

Claims

What is claimed is:

1. A computer-implemented method comprising:
obtaining a signed firmware image, the signed firmware image comprising a first code
5 module signed by a first code owner and a second code module signed by a second
code owner;
obtaining an updated first code module, the updated first code module comprising updated
code for the first code module;
verifying that the updated first code module is signed by the first code owner; and
10 updating the signed firmware image with the updated first code module in response to
verifying that the updated first code module is signed by the first code owner.
2. The method of claim 1, wherein:
the signed firmware image further comprises an access control list; and
the access control list authorizes updates to the first code module by the first code owner
15 and updates to the second code module by the second code owner.
3. The method of claim 2 further comprising:
obtaining an access control token, wherein the access control token comprises a public key
for a third code owner and authorization for the third code owner to update a third
code module of the signed firmware image;
20 verifying that the access control token is signed by an authorized code owner from the
access control list;
verifying that the authorized code owner is authorized to update the third code module;
and
updating the access control list to include the public key for the third code owner and the
25 authorization for the third code owner to update the third code module.
4. The method of claim 3 further comprising:
receiving an updated third code module from the third code owner;
verifying that the updated third code module is signed by the third code owner; and
updating the signed firmware image with the updated third code module in response to
30 verifying that the updated third code module is signed by the third code owner.
5. The method of claim 1 further comprising:
verifying that the first code owner is authorized to update the first code module prior to
updating the signed firmware image.

6. A system comprising:
at least one processor; and
a memory coupled to the at least one processor, the memory comprising instructions for performing the following:

- 5 obtaining a signed firmware image, the signed firmware image comprising a first code module signed by a first code owner and a second code module signed by a second code owner;
obtaining an updated first code module, the updated first code module comprising updated code for the first code module;
10 verifying that the updated first code module is signed by the first code owner; and
updating the signed firmware image with the updated first code module in response to verifying that the updated first code module is signed by the first code owner.

7. The system of claim 6, wherein
15 the signed firmware image further comprises an access control list; and
the access control list authorizes updates to the first code module by the first code owner and updates to the second code module by the second code owner.

8. The system of claim 7 wherein the instructions further perform the following:
20 receiving an access control token, wherein the access control token comprises a public key for a third code owner and authorization for the third code owner to update a third code module of the signed firmware image;
verifying that the access control token is signed by an authorized code owner from the access control list;
25 verifying that the authorized code owner is authorized to update the third code module;
and
updating the access control list to include the public key for the third code owner and the authorization for the third code owner to update the third code module.

9. The system of claim 8 wherein the instructions further perform the
30 following:
receiving an updated third code module from the third code owner;
verifying that the updated third code module is signed by the third code owner; and

updating the signed firmware image with the updated third code module in response to verifying that the updated third code module is signed by the third code owner.

10. The system of claim 6 wherein the instructions further perform the following:

5 verifying that the first code owner is authorized to update the first code module prior to updating the signed firmware image.

11. A computer program product comprising:
a computer-readable storage medium; and
instructions in the computer-readable storage medium, wherein the instructions, when
10 executed in a processing system, cause the processing system to perform operations comprising:
obtaining a signed firmware image, the signed firmware image comprising a first
code module signed by a first code owner and a second code module signed
by a second code owner;

15 obtaining an updated first code module, the updated first code module comprising updated code for the first code module;
verifying that the updated first code module is signed by the first code owner; and
updating the signed firmware image with the updated first code module in response
to verifying that the updated first code module is signed by the first code
20 owner.

12. The computer program product of claim 11, wherein:
the signed firmware image further comprises an access control list; and
the access control list authorizes updates to the first code module by the first code owner
and updates to the second code module by the second code owner.

25 13. The computer program product of claim 12 wherein the instructions further cause the processing system to perform operations comprising:

receiving an access control token, wherein the access control token comprises a public key
for a third code owner and authorization for the third code owner to update a third
code module of the signed firmware image;

30 verifying that the access control token is signed by an authorized code owner from the
access control list;

verifying that the authorized code owner is authorized to update the third code module;
and

updating the access control list to include the public key for the third code owner and the authorization for the third code owner to update the third code module.

14. The computer program product of claim 13 wherein the instructions further cause the processing system to perform operations comprising:

- 5 receiving an updated third code module from the third code owner;
verifying that the updated third code module is signed by the third code owner; and
updating the signed firmware image with the updated third code module in response to
verifying that the updated third code module is signed by the third code owner.

15. The computer program product of claim 11 wherein the instructions further
10 cause the processing system to perform operations comprising:
verifying that the first code owner is authorized to update the first code module prior to
updating the signed firmware image..

16. A computer-implemented method comprising:
creating a signed firmware image by a first code owner, the signed firmware image
15 comprising a first code module and a second code module;
signing the first code module;
creating an access control token to delegate authority to update the second code module to
a second code owner;
upon receiving an updated second code module comprising updated code for the second
20 code module, verifying that the updated second code module is signed by the
second code owner; and
updating the signed firmware image with the updated second code module in response to
verifying that the updated second code module is signed by the second code owner.

What is claimed is:

1. A computer-implemented method comprising:

obtaining a signed firmware image, the signed firmware image comprising at least a first code module signed by a first code owner and an access control list, wherein the access control list authorizes the first code owner to update the first code module;

obtaining an updated first code module, the updated first code module comprising updated code for the first code module and an updated access control list delegating authority to update the first code module from the first code owner to a second code owner;

verifying that the updated first code module is signed by the second code owner and that the second code owner is authorized to update based on, at least in part, the updated access control list; and

updating the signed firmware image with the updated first code module in response to verifying that the updated first code module is signed by the second code owner and that the second code owner is authorized to update the first code module.

2. The method of claim 1, further comprising:

obtaining an access control token, wherein the access control token comprises a public key for the second code owner and authorization for the second code owner to update the first code module of the signed firmware image;

verifying that the access control token is signed by an authorized code owner from the access control list;

verifying that the authorized code owner is authorized to update the first code module; and

updating the access control list to include the public key for the second code owner and the authorization for the second code owner to update the first code module.

3. The method of claim 1 further comprising:

verifying that the first code owner is authorized to update the first code module prior to updating the signed firmware image.

4. A system comprising:

at least one processor; and

a memory coupled to the at least one processor, the memory comprising instructions for performing the following:

obtaining a signed firmware image, the signed firmware image comprising at least a first code module signed by a first code owner and an access control list, wherein the access control list authorizes the first code owner to update the first code module;

obtaining an updated first code module, the updated first code module comprising updated code for the first code module and an updated access control list delegating authority to update the first code module from the first code owner to a second code owner;

verifying that the updated first code module is signed by the second code owner and that the second code owner is authorized to update based on, at least in part, the updated access control list; and

updating the signed firmware image with the updated first code module in response to verifying that the updated first code module is signed by the second code owner and that the second code owner is authorized to update the first code module.

5. The system of claim 4, wherein the instructions further perform the following:

receiving an access control token, wherein the access control token comprises a public key for the second code owner and authorization for the second code owner to update the first code module of the signed firmware image;

verifying that the access control token is signed by an authorized code owner from the access control list;

verifying that the authorized code owner is authorized to update the first code module;
and

updating the access control list to include the public key for the second code owner
and the authorization for the second code owner to update the first code module.

6. The system of claim 4 wherein the instructions further perform the following:

verifying that the first code owner is authorized to update the first code module prior
to updating the signed firmware image.

7. A computer program product comprising:

a computer-readable storage medium; and

instructions in the computer-readable storage medium, wherein the instructions, when
executed in a processing system, cause the processing system to perform operations
comprising:

obtaining a signed firmware image, the signed firmware image comprising at least a
first code module signed by a first code owner and an access control list, wherein the access
control list authorizes the first code owner to update the first code module;

obtaining an updated first code module, the updated first code module comprising
updated code for the first code module and an updated access control list delegating authority
to update the first code module from the first code owner to a second code owner;

verifying that the updated first code module is signed by the second code owner and
that the second code owner is authorized to update based on, at least in part, the updated
access control list; and

updating the signed firmware image with the updated first code module in response to
verifying that the updated first code module is signed by the second code owner and that the
second code owner is authorized to update the first code module.

8. The computer program product of claim 7, wherein the instructions further cause the
processing system to perform operations comprising:

receiving an access control token, wherein the access control token comprises a public key for the second code owner and authorization for the second code owner to update the first code module of the signed firmware image;

verifying that the access control token is signed by an authorized code owner from the access control list;

verifying that the authorized code owner is authorized to update the first code module;
and

updating the access control list to include the public key for the second code owner and the authorization for the second code owner to update the first code module.

9. The computer program product of claim 7 wherein the instructions further cause the processing system to perform operations comprising:

verifying that the first code owner is authorized to update the first code module prior to updating the signed firmware image.

10. A computer-implemented method comprising:

creating a signed firmware image by a first code owner, the signed firmware image comprising at least a first code module and an access control list, wherein the access control list authorizes the first code owner to update the first code module;

signing the first code module by the first code owner;

creating an access control token to delegate authority to update the first code module to a second code owner;

upon receiving an updated first code module comprising updated code for the first code module, verifying that the updated first code module is signed by the second code owner;
and

updating the signed firmware image with the updated first code module in response to verifying that the updated first code module is signed by the second code owner and that the second code owner is authorized to update based on, at least in part, the updated access control list.