key source informing inadequacies of the security object.

13. The non-transitory computer-readable medium of claim 12, wherein the plurality of policies comprises accepting the security object when at least one of the security object size is within a predetermined size range, the time when the security object is generated is within a predetermined time interval, the geo-location where the security object is generated is within a predetermined area, the classification of the security object is included in a predetermined security object classification group, and the role associated with the key source, a source device, or a target device is associated with a predetermined group of roles.
14. The non-transitory computer-readable medium of claim 13, wherein the plurality of policies comprises accepting the security object when the security object size is within a predetermined size range.
15. The non-transitory computer-readable medium of claim 13, wherein the plurality of policies comprises accepting the security object when the security object is generated within a predetermined time interval.
16. The non-transitory computer-readable medium of claim 13, wherein the plurality of policies comprises accepting the security object when the geo-location where the security object is generated is within a predetermined area.
17. The non-transitory computer-readable medium of claim 13, wherein the plurality of policies comprises accepting the security object when the classification of the security object is associated with a predetermined security object classification group.
18. The non-transitory computer-readable medium of claim 12, wherein the key source generates a different security object based on the hint.
19. A key orchestration device for orchestrating a security object, the device comprising:
a processor; and
memory having computer-readable instructions stored thereon that, when executed, cause the processor to:
define a plurality of policies in a database;
receive the security object for distributing to at least one communication device and at least one object attribute associated with the security object;

determine acceptability of the security object based, at least in part, on the at least one object attribute and at least one of the plurality of policies corresponding to the at least one object attribute;

transmit a rejection indicator to a key source in response to determining that the security object is unacceptable, wherein the security object is received from the key source; and

transmit a hint to the key source informing inadequacies of the security object.

20. The device of claim 19, wherein the key source generates a different security object based on the hint.